NEI 13-10 [Revision 6]

Cyber Security Control Assessments

August 2017

[BLANK PAGE]

NEI 13-10 [Revision 6]

Nuclear Energy Institute

Cyber Security Control Assessments

August 2017

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
Matthew Coulter	Duke Energy Corporation
Ronald Cowley	Talen Energy Corporation
Nathan Faith	Exelon Corporation
Pam Frey	Talen Energy Corporation
Glen Frix	Duke Energy Corporation
Jan Geib	South Carolina Electric & Gas Company
William Gross	Nuclear Energy Institute
Christopher Kelley	Exelon Corporation
Ken Levandoski	Exelon Corporation
Tony Lowry	Ameren Missouri
Jerry Mills	Duke Energy Corporation
Jay Phelps	South Texas Project Nuclear Operating Company
Don Robinson	Dominion Generation
Geoff Schwartz	Entergy
James Shank	PSEG Services Corporation
Manu Sharma	Exelon Corporation
Laura Snyder	Tennessee Valley Authority
Larry Tremonti	DTE Energy
Brad Yeates	Southern Nuclear Operating Company
Michael Zavislak	Tennessee Valley Authority

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 categories, Emergency Preparedness (EP), Balance of Plant (BOP), Indirect, and Direct 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 Revision 1 was 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 of Revision 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.

Revision 4 incorporates additional CDA classes and assessments into Appendix D, building on the work added in Revision 2. Conforming changes were made to the following Class A.1 control responses: D1.21 Third Party Products and Controls, and D3.21 Fail in Known (Safe) State.

Revision 5 addresses lessons learned from a workshop conducted in 2016 that included industry and NRC observers. Revision 5 modified Section 3 to enhance clarity for assigning CDAs to categories. Tables 1 and 2 from Revision 4 were removed and the guidance contained in those tables was moved to body of the text. Figures 1 and 2 in Appendix A were used to develop a sample template in Appendix B. The BOP category was added to the example template in Appendix B. Changes to reflect the enhancements to Revision 5 were incorporated into the examples in Appendix C. Two additional Appendices were added. Appendix E contains questions and answers based on lessons learned. Appendix F addresses NEI 08-09, Revision 6 programmatic controls for non-Direct CDAs.

Revision 6 addresses comments resulting from the NRC's review of NEI 13-10, Revision 5. Those comments were provided to NEI by letter dated July 21, 2017 (Adams Accession Number: ML17179A266). The following three items were addressed in Revision 6:

1. Revision 6 was clarified regarding the term 'safety functions' with respect to the identification of CDAs as Direct or Indirect. Conforming changes were made to questions 1 and 2 in Appendix E.

2. Question 6 of Appendix E was clarified to indicate that for limited capability devices, detection may be possible using existing administrative measures.

3. The template in Appendix B and examples in Appendix C were clarified to correctly reference the figures in Appendix A.

3 CONSEQUENCE ASSESSMENT OF CDAS

Section 3.1.6 of the CSP allows licensees to address the security controls provided in the CSP using alternate security controls if they provide at least the same protection as the required security controls. The Consequence Assessment provided in NEI 13-10 provides a method to assess alternate means of protecting low consequence CDAs (i.e., CDAs that are not Direct as described in NEI 13-10) from cyber attacks. The technical basis of the Consequence Assessment provided in this document is that the combination of the criteria for being a non-Direct CDA and the implementation of the resulting baseline cyber security controls provides equal protection as the protection provided by the required technical security controls in NEI 08-09.

Licensees may use the guidance detailed in this section to categorize low consequence CDAs into EP, BOP, or Indirect based on the potential consequence of a cyber compromise of the CDAs and to identify alternate security controls that are appropriate for the CDAs. Any CDA that has not been determined to be a low consequence CDA is a Direct CDA. Appendix D of this document provides examples of cyber assessments for certain Direct CDAs. A Consequence Assessment may result in the determination that certain baseline cyber security controls specified in Section 5 of this document, “Baseline Cyber Security Protection Criteria,” provide adequate cyber security protection for the CDA. The Consequence Assessment and the baseline 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 CDA’s SSEP function and the evaluation of the potential impacts resulting from a cyber attack on the CDA may result in the CDA being qualified to be categorized as an EP, BOP or Indirect CDA rather than a Direct CDA. However, redundancy is not used as a factor in determining if a CDA is an EP, BOP, Indirect or Direct CDA.

CDAs which perform multiple SSEP functions must be evaluated in this Consequence Assessment based the most consequential category (i.e., Direct, then either Indirect, BOP, or EP).

Consistent with Section 4.4 and 4.5 of their CSPs, 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 must be addressed programmatically in accordance with Section 3.1.6 of the CSP for CDAs. Appendix F of NEI 13-10, Revision 6, provides a template to address the NEI 08-09, Appendix E, operational and management controls for CDAs not classified as Direct. Appendix F of NEI 13-10 describes the use of existing plant programs to address the NEI 08-09, Appendix E, controls for the non-Direct CDAs, consistent with CSP Section 3.1.6.

3.1 EP CDAs

EP CDAs are those CDAs that support licensee's performance of EP functions and that have an independent alternate means of performing those functions. EP CDAs must meet the following criteria:

1. The CDA only supports an EP function and does not perform or support any other Safety, Important-to-Safety or Security function.

2. An Alternate Means assessment is performed in accordance with Section 4 of this document to demonstrate and document that an independent alternate means of performing the EP function will be available in sufficient time such that the compromise of the CDA would not adversely impact the licensee's ability to perform that EP function.

3. EP CDAs must meet all of the requirements defined in Section 4 of this document.

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

3.2 BOP CDAs

BOP CDAs are those CDAs that were added to the scope of the cyber security rule during the resolution of FERC Order 706-B. The following language was included within licensee CSPs to include the balance-of-plant into the scope of 10 CFR 73.54:

> "Within the scope of NRC's cyber security rule at Title 10 of the Code of Federal Regulations (10 CFR) 73.54, systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system."

NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, provides guidance for identifying Critical Systems and CDAs. Section 5 of NEI 10-04 provides the following guidance, in the form of questions, for identifying important-to-safety Critical Systems:

1. Is this a non-safety related system whose failure could adversely impact any of the functions identified in the previous three "Safety Systems" questions?
2. Is this a non-safety related system that is part of the primary success path and functions or actuates to mitigate a transient that either assumes the failure of or

presents a challenge to the integrity a fission product barrier?
3. Has operating experience or a probabilistic risk assessment shown that a non-safety related system function is significant to public health and safety?
4. Does the non-safety related system function to provide real-time or near-real-time plant status information to the operators for the safe operation of the plant during transients, and accidents?
5. Is this a structure, system, or component in the balance of plant that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient?
6. Is this a non-safety system required to maintain defense-in-depth and diversity requirements?

Question 5 was added to ensure licensees identify those BOP SSCs added to address FERC Order 706-B and to support meeting the commitment language in the CSP. Where a licensee answered YES to Question 5 and NO to the remaining NEI 10-04 questions, the associated CDAs can be identified as a BOP CDA for the purposes of NEI 13-10. These screening questions identifies that, if compromised, the BOP CDA could not have an adverse impact to Safety functions because: (1) the current accident or other analysis bounds the failure of the BOP CDAs or systems; (2) the plant operators apply their training and operating experiences including manual operator actions to ensure that plant conditions caused by cyber compromise of the BOP CDA are maintained within safety limits; and, (3) the equipment that performs Safety functions are isolated from the BOP CDAs. Based on the above, a cyber compromise of BOP CDAs cannot lead to adverse impact to Safety CDAs or systems. Therefore, unlike the other non-direct CDAs, the time required to detect and mitigate the cyber compromise of BOP CDAs before adverse impact to safety CDAs or systems need not be determined.

Where a licensee answered YES to any of the other NEI 10-04 screening questions, associated CDAs should be screened for Indirect, as described below.

The language added to the CSPs (and reflected in Question 5) includes a broader set of BOP CDAs than those that are of interest to FERC (e.g., the CSP language includes assets that could cause a reactivity change or transient but not result in a reactor SCRAM/trip). BOP CDAs whose failure or cyber compromise could cause a reactor SCRAM/trip require additional security controls from NEI 08-09 Appendix D to be implemented where technically feasible, as specified in Section 5.1 of this document. These controls are applied to align with NERC CIP requirements.

Some stations may choose to classify their BOP CDAs as members of the Indirect category; however, this will not alleviate the need to address the additional controls listed in Section 5.1 for BOP CDAs that are SCRAM/Trip initiators.

For BOP CDAs, licensees may comply with the requirements of Section 3.1.6 of their Cyber Security Plans by documenting that the CDA meets the criteria described above and implementing the baseline controls for BOP CDAs as described in Section 5.

3.3 INDIRECT CDAS

Indirect CDAs are those CDAs that cannot have an adverse impact on Safety or Security functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee.

Specifically, Indirect CDAs must meet the following criteria:

1. If compromised, would not have an adverse impact on Safety or Security functions.
2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions.
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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse impact:

    a) Determine and document the time period required, once an Indirect CDA has been compromised, for both detection and compensatory measures to be taken prior to an adverse impact to Safety and Security functions. The time period required may be based on existing analyses.
    b) Document a method, and associated implementing procedures, for the detection of an Indirect CDA compromise and/or failure.
    c) Document implementation strategies for compensatory measures to eliminate the adverse impact to Safety and Security functions in all operating modes.
    d) Document the technical justification for how the detection activities and compensatory measures (i.e., Steps b and c above) for the Indirect CDA compromise and/or failure are sufficient and will occur within the time period determined by the licensee in Step a.

For the purposes of the Indirect screening, the following SSCs are considered to perform Safety functions: Safety-Related or Non-Safety-Related SSCs that are relied upon to remain functional during any plant conditions to ensure:

a. The integrity of the reactor coolant pressure boundary;

b. The capability to shut down the reactor and maintain it in a safe shutdown condition; or

c. The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to those referred to in 10 CFR 50.34(a)(1), 10 CFR 50.67(b)(2), or 10 CFR 100.11.

For Indirect CDAs, licensees may comply with the requirements of Section 3.1.6 of their Cyber Security Plans by documenting that the CDA meets the criteria described above and by implementing baseline controls for Indirect CDAs as described in Section 5.

3.4 DIRECT CDAS

In general, Direct CDAs are those CDAs that have not been determined to be Indirect, BOP or EP CDAs. Since the required security controls in NEI 08-09 are addressed for Direct CDAs, it is not necessary to show that a CDA is a Direct CDA. 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 whose implementation provides a security benefit 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 and implemented elsewhere such as on another CDA. Finally, the term "type assessment" or "grouping of CDAs" refers to a situation in which multiple CDAs share substantially similar technical features, functions and capabilities. 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, a threat vector associated with the technical control exists, and the CDA is unable to inherit the associated protections 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. Section 3.1.6 of the CSP describes the criteria for the implementation of alternate security controls.

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, BOP, EP or Direct CDA.

Some examples of Direct CDAs:

- 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).

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 one or more of the corresponding cyber security controls enumerated in Appendices D and E of NEI 08-09, Revision 6. The alternative controls and/or countermeasures must eliminate threat/attack vector(s) associated with the cyber security controls, and provide at least the same degree of cyber security protection as the corresponding cyber security control. The licensee must perform and document an analysis for the use of alternative controls or countermeasures to address the cyber security controls as specified in Section 3.1.6 of the licensee's NRC-approved CSPs. This guidance may be used for CDAs associated only with EP functions, and are not otherwise relied on for Safety-Related, Important-to-Safety, or Security functions.

Where an assessment determines that cyber attacks on CDAs associated with EP functions would not adversely impact the ability to implement the EP function, because licensees can detect the consequences of the potential cyber compromise of the CDA and initiate independent alternative means in time to prevent adverse impact to the EP functions that are supported by the CDAs, then the required technical security controls for the CDAs can be addressed by application of baseline security criteria as described in Section 5.

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.

The licensee must determine whether an alternative means allows the performance of the intended emergency response function despite cyber attacks. For EP CDAs with an alternative means, licensees may comply with the requirements of Section 3.1.6 of their Cyber Security Plans by implementing the following guidance:

1. Document alternate means available for performing the intended EP function, including offsite communications.

2. Document that one or more of the alternate means are administrative, non-digital, or if digital are adequately independent.

    Note:

    a. 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.).

b. 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.

3. Document how the equipment, that a compromise of the CDA would impact, is periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed. Specifically, document how a cyber attack that would prevent the EP-related equipment from performing its intended function would be detected and responded to prior to an adverse impact on the EP-related function during a radiological emergency.

   Note:

   a. 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.

4. Document how appropriate facility personnel are trained to use the alternate method.
5. Implement and document the baseline cyber security protections (d, e, f, and g) as described in Section 5 of this document for the CDA.

5 BASELINE CYBER SECURITY PROTECTION CRITERIA

An assessment using the guidance in Section 3 permits licensees to demonstrate that alternative controls and countermeasures are sufficient to provide adequate protection of CDAs. For these CDAs, the baseline 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 baseline cyber security criteria are not met, the licensee must document and implement additional security controls to ensure adequate protections are in place for the CDA. These additional security controls are implemented using the methodology in CSP Section 3.1.6.

Changes to the baseline cyber security controls must be reviewed in accordance with the CSP to ensure the non-Direct CDAs remain adequately protected from cyber attacks.

Where a licensee chooses to credit these baseline cyber security controls for an Indirect, BOP, or EP CDA, the licensee must confirm these baseline minimum controls criteria are met. EP CDAs may be considered to be adequately protected from cyber attacks if baseline criteria d, e, f, and g are met. A BOP CDA or Indirect CDA may be considered to be adequately protected from cyber attacks if all of the following baseline criteria are met:

a) The CDA, as identified using the analysis set forth in Section 3 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,” are addressed.

