NEI 13-10 [Revision 3]

Cyber Security Control Assessments

September 2015

[BLANK PAGE]

NEI 13-10 [Revision 3]

Nuclear Energy Institute

Cyber Security Control Assessments

September 2015

Nuclear Energy Institute, 1201 F Street N. W., Suite 1100, Washington D.C. (202.739.8000)

[BLANK PAGE]

ACKNOWLEDGMENTS

This document has been prepared by the nuclear power industry with input and guidance from the United States Nuclear Regulatory Commission. While many individuals contributed heavily to this document, NEI would like to acknowledge the significant leadership and contribution of the following individuals.

Executive sponsor:

James Meister	Exelon Corporation

Core project team:

Patrick Asendorf	Tennessee Valley Authority
Nathan Faith	Exelon Corporation
Jan Geib	South Carolina Electric & Gas Company
William Gross	Nuclear Energy Institute
Christopher Kelley	Exelon Corporation
Jay Phelps	South Texas Project Nuclear Operating Company
Don Robinson	Dominion Generation
James Shank	PSEG Services Corporation
Laura Snyder	Tennessee Valley Authority
Brad Yeates	Southern Nuclear Operating Company

Industry review team:

Glen Frix	Duke Energy Corporation
Matthew Coulter	Duke Energy Corporation
Geoff Schwartz	Entergy

NOTICE

[BLANK PAGE]

EXECUTIVE SUMMARY

When the methodology to address cyber security controls was developed in the template for the cyber security plan, the industry believed there would be small handfuls of digital assets (CDAs) that would require a cyber security assessment. However, NEI understands that plants, including those with no digital safety-related systems, have identified many hundreds if not thousands of CDAs. Included are assets that range from those directly related to operational safety and security to those that, if compromised, would have no direct impact on operational safety, security, or emergency response capabilities.

This guidance document was developed to streamline the process for addressing the application of cyber security controls to the large number of CDAs identified by licensees when conducting the analysis required by 10 CFR 73.54(b). The goal is to minimize the burden on licensees of complying with their NRC approved cyber security plan, while continuing to ensure that the adequate protection criteria of 10 CFR 73.54 are met.

[BLANK PAGE]

TABLE OF CONTENTS

[BLANK PAGE]

CYBER SECURITY CONTROL ASSESSMENTS

1 INTRODUCTION

1.1 BACKGROUND

Title 10 of the Code of Federal Regulations, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," requires that licensees 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 requires that each licensee currently licensed to operate a nuclear power plant submit a cyber security plan (CSP) for Commission review and approval. Current applicants for an operating license or combined license must submit with or amend their applications to include a cyber security plan.

Further, 10 CFR 50.34(c)(2) states in part that "Each applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55 of this chapter must include a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54 of this chapter." The Cyber Security Plan establishes the licensing basis for the Cyber Security Program.

The purpose of the Cyber Security Plan is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Rule) are implemented.

Section 3.1.6 of the licensee's CSP describes how that licensee addresses cyber security controls for digital assets that have been identified for protection against cyber attacks. NEI 13-10 provides guidance licensees may use to streamline the process to address cyber security controls for CDAs consistent with the methodology described in CSP Section 3.1.6.

1.2 SCOPE

This document provides guidance licensees may use to streamline the process for addressing the application of cyber security controls to those digital assets that a site specific analysis, performed in accordance with the requirements of 10 CFR 73.54 (b)(1), determined require protection from cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

1.3 PURPOSE

The purpose of this document is to provide guidance licensees may use to address cyber security controls for CDAs consistent with the methodology described in Section 3.1.6 of the Cyber Security Plan.

2 USE OF THIS DOCUMENT

The following method may optimize the use of the guidance in this document:

a) PRINT this document.

b) GATHER CDA-related information documented when implementing CSP Sections 3.1.3, 3.1.4, and 3.1.5.

c) PERFORM a consequence assessment of CDAs using the guidance in Section 3 of this document.

d) USE the guidance in Sections 3, 4, 5, and 6 of this document to divide the CDAs identified in Milestone 2 into two categories, direct and indirect CDAs, for streamlining the application of cyber security controls to identified CDAs consistent with Section 3.1.6 of the CSP.

e) DOCUMENT the assessment and RETAIN the documents in accordance with the CSP.

In order to promote consistent implementation of the guidance, an implementing template and a series of worked examples have been developed. The examples intend to be both consistent with the guidance, and illustrative of the level of acceptable documentation. The template and examples are incorporated into Revision 1 to NEI 13-10. The body of the document is unchanged from Revision 0. The template and examples are incorporated as Appendices B and C, respectively.

Revision 2 to NEI 13-10 incorporates Section 6, "Cyber Security Control Assessments of Direct CDAs" and Appendix D. The guidance in Section 6 and Appendix D implements cyber security control assessments for direct CDAs in a manner consistent with Section 3.1.6 of CSPs.

Revision 3 to NEI 13-10 builds on the guidance incorporated into Revision 2. Minor changes were made to the body of the document to: address an omission from Revision 2 in Section 6 regarding the use of the term "access;" to make it clear that the assessments provided in Appendix D do not cover all of the cyber security controls referenced in cyber security plans; and that this guidance may be used by licensees who have used RG 5.71 as a basis for their Cyber Security Plans. Finally, enhancements to the document were made to reflect lessons learned from early use of the document. These enhancements include removal of certain examples of Direct CDAs in Section 3.2, introduction of a streamlining technique for certain balance-of-plant CDAs, corresponding clarifications to affected examples in Appendix C, and enhancements to the baseline controls for certain balance-of-plant CDAs to ensure consistency with the CIP Reliability Standards.

3 CONSEQUENCE ASSESSMENT OF CDAS

Consequence Assessment provides a method to assess alternate means of protecting CDAs from cyber attacks. Licensees may use the guidance detailed in Table 1, "Consequence Assessment," to determine which of the approaches described in this document may be used to assess alternate controls and streamline the process of addressing the application of cyber security controls to CDAs. It is intended that any CDA subject to this assessment would proceed to one of the two exit states illustrated in Figure 1.

Consequence Assessment may result in the application of certain minimum cyber security controls to specific identified CDAs. These minimum cyber security controls are described in Section 5 of this document, "Minimum Cyber Security Protection Criteria." The Consequence Assessment and the minimum requirements in Section 5 may be used as a means to address the alternative analysis requirements specified in Section 3.1.6 of the CSP. The impact of the cyber compromise of identified CDAs can be divided into two categories: direct and indirect impacts to SSEP functions. BOP CDAs can be further streamlined since some BOP CDAs do not directly mitigate accident or transient conditions, and cyber compromises or failures of some BOP CDAs do not directly prevent safety systems from performing their functions. Therefore, if the licensee verifies, and documents that a BOP CDA is not relied upon to mitigate accidents or transients, and the BOP CDA's failure or cyber compromise does not prevent safety-related structures, systems, and components from fulfilling their safety-related functions, then the licensee may identify the BOP CDA as an indirect CDA prior to using the screening methodology described in Sections 3.1 and 3.2.

Consequence Assessment also provides a method to assess alternate means of protecting EP functions, including offsite communications. The methodology of assessing alternate means for EP functions is described in Section 4, "EP Function Maintained through Alternate Means." For CDAs associated with EP functions, the licensee may perform and document an analysis for the use of alternative controls or countermeasures as described in Table 2 of this document. Table 2 provides a method that can be used to identify those EP CDAs that can be adequately protected by using the security measures provided in Section 4 of this document to comply with the licensees' CSP. Table 1 shows that this determination is performed before the screening for direct or indirect that are discussed in Sections 3.1 and 3.2 of this document. Where an assessment using the guidance in Table 2 determines that a cyber attack would adversely impact the ability to implement EP functions, Sections 3.1 and 3.2, below, provide a means for those CDAs to be screened for indirect or direct impact.

Consistent with Section 4.4 and 4.5 of their cyber security plans, licensees will establish a program to ensure that CDAs are continuously protected from cyber attacks including implementing any necessary measures to address new vulnerabilities in accordance with the CSP.

NEI 13-10 provides guidance for addressing technical cyber security controls for CDAs. As a result, cyber security controls from Appendix D, "Technical Cyber Security Controls," and selected cyber security controls from Appendix E, "Operational and Management Cyber Security Controls," of NEI 08-09 are addressed in NEI 13-10. The remaining Appendix E

operational and management controls not addressed in this document must be addressed programmatically in accordance with Section 3.1.6 of the CSP for CDAs.

3.1 INDIRECT CDAS

Indirect CDAs are those CDAs that cannot have an adverse impact on or degrade SSEP functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee. Specifically, indirect CDAs include only those CDAs that meet all three of the following criteria: (1) if compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; (2) are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, (3) the compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.

For indirect CDAs only, licensees may comply with the requirements of Section 3.1.6 of their Cyber Security Plans by implementing the guidance set forth in Table 1.

3.2 DIRECT CDAS

Direct CDAs include those CDAs that, if compromised, could result in an adverse impact to SSEP functions or systems or equipment that are used or relied on for performing SSEP functions or for making SSEP-related decisions. Direct CDAs would also include CDAs associated with support systems and equipment that, if compromised, could adversely impact systems or equipment that are used for performing SSEP functions or relied-on for making SSEP-related decisions. Direct CDAs are those CDAs that have not been determined to be indirect CDAs.

Licensees may use streamlining techniques, when applicable, for addressing the applicability of security controls to direct CDAs. These include the use of common controls, inherited controls, and type assessments when such measures adequately address attack pathways and vectors associated with the direct CDAs. These techniques can reduce the effort required for addressing protections for direct CDAs.

In general, the term “common control” means a particular security control is applied to multiple CDAs. The term “inherited controls (technical)” refers to a situation in which a CDA receives protection from technical security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by another CDA. Finally, the term “type assessment” or “grouping of CDAs” refers to a situation in which multiple CDAs share a substantially similar security posture. For type assessments, a single assessment is created noting the differences, if any, between the devices.

In cases where a technical control cannot be implemented, the threat vector associated with the technical control exists, and the CDA is unable to inherit the technical control from another CDA, an alternate control (including administrative controls if alternative technical security controls cannot be used to address the security controls) can be used to mitigate the associated risk. The alternate control must provide the same degree of protection found in the original control.

Section 6, "Cyber Security Control Assessments of Direct CDAs" and Appendix D of this document implements cyber security control assessments for direct CDAs in a manner consistent with Section 3.1.6 of CSPs.

Redundancy should not be used as a factor in determining if a CDA is an indirect or direct CDA.

Some examples of direct CDAs for which the criteria in Section 3.1 of this document do not apply include:

- Digital Emergency diesel generator governor;
- Digital turbine driven Auxiliary Feedwater pump governors;
- RCS pressure instruments with control functions and/or input to the Reactor Protection System for initiation of a plant trip;
- CDAs identified in accordance with Milestone 6; and
- Security computer alarm station server(s).

Table 1 – Consequence Assessment

Figure 1 Question	Guidance
1.1	Is the CDA associated with EP functions, including offsite communications, or are EP support systems or equipment for EP-related CDAs? If YES, proceed to question 1.2 of this table. If NO, proceed to question 1.4 of this table.
1.2	Has an assessment using the process described in Section 4 and illustrated in Figure 2 determined that the EP functions are maintained through alternate means? If YES, proceed to 1.3 of this table. If NO, proceed to 1.4 of this table.
1.3	Are minimum cyber security protection criteria d, e, f, and g, described in Section 5 of this document in place for the EP-related CDAs? If YES, current cyber security controls are adequate to meet CSP Section 3.1.6. End assessment here. If NO, implement minimum cyber security protection criteria d, e, f, and g, described in Section 5 of this document or proceed to 1.4 of this table.