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

c) The CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some non-Direct CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include but may not be limited to:

    1. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an attack pathway to isolated devices, systems, or networks.
    2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.

d) Use of portable media and mobile devices is controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.

e) Changes to the CDA are evaluated and documented before implementation to ensure the following:

1. Baseline security criteria remain in place and effective.

2. No new pathways or vulnerabilities have been created.

3. No change to CDA would now make it Direct.

4. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.

f) The CDA, or the interconnected equipment that would be affected by the compromise of the 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 any Safety, Security, or EP functions resulting from cyber attacks. Section 3.1.6(2)(d) of the CSP allows licensees to implement an alternate periodicity for security controls by documenting the basis for the alternate periodicity.

g) Ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.

5.1 BOP CDAs THAT COULD CAUSE A REACTOR SCRAM/TRIP

For BOP CDAs whose failure or cyber compromise could cause a reactor scram/trip, the following additional security controls from NEI 08-09 Appendix D are implemented where technically feasible (i.e., the CDA supports the technical functionality and features):

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.

APPENDIX A – FIGURES

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

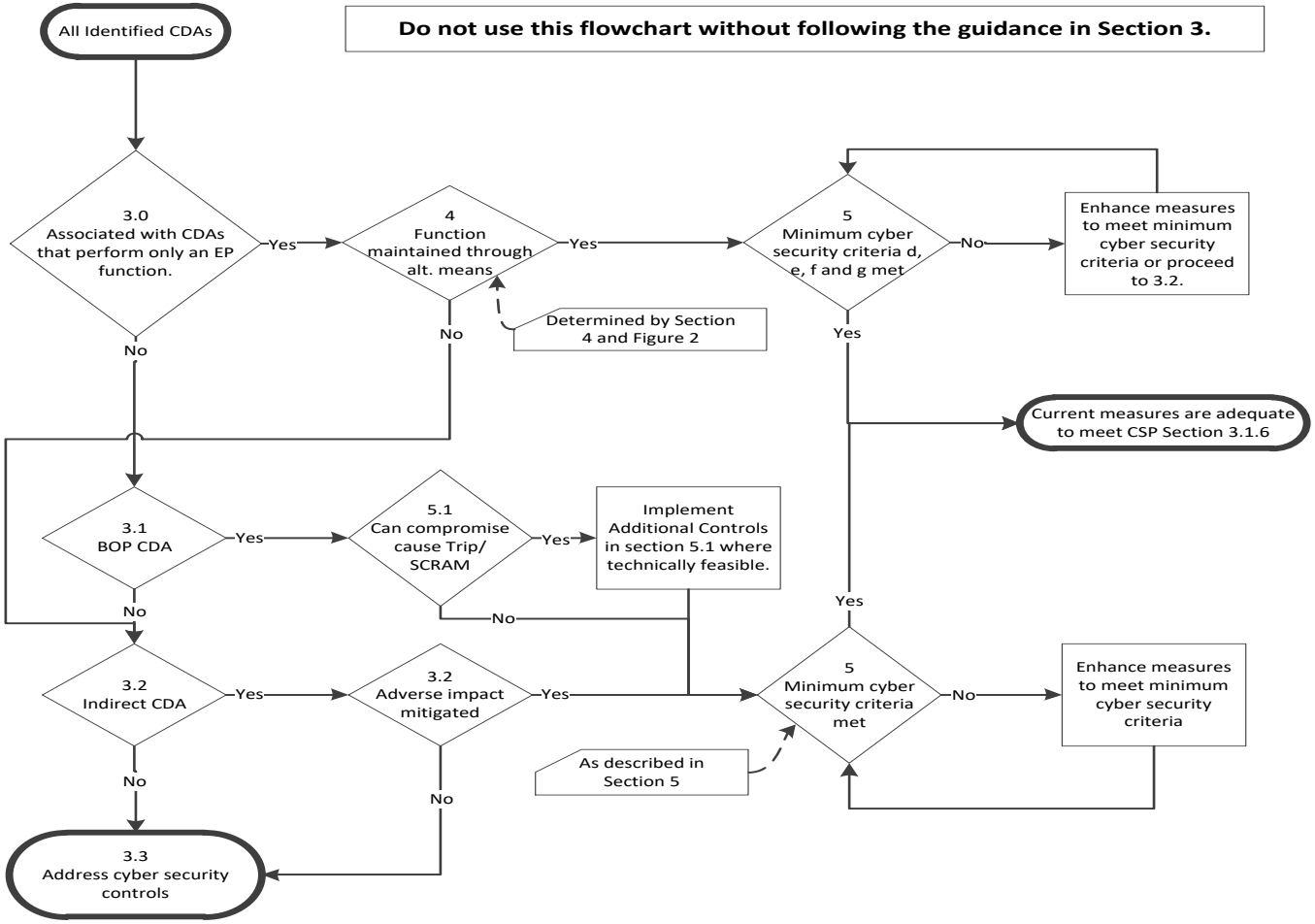

Figure 1 – Consequence Assessment

[BLANK PAGE]

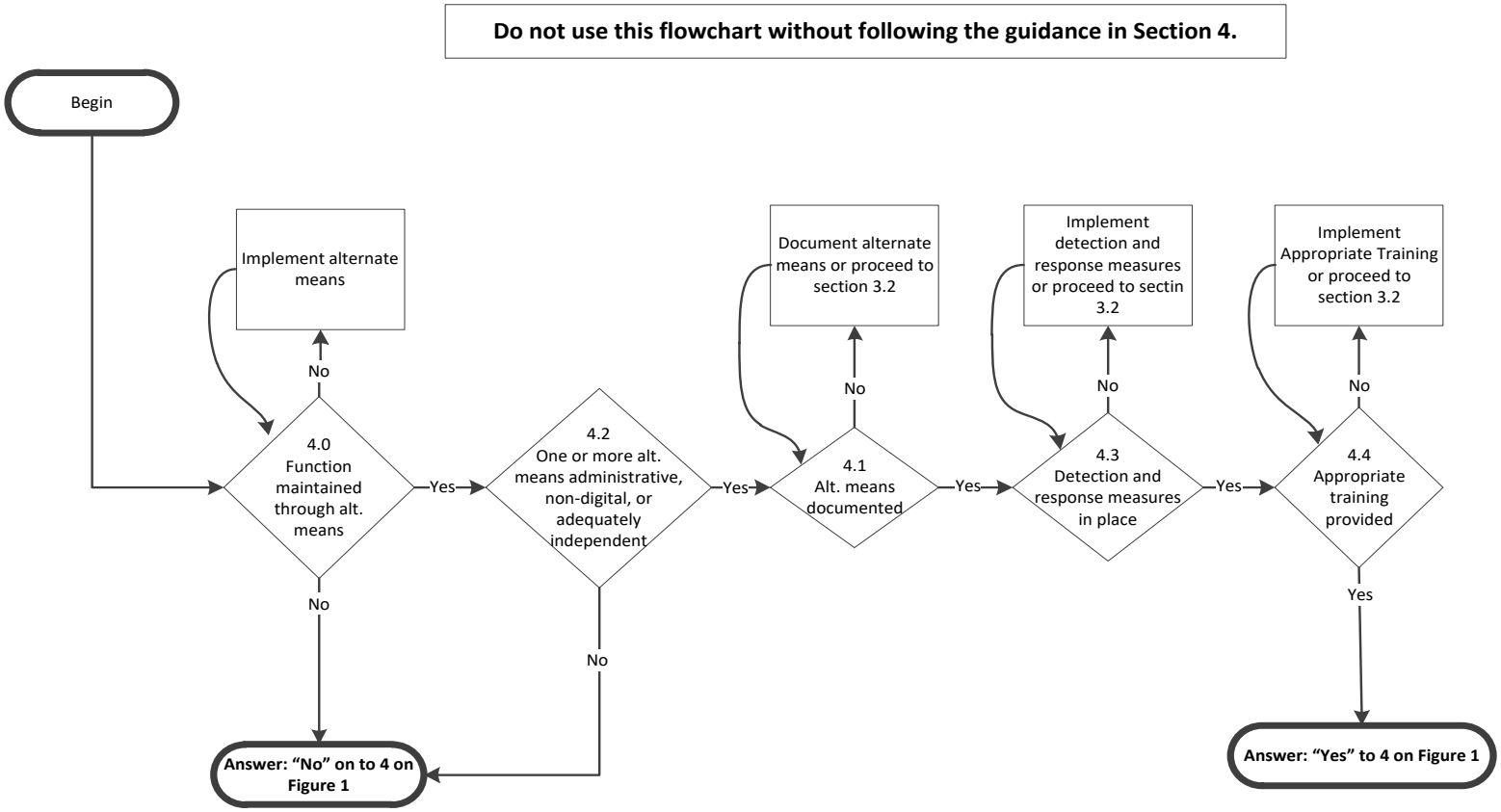

Figure 2 – Alternative Means Assessment for EP

[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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0		
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 Step 1.1	IF NO, THEN proceed to Step 2.0	
1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Step 1.2	IF NO, THEN proceed to Step 3.0	
1.2	Figure 2, Box 4.2 Are one or more of the alternate means administrative, non-digital, or	☐ YES ☐ NO

	if digital is it adequately independent? Document basis for YES or NO answer:	
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 Step 1.3	IF NO, THEN proceed to Step 3.0	
1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0	
1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0	
1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0	
1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.	

e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 1. Baseline security criteria remain in place and effective. 2. No new pathways or vulnerabilities have been created. 3. No change to CDA would now make it Direct. 4. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.

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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
	Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.	
IF YES, THEN proceed to Step 2.1	IF NO, THEN proceed to Step 3.0	

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☐ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 a near-term adverse impact on Safety or Security functions. 2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions. 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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.	
IF YES, THEN proceed to Step 3.1	IF NO, THEN proceed to Step 4.0	

3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.

IF YES, THEN proceed to Step 3.2	IF NO, THEN proceed to Step 4.0

3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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," are addressed.	
b.	The CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 1. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an	

	attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 1. Baseline security criteria remain in place and effective. 2. No new pathways or vulnerabilities have been created. 3. No change to CDA would now make it Direct. 4. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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 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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0		
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 Step 1.1		IF NO, THEN proceed to Step 2.0

1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? 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 Step 1.2	IF NO, THEN proceed to Step 3.0

1.2	Figure 2, Box 4.2 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 Step 1.3	IF NO, THEN proceed to Step 3.0

1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0

1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0

1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0	

1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☒ YES ☐ NO
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.	
	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 CDA are evaluated and documented before implementation to ensure the following: 5. Baseline security criteria remain in place and effective. 6. No new pathways or vulnerabilities have been created. 7. No change to CDA would now make it Direct. 8. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.	
	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 CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
	The Call-Out system is classified as a CDA and managed under the company’s Cyber Security Plan (CSP) and program. 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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.		
IF YES, THEN proceed to Step 2.1	IF NO, THEN proceed to Step 3.0	

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☐ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 Safety or Security functions. 2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions. 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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.		
IF YES, THEN proceed to Step 3.1	IF NO, THEN proceed to Step 4.0	

3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.

IF YES, THEN proceed to Step 3.2	IF NO, THEN proceed to Step 4.0

3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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," are addressed.	
b.	The CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 2. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an	

	attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 5. Baseline security criteria remain in place and effective. 6. No new pathways or vulnerabilities have been created. 7. No change to CDA would now make it Direct. 8. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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: 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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0		
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 Step 1.1	IF NO, THEN proceed to Step 2.0

1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? 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 Step 1.2	IF NO, THEN proceed to Step 3.0

1.2	Figure 2, Box 4.2 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 Step 1.3	IF NO, THEN proceed to Step 3.0

1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0

1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0

1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0	
1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☒ YES ☐ NO
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.	
	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 CDA are evaluated and documented before implementation to ensure the following: 9. Baseline security criteria remain in place and effective. 10. No new pathways or vulnerabilities have been created. 11. No change to CDA would now make it Direct. 12. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.	
	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 CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.	

	The MIDAS system is classified as a CDA and managed under the company's Cyber Security Plan (CSP) and program. 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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.		
IF YES, THEN proceed to Step 2.1	IF NO, THEN proceed to Step 3.0	

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☐ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 a near-term adverse impact on Safety or Security functions. 2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions. 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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.		
IF YES, THEN proceed to Step 3.1	IF NO, THEN proceed to Step 4.0	

3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.

IF YES, THEN proceed to Step 3.2	IF NO, THEN proceed to Step 4.0

3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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," are addressed.	
b.	The CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 3. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an	

	attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 9. Baseline security criteria remain in place and effective. 10. No new pathways or vulnerabilities have been created. 11. No change to CDA would now make it Direct. 12. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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)

[BLANK PAGE]

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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0

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 Step 1.1	IF NO, THEN proceed to Step 2.0

1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? 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 Step 1.2	IF NO, THEN proceed to Step 3.0

1.2	Figure 2, Box 4.2 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 Step 1.3	IF NO, THEN proceed to Step 3.0

1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0

1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0

1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0

1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☒ YES ☐ NO

d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
	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 D.1.19.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 13. Baseline security criteria remain in place and effective. 14. No new pathways or vulnerabilities have been created. 15. No change to CDA would now make it Direct. 16. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
	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 CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
	The NRC ENS system is classified as Critical Systems and CDAs and managed under the company's Cyber Security Plan (CSP) and program. 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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☐ NO
Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.		
IF YES, THEN proceed to Step 2.1	IF NO, THEN proceed to Step 3.0	

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☐ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 a near-term adverse impact on Safety or Security functions. 2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions. 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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.		
IF YES, THEN proceed to Step 3.1	IF NO, THEN proceed to Step 4.0	

3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.

IF YES, THEN proceed to Step 3.2	IF NO, THEN proceed to Step 4.0

3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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," are addressed.	
b.	The CDA and any interconnected assets do not have wireless internetworking communications technologies. Document how wireless networking is addressed for the CDA.	
c.	The CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 4. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an	

	attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 13. Baseline security criteria remain in place and effective. 14. No new pathways or vulnerabilities have been created. 15. No change to CDA would now make it Direct. 16. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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)

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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0		
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 Step 1.1	IF NO, THEN proceed to Step 2.0	
1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Step 1.2	IF NO, THEN proceed to Step 3.0	

1.2	Figure 2, Box 4.2 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 Step 1.3	IF NO, THEN proceed to Step 3.0

1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0

1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0

1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0

1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO

d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 17. Baseline security criteria remain in place and effective. 18. No new pathways or vulnerabilities have been created. 19. No change to CDA would now make it Direct. 20. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.

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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☒ NO
Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.		
IF YES, THEN proceed to Step 2.1	IF NO, THEN proceed to Step 3.0	

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☐ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 a near-term adverse impact on Safety or Security functions.
2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions.
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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.

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.

Compensatory actions are not required because there is no adverse impact to Safety or Security functions.

IF YES, THEN proceed to Step 3.1	IF NO, THEN proceed to Step 4.0

3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☒ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may 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 Safety or Security 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.	
	N/A – There is no adverse impact to Safety or Security functions.	

IF YES, THEN proceed to Step 3.2	IF NO, THEN proceed to Step 4.0

3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of	☒ YES ☐ NO

	NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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," are addressed.
	The transmitters are located in the Protected Area. In the Turbine Building.
b.	The 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 CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 5. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
	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.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
	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 D.1.19.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 17. Baseline security criteria remain in place and effective. 18. No new pathways or vulnerabilities have been created.

	19. No change to CDA would now make it Direct. 20. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
	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 CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
	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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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)

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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0		
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 Step 1.1	IF NO, THEN proceed to Step 2.0	
1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Step 1.2	IF NO, THEN proceed to Step 3.0	

1.2	Figure 2, Box 4.2 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 Step 1.3	IF NO, THEN proceed to Step 3.0

1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0

1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0

1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0

1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO

d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 21. Baseline security criteria remain in place and effective. 22. No new pathways or vulnerabilities have been created. 23. No change to CDA would now make it Direct. 24. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.

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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☒ NO
Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.		
IF YES, THEN proceed to Step 2.1	IF NO, THEN proceed to Step 3.0	

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☐ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 a near-term adverse impact on Safety or Security functions.
2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions.
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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.

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 Step 3.1	IF NO, THEN proceed to Step 4.0	
3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☒ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may be based on existing analyses.:	
	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 Safety or Security 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.	
	N/A – There is no adverse impact to Safety or Security functions.	
IF YES, THEN proceed to Step 3.2	IF NO, THEN proceed to Step 4.0	
3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.	☒ YES ☐ NO
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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,” are addressed.	
	The recorder is located in a Vital Area, the main control room, and is monitored 24/7 by licensed Reactor	

	Operators.
b.	The 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 CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 6. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
	No interconnected assets exist.
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
	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 CDA are evaluated and documented before implementation to ensure the following: 21. Baseline security criteria remain in place and effective. 22. No new pathways or vulnerabilities have been created. 23. No change to CDA would now make it Direct. 24. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
	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 CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
	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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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)

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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0		
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 Step 1.1	IF NO, THEN proceed to Step 2.0	
1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Step 1.2	IF NO, THEN proceed to Step 3.0	
1.2	Figure 2, Box 4.2 Are one or more of the alternate means administrative, non-digital, or	☐ YES ☐ NO

	if digital is it adequately independent? Document basis for YES or NO answer:	
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 Step 1.3	IF NO, THEN proceed to Step 3.0	
1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0	
1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0	
1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0	
1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.	

e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 25. Baseline security criteria remain in place and effective. 26. No new pathways or vulnerabilities have been created. 27. No change to CDA would now make it Direct. 28. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.

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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☒ YES ☐ NO

Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.

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 Step 2.1	IF NO, THEN proceed to Step 3.0

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☒ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 a near-term adverse impact on Safety or Security functions.
2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions.
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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.

IF YES, THEN proceed to Step 3.1		IF NO, THEN proceed to Step 4.0
3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☐ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.	
IF YES, THEN proceed to Step 3.2		IF NO, THEN proceed to Step 4.0
3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.	☒ YES ☐ NO
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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," are addressed.	
	Physical isolation is established by the location of the indirect CDA inside the PA.	
b.	The 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 CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 7. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
	The CDAs are protected within Defensive Level 3 in accordance with Section 4.3 of the Cyber Security Plan (CSP).
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
	The use of portable media is controlled in accordance with NEI 08-09 D.1.19 as addressed by station procedure 0PGP03-ZS-0017 ‘Control of Portable Media for Cyber Security’.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 25. Baseline security criteria remain in place and effective. 26. No new pathways or vulnerabilities have been created. 27. No change to CDA would now make it Direct. 28. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
	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 CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
	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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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)

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 (EP) Consequence Assessment: (Steps 1.0 to 1.6)

Consequence Assessment (Reference Section 3 and Appendix A, Figure 1 – "Consequence Assessment")		
1.0	Figure 1, Box 3.0 Does CDA perform ONLY an 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, important-to-safety, or security functions. For safety, important-to-safety, or security functions proceed to Step 3.0		
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 Step 1.1	IF NO, THEN proceed to Step 2.0	
1.1	Figure 2, Box 4.0 Are alternate means available for performing the intended EP function, including offsite communications? (as specified by Section 4)? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Step 1.2	IF NO, THEN proceed to Step 3.0	

1.2	Figure 2, Box 4.2 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 Step 1.3	IF NO, THEN proceed to Step 3.0

1.3	Figure 2, Box 4.1 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 Step 1.4	IF NO, THEN remediate or go to Step 3.0

1.4	Figure 2, Box 4.3 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 Step 1.5	IF NO, THEN remediate or go to Step 3.0

1.5	Figure 2, Box 4.4 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 Step 1.6	IF NO, THEN remediate or go to Step 3.0

1.6	Figure 1, Box 5 Are baseline cyber security protection criteria d, e, f, and g in place? (as described in Section 5)? Ensure each of the following baseline criteria are met.	☐ YES ☐ NO

d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
e.	Document how changes to the CDA are evaluated and documented before implementation to ensure the following: 29. Baseline security criteria remain in place and effective. 30. No new pathways or vulnerabilities have been created. 31. No change to CDA would now make it Direct. 32. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
f.	Document how the CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.

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 Step 3.0

Balance of Plant (BOP) CDA Consequence Assessment: (Steps 2.0 to 2.1)

2.0	Figure 1, Box 3.1 Is the CDA a BOP CDA as described in Section 3.2? Document the CDA's function and the basis for YES or NO answer.	☐ YES ☒ NO
Note: BOP CDAs include only those CDAs where added to program to meet FERC Order 706-B. Refer to section 3.2 of NEI 13-10 for criteria.		
IF YES, THEN proceed to Step 2.1	IF NO, THEN proceed to Step 3.0	

2.1	Figure 1, Box 5.1 Can a compromise of the CDA cause a reactor SCRAM/Trip?	☐ YES ☐ NO
If YES	IF YES, Implement these additional controls (when 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" Proceed to Step 3.2	
If NO	Proceed to Step 3.2	

Indirect CDA Consequence Assessment: (Steps 3.0 to 3.2)

3.0	Figure 1, Box 3.2 Is the CDA an indirect CDA as described in Section 3.3? 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 a near-term adverse impact on Safety or Security functions.
2. Are not indicators/annunciators solely relied-on for making Safety or Security decisions.
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. Provide analysis including the following to show the compromise can be detected and mitigated prior to adverse.

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 Step 3.1	IF NO, THEN proceed to Step 4.0	
3.1	Figure 1, Box 3.2 Adverse Impact Mitigated – Has the licensee determined, documented, and implemented the following:	☒ YES ☐ NO
a.	Determine and document the 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 Safety and Security functions. The time period required may be based on existing analyses.:	
	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 Safety or Security 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 b and c above) for indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step a.
	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 Step 3.2	IF NO, THEN proceed to Step 4.0

3.2	Figure 1, Box 5 Are the baseline Cyber Security protections described in Section 5 of NEI 13-10 in place for the CDA? Ensure each of the following baseline criteria are met.	☒ YES ☐ NO
a.	Document that the CDA, as identified using the analysis set forth in Section 3.1 or 3.2 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," are addressed.	
	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 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 CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device. In order to properly fulfill their SSEP function, some indirect CDAs are excluded from the requirement to be air-gapped or isolated by a deterministic isolation device. These CDAs include: 8. Communication systems such as a PBX, Radio systems, or other devices whose SSEP function requires external communication. These communication systems and networks must not provide an attack pathway to isolated devices, systems, or networks. 2. Log aggregation and event correlation servers which reside outside the deterministic isolation	

	device or which reside on the corporate business networks to fulfill the site wide aggregation, monitoring, and alerting functions.
	See the response for Question 1.5. b.
d.	Document how portable media and mobile devices are controlled according to NEI 08-09 D.1.19 in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.
	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 CDA are evaluated and documented before implementation to ensure the following: 29. Baseline security criteria remain in place and effective. 30. No new pathways or vulnerabilities have been created. 31. No change to CDA would now make it Direct. 32. Threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.
	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 CDA, or the interconnected equipment that would be affected by the compromise of the non-Direct 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 how ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.
	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. Cyber Security is included in Nuclear Quality Assurance Audits of the Physical Security Program. RERP (EP) is audited by Nuclear Quality Assurance.
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 baseline Cyber Security protection criteria described in Section 5 OR proceed to step 4.0
4.0	This is a Direct CDA. 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 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

Table A.1

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.
D1.21	Third Party Products and Controls (D1.21)				X	These CDAs by definition do not support installation of third-party software; therefore this control is not applicable.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
D3.21	Fail in Known (Safe) State (D3.21)			X		The engineering process ensures and documents that components fail in a state that is bounded with the design basis of the plant.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.
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.

Control Number	Control	Common	Apply to CDA	Alternate	Not Applicable	Basis
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.

[BLANK PAGE]

Class A.2 through B.3 Class Descriptions

Table A.2

Class A.2 CDAs	Class A.3 CDAs	Class B.1 CDAs	Class B.2 CDAs	Class B.3 CDAs
Software Attributes	**Software Attributes**	**Software Attributes**	**Software Attributes**	**Software Attributes**
• Program code (instruction-level code) is factory installed by manufacturer and cannot be altered nor can any code be injected (e.g. no buffer or heap overflow)	• Program code (instruction-level code) is factory installed by manufacturer and cannot be altered nor can any code be injected (e.g. no buffer or heap overflow)	• Program code (instruction-level code) is factory installed by manufacturer and cannot be altered nor can any code be injected (e.g. no buffer or heap overflow)	• Program code (instruction-level code) is factory installed by manufacturer and cannot be altered nor can any code be injected (e.g. no buffer or heap overflow)	• Program code (instruction-level code) is factory installed by manufacturer, but it may be possible to replace this program code by doing a firmware update in the field. • If the CDA supports a USB port ('master' or 'slave') it is factory-programmed to support a specific subset of bulk-data/file-exchange methods (e.g., save or reload CDA configuration settings or load new firmware). The CDA does not support interoperation with any other form of USB object classes or devices or allow automatic/manual installation of third-party drivers for such object classes or devices.
HMI: • Only operational parameters (no configuration settings) can be changed using the local, integral HMI • No configuration changes can be made via the integral HMI • The HMI has no access enforcement mechanisms	HMI: • Operational parameters can be changed using the local, integral HMI • Configuration settings can be changed using the local, integral HMI • The HMI has at least one form of software access enforcement	HMI (If CDA has HMI): • Operational parameters can be changed using the local, integral HMI • Configuration settings can be changed using the local, integral HMI • The HMI has at least one form of software access enforcement	HMI (If CDA has HMI): • Operational parameters can be changed using the local, integral HMI • Configuration settings can be changed using the local, integral HMI • The HMI has at least one form of software access enforcement	HMI (If CDA has HMI): • Operational parameters can be changed using the local, integral HMI • Configuration settings can be changed using the local, integral HMI • The HMI has at least one form of software access enforcement

	mechanism • Does not support multi-users and individual authentication for those users	mechanism • Does not support multi-users and individual authentication for those users	mechanism • Does not support multi-users and individual authentication for those users	mechanism • Does not support multi-users and individual authentication for those users
• Configuration setting changes can only be made using a maintenance tool and only by taking the CDA out of service	• Configuration setting changes can also be made using a maintenance tool and only by taking the CDA out of service	• Configuration setting changes can also be made using a maintenance tool and only by taking the CDA out of service	• Configuration changes can also be made using a maintenance tool and only by taking the CDA out of service.	• Configuration changes can also be made using a maintenance tool and only by taking the CDA out of service. • Configuration changes may also be made locally via a console port and/or USB thumb drive/memory card as well as remotely via the asynchronous serial communication channel, but only by taking the CDA out of service
• Does not contain an externally accessible file system	• Does not contain an externally accessible file system	• Does not contain an externally accessible file system	• Does not contain an externally accessible file system	• Does not contain an externally accessible file system but may support bulk data extraction and configuration loading/saving via the USB/memory card interfaces.
• Firmware updates not supported/not possible by the hardware design	• Firmware updates not supported and not possible by the hardware design	• Firmware updates not supported and not possible by the hardware design	• Firmware updates not supported and not possible by the hardware design	• CDA supports firmware update/replacement with removal of the CDA from the service and use of special tools and software
• Contain vendor software that performs/supports a pre-defined set of features and functions and supports no ability to add or remove software	• Only contains vendor's software that performs/supports a pre-defined set of features and functions and supports no ability to add or remove software	• Only contains vendor's software that performs/supports a pre-defined set of features and functions and supports no ability to add or remove software	• Only contains vendor's software that performs/supports a pre-defined set of features and functions and supports no ability to add or remove software.	• Only contains vendor's software that performs/supports a pre-defined set of features and functions and supports no ability to add or remove software
Communication: • Contains no communication software functionality	Communication: • Contains no communication software functionality	Communication: • The CDA uses an industrial protocol using poll-response based message exchanges over	Communication: • The CDA uses an industrial protocol using poll-response based message exchanges over	Communication: • The CDA uses an industrial protocol using poll-response based message exchanges over