Figure 1 Question	Guidance
1.4	Has the licensee determined that the CDA is an indirect CDA as described in Section 3.1 of this document? If YES, proceed to 1.5 of this table If NO, proceed to 1.7 of this table.
1.5	Has the licensee documented, and implemented the following? 1. Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or SSEP functions (in all operating modes). The minimum time period required may be based on existing analyses. 2. Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period. 3. Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes. 4. Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for the indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1. If YES then proceed to 1.6 of this table. If NO, proceed to 1.7 of this table.
1.6	Are the minimum cyber security protections described in Section 5 of this document in place for the CDA? If YES, then current cyber security controls are adequate to meet CSP Section 3.1.6. End assessment here. If NO, implement the minimum cyber security protection criteria described in Section 5 of this document or proceed to 1.7 of this table.
1.7	Address the cyber security controls as referenced in Section 3.1.6 of the licensee's CSP. The guidance in Section 6 of NEI 13-10 may be used.

4 EP FUNCTION MAINTAINED THROUGH ALTERNATE MEANS

As specified in Section 3.1.6 of licensees' NRC-approved CSPs, a licensee has the flexibility to perform and document an analysis for the implementation of alternative controls and/or countermeasures for EP CDAs that eliminate threat/attack vector(s) associated with, and that provide at least the same degree of cyber security protection as one or more of the corresponding cyber security controls enumerated in Appendices D and E of NEI 08-09, Revision 6. The licensee must perform and document an analysis for the use of alternative controls or countermeasures as described in Table 2 to address the cyber security controls as specified in Section 3.1.6 of the licensee's NRC-approved CSPs. Table 2 is illustrated in Figure 2, which can be found in Appendix A to this document. This guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions.

Where an assessment using the guidance in Table 2 determines that cyber attacks on CDAs associated with EP functions would not adversely impact the ability to implement the EP function, due to the availability of an alternate means of performing that function, then the CDAs may be considered adequately protected. The guidance in Table 2 can be used to determine whether an alternative means allows the EP equipment to remain operable to perform the intended emergency response function despite cyber attacks.

Changes to measures credited as providing an alternate method of maintaining the EP function must be subject to review (e.g., existing program reviews, procedure revision reviews, or use of configuration management) to ensure the changes would not challenge the adequacy of the alternate method.

Table 2 – Alternative Means Assessment for EP CDAs

Figure 2 Question	Guidance
2.1	Are alternate means available for performing the intended EP function, including offsite communications? If YES, proceed to question 2.2 of this table. If NO, proceed to 1.4 in Table 1 or implement alternate means and then proceed to 2.2 of this table.

Figure 2 Question	Guidance
2.2	Is one or more of the alternate means administrative, non-digital, or if digital are adequately independent? If YES, proceed to question 2.3 of this table. If NO, proceed to question 1.4 of Table 1. Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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.). Administrative methods, including actions performed by personnel, can be considered as an alternate means provided they do not depend on identified CDA(s) for which controls have not been assessed.
2.3	Is the alternate means documented? If YES, proceed to 2.4 of this table. If NO, proceed to 1.4 in Table 1 or document the alternate means and then proceed to 2.4 of this table. **Note: the means must be documented in a plan, policy, or implementing procedure.**
2.4	Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? Specifically, can a cyber attack that would prevent the EP-related equipment from performing its intended function be detected and responded to prior to an adverse impact on the EP-related function during a radiological emergency? If YES, proceed to 2.5 of this table. If NO, proceed to 1.4 in Table 1 or implement detection and response measures and then proceed to 2.5 of this table. 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.

Figure 2 Question	Guidance
2.5	Are appropriate facility personnel trained to use the alternate method? If YES, then the function is maintained through alternate means, proceed to 1.3 in Table 1. If NO, proceed to 1.4 in Table 1 or perform training of appropriate facility personnel and then proceed to 1.3 in Table 1.

5 MINIMUM CYBER SECURITY PROTECTION CRITERIA

An assessment using the guidance in Section 3.1 permits licensees to demonstrate that alternative controls and countermeasures are sufficient to provide adequate protection of indirect CDAs. For these CDAs, the minimum set of cyber security protections are sufficient to provide high assurance that the CDAs are adequately protected against cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

Where these minimum cyber security criteria are not met, the licensee must document and implement additional cyber security controls to ensure adequate protections are in place for the CDA. These additional cyber security controls are implemented using the methodology in CSP Section 3.1.6.

Changes to the minimum cyber security controls must be reviewed in accordance with the CSP to ensure the indirect CDAs remain adequately protected from cyber attacks.

Where a licensee chooses to credit these minimum cyber security controls for an indirect CDA, the licensee must confirm these baseline minimum controls criteria are met.

An indirect CDA may be considered to be adequately protected from cyber attacks if all of the following minimum criteria are met:

a) The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 “Physical and Operational Environment Protection,” is addressed.

b) The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies.

c) The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device.

d) Use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices.

e) Changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, “Addition and Modification of Digital Assets.”

f) The indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and

mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks.

g) Ongoing Monitoring and Assessment in accordance with CSP is performed.

For indirect BOP CDAs whose failure or cyber compromise could cause a reactor scram/trip, the follow additional security controls from NEI 08-09 Appendix D are implemented where technically feasible:

D.1.2, “Account Management”

D.1.6, “Least Privilege”

D.1.7, “Unsuccessful Login Attempts”

D.4.1, “Identification and Authentication Policies and Procedures”

D.4.3, “Password Requirements”

D.5.5, “Installing Operating Systems, Applications and Third-Party Software Updates”

6 CYBER SECURITY CONTROL ASSESSMENTS OF DIRECT CDAS

Section 3.2, "Direct CDAs," describes several streamlining techniques for performing cyber security control assessments. These techniques include the use of common controls, alternate controls, control inheritance, and type assessments.

Appendix D to this document implements type assessments for direct CDAs. Appendix D provides a class description and a corresponding cyber security control assessment table for the class. The class description enumerates generic properties of a digital device relevant to addressing technical cyber security controls for devices having those properties. The class description also includes examples of digital devices in that class. The cyber security control assessment table addresses technical cyber security controls for the class. The assessment is provided in tabular format for ease of reference; however, the table may be incorporated into other tools at the licensee's discretion.

Access– the term "access" as used in NEI 08-09 Rev. 6 Appendix D is defined as access to data, program code, logic or configuration settings within a CDA through a local or remote, machine or human interface that could result in an adverse impact to an SSEP function.

The cyber security control assessment table includes the following columns:

- "Control Number" – the cyber security control number corresponding to NEI 08-09, Revision 6, Appendices D or E;
- "Control" – the cyber security control name corresponding to NEI 08-09;
- "Common" – the control may be implemented organizationally and applied to all CDAs;
- "Apply to CDA" – licensee must address this control for the CDA or class;
- "Alternate" – the cyber security control may be met through alternate means;
- "Not Applicable" – the cyber security control is not applicable to the CDA; and,
- "Basis" – provides a justification for the determination of control applicability (i.e., common, apply to CDA, alternate, or not applicable). The Basis column references or reproduces statements from the class document to support the justification. NOTE: cyber security control references in the Basis column of a specific assessment table are indices to those cyber security controls within that same assessment table.

The guidance in Appendix D of NEI 13-10 may be used as follows:

1) Determine the class for a given CDA using the CDAs technical documentation and the class description in Appendix D.

2) Use the Appendix D cyber security control assessment table for the class to identify those cyber security controls marked, "Apply to CDA."

3) Address the controls identified in Step 2, above, in accordance with CSP Section 3.1.6.

Documentation of how the class was determined in Step 1, above, and how the cyber security controls were addressed in Step 3, above, should be retained and available for inspection.

Once the "class" of a given CDA has been determined, that information may be shared among licensees. For example, if a licensee determines that a Rosemount 3153N digital transmitter is a Class A.1 device, that information may be shared with other licensees. Because it may be the case that devices with the same make and model number may not be identical (i.e., some devices with the same make and model number may have differing digital capabilities), licensees should confirm their CDAs meet the class description.

[BLANK PAGE]

APPENDIX A – FIGURES

Appendix A provides figures illustrating the guidance in Sections 3 and 4 of this document.

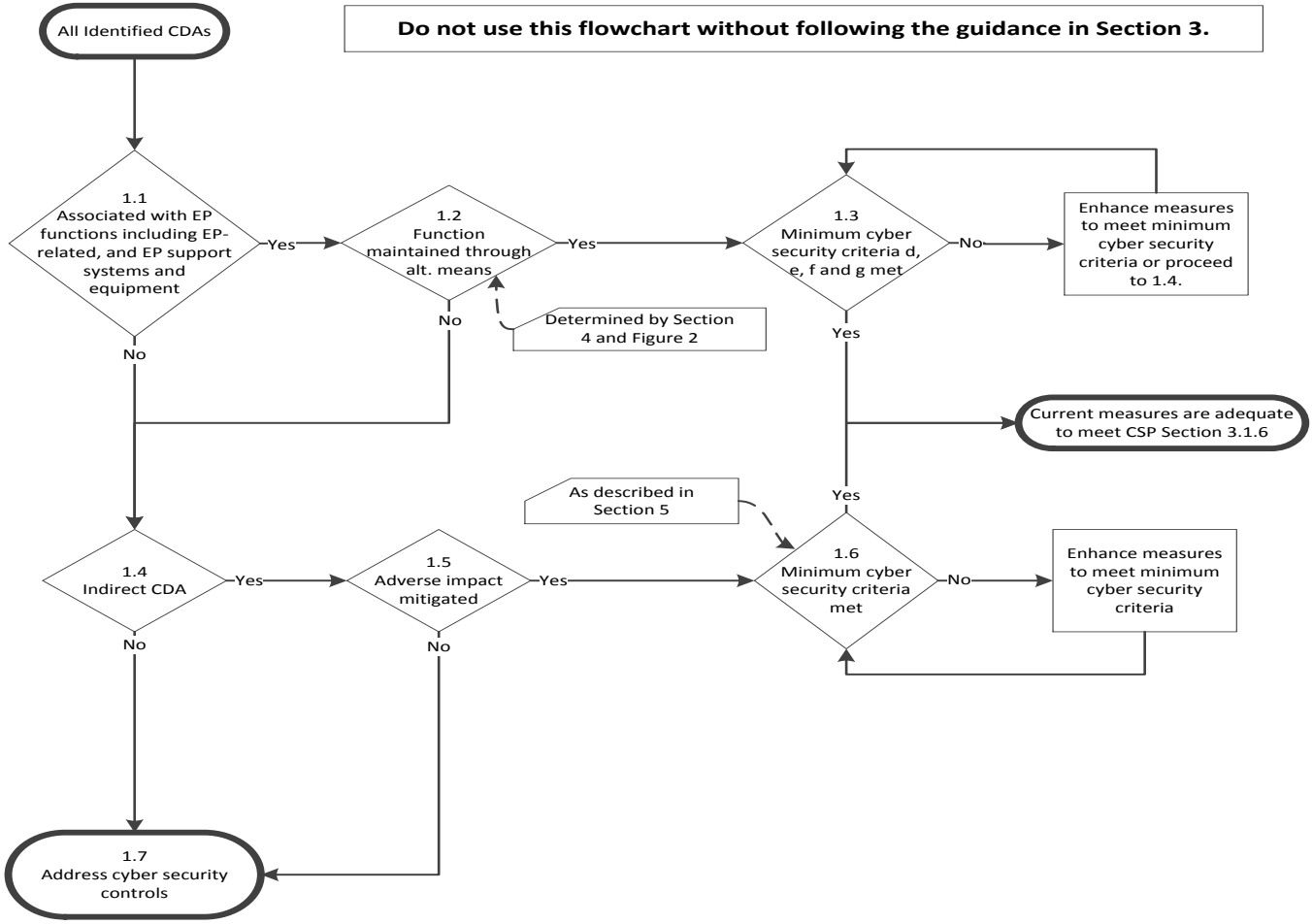

Figure 1 – Consequence Assessment

[BLANK PAGE]