		an asynchronous serial communications channel. Communication functionality of the CDA are limited to information or data extraction and do not support the capability for control execution, manipulation of CDA I/O or sending parameters or data to the CDA. • Communication functions do not allow for modification of the configuration of the CDA or for making program changes to the CDA.	an asynchronous serial communications channel. Communication functionality of the CDA can be adjusted and altered by the user and may include reading and writing data from and to the CDA to fetch values, change/set parameters, execution of pre-configured control functions and manipulation of CDA process control outputs. • Communication functions do not allow for modification of the configuration of the CDA or for making program changes to the CDA.	an asynchronous serial communications channels. Communication functionality of the CDA can be adjusted and altered by the user and may include reading and writing data from and to the CDA to fetch values, change/set parameters, execution of pre-configured control functions and manipulation of CDA process control outputs. • The functionality and configuration of the CDA can also be altered via these communication links using software tools (possibly vendor-proprietary) specifically designed for that purpose. • The asynchronous communications capability does not support modification of code, instructions, or code injection to the CDA.
• CDA does not perform audit/event logging of user activities or communication activities or local runtime events.	• CDA does not perform audit/event logging of user activities or communication activities or local runtime events.	• CDA does not perform audit/event logging of user activities or communication activities or local runtime events.	• CDA does not perform audit/event logging of user activities or communication activities or local runtime events.	• CDA does not perform audit/event logging of user activities or communication activities or local runtime events.
• The CDA does not suppler a local console port or command line interpreter functionality	• The CDA does not suppler a local console port or command line interpreter functionality	• The CDA does not suppler a local console port or command line interpreter functionality	• The CDA does not suppler a local console port or command line interpreter functionality	• The CDA has a local, special-purpose communications interface (a.k.a. a console port), typically a low-speed, asynchronous, EIA-232 compatible, that is used to enable user interaction with a

				device's integral command-line interpreter (e.g., a "shell" or "command prompt") via an ASCII 'dumb terminal' or a computer/program emulating a dumb terminal
Hardware Attributes	**Hardware Attributes**	**Hardware Attributes**	**Hardware Attributes**	**Hardware Attributes**
• Contain PROM, RAM, EEPROM, and possibly integrated components (e.g., FPGA) that include factory-configurable functionality and factory-configurable firmware	• Contain PROM, RAM, EEPROM, and possibly integrated components (e.g., FPGA) that include factory-configurable functionality and factory-configurable firmware.	• PROM, RAM, EEPROM and possibly integrated components (e.g., FPGA) that include factory-configurable functionality and factory-configurable firmware.	• PROM, RAM, EEPROM and possibly integrated components (e.g., FPGA) that include factory-configurable functionality and factory-configurable firmware.	• PROM, RAM, EEPROM and possibly integrated components (e.g., FPGA) that include factory-configurable functionality and factory-configurable firmware.
• May contain bulk storage for data accumulation purposes but provides no external access to that bulk storage	• May contain bulk storage for data accumulation purposes but provides no external access to that bulk storage	• May contain bulk storage for data accumulation purposes but provides no external access to that bulk storage	• May contain bulk storage for data accumulation purposes but provides no external access to that bulk storage	• May contain bulk storage for data accumulation purposes and for configuration setting storage and • May support external access to that bulk storage.
HMI: • Has a minimal-functionality, • Local access only	HMI: • Has a minimal-functionality, • Local access only • May employ a physical access protection mechanism such as a key or fob	HMI: • Has a minimal-functionality, • Local access only • May employ a physical access protection mechanism such as a key or a fob	HMI: • Has a minimal-functionality, • Local access only • May employ a physical access protection mechanism such as a key or fob	HMI: • Has a minimal-functionality, • Local access only • May employ a physical access protection mechanism such as a key or fob
• Contains no communication hardware other than a configuration and maintenance port	• Contains no communications hardware other than a configuration and maintenance port	• Supports only asynchronous, low-speed, serial communications capability using either an RS-232, RS-422 or RS-485 hardware interface (regardless of any subsequent media conversion, e.g. to fiber	• Supports only asynchronous, low-speed, serial communications capability using either an RS-232, RS-422 or RS-485 hardware interface (regardless of any subsequent media conversion, e.g. to fiber	• Supports only asynchronous or synchronous, low-speed, serial communications capability using either an RS-232, RS-422, or RS-485 or vendor-proprietary hardware interface (e.g. Modbus+™ or Profibus™)

		optic cable)	optic cable).	regardless of any subsequent media conversion (such as to fiber optic cable).
• Contains a maintenance and configuration port but no other peripherals, interfaces, or ports	• Contains a maintenance and configuration port but no other peripherals, interfaces, or ports	• Contains a maintenance and configuration port as well as one or more asynchronous communication ports but no other peripherals, interfaces or ports	• Contains a maintenance and configuration port as well as one or more asynchronous communication ports but no other peripherals, interfaces or ports.	• Contains a console port and one or more non-Ethernet serial communication ports (synchronous or asynchronous) • May support a restricted functionality USB port and/or memory card slot for bulk data retrieval and configuration exporting and restoration but no other peripherals, interfaces or ports
Note: If the CDA contains peripherals, interfaces, or ports beyond those allowed by the class criteria, the CDAs can meet this criteria by physically disabling the peripheral, interfaces or ports in a manner that prevents restoration, reactivation or bypass.	Note: If the CDA contains peripherals, interfaces, or ports beyond those allowed by the class criteria, the CDAs can meet this criteria by physically disabling the peripheral, interfaces or ports in a manner that prevents restoration, reactivation or bypass.	Note: If the CDA contains peripherals, interfaces, or ports beyond those allowed by the class criteria, the CDAs can meet this criteria by physically disabling the peripheral, interfaces or ports in a manner that prevents restoration, reactivation or bypass.	Note: If the CDA contains peripherals, interfaces, or ports beyond those allowed by the class criteria, the CDAs can meet this criteria by physically disabling the peripheral, interfaces or ports in a manner that prevents restoration, reactivation or bypass.	Note: If the CDA contains peripherals, interfaces, or ports beyond those allowed by the class criteria, the CDAs can meet this criteria by physically disabling the peripheral, interfaces or ports in a manner that prevents restoration, reactivation or bypass.
• May support an interface to external devices/systems implemented using analog, contact, pulse process control I/O signals	• May support an interface to external devices/systems implemented using analog, contact, pulse process control I/O signals	• May support an interface to external devices/systems implemented using analog, contact, pulse process control I/O signals	• May support an interface to external devices/systems implemented using analog, contact, pulse process control I/O signals	• May support an interface to external devices/systems implemented using basic analog, contact, pulse process control I/O signals
Location	**Location**	**Location**	**Location**	**Location**
• Protected Area (PA) or Vital Area (VA)	• Protected Area (PA) or Vital Area (VA)	• Protected Area (PA) or Vital Area (VA)	• Protected Area (PA) or Vital Area (VA)	• Protected Area (PA) or Vital Area (VA)
Information Classification:	**Information Classification**	**Information Classification**	**Information Classification**	**Information Classification**
• CDA contains plant process data not classified as security-related (SRI) or Safeguards Information (SGI)	• CDA contains plant process data not classified as security-related (SRI) or Safeguards Information (SGI)	• CDA contains plant process data not classified as security-related (SRI) or Safeguards Information (SGI)	• CDA contains plant process data not classified as security-related (SRI) or Safeguards Information (SGI)	• CDA contains plant process data not classified as security-related (SRI) or Safeguards Information (SGI)

Plant Design / Maintenance	Plant Design / Maintenance	Plant Design / Maintenance	Plant Design / Maintenance	Plant Design / Maintenance
• Removal from service can only be done locally at the CDA	• Removal from service can only be done locally at the CDA	• Removal from service can only be done locally at the CDA	• Removal from service can only be done locally at the CDA	• Removal from service can only be done locally at the CDA

Examples of Class A.2 CDAs:

Micon model# AI-518
Universal PID Controller

HANYOUNG model# BK-6
Digital Temperature Indicator

Examples of Class A.3 CDAs:

CubicleBus model# 3WL11
low-voltage bus air breaker

TORAY UVT-300 Automatic
Water Chemical Analyzer

Examples of Class B.1 CDAs:

SEL Model# 2414 Transformer Monitor
with DNP3.0

VAMP 245 Feeder and Motor Protective Relay
with DNP3.0

Examples of Class B.2 CDAs:

Omron Model# GCF-612 PLC
with DNP 3.0 protocol

KH300AG-Kehao-Universal Colored Recorder
with Modbus RTU

KOYO ‘Click’ PLC Family
with Ethernet and RS485 Modbus RT

Examples of Class B.3 CDAs:

SEL Model 351S Multi-Function Relay
with Serial DNP 3.0 Communications

Modicon Quantum PLC
with Modbus-plus (MB+) Communications

BOSH LTC0385 Series DinionXF
Security Camera

Class A.2 through B.3 Cyber Security Control Assessment

Table A.3

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 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.	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.	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.	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.	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	In the case of CS/CDAs that do not support multiple user accounts or multi-level access based on separate passwords or that only utilize a single, universal password for all user access, this security control would not be applicable.		X	X		Although a Class A.3 CDA does not have individual user accounts, its integral HMI provides access to both operational and configuration settings and modifications could adversely impact its safety, security, or emergency preparedness functions. Thus the attack vector associated with this control exists and the control must be addressed. Therefore, by using the method provided in Section 3.1.6 of the CSP, this security control is addressed by the following alternative means by implementing, verifying, validating, and documenting the following: • The access enforcement mechanisms implemented to meet D1.3 are managed so that only authorized individuals have access to the CDA's HMI. • The procedures for granting, revoking, and revising the access enforcement mechanism (e.g., changing the password, the key combination) are documented and managed and include		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
											ensuring that personnel who are still authorized are made aware of the changes and that personnel whose access is revoked or no longer require access licensees promptly recover any physical mechanism used for access (e.g., a fob, or key).																
D1.3	Access Enforcement (D1.3)		X	X		Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions or systems or equipment that perform those functions. Therefore the attack vector associated with this control exists and the control must be addressed. Although the A.2 CDAs lack the capability to implement this control, using the method provided in Section 3.1.6 of the licensees' cyber security plans, this security control is addressed by implementing the following to provide equal protections as this security control: If the CDA is not located in VA: • The CDA is in a locked, alarmed cabinet or line-supervised and tampered cabinet and • The alarm is monitored so that all alarms are immediately assessed to determine whether the access to the cabinet is authorized and this assessment process is documented in a plant procedure and • The access to the cabinet is controlled so that only authorized individuals are permitted access to the cabinet and • Documented procedures are		X	X		A primary attack vector associated with A.3 CDAs is unauthorized access of operational parameters or configuration via the HMI. Additionally, the CDA does not have the following abilities that can be used to address this security: • Assign user rights and privileges on the CDA consistent with the user authorizations • Define and documents privileged functions and security-relevant information for the CDAs. • Authorize personnel access to privileged functions and security-relevant information consistent with established policies and procedures. • Restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to authorized personnel (e.g., security administrators). • Define and documents privileged functions for CDAs. • Require dual		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						used when authorizing individuals' access to the cabinet as well as when issuing those personnel a key to the cabinet. For Class A.2 devices in a Vital Area, the licensees can address the required security controls that address unauthorized manipulation of operating parameters via the HMI by implementing the measures described above, or by verifying and documenting that the Licensee has established, implemented, and maintains a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas during non-emergency conditions. The list must include only those individuals who have a continued need for access to those specific vital areas in order to perform their duties and responsibilities. The list must be approved by a cognizant licensee manager or supervisor who is responsible for directing the work activities of the individual who is granted unescorted access to each vital area, and updated and re-approved no less frequently than every 31 days.					authorization for critical privileged functions and to create any privileged access for users. As a result, this security control is address by using its self-protection mechanism (e.g., password, key) to restrict HMI user access; however they do not have the ability to log attempts to bypass those mechanisms. Additionally, using the method provided in Section 3.1.6 of the CSP, this security control is addressed by implementing the measures described in control D1.2 and D1.5. Alternate method: The CDA does not support individual user identifiers, but does support authenticators which are able to be implemented to authenticate users prior to access to the device. Implementation of Authentication Mechanisms provides protection for unauthorized access to devices. Alternate method: The device is located inside the protected area and is in a physically secure cabinet (for example, has locking mechanism such as key lock or tamper tape) where the locking mechanism is authorized for use through a work authorization process (for example, work order). Alternate method: The device is located in the Control Room, Central Alarm Station (CAS), or Secondary Alarm Station (SAS).															