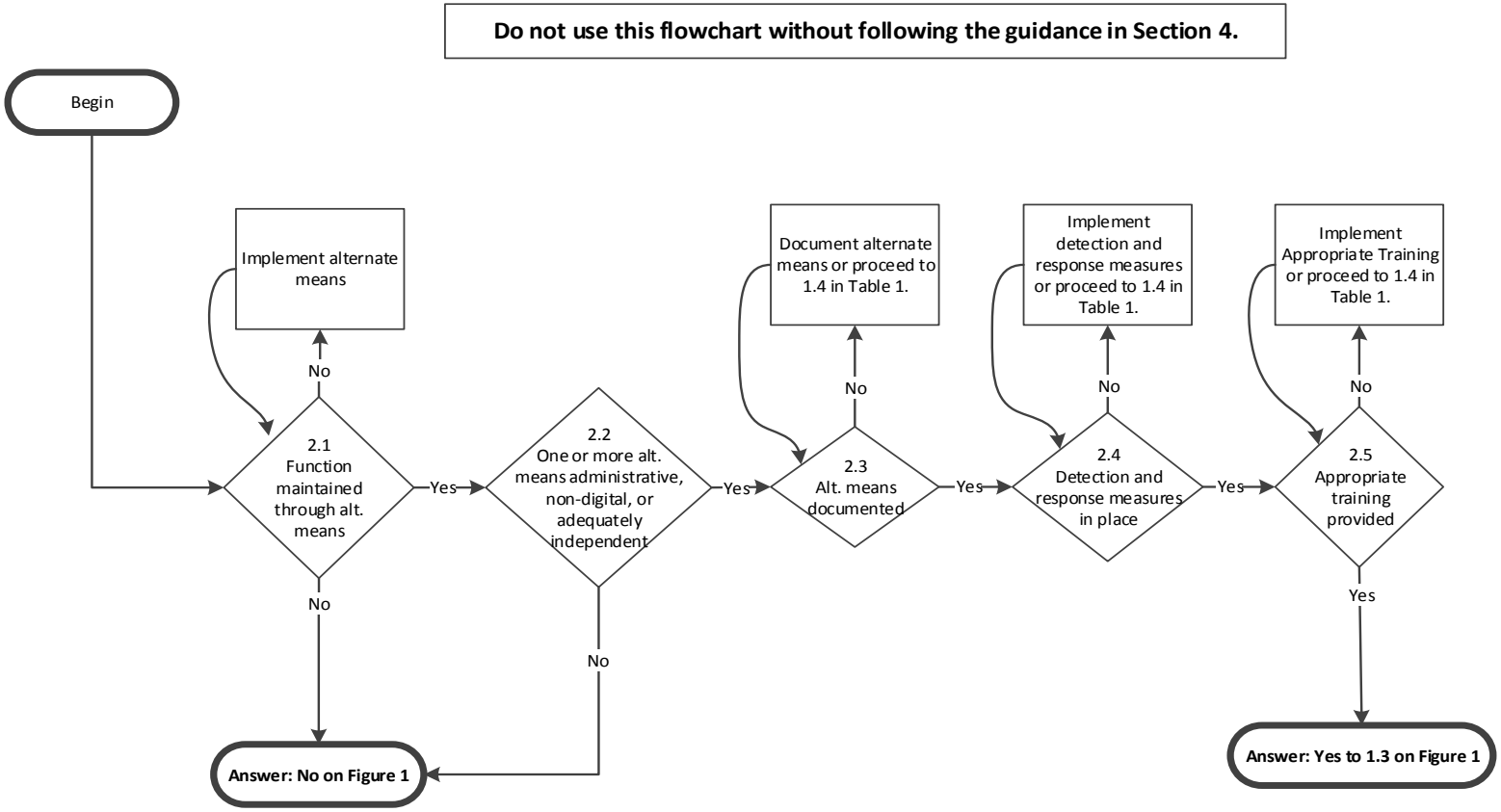

Figure 2 – Alternative Means Assessment for EP

[BLANK PAGE]

APPENDIX B – TEMPLATE

Appendix B provides an example implementing template consistent with the guidance.

[BLANK PAGE]

CDA IMPACT ASSESSMENT FORM

CDA Identification:

CDA Number: CDA Description: Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's:

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.1	Q1.1 EP-related or EP support systems and equipment?	☐ YES ☐ NO
Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4		
If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below:		
If YES, document applicable NUREG -0654 Section(s) the CDA supports below:		
If YES, document the Emergency Planning function(s) the CDA supports below:		
IF YES, THEN proceed to Figure 2, Question 2.1.	IF NO, THEN proceed to Figure 1, Question 1.4.	
1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Figure 2, Question 2.2.	IF NO, THEN proceed to Figure 1, Question 1.4.	
2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☐ YES ☐ NO

Note: 1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.		
IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.	
2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☐ YES ☐ NO
Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.		
IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.		
IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	

e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
Note: Indirect CDAs include only those CDAs that meet all three of the following criteria: 1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; 2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, 3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.		
IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.	
1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.):	
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.	
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or Safety or Security functions in all operating modes.	
d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.	

IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.	
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.	
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.	
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.	

g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).

1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☐ YES ☐ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	_____
	Name (Signature)
Reviewer:	_____
	Name (Signature)
Other Review (as applicable):	_____
	Name (Signature)
Final Approval:	_____
	Name (Signature)

APPENDIX C – EXAMPLES

Appendix C provides examples intended to be both consistent with the guidance, and illustrative of the level of acceptable documentation.

[BLANK PAGE]

EXAMPLE: EMERGENCY CALL-OUT SYSTEM

CDA Identification:

CDA Number: ECOS CDA Description: Emergency Call-Out System
Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's:

Call-out CDA #1

Call-Out CDA #2

The criteria for grouping the above CDAs are provided in plant procedure Doc XXXX

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.1	Q1.1 EP-related or EP support systems and equipment?	☒ YES ☐ NO
Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4		
If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below: 10 CFR 50.47 (b)(2) – On-shift facility licensee responsibilities for emergency response are unambiguously defined, adequate staffing to provide initial facility accident response in key functional areas is maintained at all times, timely augmentation of response capabilities is available and the interfaces among various onsite response activities and offsite support and response activities are specified.		
If YES, document applicable NUREG -0654 Section(s) the CDA supports below: Section II.B – Onsite Emergency Organization		
If YES, document the Emergency Planning function(s) the CDA supports below: 10 CFR 50.47 (b)(2) – Addresses NUREG -0654 Section II.B.5 requirement for licensee to augment on-shift capabilities within a short period after declaration of an emergency. Licensee must be able to augment on-shift capabilities within a short period after declaration of an emergency and establish procedures for alerting, notifying, and mobilizing emergency response personnel and provisions for alerting or activating emergency personnel in each response organization. Each organization shall provide for timely activation and staffing of the facilities and centers described in the plan. (Applicable for emergency call-out systems/assets.)		
IF YES, THEN proceed to Figure 2, Question 2.1.	IF NO, THEN proceed to Figure 1, Question 1.4.	

1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☒ YES ☐ NO

On Site Notification:
Hi Comm
Owner Controlled Notification System (OCANS)
Backup Method - Use of vehicular PA system or Bullhorn

Off Site Notification:
ECOS - Notification of other plant personnel who are offsite is achieved by the Shift Manager/delegate activating an automatic call out system
EP 292 Emergency Call Out Backup Method – Energy Systems Operations Center staff call out to ERO member

IF YES, THEN proceed to Figure 2, Question 2.2.	IF NO, THEN proceed to Figure 1, Question 1.4.

2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☒ YES ☐ NO

Note:
1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.

On- Site Notification:
Hi-Com System – Non Digital
The Hi-Comm System provides both party-to-party and paging announcement capabilities. It is a single-channel page/party system with speakers and hand-sets located throughout the plant. Hi Comm system is a Gaitronics analog system.

And

Owner Controlled Area Notification System (OCANS) – Digital
The Owner Controlled Area Notification System (OCANS) uses the Plant Radio System and speakers located throughout the plant site.

Back-up Method
Use of vehicular PA system or Bullhorn – Non- Digital

Off-Site Notification:
Emergency Call-Out System (ECOS) – Digital, ECSO is under the control of Dialogic Communications Corporation (DCC)

The plant utilizes DCC "Communicator!NXT" as the primary Emergency Call-Out System (ECOS) for emergency staff augmentation. This off-site system has two locations, one in TN (primary) and the other in AZ (back-up). The ECOS system can be activated in two ways, via telephone or computer via the Internet.

The back-up Call-Out method is adequately independent. It uses administrative corporate phone system at the corporate Systems Operation Center located at headquarters. The administrative phone system is under the control of the local telephone company.

IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.

2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☒ YES ☐ NO

Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.

The Call-Out assets are documented in the RERP Plan and RERP Procedures EP-290 Emergency Notifications, EP-292 Emergency Call Out Backup Method, and the RERP Telephone directory (including Attachment A).

IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.

Procedures EP-290 “Emergency Notifications” and EP-292, “Emergency Call-Out Backup Method” document the primary and backup methods for initiating and verifying an emergency call-out. The equipment used to initiate call-out is exercised periodically during scheduled drills and events to ensure it is capable of performing its intended design function. The potential compromise or failure of the call-out system is bounded by the aforementioned procedures which require an operator to initiate the backup call-out process as documented in EP-292 when the primary call-out process cannot be successfully completed in accordance with EP-290.

Performance Tracking (PT) Event XX11 - Perform Activation of the Emergency Call Out System. Performed once a quarter, any time during the quarter.
PT Event XX37 – Perform ECOS Knowledge Assessment of SOC Personnel. Performed every two years as a table top drill for the backup call out method EP-292
PT Event PX52 – Verify the Emergency Call Out List is up to Date. Performed every 180 days.
PT Event AG41 – perform Hi Comm hand set checks – performed quarterly

Call-Out equipment is used during the various RERP drills scheduled throughout the year and functionality is tested during the drills.

IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☒ YES ☐ NO
EVENT XX37 - Perform ECOS Knowledge Assessment of SOC Personnel. Performed every two years as a table top drill for the backup call out method EP-292 Nuclear Generation Selection, Training and Qualification Program Description QP-ER-665 describes the ERO roles that require initial and requalification for Course Plan CP-ER-831 RERP – Emergency Notifications that includes training on RERP Call Out methods including entry conditions that require the use of back up methods. Call-out assets are used during the various RERP drills scheduled throughout the year.		
IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	

1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria is met.	☒ YES ☐ NO
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
	The use of portable media and mobile devices (PMMD) is controlled according to NEI 08-09 D.19 as specified by the MMA23 Control of Digital Tools program.	
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.	
	Changes to the Call-Out system assets under licensee/plant control are required to be completed in accordance with procedure MES02 "Design Configuration Management" and the RERP Plan is evaluated for impact in accordance with procedure MLS08 "Licenses, Plans and Programs" as required by 10CFR 50.54(Q).	
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.	
	Procedure EP-290 "Emergency Notifications" documents operator initiation and verification for the emergency call-out process. When the operator is unable to successfully complete and verify the call-out process within the documented or analyzed timeframe using the primary system, EP-290 directs the operator to utilize the backup call-out process in accordance with EP-292 "Emergency Call-Out Backup Method" to preclude an adverse impact to the call-out function. The primary and backup call-out methods are tested as part of scheduled EP drills and exercises. The plant also conducts the following check to ensure that ECOS is operate properly including that the ECOS is not compromised: Performance Tracking (PT) Event XX11 - Perform Activation of the Emergency Call Out System. Performed once a quarter, any time during the quarter.	