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D1.4	Information Flow Enforcement (D1.4)				X	By definition, a Class A.2 CDA has no communication ports or interfaces (or they have been physically disabled), other than the special-purpose connection which is used exclusively for configuration of the Class A.2 CDAs. Therefore the attack vector associated with this control does not exist and the control is not required.				X	By definition, a Class A.3 CDA has no communication ports or interfaces (or they have been physically disabled), other than the special-purpose connection used for configuration of the Class A.3 CDAs and the maintenance tool is not connected to another device or network when connected to the CDA. Therefore the attack vectors associated with this security control do not exist, and this security control is not required.				X	By definition, a Class B.1 CDA is factory-programmed and/or designed to only allow CDA information extraction through the asynchronous serial communications channel using poll-response based message exchanges and does not support control execution, output manipulation or alteration of settings, code, instructions or the configuration of the CDA. Therefore the attack vectors associated with this security control does not exist, and this security control is not required.		X	X		By definition, a Class B.2 CDA is factory-programmed and/or designed to allow CDA information extraction through the asynchronous serial communications channel using poll-response based message exchanges in an industrial protocol. The CDA's asynchronous communication protocols also support pre-configured control function execution, output (analog, pulse, and/or contact) manipulations (which may include controlling plant equipment), and alteration of operational parameters but not alteration of configuration settings or the program code of the CDA. Therefore the attack vectors associated with illegal or unauthorized information flows exist, and this security control must be addressed. Since the B.2 CDAs lack the capability to implement this control, using the method provided in Section 3.1.6 of the cyber security plan, this security control is alternately addressed by 1) Inheriting the cyber security protections from the system/device to which the CDA is communicating using the industrial protocols by identifying those systems/devices as CDAs and protecting them accordingly, and 2) By implementing the control measures described in control D3.6 below.		X	X		By definition, a Class B.3 CDA is factory-programmed and/or designed to allow CDA information extraction through the asynchronous serial communications channel using poll-response based message exchanges in an industrial protocol. The CDA's asynchronous communication protocols also support pre-configured control function execution, output (analog, pulse, and/or contact) manipulations (which may include controlling plant equipment). The asynchronous serial communication capabilities include the ability to make alterations to CDA configuration settings and possibly the functional capabilities of the CDA (but not its program code). Therefore the attack vectors associated with illegal or unauthorized information flows exist, and this security control must be addressed. Since the B.3 CDAs lack the capability to implement this control, using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by 1) Inheriting the cyber security protections from the system/device to which the CDA is communicating using the industrial protocols by identifying those systems/devices as CDAs and protecting them accordingly, and 2) By implementing the control measures described in control D3.6 below.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D1.5	Separation of Functions (D1.5)		X	X		Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. Therefore the attack vector associated with this control exists and the control must be addressed. One method to address this security control is by verifying, validating, and documenting the following to ensure that no single individual has functional control over, or responsibility for, all of the factors and activity associated with operational parameter or configuration changes of the CDA: • Per licensee plant procedures, the work order for maintenance activities for the CDA is managed and authorized by an individual other than the person performing the maintenance. • Per licensee plant procedures, scheduling of maintenance work and assignment maintenance personnel for the work is performed by individuals other than the individual performing the work • Per licensee plant procedures, access to the specialized tools or keys to access cabinet is controlled by personnel other than the personnel performing the maintenance. • Ensures that those individuals are trustworthy and reliable per 10 CFR 73.56.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D1.6	Least Privilege (D1.6)			X		Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. Therefore the attack vector associated with this control exists and the control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address D1.3 and D1.5 as alternate security measures that provide equal protection as this security control.			X		Class A.3 CDAs have self-protection mechanism (e.g., password, key) to restrict HMI user access; however they do not have the ability to assign the restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The integral HMI allows manipulation of operational and configuration parameters that could lead to an adverse impact to SSEP functions. Therefore the attack vector associated with this control exists and the control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by implementing the measures described in control D1.3 and D1.5 as described above.			X		See Class A.3 Basis.			X		See Class A.3 Basis.			X		See Class A.3 Basis.
D1.7	Unsuccessful Login Attempts (D1.7)				X	Class A.2 CDAs do not support passwords therefore there is no requirement to address attack vectors associate with password guessing. Therefore, this control does not apply and is not required.		X	X		A primary attack vector associated with A.3 CDAs is unauthorized access of operational parameters or configuration via the HMI. Class A.3 CDAs have a self-protection mechanism (e.g., password, key) to restrict HMI user access; however they do not have the ability to log attempts to bypass those mechanisms. Unauthorized access to the HMI could enable alteration of configuration settings that could adversely impact SSEP functions. Therefore this control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by implementing the following measures: • Either this security control is address by using its self-protection mechanism (e.g., password, key) to restrict HMI user access and by using the security measures		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
											implemented to address the security controls D1.3 and D1.5. • Or else the licensee has verified and documented the following to address this security control: 1) The CDA is in a locked, alarmed cabinet and the alarm is monitored in real time and immediately assessed, following a documented procedure, to determine whether access to the cabinet is authorized. If the CDA is in a locked cabinet but it is not an alarmed cabinet, the licensee implements measures (e.g., security officer rounds and periodic monitoring of tamper seals) to detect unauthorized access to the CDA. 2) Access to the cabinet is controlled and managed so that only authorized individuals are permitted access to the cabinet, and documented procedures are used when authorizing individuals' access to the locked cabinet as well as when issuing those personnel a key to open the cabinet. Alternate method: The Device is located in the Control Room, Central Alarm Station (CAS), or Secondary Alarm Station (SAS). Alternate method: Tamper tape, security rounds,															

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
											operator rounds provide detection of attempts of unauthorized access.															
D1.8	System Use Notification (D1.8)	**X**		**X**		Although the Class A.2 CDA lacks the technical capability to implement the control, the attack vectors associated with this control still exist (unauthorized access), and therefore this control is applicable to the Class A.2 CDAs and will be addressed by providing an equivalent alternative countermeasure. The plant access authorization program requires that each individual granted access to the site to sign a document that describes his/her responsibilities. This is an acceptable alternative countermeasure for this device type. Alternatively, the control itself requires/allows for the use of physical notices in cases in which a CDA cannot support automated mechanisms for System Use Notifications.	**X**		**X**		See Class A.2 Basis.	**X**		**X**		See Class A.2 Basis.	**X**		**X**		See Class A.2 Basis.	**X**		**X**		See Class A.2 Basis.
D1.9	Previous Logon Notification (D1.9)			**X**		Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. Therefore the attack vector associated with this control exists and the control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address D1.3 and D1.5 as alternate security measures that provide equal protection as this security control.			**X**		Class A.3 CDAs have a self-protection mechanism (password, key, etc.) to restrict HMI user access; however they do not have the ability to log the use of those mechanisms. Unauthorized access to the HMI could enable alteration of configuration settings which could adversely impact SSEP functions. Thus the attack vector associated with this control exists and the control must be addressed. This security control is addressed by security measures implemented to address D1.7 as an alternative security control.			**X**		See Class A.3 Basis.			**X**		See Class A.3 Basis.			**X**		See Class A.3 Basis.
D1.10	Session Lock (D1.10)		**X**	**X**		Unauthorized manipulation of Class A.2 CDAs' HMI could lead to adverse impacts to SSEP functions.		**X**	**X**		See Class A.2 Basis Alternate method: • Logically lock the device		**X**	**X**		See Class A.3 Basis.		**X**	**X**		See Class A.3 Basis.		**X**	**X**		See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						Therefore the attack vector associated with this control exists and the control must be addressed. Since the A.2 CDAs lack the capability to implement this control, using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed (1) by the security measures implemented to address D1.3 and D1.5 and (2) by verifying, validating, and documenting that licensees have plant procedures that require authorized personnel to physically remain in continual attendance at the CDA/cabinet as long as the cabinet containing the CDA remains open and unlocked; or by doing the following: • Physically restrict access to the CDA, • Monitor and record physical access to the CDA to timely detect and respond to intrusions, • Use auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals)to detect unauthorized access and modifications to the CDAs, • Ensure that individuals who have access to the CDA are qualified, and • Ensure that those individuals are trustworthy and reliable per 10 CFR 73.56 Alternate method: The device is located in the					upon leaving the device. • Ensure that individuals who have access to the CDA are qualified, and • Ensure that those individuals are trustworthy and reliable per 10 CFR 73.56. Alternate method: The device is located in the Control Room, Central Alarm Station (CAS), or Secondary Alarm Station (SAS).															

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						Control Room, Central Alarm Station (CAS), or Secondary Alarm Station (SAS).																				
D1.11	Supervision and Review – Access Control (D1.11)			X		Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. Therefore the attack vector associated with this control exists and the control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address D1.3 and D1.5 as alternate security measures that provide equal protection as this security control.			X		Class A.3 CDAs have a self-protection mechanism (password, key, etc.) to restrict HMI user access; however they do not have the ability to log the use of those mechanisms. Unauthorized access to the HMI could enable alteration of configuration settings which could adversely impact SSEP functions. Thus the attack vector associated with this control exists and the control must be addressed. By using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by verifying and documenting the review of the measures implemented to address D1.3 and by addressing any identified abnormalities based on licensee's procedures for detecting and responding to potential security concerns.			X		See Class A.3 Basis.			X		See Class A.3 Basis.			X		See Class A.3 Basis.
D1.12	Permitted Actions Without Identification and Authentication (D1.12)				X	Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. However, access to the CDA is controlled and managed by security measures implemented to address D1.3 and D1.5, and therefore, no one can access the integral HMI unless the user is authorized and provided means to access the locked and alarmed cabinet of the A.2 CDAs as described in D1.3 and D1.5. Therefore the attack vector associated with this control does not exist and this control is not applicable.				X	Class A.3 CDAs have integral self-protection mechanisms (password, key) to control access to their HMIs and thus do not permit use of the integral HMIs without authentication. Thus this security control is not applicable.				X	See Class A.3 Basis.		X		X	Class B.2 CDAs, if they have an integral, local HMI, also have integral self-protection mechanisms (e.g., password, key) to control access to their HMIs and thus do not permit use of the integral HMIs without authentication. Thus this security control is not applicable. Note: If B.2 CDAs allow personnel to perform certain actions during an emergency condition, this security control applies. This security control is address by identifying and documenting plant procedures that accomplish the following: • Specify plant personnel actions that the personnel can		X		X	See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
																					perform on CDAs during normal and emergency conditions without identification or authentication. • Specify actions that plant personnel can perform without identification and authentication.					
D1.13	Automated Marking (D1.13)				**X**	A Class A.2 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.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.
D1.14	Automated Labeling (D1.14)				**X**	A Class A.2 CDA by definition has no peripherals or interfaces and thus no capability to generate computer-readable output. Plus, a Class A.2 CDA does not contain any SGI or SRI information. Thus, the attack vector addressed by this control does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.
D1.15	Network Access Control (D1.15)				**X**	By definition, a Class A.2 CDA has no communication ports or interfaces (or they have been physically disabled) and thus it is incapable of network connectivity and communication with other systems and devices and thus the associated attack vector does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.			**X**		By definition, a Class B.2 CDA has only serial, asynchronous communication ports or interfaces as well as a special-purpose connection used for the configuration of the Class B.2 CDAs. The serial port provides read/write access to CDA data plus control over outputs and pre-defined CDA functions but cannot be used to alter the CDA's functionality, configuration settings, or program code. Therefore, the attack vectors associated with illegal or unauthorized network access (serial communication) exist. Since the B.2 CDAs lack the capability to implement this control, using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address			**X**		By definition, a Class B.3 CDA has only serial, asynchronous communication ports or interfaces as well as a special-purpose connection used for the configuration of the Class B.3 CDAs. The serial port 1) provides read-only access to CDA data, 2) can send commands to the CDAs to control the CDA's outputs and/or pre-defined CDA functions, and 3) can be used to alter the CDA's functionality by modification of its configuration settings (but not its program code). Therefore, the attack vectors associated with illegal or unauthorized network access (serial communication) exist. Since the B.3 CDAs lack the capability to implement this control, using the method provided in Section 3.1.6 of the cyber security plan, this security control

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
																					D1.4 above.					is addressed by the security measures implemented to address D1.4 above.
D1.16	"Open/Insecure" Protocol Restrictions (D1.16)				X	By definition, a Class A.2, CDA has no communication ports or interfaces (or they have been physically disabled) other than the special-purpose connection used for configuration of the Class A.2 CDAs. Thus the attack vector associated with this control does not exist and the control is not required.				X	By definition, a Class A.3 CDA has no communication ports or interfaces (or they have been physically disabled) and thus is incapable of supporting insecure/open protocols, network connectivity, and communication with other systems and devices (with the exception being any maintenance tool used for configuration of the Class A.3 CDA) and thus the associated attack vector does not exist and the control is not required.				X	By definition, a Class B.1 CDA has no interfaces, peripherals or ports (or they have been physically disabled) other than the special purpose connection used only for configuration purposes and serial ports for asynchronous communication using industrial protocols that do not contain user authentication information or credentials. Thus the attack vector associated with this control does not exist and the control is not required.				X	By definition, a Class B.2 CDA has no interfaces, peripherals, or ports (or they have been physically disabled) other than the special purpose connection used only for configuration purposes and serial, asynchronous communication ports that allow communication using industrial protocols that is open and do not contain user authentication information or credentials. However, the system/device to which a CDA is communicating is protected at the level of the CDA and the communication wiring between the CDA and the system/device are physically protected as described in the D3.6 security control. Thus the attack vector associated with this control does not exist and the control is not required.				X	See Class B.2 Basis.
D1.17	Wireless Access Restrictions (D1.17)				X	By definition, a Class A.2 CDA has no wireless communication functionality/capability (nor do any maintenance tool used for making configuration changes) and thus the attack vector addressed by this control does not exist and the portion of the control associated with the Class A.2 CDAs' functionality is not required. NOTE: This control also includes a requirement for periodic scans to detect unauthorized wireless connectivity to plant LANs containing CDAs. That requirement is separate from the elements of the control that pertain to the individual CDAs themselves (see above) and monthly scans will be made for unauthorized wireless				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						devices per plant procedure.																				
D1.18	Insecure and Rogue Connections (D1.18)				X	A Class A.2 CDA by definition has no communication functionality/capability (except for the maintenance tool interface, which can only be accessed by taking the CDA out of service), no peripherals, no interfaces (except for the local/integral limited-functionality HMI), and no wireless communications connectivity/functionality and thus the attack vector addressed by this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	The licensees verified and documented that B.1 CDA has one or more serial asynchronous communication ports that allow communication using an industrial, poll-response protocol with pre-defined functionality. If the CDA supports multiple serial ports then any such ports not being used must be physically disabled. The CDA has no other peripherals, interfaces or ports (or they have been physically disabled.) Thus the attack vector associated with this control does not exist and the control is not required.		X		X	B.2 CDAs has one serial asynchronous communication port that allows communication using an industrial, poll-response protocol with pre-defined functionality. The licensee verified and documented that the system/device to which CDA is communicating is protected as a CDA and the communication wiring between the CDA and the system/device are physically protected as described in D3.6 security control. Thus the attack vector associated with this control does not exist and the control is not required. However, if the B.2 CDA has more than one serial asynchronous communication ports that allow communication using an industrial, poll-response protocol with pre-defined functionality, the attack vectors associated with this security control exist. This security control is addressed by licensees verifying and documenting that (1) the communication wiring between the CDA and the system/device are physically protected as described in the D3.6 security control and (2) ports not being used are physically disabled and periodically verified that these ports remained physically disabled. The periodicity is in accordance with the licensees' cyber security plans.		X		X	See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D1.19	Access Control for Portable and Mobile Devices (D1.19)	X	X			The configuration of the Class A.2 CDA can be altered via a maintenance tool. Such modifications, made maliciously or accidentally, could change the A.2 CDAs' functions and could cause adverse impacts to the CDAs' SSEP functions. The maintenance tool provides an attack vector and thus this security control needs to be addressed. The security control is addressed by the following: • Establishing and documenting the usage restrictions and implementation guidance for controlled portable and mobile devices • Authorizing, monitoring, and controlling device (e.g., maintenance tool) access to CDAs • Enforcing and documenting that maintenance tool security and integrity are maintained at a level consistent with the B.1 CDA that the maintenance tool supports • Enforcing and documenting that the maintenance tool is only used in one security level and is not moved between security levels	X	X			See Class A.2 Basis.	X	X			See Class A.2 Basis.	X	X			See Class A.2 Basis.	X	X			See Class A.2 Basis.
D1.20	Proprietary Protocol Visibility (D1.20)				X	By definition, a Class A.2 CDA has no communication ports or interfaces (or they have been physically disabled) and thus is incapable of supporting insecure/open protocols, network connectivity, and communication with other systems and devices (with the exception being any maintenance tool used for configuration of the Class A.2 CDA) and thus the associated attack vector does not exist and the				X	See Class A.2 Basis.				X	By definition, a Class B.1 CDA has no network connectivity, ports or interfaces (or they have been physically disabled) other than one or more asynchronous serial connections configured for well-known industrial protocols. The B.1 CDA does not use any proprietary protocols that would prevent the licensee from detecting unauthorized or malicious activity Therefore the attack vector associated with this control does				X	See Class B.1 Basis.				X	See Class B.1 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						control is not required.										not exist and the control is not required										
D1.21	Third Party Products and Controls (D1.21)				**X**	The intent of this control is to ensure the inability to: (1) install third-party system-/network-level protection due to a vendor or licensing conflict, or (2) install third party system-/network-level protection due to a potential loss of service support from a vendor, does not cause the security posture of the CDA to be less than is needed to meet the performance requirements of the rule or to support he licensee's overall CSP defensive model. These CDAs by definition do not support installation of third-party software; therefore this control is not applicable.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.
D1.22	Use of External Systems (D1.22)				**X**	By definition, a Class A.2 CDA has no communication ports or interfaces (or they have been physically disabled) other than the special-purpose connection used for configuration of the Class A.2 CDAs. Therefore the attack vector associated with this control does not exist and the control is not required.				**X**	As described in the justifications for security control D.1.18, the licensee verified and documented that a Class A.3 CDA has no communication ports or interfaces (or they have been physically disabled) other than the special-purpose connection used for configuration of the Class A.3 CDAs. Additionally when maintenance tools are used with the CDA they are not connected to a network or other devices at the same time. Therefore, the attack vector associated with this control does not exist and the control is not required.				**X**	As described in the justifications for security control D1.18, the licensee verified and documented that a Class B.1 CDA has only serial, asynchronous communication ports and no other peripherals or interfaces (or they have been physically disabled), as well as a special-purpose connection used for configuration of the Class B.1 CDAs. The serial ports are configured to use an industrial protocol with pre-defined message types and commands. Additionally when maintenance tools are used with the CDA, they are not connected to a network or other devices at the same time and the licensee has verified that any system communicating with the CDA has been protected at the same level as the CDA. Therefore, the attack vector associated with this control does not exist and the control is				**X**	See Class B.1 Basis.				**X**	See Class B.1 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
																not required.										
D1.23	Public Access Access Protections (D1.23)				**X**	A Class A.2 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.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.
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.	**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.	**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.	**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.	**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**	**X**		Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. Therefore the attack vector associated with this control exists and the control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by documenting the following as the auditable events for Class A.2 CDAs: 1. Unexpected failures of the CDA; 2. Unexplained behavior of the CDA; 3. Configuration of CDA changes; and, 4. Unauthorized access is detected. These elements are to be included within the audits described in D2.6.		**X**	**X**		See Class A.2 Basis.		**X**	**X**		See Class A.2 Basis.		**X**	**X**		See Class A.2 Basis.		**X**	**X**		See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D2.3	Content of Audit Records (D2.3)		X	X		Class A.2. CDAs do not have the ability to log and record user activities, therefore, by using the method describe in Section 3.1.6 of the cyber security plant, this control is addressed by security measures that are implemented by the following: • Documenting the D1.2 security activities; • Reviewing information collected under the licensee's current maintenance, testing, calibration, and identifying the information that will be used to support the detection of the unauthorized access to the CDA and to perform security incident analysis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.
D2.4	Audit Storage Capacity (D2.4)				X	A Class A.2 CDA is incapable of logging/recording user activities performed through its integral HMI. The audit information associated with the user activities performed via the CDA's HMI are manual collected and therefore, the attack vectors associated with this security do not exist. Thus this security control is not applicable.				X	See Class A.2 Basis.				X	See Class A.2 Basis.			X		See Class A.2 Basis. Additionally, a Class B.2 CDA is incapable of logging/recording communications (commands) from the system/device to which the CDA is communicating. However, the system/device to which the CDA is communicating maintains logging information in order to address this security control. Thus by using the method provided in Section 3.1.6 of the CSP, this security control is addressed by verifying that the system/device to which the CDA is communicating logs applicable communications to the CDA and inheriting it.			X		See Class B.2 Basis.
D2.5	Response to Audit Processing Failures (D2.5)				X	A Class A.2 CDA has a local integral HMI as its only user interface and incapable of logging/recording user activities performed through that HMI. The audit information associated with the user activities of Class A.2 CDAs are manual collected and therefore, the attack vectors associated with this security do not exist. Thus this security control is				X	See Class A.2 Basis.				X	See Class A.2 Basis.			X		A Class B.2 CDA may have a local integral HMI as its only user interface and is incapable of logging/recording user activities performed through that HMI. The audit information associated with the user activities of Class B.2 CDAs is manually recorded and therefore, the attack vectors associated with this security do not exist relative to the integral HMI.			X		See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						not applicable.															Thus this security control is not applicable for attack vectors associated with the integral HMI. However, although a Class B.2 CDA is incapable of logging/recording communications (commands) from the system/device to which the CDA is communicating, the system/device to which the CDA is communicating maintains logging information. Thus, this security control is addressed by the system/device that sent such messages (e.g., an operator workstation) and using Section 3.1.6 of the cyber security plan, the B.2 CDA inherits the protections provided by the system/device.									
D2.6	Audit Review, Analysts and Reporting (D2.6)		X	X		Class A.2 CDAs are incapable of logging/recording user activities performed through their HMI. The audit information associated with the user activities of Class A.2 CDAs is manually collected. Thus, by using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by periodically reviewing (manual reviews) the information collected under D2.2 and D2.3. Periodicity is consistent with the cyber security plan.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis. Additionally, although a Class B.2 CDA is incapable of logging/recording communications (commands) from the system/device to which the CDA is communicating, the system/device to which the CDA is communicating maintains logging information. Thus, this security control is addressed by the system/device that sent such messages (e.g., an operator workstation) and using Section 3.1.6 of the cyber security plan, the B.2 CDA inherits the protections provided by the system/device.		X	X		See Class B.2 Basis.
D2.7	Audit Reduction and Report Generation (D2.7)				X	Class A.2 CDAs are incapable of logging/recording user activities performed through the HMI. The audit information associated with the user activities of Class A.2 CDAs are manually collected and therefore the attack vector associated with this cyber security control does not exist.		X	X		A Class A.3 CDA does not have capability to collect and record user activities performed through its integral HMI. The log information associated with the users' activities performed through the integral HMI is manually collected and reviewed and evaluated separate from the CDA.		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
											Thus, by using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by periodically reviewing (manual reviews) the information collected under D2.2 and D2.3. Periodicity is consistent with the cyber security plan.															
D2.8	Time Stamps (D2.8)		X	X		Since a Class A.2 CDA is incapable of collecting log information (if it has an integral HMI), that information is to be manually collected per the measures specified in D2.3 and as part of those measures the date and time of events are manually recorded as an alternative countermeasure.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis. Additionally, for auditable events initiated via industrial protocol messages sent over a CDA's asynchronous serial communication channels and the time stamping of those events, this security control is addressed by having the system/device that sent such messages (e.g., an operator workstation) apply the time tags. Therefore, by using Section 3.1.6 of the cyber security plan, this security control is addressed by the licensee verifying and documenting that the time stamping of the auditable events are addressed by the system/device and the B.2 CDA inherits the protection.		X	X		See Class B.2 Basis.
D2.9	Protection of Audit Information (D2.9)		X	X		Class A.2 CDAs are incapable of logging/recording user activities performed through the HMI. The audit information associated with the user activities of Class A.2 CDAs are manually collected. Therefore, using the method provided in Section 3.1.6 of the cyber security plan this control is addressed by plant procedures protecting the information collected under D2.3 from falsification or unauthorized modification.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis. Additionally, although a Class B.2 CDA is incapable of logging/recording communications (commands) from the system/device to which the CDA is communicating, the system/device to which the CDA is communicating maintains logging information. Thus, this security control is addressed by the system/device that sent such messages (e.g., an operator workstation) and using the Section 3.1.6 of the cyber security plan, the B.2 CDA inherits the protections provided by the		X	X		See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
																					system/device.					
D2.10	Non-Repudiation (D2.10)			X		Class A.2 CDAs are incapable of logging/recording user activities performed through the HMIs (if they have one). The audit information associated with the user activities of Class A.2 CDAs is manually collected. By using the method provided in Section 3.1.6 of the cyber security plan, this control is addressed by control D2.9.			X		See Class A.2 Basis.			X		See Class A.2 Basis.			X		See Class A.2 Basis.			X		See Class A.2 Basis.
D2.11	Audit Record Retention (D2.11)	X	X	X		The information collected under D2.2 is retained in accordance with NRC record retention regulations.	X	X	X		See Class A.2 Basis.	X	X	X		See Class A.2 Basis.	X	X	X		See Class A.2 Basis.	X	X	X		See Class A.2 Basis.
D2.12	Audit Generation (D2.12)			X		By definition, a Class A.2 CDA does not log/record user activity via the local/integral HMI or the special maintenance and configuration tool. For the Class A.2 CDAs, the audit information is manually collected. By using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by security measure taken by the licensee to address controls D2.2 and D2.3 and any identified security issues are put into the licensee's CAP program to ensure that those issues are promptly documented and tracked.			X		See Class A.2 Basis.			X		See Class A.2 Basis.			X		See Class A.2 Basis.			X		See Class A.2 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.	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.	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.	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.	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.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D3.2	Application Partitioning/Security Function Isolation (D3.2)				X	The Class A.2 CDA does not support any security functionality and the licensee verified that its vendor-provided software is designed to ensure that its essential SSEP functionality is not disrupted or adversely impacted because of user interaction via the local/integral HMI. Thus the attack vector addressed by this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	The Class B.1 CDA does not support any security functionality and the licensee verified its vendor-provided software is designed to ensure that its essential SSEP functionality is not disrupted or adversely impacted because of user interaction via the local/integral HMI or due to the use of the serial communication port(s). Thus the attack vector addressed by this control does not exist and the control is not required.				X	See Class B.1 Basis.				X	See Class B.1 Basis.
D3.3	Shared Resources (D3.3)				X	The Class A.2 CDA device does not share any resources or use any shared resources and it does not contain any SRI or SGI of value to an adversary. Thus the attack vector associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.
D3.4	Denial of Service Protection (D3.4)				X	The Class A.2 CDA device has no interfaces or peripherals aside from its integral HMI, and the licensee verified the HMI cannot cause a denial of service attack, and thus the attack vector associated with this control does not exist and the control is not required.				X	Licensee verified that the Class A.3 CDA has no interfaces or peripherals aside from its integral HMI and any I/O it supports, and the licensee verified that the HMI cannot cause a denial of service attack, and thus the attack vector associated with this control does not exist and the control is not required.				X	Licensee verified that the Class B.1 CDA has no interfaces or peripherals aside from its integral HMI (if it has one), asynchronous serial ports and any I/O it supports, and the licensee verified that the HMI and serial communications cannot cause a denial of service attack, and thus the attack vector associated with this control does not exist and the control is not required.				X	See Class B.1 Basis.				X	See Class B.1 Basis.