	PT Event XX37 – Perform ECOS Knowledge Assessment of SOC Personnel. Performed every two years as a table top drill for the backup call out method EP-292 PT Event PX52 – Verify the Emergency Call Out List is up to Date. Performed every 180 days. PT Event AG41 – Perform Hi Comm Hand Set Checks – performed quarterly Call Out equipment is used during the various RERP drills scheduled throughout the year and functionality is tested during the drills.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.
	The Call-Out system is classified as a CDA and managed under the company's Cyber Security Plan (CSP) and program. As a result is it subject to ongoing monitoring and assessment as described in NEI 08-09 Rev. 6 Section 4.4 including periodic reviews to evaluate and improve as needed the effectiveness of the cyber security controls needed to protect Call-Out system from potential cyber attack. Cyber Security is included in Nuclear Quality Assurance Audits of the Physical Security Program. RERP (EP) is audited by Nuclear Quality Assurance.

IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
Note: Indirect CDAs include only those CDAs that meet all three of the following criteria: 1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; 2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, 3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.		
IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.	
1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.):	
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.	
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes.	
d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.	

IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.	
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.	
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.	
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.	

g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).

1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☐ YES ☒ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	
No outstanding actions identified.	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	_____ Name (Signature)
Reviewer:	_____ Name (Signature)
Other Review (as applicable):	_____ Name (Signature)
Final Approval:	_____ Name (Signature)

EXAMPLE: METEOROLOGICAL INFORMATION DOSE ASSESSMENT SYSTEM (MIDAS)

CDA Identification:

CDA Number: MIDAS CDA Description: Meteorological Information Dose Assessment System (MIDAS)
Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's:

EOF Workstation 1

TSC Workstation 2

The criteria for grouping the above CDAs are provided in plant procedure Doc XXXX

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")			
1.1	Q1.1 EP-related or EP support systems and equipment?	☒ YES	☐ NO
Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4			
If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below: 10 CFR 50.47 (b)(5) – Procedures have been established for notification, by the licensee, of State and local response organizations and for notification of emergency personnel by all organizations; the content of initial and followup messages to response organizations and the public has been established; and means to provide early notification and clear instruction to the populace within the plume exposure pathway Emergency Planning Zone have been established. 10 CFR 50.47 (b)(9) – Methods, systems and equipment for assessing and monitoring actual or potential offsite consequences of a radiological emergency condition.			
If YES, document applicable NUREG -0654 Section(s) the CDA supports below: Section II.E.4 Notification Methods and Procedures and Section II.I. - Accident Assessment			
If YES, document the Emergency Planning function(s) the CDA supports below: 10 CFR 50.47 (b)(5) – Addresses NUREG -0654 Section II.I requirements for licensees to estimate of quantity of radioactive material released or being released and the points and height of releases. 10 CFR 50.47 (b)(9) – Addresses NUREG -0654 Section II.I requirements for licensees to provide methods, equipment and expertise to make rapid assessments of the actual or potential magnitude and locations of any radiological hazards through liquid or gaseous release pathways. Actual or projected dose rates at site boundary; projected integrated dose at site boundary; projected dose rates and integrated dose at the projected peak and at 2, 5 and 10 miles, including sector(s) affected. Each licensee shall establish the methodology for determining the release rate/projected doses if the instrumentation used for assessment			

are off-scale or inoperable. Each organization, where appropriate, shall provide methods, equipment and expertise to make rapid assessments of the actual or potential magnitude and locations of any radiological hazards through liquid or gaseous release pathways. This shall include activation, notification means, field team composition, transportation, communication, monitoring equipment and estimated deployment times. Provisions shall be made for estimating integrated dose from the projected and actual dose rates and for comparing these estimates with the protective action guides. (Applicable for systems/applications used to project site & offsite dose rates and assessment).		
IF YES, THEN proceed to Figure 2, Question 2.1.	IF NO, THEN proceed to Figure 1, Question 1.4.	
1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☒ YES ☐ NO
The MIDAS system is an automated software tool used to assess and estimate dose. The system is designed to support automatic wind, speed and direction updates from MET tower instruments, but can be used in an offline mode, which requires manual data entry. When auto or manual data entry for MIDAS is not available or compromised, dose estimates can be manually calculated. EP Procedure NC.EP-EP.ZZ-0309 "Dose Assessment (MIDAS) Instructions provides guidance for performing alternate dose assessment functions in the event that MIDAS is unavailable at any location. EP Procedure NC.EP-EP.ZZ-0313 "Advanced Dose Assessment (MIDAS) Instructions" provides clear guidance for performing alternate dose assessment functions in the event that MIDAS is unavailable or compromised at any location. EP Procedure NC.EP-EP.ZZ-0309 "Dose Assessment (MIDAS) Instructions provides clear guidance for performing manual dose assessment functions in the event that automatic data transmission is unavailable or compromised.		
IF YES, THEN proceed to Figure 2, Question 2.2.	IF NO, THEN proceed to Figure 1, Question 1.4.	
2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☒ YES ☐ NO
Note: 1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.		
Offline MIDAS dose assessments require the use of dedicated MIDAS workstations, so they are not adequately independent, however manual dose assessment calculations do not require the use of MIDAS workstations and are adequately independent. EP Procedure NC.EP-EP.ZZ-0309 "Dose Assessment (MIDAS) Instructions" provides clear guidance for performing dose assessment functions. The two PWR plant methods use R41 monitor readings and provide for local readings using portable instrumentation which is independent of any other monitoring equipment. The BWR Filtration Recirculation Ventilation System (FRVS) and South Plant Vent (SPV) instruments or the Radiation Monitoring System (RMS) Computer system are used. During accident conditions, personnel are sent from the Operations Control Center (OCC) after being briefed and communicate back to the OCC using available communication methods which could include NETS, Gaitronics, field radios, PBX phone system or face to face communication. Other data required to support manual MIDAS estimates would be available using emergency communications tools.		
IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.	

2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☒ YES ☐ NO

Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.

EP Procedure NC.EP-EP.ZZ-0309 "Dose Assessment (MIDAS) Instructions" provides guidance for performing dose assessment functions. The two PWR plant methods use R41 monitor readings and provide for local readings using portable instrumentation which is independent of any other monitoring equipment. EP Procedure NC.EP-EP.ZZ-0313 "Advanced Dose Assessment (MIDAS) Instructions" provides guidance for performing alternate dose assessment functions at the BWR station using Drywell Atmosphere Post Accident (DAPA) Values. At the BWR station, either the Radiation Monitoring System (RM-11) or local instruments for FRVS and SPV which are adequately independent of other monitoring equipment.

IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.

The MIDAS system is exercised for drills and exercises that result in postulated releases. Based functionality checks are part of system use. The R41 monitor is part of the surveillance program and the portable radiation monitor instruments are used by Radiation Protection on a daily basis. At the BWR station the FRVS and SPV monitors are part of the surveillance program and the portable radiation monitor instruments are used by Radiation Protection on a daily basis. Maintenance Plans 27353, S1406174, S1406176, S1406182, S1406183, S1406184, 27354, S2405845, S2405846 and S2405847 test the R41 monitors. At the BWR station Maintenance Plans PM024769 and PM000427 test the R41 monitors.

Gap: To consider a MIDAS compromise of not only a loss of availability but also integrity, a test case with known inputs and outputs should be documented and entered prior to using MIDAS in either the online or offline mode for dose assessment to provide reasonable assurance the MIDAS algorithm is performing as designed. This corrective action must be completed prior to the Milestone 8 full program implementation date. Once implemented, Question 2.4 should be marked "YES."

IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☒ YES ☐ NO

Emergency Planning training includes exercising the capability to manually perform dose estimates. Radiation Protection shift technicians use the equipment daily and are trained in its use. At PSEG, the technicians and

Radiation Protection Supervision are required to have the "Shift Radiation Protection Emergency Plan Response - 50076698" and "Operate RM-11 - 50011690" qualification prior to being allowed to hold a shift or supervisory position.		
IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria are met.	☒ YES ☐ NO
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
	The use of portable media and mobile devices (PMMD) as specified by the IT-AA-505 PMMD program is controlled for the MIDAS system in accordance with procedure IT-AA-505-1001. To further reduce malware threats, a white-listing product has been installed on MIDAS workstations.	
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.	
	Changes to the MIDAS system are required to be completed in accordance with procedure CC-AA-102 "Configuration Change Control for Permanent Physical Plant Changes " and evaluated for impact in accordance with 10 CFR 50.54(Q).	
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.	
	Document the actions taken to periodically ensure equipment is capable of performing its intended function: The MIDAS system is checked periodically as part of numerous scheduled drills and exercises. A procedure change is being processed prior to the Milestone 8 due date to EP Procedure NC.EP-EP.ZZ-0309 "Dose Assessment (MIDAS) Instructions" to ensure MIDAS users validate the availability and integrity of MIDAS by entering a test case with known inputs and outputs prior to using MIDAS in either the online or offline mode for dose assessment. Alternate means of performing dose assessment are available and documented in EP Procedure NC.EP-EP.ZZ-0309 "Dose Assessment (MIDAS) Instructions" and preclude an adverse impact to EP functions resulting from cyber attack and the need for additional detection and mitigation capabilities.	
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.	
	The MIDAS system is classified as a CDA and managed under the company's Cyber Security Plan (CSP) and program. As a result it is subject to ongoing monitoring and assessment as described in NEI 08-09 Rev. 6 Appendix A Section 4.4 including periodic reviews to evaluate and improve as needed the effectiveness of the cyber security controls needed to protect MIDAS from potential cyber attack.	
IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
Note: Indirect CDAs include only those CDAs that meet all three of the following criteria: 1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; 2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, 3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.		
IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.	
1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.):	
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.	
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes.	
d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.	

IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.	
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.	
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.	
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.	

g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.
If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).
1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☒ YES ☐ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	
CAP Notification XXXXXXXX was created to consider not only a MIDAS compromise associated with the loss of system availability but also integrity by creating & documenting a test case with known inputs and outputs in Procedure NC.EP-EP.ZZ-0309 "Dose Assessment (MIDAS) Instructions" prior to using MIDAS in either the online or offline mode for dose assessment to provide reasonable assurance the MIDAS algorithm is performing as designed. This corrective action must be completed prior to the Milestone 8 full program implementation date. Once implemented, Question 2.4 should be marked "YES."	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	_____
	Name (Signature)
Reviewer:	_____
	Name (Signature)
Other Review (as applicable):	_____
	Name (Signature)
Final Approval:	_____
	Name (Signature)

EXAMPLE: NRC NOTIFICATION AND COMMUNICATION

CDA Identification:

CDA Number: N/A CDA Description: NRC Notification and Communication
Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's:

NRC Emerg Notif Sys (ENS)

Admin Phone Lines

Satellite Phones

Health Physics Net
The criteria for grouping the above CDAs are provided in plant procedure Doc XXXX

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")

1.1	Q1.1 EP-related or EP support systems and equipment?	☒ YES	☐ NO

Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4

If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below:
10 CFR 50.47 (b)(3) – Arrangements for requesting and effectively using assistance resources have been made, arrangements to accommodate State and local staff at the licensee's Emergency Operations Facility have been made, and other organizations capable of augmenting the planned response have been identified.
10 CFR 50.47 (b)(6) – Provisions exist for prompt communications among principal response organizations to emergency personnel and to the public.