D3.5	Resource Priority (D3.5)				X	The licensee verified that the Class A.2 CDAs perform real-time processing, do not support multiple processes or threads running simultaneously, and that this Class A.2 CDA contains no additional resources requiring prioritization. The attack vector associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D3.6	Transmission Integrity (D3.6)				X	By definition, a Class A.2, CDA has no communication ports or interfaces (or they have been physically disabled) other than the special-purpose connection used for configuration of the Class A.2 CDAs. Thus the attack vector associated with this control does not exist and the control is not required.				X	The By definition, Class A.3 CDAs do not communicate with any other digital device or system except via basic analog, contact, or pulse I/O signals that are hard-wired and do not support any communication functionality (expect with the maintenance tool and only by taking the CDA out of service). The Class A.3 CDA is physically incapable of receiving or transmitting any communications. The attack vector associated with this control does not exist and the control is not required.				X	By definition, a Class B.1 CDA is factory-programmed and/or designed to only allow CDA information extraction through the asynchronous serial communications channel using poll-response based message exchanges. Additionally, the loss or degradation of the integrity, confidentiality or available of the information or data from the CDA could not result in adverse impact to SSEP functions. Therefore attack vectors associated with this security control does not exist and this security control is not applicable.		X	X		By definition, a Class B.2 CDA has only serial, asynchronous communication ports aside from the special connection only used for configuration of the Class B.2 CDAs and any basic analog, contact, or pulse I/O signals. The industrial protocols used by these CDAs do not support message validation and authentication mechanisms but can be used to control outputs connected to plant equipment and control pre-configured control functions [this include alterations to CDA configuration settings and the functional capabilities of the CDA (but not its program code)]. Therefore, the attack vector associated with this control exists. By using the method provided in Section 3.1.6 of the CSP, this security control is addressed by physically protecting the communication to prevent tampering by using one of the following methods: • Cable are contained in metal conduit and sealed junction boxes • Ensuring cabling is in locked room, etc.) to prevent tempering. • Cabling is in an area that contain concentrations of cables (e.g. cable spreading rooms, cable vaults, junction boxes, cable panels, cable trays, etc.); the cables are not easily accessible (physical contact without the aid of scaffolding or a ladder); and the cables are not easily recognizable by an adversary.		X	X		See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D3.7	Transmission Confidentiality (D3.7)				X	By definition, a Class A.2, CDA has no communication ports or interfaces (or they have been physically disabled) other than the special-purpose connection used for configuration of the Class A.2 CDAs. Thus the attack vector associated with this control does not exist and the control is not required.				X	The Class A.3 CDAs do not communicate with any other digital device or system (except for the maintenance tool and only by taking the CDA out of service) except by means of analog, contact, and/or pulse I/O signals which are hard-wired and do not support any communication functionality. The Class A.3 CDA is physically incapable of receiving or transmitting any communications. The attack vector associated with this control does not exist and the control is not required.				X	By definition, a Class B.1 CDA has serial, asynchronous communication ports as well as a special-purpose connection used for configuration of the Class B.1 CDAs and no other peripherals or interfaces (or they have been hardware disabled). The industrial protocols used on the serial ports do not contain any SRI or SGI or other information that requires confidentiality. Thus the attack vectors associated with the asynchronous communication channel for this security does not exist.				X	See Class B.1 Basis.				X	See Class B.1 Basis.
D3.8	Trusted Path (D3.8)				X	The Class A.2 CDA does not support any security functionality or user authentication process and thus the attack vector associated with this control does not exist and the control is not required.				X	The Class A.3 CDA has an integral limited functionality HMI and supports no user credential validation, thus the attack vector associated with this control does not exist and the control is not required.				X	See Class A.3 Basis.				X	The Class B.2 CDA has an integral limited functionality HMI and has no communication path between the user and the security functions of the CDA. Thus the attack vector associated with this control does not exist and the control is not required.				X	See Class B.2 Basis.
D3.9	Cryptographic Key Establishment and Management (D3.9)				X	The Class A.2 CDA does not use cryptography. Thus the attack vector associated with this control does not exist and the control is not required.				X	The Class A.3 CDA does not use cryptography nor is it necessary to address any of its security controls including inherited controls. Thus the attack vector associated with this control does not exist and the control is not required.				X	See Class A.3 Basis.				X	See Class A.3 Basis.				X	See Class A.3 Basis.
D3.10	Unauthorized Remote Activation of Services (D3.10)				X	The Class A.2 CDA is incapable of using collaborative computing mechanisms, and does not use or contain any cameras or microphones. As a result, the attack vector directly associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.
D3.11	Transmission of Security Parameters (D3.11)				X	The Class A.2 CDA does not support the transmission of security parameters, does not contain any SRI or SGI of value to an adversary, nor does it support any type of communication capability except for interfacing to a maintenance tool (or such				X	See Class A.2 Basis.				X	The Class B.1 CDA does not support the transmission of security parameters, does not contain any SRI or SGI of value to an adversary. Communications are limited to interfacing to a maintenance tool and asynchronous serial				X	See Class B.1 Basis.				X	See Class B.1 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						capabilities have been physically disabled). As a result, the attack vector directly associated with this control does not exist and the control is not required.										communications using industrial protocols. There are no other peripherals or interfaces (or such capabilities have been physically disabled). As a result, the attack vector directly associated with this control does not exist and the control is not required.											
D3.12	Public Key Infrastructure Certificates (D3.12)				**X**	The Class A.2 CDA does not use cryptography for any of its capabilities and does not use or support public key certificates. Thus the attack vector associated with this control does not exist and the control is not required.				**X**	The Class A.3 CDA does not contain any SGI or SRI information. Additionally, the Class A.3 CDA does not use cryptography for any of its capabilities, and does not use PKI to support any other security control, including inherited controls. The attack vector associated with this control does not exist and the control is not required.				**X**	See Class A.3 Basis.				**X**	See Class A.3 Basis.				**X**	See Class A.3 Basis.
D3.13	Mobile Code (D3.13)				**X**	The Class A.2 CDA is incapable of receiving, serving, or executing mobile code and has no communication capabilities except for interfacing to a maintenance tool (or such capabilities have been physically disabled). As a result, the attack vector directly associated with this control does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.
D3.14	Secure Name/Address Resolution Service (Authoritative/Trusted Source) (D3.14)				**X**	The Class A.2 CDA does not use any address resolution services. As a result, the attack vector directly associated with this control does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.
D3.15	Secure Name/Address Resolution Service (Recursive or Caching Resolver) (D3.15)				**X**	The Class A.2 CDA does not use any address resolution services. As a result, the attack vector directly associated with this control does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D3.16	Architecture and Provisioning for Name/Address Resolution Service (D3.16)				X	The Class A.2 CDA does not use any address resolution services. As a result, the attack vector directly associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.
D3.17	Session Authenticity (D3.17)				X	The Class A.2 CDA does not communicate with any other device except via basic analog, pulse I/O, or contact. The Class A.2 CDA is otherwise physically incapable of sending or receiving any communication. The Class A.2 CDA does not support communication sessions or networking functions. The attack vector associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	By definition, a Class B.1 CDA has no interfaces, peripherals or ports (or they have been physically disabled) other than the special purpose connection used only for configuration purposes and serial ports for asynchronous communication using industrial protocols that are functionally restricted to only permit the extraction of CDA data. Thus the attack vector associated with this control does not exist and the control is not required.			X		By definition, a Class B.2 CDA has no interfaces, peripherals, or ports (or they have been physically disabled) other than the special purpose connection used only for configuration purposes and serial ports for asynchronous communication using industrial protocols which do not support authentication mechanisms but enable control of pre-defined functions and CDA outputs connected to plant equipment. Thus the attack vector associated with this control exists. Therefore, by using the method provided in Section 3.1.6 of the CSP, this security control is addressed by protecting the system/device to which the CDA is communicating from cyber attack at the same level of confidence as the B.2 CDA and by security measures implemented to address the D3.6 security control.			X		By definition, a Class B.3 CDA has no interfaces, peripherals, or ports (or they have been physically disabled) other than the special purpose connection used only for configuration purposes and serial ports for asynchronous communication using industrial protocols which do not support authentication mechanisms but enable control of pre-defined functions and CDA outputs connected to plant equipment and include the ability to make alterations to CDA configuration settings and possibly the functional capabilities of the CDA (but not its program code). Thus the attack vector associated with this control exists. Therefore, by using the method provided in Section 3.1.6 of the CSP, this security control is addressed by protecting the system/device to which the CDA is communicating from cyber attack at the same level of confidence as the B.3 CDA and by security measures implemented to address the D3.6 security control.
D3.18	Thin Nodes (D3.18)				X	The licensee verified that the Class A.2 CDA only provides the minimum capabilities to perform its function, supports only vendor-specified functionality, and its programming cannot be altered. Therefore this control has been addressed by the vendor.				X	The licensee verified that the Class A.3 CDA only provides the minimum capabilities to perform its function, supports only vendor-specified functionality, and its programming cannot be altered. This control has been addressed by the vendor. Thus, attack vectors associated with this security does not exist and the control is not required.				X	See Class A.3 Basis.				X	See Class A.3 Basis.				X	See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
D3.19	Confidentiality of Information at Rest (D3.19)				X	The Class A.2 CDA does not contain any information, settings, or parameters that are SGI or SRI information. The attack vector associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.
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.	X	X			See Class A.2 Basis.	X	X			See Class A.2 Basis.	X	X			See Class A.2 Basis.	X	X			See Class A.2 Basis.
D3.21	Fail in Known (Safe) State (D3.21)			X		The engineering process ensures and documents that components fail in a state that is bounded with the design basis of the plant.			X		See Class A.2 Basis.			X		See Class A.2 Basis.			X		See Class A.2 Basis.			X		See Class A.2 Basis.
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 policies and procedures.	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 policies and procedures.	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 policies and procedures.	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 policies and procedures.	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 policies and procedures.
D4.2	User Identification and Authentication (D4.2)			X		Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. For A.2 CDAs, the access to the CDA is managed by controlling the access the CDAs thus using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address D1.3 and D1.5 as alternate security measures that provide equal protection as this security control.			X		By definition, a Class A.3 CDA have a self-protection mechanism (password, key, etc.) to restrict HMI user access; however they do not have the ability uniquely identify each user. Therefore, using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by implementing security measures provided in implementing security measures provided in D1.2 and D1.3.			X		See Class A.3 Basis.			X		See Class A.3 Basis.			X		See Class A.3 Basis.
D4.3	Password Requirements (D4.3)				X	Class A.2 CDAs do not support passwords therefore there is no requirement to address password complexity, duration or length in relation to Class A.2 CDAs so this			X		By definition, Class A.3 CDAs have a self-protection mechanism (e.g., password, key) to restrict HMI user access; however they do not support password requirements			X		See Class A.3 Basis.			X		See Class A.3 Basis.			X		See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						control does not apply and is not required.					that are sufficient to address the attack vectors associated with this security control. Therefore by using the method provided in Section 3.1.6 of the cyber security plan, the licensee has implemented security measures specified in control D4.2 to minimize the attack vectors associated with this control.														
D4.4	Non-Authenticated Human Machine Interaction (HMI) Security (D4.4)				**X**	Although Class A.2 CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions, access to the CDA is controlled and managed by security measures implemented to address D1.3 and D1.5.Thus no one can access the integral HMI unless the user is authorized and provided means to access the cabinet of the A.2 CDAs as described in D1.3 and D1.5. Therefore the attack vector associated with this control does not exist and this control is not applicable				**X**	All user interaction with the class A.3 CDA is via its access-restricted, integral HMI (which does require some form of authentication: password, fob, key, etc.) and thus there are no unauthenticated user interactions. Therefore, this control does not apply.				**X**	See Class A.3 Basis.				**X**	See Class A.3 Basis.				**X**	See Class A.3 Basis.
D4.5	Device Identification and Authentication (D4.4)		**X**	**X**		By definition, a Class A.2 CDA may (only) support connectivity to and communication with maintenance tools used to make configuration settings and changes. Modifications to the CDAs' configuration can change how A.2 CDAs function and could cause an adverse impact to SSEP functions. The maintenance tool provides a potential attack vector to Class A.2 CDAs and thus this control must be addressed. The licensee can address this security control by implementing D1.19 and E4.2.		**X**	**X**		By definition, a Class A.3 CDA may (only) support connectivity to and interfacing with maintenance tools used to make configuration settings and changes. The configuration of the Class A.3 CDA can be altered via use of the maintenance tools. The modifications to the CDAs' configurations can change how A.3 CDAs function and could cause adverse impacts to their SSEP functions. Therefore the attack vector exists. This control must be addressed and this can be accomplished by implementing D1.19 and E4.2.		**X**	**X**		By definition, a Class B.1 CDA supports connectivity to and interfacing with both maintenance tools used to make configuration settings and changes, and other systems or devices via its asynchronous, serial communication channels. The licensee has verified, validated and documented that the CDA meets the B.1 criteria. Thus the attack vectors associated with the asynchronous, serial communication channel for this security control does not exist. But, because the configuration of the Class B.1 CDA can be altered via the use of maintenance tool the attack vector does exist and the control must be addressed.		**X**	**X**		By definition, a Class B.2 CDA supports connectivity to and interfacing with both maintenance tools used to make configuration settings and changes, and other systems or devices via its asynchronous, serial communication channels. Since the configuration of the Class B.2 CDA can be altered via the use of maintenance tool the attack vector does exist and the control must be addressed. Modifications to the CDAs' configuration could cause an adverse impact to the CDA's SSEP functions. The licensee can address this security control by implementing D1.19 and E4.2.		**X**	**X**		See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
																Modifications to the CDAs' configuration could cause an adverse impact to the CDA's SSEP functions. The licensee can address this security control by implementing D1.19 and E4.2.					The asynchronous serial channels allow for CDA information extraction as well as for CDA output control (and possibly plant equipment control) and to control pre-defined CDA functionality. Thus the attack vectors associated with this control exist for the asynchronous, serial communication channel and must be addressed. Since the B.2 CDAs lack the capability to implement this control, by using the method provided in Section 3.1.6 of the CSP, the attack vectors associated with this asynchronous communication channel are addressed by the security measures implemented to address control D1.4.					
D4.6	Identifier Management (D4.6)			**X**		By definition, a Class A.2 CDA has no user identifiers and thus there is no automated way for the CDA to manage identifiers. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address D1.3 and D1.5 as alternate security measures that provide equal protection as this security control.			**X**		See Class A.2 Basis.			**X**		See Class A.2 Basis.			**X**		See Class A.2 Basis.			**X**		See Class A.2 Basis.
D4.7	Authenticator Management (D4.7)				**X**	By definition, a Class A.2 CDA has no authenticators and thus there is no requirement to manage them in relation to a Class A.2 CDA. Thus the attack vector associated with this control does not exist and the control is not required.			**X**		The Class A.3 CDA has an access-restricted integral HMI that requires a user to have some form of authenticator (e.g. a password, fob, key, etc.) so that only authorized personnel may utilize the HMI. Therefore the attack vector associated with this control exists and the control must be addressed. Therefore by using the method provided in Section 3.1.6 of the cyber security plan, the licensees implemented security measures provided in D1.2 and D1.3 to address this security			**X**		See Class A.3 Basis.			**X**		See Class A.3 Basis.			**X**		See Class A.3 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
											control.															
D4.8	Authenticator Feedback (D4.8)				X	A Class A.2 CDA by definition has a non-authenticated HMI. Since the CDA has no user authentication mechanisms and does not contain any SRI or SGI information, the attack vector associated with this control does not exist and the control is not required.		X	X		Class A.3 CDAs may restrict access to the HMI via password protection. However the CDA may or may not obscure the entry of the authenticator (i.e., password), therefore protection of the authenticator feedback is required to ensure that authentication credentials cannot be observed during use. This control is addressed by plant procedure that requires personnel to obscure the CDA HMI while entering any password.		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.		X	X		See Class A.3 Basis.
D4.9	Cryptographic Module Authentication (D4.9)				X	A Class A.2 CDA does not use cryptography. Therefore cryptographic functions/protections are not required and the attack vector associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.
D5.1	Removal of Unnecessary Services and Programs (D5.1)				X	Licensee has verified that this Class A.2 CDA by design does not contain unnecessary or unused applications, utilities, tools, or services that could be eliminated to reduce the available attack surface. Therefore, there is no need to remove unnecessary services or programs, and the attack vector associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.
D5.2	Host Intrusion Detection System (HIDS) (D5.2)				X	Class A.2 CDAs have no communication capabilities aside from their configuration connection (or these capabilities have been physically disabled) and the program code of the A.2 CDA cannot be changed. Thus the attack vector associated with this control does not exist and the control is not required.				X	By definition, a Class A.3 CDA has no communication ports or interfaces (or they have been physically disabled), other than the special-purpose connection used connect maintenance equipment for configuration modification of the Class A.3 CDAs. Additionally, A.3 CDA does not have an interface through which a				X	A Class B.1 CDA is not isolated and has serial asynchronous communications with other systems or devices. But because these communications are functionally constrained per the B.1 criteria. Additionally, B.1 CDA does not have an interface through which a user can gain access and program code (e.g.,				X	See Class B.1 Basis.				X	A Class B.3 CDA has serial asynchronous communications with other systems or devices. The serial asynchronous communication ports for a class B.3 CDA are functionally restricted but do permit the control of CDA outputs, the control of pre-configured CDA functions and alteration of CDA configuration