If YES, document applicable NUREG -0654 Section(s) the CDA supports below:
Section II.C – Emergency Response Support and Resources
Section II. F – Emergency Communications

If YES, document the Emergency Planning function(s) the CDA supports below:
10 CFR 50.47 (b)(3) – Addresses NUREG -0654 Section II.C.1.C requirement for licensee to provide external telecommunications capability.
10 CFR 50.47 (b)(6) – Addresses NUREG -0645 Section II.F.1 requirement for licensees to provide reliable primary and backup means of communication for licensees, local, and state response organizations.

External communications systems:
Licensee shall make provisions for incorporating the Federal response capability into its operation plan, including specific licensee, State and local resources available to support the Federal response, e.g., air fields, command posts, telephone lines, radio frequencies and telecommunications centers.

Each organization shall establish reliable primary and backup means of communication for licensees, local, and State response organizations.

IF YES, THEN proceed to Figure 2, Question 2.1.	IF NO, THEN proceed to Figure 1, Question 1.4.

1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☒ YES ☐ NO

See below descriptions.
The primary method of NRC notification and communication is the FTS-2001 Emergency Notification System.
The alternate methods are the Administrative Telephone System and the satellite telephones.

NRC Notification and Communication

	Control Room	Technical Support Center (TSC)	Technical Support Center (TSC)	Emergency Operations Facility
Primary Method	ENS & ERDS	ENS	HPN	HPN
Back-up Method	Administrative Telephone System	Administrative Telephone System	Administrative Telephone System	Administrative Telephone System
Back-up Method	Satellite Phone	Satellite Phone	Satellite Phone	Satellite Phone

Note: The Emergency Response Data System (ERDS) virtual private network (VPN) used to communicate plant conditions with the NRC is not in scope of Cyber Security Rule; reference NEI 10-04 Rev 2.

IF YES, THEN proceed to Figure 2, Question 2.2.	IF NO, THEN proceed to Figure 1, Question 1.4.

2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☒ YES ☐ NO

Note:
1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.

Both alternate (back-up) methods are digital but are adequately independent of each other and the NRC FTS-2001 Emergency Telephone System (ENS). See description of the methods below. The Administrative Telephone Lines are land line phones that use 1970's analog technology. The satellite phones connect directly to orbiting satellites.

Primary - NRC FTS-2001 ENS system

The ENS provides seven communication functions to nuclear power reactor emergency response facilities. These communication functions are considered essential to the NRC response to an event at a nuclear power plant. The ETS service is currently provided using direct access lines (DALs) to the Federal Government's long distance network, FTS 2001. These dedicated lines provide a direct connection to FTS 2001 and are not switched at the local central office. This design feature is important because of possible call volume saturation at the local telephone office during an emergency. FTS 2001 provider is MCI WorldCom.
The FTS 2001 does not use any private, licensee or other, transmission facilities and rides in the normal transmission systems provisioned for voice traffic used by the rest of the Public Switched Telephone Network (PSTN). There is a system in place to give them a priority response based upon physical infrastructure and a class of service mark

Alternate - Administrative Phone Line (prefix 586) Communication (via telephone)
Administrative phone use Gen Band DMS100 Telephone System. The DMS-100 Switch Digital Multiplex System (DMS) uses telephone exchange switches manufactured by Nortel Networks and can control 100,000 telephone lines. The purpose of the DMS-100 Switch is to provide local service and connections to the PSTN public telephone network. It is designed to deliver services over subscribers' telephone lines and trunks. The Gen Band DMS 100 supplying the Centrex services to the plant is owned and maintained by CenturyLink. DTE Energy only takes service from it and has no access to any of its programming and /or translations. The Administrative phones allow communication within the site and with outside agencies during normal operations. These phones are also be used as a backup to the RERP telephone system. These lines are normal commercial phone lines routed both overhead underground to the Communications Building.

Alternate - Satellite Phones
A satellite telephone or satphone is a type of mobile phone that connects to orbiting satellites instead of terrestrial cell sites. Satellite phones are Iridium 9555.

IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.

2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☒ YES ☐ NO

Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.

Alternate means are documented in the plant RERP Plan and Attachment A to the RERP Emergency Telephone Directory.

IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a

timeframe sufficient to mitigate the adverse consequences of a cyber attack.

10 CFR 50 Appendix E, Section E Emergency Preparedness Facilities, 9.d states "Provisions for communications by the licensee with NRC Headquarters and the appropriate NRC Regional Office Operations Center from the nuclear power reactor control room, the onsite technical support center, and the emergency operations facility. Such communications shall be tested monthly."

The following performance tracking events perform the required monthly checks:
PT Event XX02 - Perform RERP Communication Checks in the Main Control Room. Performed monthly.

PT Event XX03 - Perform RERP Communication Checks in the Technical Support center (TSC). Performed monthly.
PT Event XX02 - Perform RERP Communication Checks in the Emergency Operations Facility (EOF). Performed monthly.
Communication equipment is used during the various RERP drills scheduled throughout the year and functionality is tested during the drills.

EP procedure [insert reference(s)] and training [insert reference(s)] document the primary and backup communications methods available to support communications. Equipment used to support emergency communications is tested periodically during scheduled drills and events to ensure it is capable of performing its intended design function. The potential compromise or failure of the FTS-2001 Emergency Notification System is bounded by the aforementioned procedures and training which direct users how to react to the effects of a compromise and to use the alternate methods (e.g. Administrative Telephone System and the satellite telephones) when the primary ENS system is unable to perform its intended design function.

IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☒ YES ☐ NO

Nuclear Generation Selection, Training and Qualification Program Description QP-ER-665 describes the ERO roles that require initial and requalification for Course Plan CP-ER-831 RERP – Emergency Notifications that includes training on RERP communication methods including back up methods. Those ERO positions that are required to communicate and make notifications to the NRC are trained to this requirement. This requires a periodic requalification of approximately every 12 months:
Control Room – Nuclear Operator, Nuclear Supervising Operator, Shift Manager, Control Room Supervisor/Incident Assessor, RERP Advisor, Shift Technical Advisor
TSC – Emergency Director, NRC Technical Communicator, TSC Administrator, TSC Communicator
EOF – Emergency Officer, EOF Administrator, EOF Communicator.

Communication assets are used during the various RERP drills scheduled throughout the year.

IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria is met.	☒ YES ☐ NO
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document	

	portable media and mobile device controls in place.
	The use of portable media and mobile devices (PMMD) as specified by the MMA23 Control of Digital Tools program. .The licensee/plant obtained services from Iridium for satellite phones and SBC/AT&T for PSTN. These companies are service providers, and the licensee/plant has no contractual control over satellite phones and externally hosted telephony infrastructure that would allow the licensee to require these service providers to implement MMA23 portable media and mobile device control requirements. The satellite phones and externally hosted telephony infrastructure and service providers do provide adequate protections against cyber attacks to ensure that the infrastructure meets the EP requirements. In the case that the phones have ports to which portable media can be connected, the licensees should address cyber security control D1.19.
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
	Changes to NRC communication systems and assets under licensee/plant control are required to be completed in accordance with procedure MES02 "Design Configuration Management" and the RERP Plan is evaluated for impact in accordance with procedure MLS08 "Licenses, Plans and Programs" as required by 10CFR 50.54(Q).
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
	10 CFR 50 Appendix E, Section E Emergency Preparedness Facilities, 9.d require provisions for communications by the licensee with NRC Headquarters and the appropriate NRC Regional Office Operations Center from the nuclear power reactor control room, the onsite technical support center, and the emergency operations facility. Such communications shall be tested monthly. The alternate administrative phone system Centrex DMS-100 digital components (server and switching) are used by site personnel every day, any adverse impact will be detected and responded to accordingly. The following performance tracking events perform the required monthly checks: PT Event XX02 - Perform RERP Communication Checks in the Main Control Room. PT Event XX03 - Perform RERP Communication Checks in the Technical Support center (TSC). PT Event XX02 - Perform RERP Communication Checks in the Emergency Operations Facility (EOF). Also, communication equipment is used during the various RERP drills scheduled throughout the year and functionality is tested during the drills. EP procedure [insert reference(s)] and training [insert reference(s)] document the primary and backup communications methods available to support communications. Equipment used to support emergency communications is tested periodically during scheduled drills and events to ensure it is capable of performing its intended design function. The potential compromise or failure of the FTS-2001 Emergency Notification System is bounded by the aforementioned procedures and training which direct users how to react to the effects

	of a compromise and to use the alternate methods (e.g. Administrative Telephone System and the satellite telephones) when the primary ENS system cannot be used for any reason..
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.
	The NRC ENS system is classified as Critical Systems and CDAs and managed under the company's Cyber Security Plan (CSP) and program. As a result they are subject to ongoing monitoring and assessment as described in NEI 08-09 Rev. 6 Section 4.4 including periodic reviews to evaluate and improve as needed the effectiveness of the cyber security controls needed to protect the NRC ENS system from potential cyber attack. Cyber Security is included in Nuclear Quality Assurance Audits of the Physical Security Program. RERP (EP) is audited by Nuclear Quality Assurance.

IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
Note: Indirect CDAs include only those CDAs that meet all three of the following criteria: 1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; 2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, 3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.		
IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.	
1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.):	
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.	
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes.	
d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.	

IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.	
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.	
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.	
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.	

g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).

1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☐ YES ☒ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	
No outstanding actions identified.	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	_____
	Name (Signature)
Reviewer:	_____
	Name (Signature)
Other Review (as applicable):	_____
	Name (Signature)
Final Approval:	_____
	Name (Signature)

[BLANK PAGE]

EXAMPLE: HIGH PRESSURE FEEDWATER HEATER LEVEL TRANSMITTERS

CDA Identification:

CDA Number: See Below CDA Description: High Pressure Feedwater Heater 2A Level Transmitters Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's: ILT03783A ILT03783B The criteria for grouping the above CDAs are provided in plant procedure Doc XXXX

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")			
1.1	Q1.1 EP-related or EP support systems and equipment?	☐ YES	☒ NO
Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4			
If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below:			
If YES, document applicable NUREG -0654 Section(s) the CDA supports below:			
If YES, document the Emergency Planning function(s) the CDA supports below:			
IF YES, THEN proceed to Figure 2, Question 2.1.		IF NO, THEN proceed to Figure 1, Question 1.4.	
1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☐ YES	☐ NO
IF YES, THEN proceed to Figure 2, Question 2.2.		IF NO, THEN proceed to Figure 1, Question 1.4.	

2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☐ YES ☐ NO

Note:
1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.

IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.

2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☐ YES ☐ NO

Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.

IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.

IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO

IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO

d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☒ YES ☐ NO

Note: Indirect CDAs include only those CDAs that meet all three of the following criteria:
1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions;
2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and,
3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.

The function of the transmitters is to provide high pressure heater level input to the Heater Drains Bridge Controller. The Level Transmitters meet each of criteria for Indirect CDA as discussed below.

The Guided Wave Level Transmitters are an A/B redundant pair that have a failover based on logic provided by the Heater Drains Bridge Controller (PLC). The Transmitters are classified as Important to Safety due to their Functional Importance Determination (FID). Post Modification Testing (IMSI-50092) describes the Heater Drain logic. Transmitters are only required to function in Mode 1. The transmitters provide level indication and level control for feedwater heater 2A.

The failure of one or both level transmitters for a single Heater will cause a Dump to the Condenser. In this evaluation these devices are evaluated as a pair in a single heater train. In their current configuration, there is no pathway for a cyber attack to propagate to the other CDAs. Should the configuration of these devices change (e.g., these devices be network enabled) or the associated procedures change, this analysis would need to be revisited (enabling the network would introduce a pathway for cyber attack and changing of the associated procedures may change the outcome of the this analysis.)

The level transmitters meet the Indirect CDA criteria:

1. No adverse impact on systems that perform a Safety or Security Function. A compromise of these CDAs can result in a reduction in power which does not have adverse impact on a Safety function.
2. Is not an indicator relied upon to for making Safety or Security related decisions.
3. Compensatory actions are not required because there is no adverse impact to Safety or Security functions.

IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☒ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.): There is no minimum time period required for detection and compensatory measures.	

	N/A – There is no adverse impact to Safety or Security functions.
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.
	N/A – There is no adverse impact to Safety or Security functions.
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes.
	N/A – There is no adverse impact to Safety or Security functions.
d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.
	N/A – There is no adverse impact to Safety or Security functions.

IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met.	☒ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.	
	The transmitters are located in the Protected Area. In the Turbine Building.	
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
	The transmitters have no wireless capability.	
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.	
	The transmitters are connected via a 4-20ma signal to the ABB DCS. There is no direct connection to the DCS via digital communications as defined in CSPP-002. Therefore, the transmitters are considered to be air-	

	gapped.
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.
	The transmitters are scoped as a CDA in station cyber security program; therefore CSPP-001 "Plant Digital Asset Control of Removable Media/Devices" is applicable to this asset. All Hart Communicators and Laptops used to Configure the transmitters are enrolled in station Removable Media/Devices program. CSPP-001 is station's program that meets the requirements of NEI 08-09 D1.19.
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
	Changes to the transmitters, other than calibration adjustments, require an Engineering Change Package controlled by SAP-133 "Design Control/Implementation and Interface". Digital components require an assessment by Cyber Security per CSPP-002 "Digital Asset Identification" and ES-560.601 "Critical Digital Asset Assessment"
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
	The transmitters indicate in the Control Room which is manned 24/7. While the plant is in Mode 1 any issues with Feedwater Heater 2 would be identified by Operations via channel check or MCB annunciator that will alert on a Single heater level transmitter failure or compromise along with an alarm on the HMI for the Heater Drains DCS. Heater Drains DCS maintains 7 days of 1 second data to perform analysis of any identified issues. The plant Historian will maintain 1 minute date indefinitely to perform analysis of any identified issues. The transmitters are not in service in Modes 2-6. There is no Preventive Maintenance task for this instrument. Any problems with the transmitters are entered into the corrective action program and are processed as necessary. Calibration or replacement is controlled by SAP-300 (Conduct of Maintenance) and ICP-205.016.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.
	N/A – There is no adverse impact to Safety or Security functions. However, the configuration management and analysis of changes to the transmitters and associated procedures are maintained per the CSP to ensure that any

	modifications to the recorder or plant procedures do not adversely impact the answers to Question 1.4.
If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).
1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☐ YES ☒ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	_____ Name (Signature)
Reviewer:	_____ Name (Signature)
Other Review (as applicable):	_____ Name (Signature)
Final Approval:	_____ Name (Signature)

[BLANK PAGE]

EXAMPLE: REACTOR COOLANT PUMP SEAL FLOW RECORDERS

CDA Identification:

CDA Number: See Below CDA Description: RCP Seal Flow Recorders Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's: N1CVFR0156 N2CVFR0156 N1CVFR0157 N2CVFR0157 N1CVFR0158 N2CVFR0158 N1CVFR0159 N2CVFR0159
The criteria for grouping the above transmitters are provided in plant procedures Doc XXX.

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")			
1.1	Q1.1 EP-related or EP support systems and equipment?	☐ YES	☒ NO
Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4			
If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below:			
If YES, document applicable NUREG -0654 Section(s) the CDA supports below:			
If YES, document the Emergency Planning function(s) the CDA supports below:			
IF YES, THEN proceed to Figure 2, Question 2.1.		IF NO, THEN proceed to Figure 1, Question 1.4.	
1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☐ YES	☐ NO
IF YES, THEN proceed to Figure 2, Question 2.2.		IF NO, THEN proceed to Figure 1, Question 1.4.	

2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☐ YES ☐ NO
Note: 1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.		
IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.	
2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☐ YES ☐ NO
Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.		
IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.		
IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO

d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☒ YES ☐ NO
Note: Indirect CDAs include only those CDAs that meet all three of the following criteria: 1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; 2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, 3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.		
The recorder function is to provide flow indication in gallons per minute for individual reactor coolant pump flow associated with seal injection, #1 Seal Leakoff, and #2 Seal Leakoff. As outlined below, the RCP Seal Flow Recorders meet the Indirect CDA Criteria. The "yes" answer to the question is based on the consequences of the potential cyber compromise of the recorder discussed below. Specific answers on meeting the criteria are addressed in responses in section 1.5, below. 1. No adverse impact on systems that perform a Safety or Security Function. 2. Indications are not relied upon to for making Safety or Security related decisions. 3. Compensatory actions are not required because there is no adverse impact to Safety or Security functions. NOTE: As the result of the screening of the RCP Seal Flow Recorders, the CSAT may wish to revisit the determination of whether or not these digital devices are CDAs.		
IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.	

1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☒ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.): There is no minimum time period (indefinite).	
	This recorder is used for historical logging and trending, and is not used to drive operator actions. Plant procedures allow this device to be out of service for an indefinite period of time. Loss or incorrect indication of the recorder cannot result in an adverse impact to Safety or Security functions.	
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.	

	N/A – There is no adverse impact to Safety or Security functions.
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes.
	N/A – There is no adverse impact to Safety or Security functions.
d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.
	N/A – There is no adverse impact to Safety or Security functions.

IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met.	☒ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.	
	The recorder is located in a vital area, the main control room, and is monitored 24/7 by licensed Reactor Operators.	
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
	The device has no wireless networking.	
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.	
	No interconnected assets exist.	
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
	The use of portable media is controlled in accordance with station procedure 0PGP03-ZS-0017 'Control of Portable Media for Cyber Security'.	

e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
	The device is controlled by that stations design control process outlined in 0PGP03-ZE-0309 'Design Change Package'. Digital components require an assessment by Cyber Security per 0PGP03-ZS-0012 'Cyber Security Assessment of Digital Assets'.
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
	The recorder is monitored at least once per operator shift in accordance with operations expectations for control board monitoring as outlined in Conduct of Operations, Chapter 2. One licensed Reactor Operator is tasked with walking down the all control board indications within 2 hours of taking the watch. The remaining control room staff of 4 – 5 individuals will perform a similar walkdown prior to the end of their 12 hour shift.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.
	N/A – There is no adverse impact to SSEP functions. However, the configuration management and analysis of changes to the recorders and procedures are maintained per the CSP to ensure that any modifications to the recorder or plant procedures do not adversely impact the answers to Question 1.4.

If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).

1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☐ YES ☒ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	
	Name (Signature)
Reviewer:	
	Name (Signature)
Other Review (as applicable):	
	Name (Signature)
Final Approval:	
	Name (Signature)

[BLANK PAGE]

EXAMPLE: HEATER DRAINS BRIDGE CONTROLLER

CDA Identification:

CDA Number: XPN6035-D-3 CDA Description: Heater Drains Bridge Controller (PLC, BRC400) Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's:

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")			
1.1	Q1.1 EP-related or EP support systems and equipment?	☐ YES	☒ NO
Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4			
If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below:			
If YES, document applicable NUREG -0654 Section(s) the CDA supports below:			
If YES, document the Emergency Planning function(s) the CDA supports below:			
IF YES, THEN proceed to Figure 2, Question 2.1.		IF NO, THEN proceed to Figure 1, Question 1.4.	
1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☐ YES	☐ NO
IF YES, THEN proceed to Figure 2, Question 2.2.		IF NO, THEN proceed to Figure 1, Question 1.4.	
2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☐ YES	☐ NO

Note: 1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.		
IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.	
2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☐ YES ☐ NO
Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.		
IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.		
IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	

e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☒ YES ☐ NO
Note: Indirect CDAs include only those CDAs that meet all three of the following criteria: 1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; 2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, 3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.		
ITMR SYSTEM FUNCTION & PERFORMANCE CRITERIA ANALYSIS for Heater Drain System. Maintenance Rule - 1a.) Loss of HD would result in conditions that could result in an Unplanned Scram of the plant, providing an effective measure of effectiveness of maintenance on the ITMR functions of this SSC. AOP-204.1 requires reduction of power to 700 mw at 3% turbine load per minute from current power. Station Megawatts at 100% power is 1016-1023 depending on the season. FSAR Section 15.2.10 Excessive Heat Removal Due To Feedwater System Malfunction describes the accident and consequences of losing the Heater Drains. This condition is classified as Category II Faults of Moderate Frequency and does not adversely impact safe shutdown. 1. No adverse impact on systems and equipment that perform Safety or Security functions 2. Indications are not relied on for making Safety or Security functions 3. Compensatory measures are not required because there is no adverse impact to Safety or Security functions		
IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.	

1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☒ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.):	
	N/A – There is no adverse impact to Safety or Security functions.	
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.	
	N/A – There is no adverse impact to Safety or Security functions.	
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes.	
	N/A – There is no adverse impact to Safety or Security functions.	

d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.
	N/A – There is no adverse impact to Safety or Security functions.

IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.

1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met.	☒ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.	
	Physical isolation is established by the location of the indirect CDA inside the PA.	
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
	There are no wireless capabilities on the CDAs, thus the threat vector does not exist.	
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.	
	The CDAs are protected within Defensive Level 3 in accordance with Section 4.3 of the Cyber Security Plan (CSP).	
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	
	The use of portable media is controlled in accordance with NEI 08-09 D1.19 as addressed by station procedure 0PGP03-ZS-0017 'Control of Portable Media for Cyber Security'.	
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.	
	The device is controlled by that stations design control process outlined in 0PGP03-ZE-0309 'Design Change Package'. Digital components require an assessment by Cyber Security per 0PGP03-ZS-0012 'Cyber Security	

	Assessment of Digital Assets'.
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
	Compromise of Heater Drain controls would likely cause heater level perturbation and possibly plant trip prior to mitigation of a cyber attack. The CDAs are periodically checked to ensure that the equipment is capable of performing design function. This is equipment does not however adversely impact a Safety or Security function.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.
	Configuration management and analysis of changes to the HD Bridge Controller are maintained per the CSP to ensure that any modifications to the system or plant procedures do not adversely impact the answers to Question 1.4 and the results of this analysis.

If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).

1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☐ YES ☒ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	_____
	Name (Signature)
Reviewer:	_____
	Name (Signature)
Other Review (as applicable):	_____
	Name (Signature)
Final Approval:	_____
	Name (Signature)

[BLANK PAGE]

EXAMPLE: SECURITY RADIO SYSTEM

CDA Identification:

CDA Number: SECRAD CDA Description: Security Radio System Additional CDA Numbers, IF performing assessment of grouped CDAs. Ensure you have documented criteria and technical basis for grouping CDA's: Base Station Repeater Portable #1 Portable #2

Emergency Planning Consequence Assessment:

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")			
1.1	Q1.1 EP-related or EP support systems and equipment?	☐ YES	☒ NO
Note: The following guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions. For safety-related, important-to-safety, or security functions proceed to Figure 1, Question 1.4			
If YES, document applicable 10 CFR 50.47 Planning Standard(s) the CDA supports below:			
If YES, document applicable NUREG -0654 Section(s) the CDA supports below:			
If YES, document the Emergency Planning function(s) the CDA supports below:			
IF YES, THEN proceed to Figure 2, Question 2.1.		IF NO, THEN proceed to Figure 1, Question 1.4.	
1.2	Q2.1 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4 and Figure 2)? Document basis for YES or NO answer:	☐ YES	☐ NO
IF YES, THEN proceed to Figure 2, Question 2.2.		IF NO, THEN proceed to Figure 1, Question 1.4.	
2.2	Q2.2 Are one or more of the alternate means administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☐ YES	☐ NO

Note: 1.) Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means 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 means provided they do not depend on identified CDA(s) for which controls have not been assessed.		
IF YES, THEN proceed to Figure 2, Question 2.3.	IF NO, THEN proceed to Figure 1, Question 1.4.	
2.3	Q2.3 Is the alternate means documented? (as described in Section 4). Document basis for YES or NO answer:	☐ YES ☐ NO
Note: The alternate means must be documented in a plant plan, policy, or implementing procedure.		
IF YES, THEN proceed to Figure 2, Question 2.4.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.4	Q2.4 Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? (as described in Section 4). 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 means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.		
IF YES, THEN proceed to Figure 2, Question 2.5.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
2.5	Q2.5 Are appropriate facility personnel trained to use the alternate method? (as described in Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Figure 1, Question 1.3.	IF NO, THEN remediate or go to Figure 1, Question 1.4.	
1.3	Q1.3 Are minimum cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following minimum criteria are met.	☐ YES ☐ NO
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.	

e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions taken to support ongoing monitoring and assessment.

IF YES, THEN current measures are adequate to meet Section 3.1.6 of the Cyber Security Plan.	IF NO, THEN remediate or go to Figure 1, Question 1.4.

Indirect CDA Consequence Assessment:

1.4	Q1.4 Is the CDA an indirect CDA as described in Section 3.1? Document the CDA's function and the basis for YES or NO answer.	☒ YES ☐ NO
Note: Indirect CDAs include only those CDAs that meet all three of the following criteria: 1.) If compromised, would not have an adverse impact on systems and equipment that perform Safety or Security functions; 2.) Are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, 3.) The compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.		
The Security Radio system is used to comply with the following regulatory requirements documented in 10 CFR 73.55(j): • Establish and maintain continuous communication capability with onsite and offsite resources • Ensure individuals assigned to each alarm station are capable of calling for assistance in accordance with the security plans and the licensee's procedures • Ensure all on-duty security force personnel are capable of maintaining continuous communication with an individual in each alarm station, and vehicle escorts maintain continuous communication with security personnel The compromise or failure of the Security Radio system will not result in a near-term adverse impact or inability to perform the Security communications requirements above. The Security Radio System meets the criteria for an indirect CDA because the following additional independent communications methods are continuously available to support Security communications: • Wired phone system • Wireless phone system (e.g. Spectralink) • Wired intercom system • Plant page system Cellular phones (site specific - not available to all officers)		
IF YES, THEN proceed to Figure 1, Question 1.5.	IF NO, THEN proceed to Figure 1, Question 1.7.	
1.5	Q1.5 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☒ YES ☐ NO
a.	Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or Safety or Security functions (in all operating modes). Document below how a CDA compromise would be detected and the compensatory measures in place prior to an adverse impact:	
	Minimum time required for detection and compensatory measure (Note: The minimum time period required should be based on existing analyses.): See below	
	Loss or impairment of communications methods is exercised and radio jamming and/or spoofing is presumed in Security exercises. Should the Security Radio system fail or be compromised in a way that precludes officers from using it to effectively communicate, in accordance with procedure SECURITY-101, officers are trained and instructed to utilize alternate, adequately independent communications methods to communicate as required. The minimum time period in this case is the time required for an officer to identify the Security radio system is not available or effective and for him/her to identify and begin using one of the previously documented alternate means of communication. Upon failure or compromise the previously mentioned adequately independent communications methods are relied upon to fulfill the 10 CFR 73.55(j)	

	communication requirements prior to an adverse impact. A site-specific analysis has concluded the use of wired communication methods can be used for initial officer deployment and redirects (where applicable) to preclude an adverse impacts to 10 CFR 73.55(j) communication requirements. The time required to detect and compensate for a Radio system failure or compromise does not prevent officers from meeting required response timelines as defined in the site-specific protective strategy.
b.	Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period.
	Detection occurs upon the officer recognizing the inability to effectively communicate or confirm receipt of a message. Security procedure [insert reference(s) here] and/or training [insert reference(s) here] reinforce the use of primary and alternate communication methods.
c.	Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes.
	Upon failure or compromise of the Security Radio system, officers are trained and instructed to utilize alternate, adequately independent communications methods to communicate as required. The implementation strategy to preclude an adverse impact associated with the loss or compromise of the Security Radio System is to credit the following adequately independent communication methods that ensure officers maintain the ability to communicate as required to fulfill 10 CFR 73.55(j) communication requirements: • Wired phone system • Wireless phone system (e.g. Spectralink) • Wired intercom system • Plant page system • Cellular phones (not available to all officers) Critical messages (e.g. Security code announcements) are communicated in parallel across both wired (e.g. Plant page or Intercomm system) and wireless communications systems (e.g. radio, Spectralink or cellular).
d.	Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1.
	Detection of the loss of the ability to communicate occurs when an officer identifies he/she is unable to communicate using their Security System portable radio. The aforementioned available alternate, independent communications methods and systems are sufficient to preclude a near-term adverse impact to the 10 CFR 73.55(j) communication requirements. A site-specific analysis supports the use of wired communication methods that can also be used for initial officer deployment and redirects (where applicable) to preclude an adverse impacts to 10 CFR 73.55(j) communication requirements. The time required to detect and compensate for a Radio system failure or compromise does not prevent officers from meeting required response timelines as defined in the site-specific protective strategy.
IF YES, THEN proceed to Figure 1, Question 1.6.	IF NO, THEN proceed to Figure 1, Question 1.7.
1.6	Q1.6 Are the minimum Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following minimum criteria are met. ☒ YES ☐ NO
a.	The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a

	Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection," is addressed. Document the location of the CDA and Section E.5 controls if located outside the PA.
	Most of the Security system base stations, repeaters, antennas and other infrastructure are located within the protected area of the facility. Fixed Radio system infrastructure located outside the protected area is physically protected consistent with the requirements of NEI 08-09, Appendix E, Section E.5 "Physical and Operational Environment Protection." Portable radios and other wireless communications accessories are carried by officers on their person or are maintained in a protected facility inside the PA when not in use.
b.	The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.
	The Security Radio system is designed to communicate wirelessly and therefore this control is addressed via an equivalent alternative. Specifically, the portable radio and the Radio system infrastructure (e.g. base stations and repeaters) incorporated cyber security protections provided by the vendors to provide equivalent protections. The vendor's cyber security specifications are provided in plant document XXXX. The fixed Radio system infrastructure are maintained on a separate, isolated, logical network that is not shared with other plant voice or data networks.
c.	The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. Document how information enforcement flow is addressed for the CDA.
	See the response for Question 1.5. b.
d.	The use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices. Document portable media and mobile device controls in place.
	The use of portable media and mobile devices (PMMD) as specified by the IT-AA-505 PMMD program is controlled for the Radio System in accordance with procedure IT-AA-505-1001.
e.	Document how changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, "Addition and Modification of Digital Assets." Document how changes to indirect CDAs are controlled.
	Changes to the Security Radio System are required to be completed in accordance with procedure CC-AA-102 "Configuration Change Control for Permanent Physical Plant Changes " and evaluated for impact in accordance with 10 CFR 50.54(P).
f.	Document how the indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks. Document the actions taken to periodically ensure equipment is capable of performing its intended function.
	The Security Radio System is utilized by officers intermittently on a 24x7x365 basis. A site specific analysis supports the conclusion that its loss or compromise would typically be identified via routine Radio System checks.
g.	Document ongoing monitoring and assessment in accordance with CSP is performed. Document the actions

	taken to support ongoing monitoring and assessment.
	The Security Radio System is classified as a Critical System and its components classified as CDAs. The Security Radio System is managed under the company's Cyber Security Plan (CSP) and program. As a result is it subject to ongoing monitoring and assessment as described in NEI 08-09 Rev. 6 Section 4.4 including periodic reviews to evaluate and improve as needed the effectiveness of the cyber security controls needed to protect the system from potential cyber attack.
If YES	The current Cyber Security controls are adequate to meet the Cyber Security Plan, Section 3.1.6. END ASSESSMENT HERE.
If NO	Remediate to meet the minimum Cyber Security protection criteria described in Section 5 OR proceed to Question 1.7 (see Figure 1).
1.7	Address cyber security controls in accordance with Section 3.1.6 of the licensee's Cyber Security Plan.

Outstanding Action Tracking:	☐ YES ☒ NO
Note: Insert here any outstanding actions required to satisfactorily complete this assessment.	

CYBER SECURITY ASSESSMENT TEAM APPROVAL	
Initiator:	_____
	Name (Signature)
Reviewer:	_____
	Name (Signature)
Other Review (as applicable):	_____
	Name (Signature)
Final Approval:	_____
	Name (Signature)

[BLANK PAGE]

APPENDIX D – DIRECT CDA CLASSES AND ASSESSMENTS

Appendix D provides a class description and a corresponding cyber security control assessment table for the class. See Section 6 of this document for further information.

[BLANK PAGE]

Class A.1 CDA (Low-Functionality, Direct Impact)

Software Attributes of Class A.1 CDAs:

- Program code (e.g. instruction-level code) cannot be altered and does not utilize or support operating system or application software
- Changes to operational parameters or operational settings can only be implemented using maintenance and test equipment
- Configuration changes can only be implemented by taking the device out of service
- Device does not support any sort of event logging
- Device does not support application or 3rd party software

Hardware Attributes of Class A.1 CDAs:

- Device includes PROM, RAM, EEPROM and possibly integrated components (e.g. FPGA) with factory-configurable firmware and functionality
- Device has no remote or local, integral HMI (but may have local display-only indicators)
- Device has no communications hardware/software but may have interfaces to external devices/systems using analog/contact/pulse I/O signals
- Device has no peripherals, interfaces or ports (e.g. media access, serial, etc.)

Location of Class A.1 CDAs:

- Protected Area (PA) or Vital Area (VA)

Information Classification for Class A.1 CDAs:

- CDA contains plant process data not classified as security-related or Safeguards Information (SGI)

Examples of Class A.1 CDAs:

Love Controls Series SC1290 & SC1490 Thermocouple Limit/Alarm Switch Module

KNS Perfecta Model: VPI-3EAN unit

Rosemount 3153N digital transmitters

[BLANK PAGE]

Class A.1 CDA (Low-Functionality, Direct Impact) Cyber Security Control Assessment

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D1.1	Access Control Policy and Procedures (D1.1)	**X**	**X**			The Access Control Policy and Procedures control is a common control applicable to the licensee organization. Its requirements should be applied to CDAs based upon defined and documented access control policies and procedures.
D1.2	Account Management (D1.2)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.3	Access Enforcement (D1.3)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.4	Information Flow Enforcement (D1.4)				**X**	Class A.1 devices do not have any communications hardware/software, peripherals, interfaces, or ports (e.g., media access, serial). Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.5	Separation of Functions (D1.5)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D1.6	Least Privilege (D1.6)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.7	Unsuccessful Login Attempts (D1.7)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.8	System Use Notification (D1.8)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.9	Previous Logon Notification (D1.9)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.10	Session Lock (D1.10)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable
D1.11	Supervision and Review – Access Control (D1.11)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D1.12	Permitted Actions Without Identification and Authentication (D1.12)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, this control is not applicable.
D1.13	Automated Marking (D1.13)				**X**	Class A.1 devices do not have the capability to generate any form of output. Class A.1 devices that do provide output only generates plant process data output that does not contain security-related information (SRI) or SGI. Since SRI and SGI are not present, this control is not applicable.
D1.14	Automated Labeling (D1.14)				**X**	Class A.1 devices do not have the capability to generate any form of output. Class A.1 devices that do provide output only generates plant process data output that does not contain security-related information (SRI) or SGI. Since SRI and SGI are not present, this control is not applicable.
D1.15	Network Access Control (D1.15)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.16	"Open/Insecure" Protocol Restrictions (D1.16)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D1.17	Wireless Access Restrictions (D1.17)				**X**	Class A.1 devices do not have any communications (including wireless) hardware/software as described in the Class A.1 description. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable Note: This control also requires periodic scans for unauthorized wireless devices and rogue access points on plant LANs. Even though this control is not applicable directly to class A.1 CDAs, the additional requirement for periodic scans still applies to the plant's defensive architecture.
D1.18	Insecure and Rogue Connections (D1.18)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.19	Access Control for Portable and Mobile Devices (D1.19)				**X**	Class A.1 devices do not have any peripherals, interfaces, or ports (e.g., media access, serial). The CDA cannot be impacted by any portable devices/media. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable. .
D1.20	Proprietary Protocol Visibility (D1.20)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D1.21	Third Party Products and Controls (D1.21)	**X**	**X**			The Third Party Products and Controls control is applicable to class A.1 CDAs and may be implemented as a common control. This control ensures any known, uncorrected/unmitigated CDA cyber vulnerabilities or weaknesses are documented in the site Corrective Action Program, properly evaluated, and addressed/mitigated as required by the CSP. CDA vulnerabilities shall also be addressed by the E3.2 Flaw Remediation control.
D1.22	Use of External Systems (D1.22)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D1.23	Public Access Access Protections (D1.23)				**X**	A Class A.1 CDA by definition does not contain any SGI or SRI information, and thus the attack vector addressed by this control does not exist and the control is not required.
D2.1	Audit and Accountability Policy and Procedures (D2.1)	**X**	**X**			The Audit and Accountability Policy and Procedures control is a common control applicable to the licensee organization. Its requirements should be applied to CDAs based upon defined and documented auditing and accountability policies and procedures.
D2.2	Auditable Events (D2.2)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D2.3	Content of Audit Records (D2.3)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.4	Audit Storage Capacity (D2.4)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.5	Response to Audit Processing Failures (D2.5)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.6	Audit Review, Analysts and Reporting (D2.6)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.7	Audit Reduction and Report Generation (D2.7)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D2.8	Time Stamps (D2.8)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.9	Protection of Audit Information (D2.9)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.10	Non-Repudiation (D2.10)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.11	Audit Record Retention (D2.11)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D2.12	Audit Generation (D2.12)				**X**	Class A.1 devices have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings), settings, or configuration of the CDA. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D3.1	CDA, System and Communications Protection Policy and Procedures (D3.1)	**X**	**X**			The CDA, System and Communications Protection Policy and Procedures control is a common control applicable to the licensee organization. Its requirements should be applied to CDAs based upon defined and documented system and communication protection policies and procedures.
D3.2	Application Partitioning/Security Function Isolation (D3.2)				**X**	Class A.1 CDAs have no operating system and only support program functions defined by the manufacturer, and their program code and configuration cannot be altered. Thus, the attack vector associated with this control does not exist and therefore this security control is not applicable.
D3.3	Shared Resources (D3.3)				**X**	Class A.1 CDAs have no operating system and only support program functions defined by the manufacturer, and their program code and configuration cannot be altered. Thus, the attack vector associated with this control does not exist and this security control is not applicable.
D3.4	Denial of Service Protection (D3.4)				**X**	Class A.1 CDAs have no operating system, communication capabilities, and only support program functions defined by the manufacturer, and their program code and configuration cannot be altered. Thus, the attack vector associated with this control does not exist and therefore the control, or alternative countermeasure, is not applicable.
D3.5	Resource Priority (D3.5)				**X**	Class A.1 CDAs have no multi-tasking operating system and only support program functions defined by the manufacturer, and their program code and configuration cannot be altered. Thus, the attack vector associated with this control does not exist and this security control is not applicable.
D3.6	Transmission Integrity (D3.6)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. The signals transmitted by these CDAs do not adverse impact the SSEP functions or other CDAs. Thus, the attack vector associated with this control does not exist and this security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D3.7	Transmission Confidentiality (D3.7)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. Any external connections are adequately protected against tampering. Thus, the attack vector associated with this control does not exist and the security control is not applicable.
D3.8	Trusted Path (D3.8)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) and configuration in the CDAs cannot be altered Additionally Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description. Therefore, this cyber security control is not applicable.
D3.9	Cryptographic Key Establishment and Management (D3.9)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description, do not use cryptography and do not contain SRI or SGI information. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable
D3.10	Unauthorized Remote Activation of Services (D3.10)				**X**	Class A.1 devices have no interface through which a user can gain access and Class A.1 devices do not have any communications hardware/software. Therefore, attack vectors associated with this security control do not exist and this control is not applicable.
D3.11	Transmission of Security Parameters (D3.11)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description and does not transmit or receive any security parameters. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D3.12	Public Key Infrastructure Certificates (D3.12)				**X**	Class A.1 devices do not have any communications hardware/software as described in the Class A.1 description, do not use cryptography, and do not contain SRI or SGI information. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.
D3.13	Mobile Code (D3.13)				**X**	Class A.1 devices do not use or support operating system, third-party, or application software and do not support mobile code. In addition, CDAs do not support any communications hardware/software or any peripherals, interfaces, or ports (e.g., media access, serial). Therefore, this cyber security control is not applicable.
D3.14	Secure Name/Address Resolution Service (Authoritative/Trusted Source) (D3.14)				**X**	Class A.1 devices have no interface through which a user can gain access and Class A.1 devices do not have any communications hardware/software. Therefore, attack vectors associated with this security control do not exist and this control is not applicable.
D3.15	Secure Name/Address Resolution Service (Recursive or Caching Resolver) (D3.15)				**X**	Class A.1 devices have no interface through which a user can gain access and Class A.1 devices do not have any communications hardware/software. Therefore, attack vectors associated with this security control do not exist and this control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D3.16	Architecture and Provisioning for Name/Address Resolution Service (D3.16)				**X**	Class A.1 devices have no interface through which a user can gain access and Class A.1 devices do not have any communications hardware/software. Therefore, attack vectors associated with this security control do not exist and this control is not applicable. NOTE: Although Class A.1 CDAs do not use DNS services if any other class of CDAs do require that support then this control would be applicable to the plant's defensive architecture and DNS servers.
D3.17	Session Authenticity (D3.17)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Additionally, CDAs do not use or support operating systems or application software. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D3.18	Thin Nodes (D3.18)				**X**	Class A.1 CDAs do not support communication hardware/software and so cannot be incorporated into a centralized-architecture system design. Also these CDAs have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D3.19	Confidentiality of Information at Rest (D3.19)				**X**	Class A.1 CDAs do not contain, process, or store security-related information (SRI) or SGI. Since SRI or SGI are not contained, stored, or processed on the device, this control is not applicable.
D3.20	Heterogeneity (D3.20)	**X**	**X**			This security control can be commonly addressed by the plant by inheriting the protection provided by the licensee's program to address common mode failure issues associated with safety and security systems.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D3.21	Fail in Known (Safe) State (D3.21)		**X**			For Class A.1 CDAs this cyber security control must be addressed in accordance with Section 3.1.6 of the CSP. A Failure Modes and Effects Analysis (FMEA) is one acceptable approach to achieving this control.
D4.1	Identification and Authentication Policies and Procedures (D4.1)	**X**	**X**			The Identification and Authentication Policies and Procedures control is a common control applicable to the licensee organization. Its requirements should be applied to CDAs based upon defined and documented identification and authentication polices and procedures.
D4.2	User Identification and Authentication (D4.2)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.
D4.3	Password Requirements (D4.3)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.
D4.4	Non-Authenticated Human Machine Interaction (HMI) Security (D4.4)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered. Therefore, the attack vector associated with this control does not exist and this cyber security control is not applicable.
D4.5	Device Identification and Authentication (D4.4)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered, and do not have any communications hardware/software/ports/media access. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D4.6	Identifier Management (D4.6)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered and do not have any communications hardware/software/ports/media access. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D4.7	Authenticator Management (D4.7)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered, and do not have any communications hardware/software/ports/media access. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D4.8	Authenticator Feedback (D4.8)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) in the CDAs cannot be altered, and do not have any communications hardware/software/ports/media access. Therefore, an attack vector associated with this control does not exist and this cyber security control is not applicable.
D4.9	Cryptographic Module Authentication (D4.9)				**X**	Class A.1 devices do not use cryptography, therefore attack vectors associated with this security control do not exist and this control is not applicable.
D5.1	Removal of Unnecessary Services and Programs (D5.1)				**X**	Class A.1 CDAs have no operating systems or communication capabilities, only support program functions defined by the manufacturer, their program code and configuration cannot be altered, and do not have any unnecessary services or programs. Thus, an attack vector associated with this control does not exist and therefore the control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
D5.2	Host Intrusion Detection System (HIDS) (D5.2)				**X**	Class A.1 devices have no interface through which a user can gain access and program code (e.g., instruction-level code, configuration, settings) and configuration of the CDAs cannot be altered. The CDA cannot be impacted by any portable devices/media. Therefore, attack vectors associated with this security control do not exist and this control is not applicable.
D5.3	Changes to File System and Operating System Permissions (D5.3)				**X**	Class A.1 devices have no interface through which a user can gain access and have no alterable software/code/settings. Additionally, Class A.1 devices do not use or support operating system or application software and do not support application or third-party software. Therefore, attack vectors associated with this security control do not exist and this control is not applicable.
D5.4	Hardware Configuration (D5.4)				**X**	Class A.1 devices do not have peripherals, interfaces, or media access ports. Class A.1 device hardware is dedicated to a single plant process function and its hardware cannot be altered. Therefore, the attack vectors associated with this security control do not exist and the security control is not applicable.
D5.5	Installing Operating Systems, Applications, and Third-Party Software Updates (D5.5)				**X**	Class A.1 devices have no interface through which a user can gain access and have no alterable software/code/settings. Therefore, attack vectors associated with this security control do not exist and this control is not applicable.
E3.3	Malicious Code Protection (E3.3)				**X**	Class A.1 devices have no interface through which a user can gain access and have no alterable software/code/settings. The CDA cannot be impacted by any portable devices/media. Thus, the attack vector associated with this control does not exist and this security control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
E3.4	Monitoring Tools and Techniques (E3.4)				**X**	Class A.1 devices have no interface through which a user can gain access and have no alterable software/code/settings. The CDA cannot be impacted by any portable devices/media. Thus, the attack vector associated with this control does not exist and this security control is not applicable.
E3.7	Software and Information Integrity (E3.7)				**X**	Class A.1 devices have no interface through which a user can gain access and have no alterable software/code/settings. The CDA cannot be impacted by any portable devices/media. Thus, the attack vector associated with this control does not exist and this security control is not applicable.
E3.8	Information Input Restrictions (E3.8)				**X**	Class A.1 devices have no interface through which a user can gain access and have no alterable software/code/settings. The CDA cannot be impacted by any portable devices/media. Thus, the attack vector associated with this control does not exist and this security control is not applicable.
E3.9	Error Handling (E3.9)				**X**	Class A.1 devices have no user interface, cannot generate error messages, and do not contain either SRI or SGI information. Therefore, the attack vector associated with this control does not exist, and the control is not applicable.