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
											user can gain access and program code (e.g., instruction-level code, configuration, settings) and configuration of the CDAs cannot be altered. The attack vectors associated maintenance tool (which is a portable media) for this security control is addressed by protection provided on the tool. Thus, based on the above, attack vectors associated with this security control do not exist and this security control is not required.					instruction-level code, configuration, settings) and configuration of the CDAs cannot be altered. The attack vectors associated maintenance tool (which is a portable media) for this security control is addressed by protection provided on the tool. Thus, based on the above, attack vectors associated with this security control do not exist and this security control is not required.										settings (but not its program code.) Thus, the attack vector associated with this control exists and this security control must be addressed. By using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address D3.6 and applying this security control to the systems/devices that the CDA is communicating and the CDA inheriting the protection provided by the systems/device.
D5.3	Changes to File System and Operating System Permissions (D5.3)				**X**	Licensee has verified that this Class A.2 CDA does not have a file system or user alterable security settings. Therefore, the attack vector associated with this control does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.
D5.4	Hardware Configuration (D5.4)				**X**	Licensee has verified that this Class A.2 CDA does not support extraneous, unnecessary hardware and specifically does not incorporate ports, interfaces, or peripheral devices that could be used as attack vectors (or they have been physically disabled). This type of CDA has factory-installed program code that is non-alterable. Thus the attack vector associated with this control does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.		**X**		**X**	The licensee has verified that this B.2 CDA does not support extraneous, unnecessary hardware and specifically does not incorporate ports, interfaces, or peripheral devices that could be used as attack vectors. This type of CDA has factory-installed program code that is non-alterable. Note: If the CDA supports multiple serial ports where some are not assigned for use, this security control could be applicable. The licensees can address this security control by verifying and documenting that any such ports not being used are physically disabled.		**X**		**X**	See Class B.2 Basis.
D5.5	Installing Operating Systems, Applications, and Third-Party Software Updates (D5.5)				**X**	This type of CDA cannot be patched since its program code is factory-installed and cannot be altered. Therefore the attack vector associated with this control does not exist and the control is not required.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.				**X**	See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
E1.3	Media Labeling/Marking (E1.3)				X	By definition, the Class A.2 CDA has no support for removable media or peripherals for generating output (other than analog, contact and pulse I/O signals) and thus the attack vector associated with this control does not exist and the control is not required.				X	By definition, the Class A.3 CDA does not support any interfaces that accept portable media and does not contain any type of SGI or SRI information, thus the attack vector associated with this control only applies to the maintenance tool.				X	See Class A.3 Basis.				X	See Class A.3 Basis.				X	See Class A.3 Basis.
E1.6	Media Sanitation and Disposal (E1.6)				X	By definition, the Class A.2 CDA does not support any interfaces or peripheral devices that accept portable media and does not contain any type of SGI or SRI information, thus the attack vector associated with this control does not exist and the control is not required.				X	By definition, the Class A.3 CDA does not support any interfaces that accept portable media and does not contain any type of SGI or SRI information, thus the attack vector associated with this control does not exist and the control is not required.				X	See Class A.3 Basis.				X	See Class A.3 Basis.				X	See Class A.3 Basis.
E3.3	Malicious Code Protection (E3.3)				X	By definition, the program code of the Class A.2 CDA cannot be altered and thus the attack vector associated with this control does not exist and the control is not required.				X	By definition, the Class A.3 CDA cannot be infected by malicious code as its firmware cannot be changed. But the functions of the CDA can be altered by manipulation of configuration parameters which are accessible via the integral HMI and the maintenance tool. The maintenance tool thus provides an attack vector and must be protected against malicious code. The malicious code protection mechanisms for the maintenance tool are addressed per D1.19 and E4 family of security controls.				X	See Class A.3 Basis.				X	See Class A.3 Basis.				X	By definition, the Class B.3 CDA cannot be infected by malicious code as its firmware cannot be changed. But the functions of the CDA can be altered by manipulation of configuration parameters which are accessible via the integral HMI, the maintenance tool, and the system/device to which the CDA is communicating. Thus the maintenance tool and the system/device provide an attack vector and must be protected against malicious code. The malicious code protection mechanisms for the maintenance tool are addressed per D1.19 and E4 family of security controls and for the system/devices are addressed by security measures implemented to address E3.8.
E3.4	Monitoring Tools and Techniques (E3.4)				X	This control applies to the plant-wide security monitoring capability and multi-level security architecture and Class A.2 CDAs do not collect or provide any information of value to a plant-wide monitoring functionality. Thus this control is not applicable to Class A.2 CDAs and the control				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						is not required.																				
E3.6	Security Functionality Verification (E3.6)		X	X		This security control is addressed by verifying and documenting that security measures implemented to address D1.3 are periodically evaluated in accordance with 10 CFR 73.55(m) to ensure that the implemented security measures are operating correctly and effectively to prevent and detect unauthorized access.		X			Because the Class A.3 CDA employs some form of HMI user access restriction the attack vector associated with this control exists and the control must be addressed. The correct operation of integral access protection mechanisms (e.g., password, keylock, fob) of CDAs are verified and documented, periodically in accordance with 10 CFR 73.55(m), upon startup and restart, upon command by a user with appropriate privilege, and when anomalies are discovered. If a locked and alarm cabinet or other security measures are used to address the required security controls, per plant procedure, the correct operation of these security measures are verified and documented, periodically in accordance with 10 CFR 73.55(m).		X			See Class A.3 Basis.		X			See Class A.3 Basis.		X			See Class A.3 Basis.
E3.7	Software and Information Integrity (E3.7)			X		Although the program code of an A.2 CDA cannot be altered these CDAs have integral HMIs that allow anyone (authorized or unauthorized) to manipulate operational parameters which could lead to an adverse impact to SSEP functions. The A.2 CDA's configuration can be modified using special tools and this can alter the CDA's functionality. Therefore the attack vector associated with this control exists and the control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by the security measures implemented to address D1.3 and D1.5 as alternate security measures that provide equal protection as this security control			X		A Class A.3 CDA is a stand-alone device that does not support communication with other devices, has no remote communications, and its programming cannot be changed. The primary attack vectors associated with A.3 CDAs are unauthorized manipulation of operational parameters or configuration via the HMI and unauthorized manipulation of configuration via a maintenance tool and/or a special-purpose connection. Class A.3 CDAs have self-protection mechanisms (e.g., password, key) to restrict HMI user access; however they do not have the ability to validate operational or configuration changes. Unauthorized access to the HMI could enable alteration of configuration settings that could			X		A Class B.1 CDA has limited communications capability, and its programming cannot be changed, including via its communications functions. The primary attack vectors associated with B.1 CDAs are unauthorized manipulation of operational parameters or configuration via the HMI and unauthorized manipulation of configuration via a maintenance tool and/or a special-purpose connection. Class B.1 CDAs have self-protection mechanisms (e.g., password, key) to restrict HMI user access; however they do not have the ability to validate operational or configuration changes. Unauthorized access to the HMI could enable alteration of configuration settings that could adversely impact SSEP functions.		X	X		See Class B.1 Basis. Additionally, relative to the asynchronous serial ports, the attack vector associated with this control also exists and this security control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control may be addressed by licensees protecting the system/device as CDAs and inheriting the protection provided by the system/device.		X	X		See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						to address attack vectors associated with the integral HMI. Additionally, the security measures implemented to address D4.5 and E4.2 as alternate security measures that provide equal protection as this security control to address attack vectors associated with modification of the A.2 CDA's configuration using maintenance tools.					adversely impact SSEP functions. Therefore this control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by implementing security measures to address D1.2, D1.3, D2.2 and D2.3					Therefore this control must be addressed. Using the method provided in Section 3.1.6 of the cyber security plan, this security control is addressed by security measures implemented to address D1.2, D1.3, D2.2 and D2.3										
E3.8	Information Input Restrictions (E3.8)				**X**	Class A.2 CDAs have no interface through which a user can gain access and change program code (e.g., instruction-level code, configuration, or settings) or configuration of the CDA and does not log/record user activity via the local/integral HMI. A.2 CDAs only allow a modification of operational parameters by anyone who has access to its integral HMI. Class A.2 device HMIs only expose functionality to change operational set points, and do not accept non-pre-programmed or non-pre-defined inputs that would require input restrictions. Therefore, attack vectors associated with this security controls do not exist and the control is not required.			**X**		A Class A.3 CDA by definition has an access-restricted integral HMI that provides access to operational and configuration settings. Since the malicious modification of those could have an adverse impact on SSEP functions, the attack vectors associated with the HMI exist and the control must be addressed. This control is addressed using alternative countermeasures as provided in control E3.7.			**X**		See Class A.3 Basis.			**X**		A Class B.2 CDA is designed to receive input data from the integral HMI and the system/device to which the CDA is communicating. However, the CDA does not have the capability to check or screen the input data accuracy, completeness, validity, or authenticity. Since the malicious input data from the integral HMI and the system/device could adversely impact SSEP functions, the attack vectors associated with the HMI exist and the control must be addressed. Therefore, by using the method provided in Section 3.1.6 of the CSP, this security control is addressed by the following: • For the integral HMI, this control is addressed by security measures implemented to address E3.7. • For the system/device, the licensees verified and documented that the CDA only recognized the factory predefined data (commands). Additionally, licensees protect the system/device as CDAs and inherit the protection provided by the system/device and verify and document that all other ports are physical disabled, if CDA has other ports.			**X**		See Class B.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
E3.9	Error Handling (E3.9)				X	A Class A.2 CDA by definition does not contain SRI or SGI information of value to an adversary and does not produce error messages. Thus the attack vector associated with this control does not exist and the control is not required.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.				X	See Class A.2 Basis.
E4.2	Maintenance Tools (E4.2)		X	X		A Class A.2 CDA by definition may allow changes to its configuration using a maintenance tool or via a special-purpose interface and only by taking the Class A.2 CDA out of service (which can only be done locally, at the CDA). These CDAs generally have no integral technical ability to verify the accuracy or validity of configuration setting changes made with those tools. The modifications to the CDAs' configurations can change how A.2 CDAs function and could cause adverse impact to the SSEP systems or equipment or functions and therefore the attack vector associated with this control exists and the control must be addressed. The licensee can address this security control by accomplishing the following: • Ensuring the maintenance tool is not connected to another device or network (including wireless networks) when connected to the CDA. Portable media connected to the maintenance tool while the maintenance tool is connected to the CDA are controlled in accordance with D1.19. • Approving, monitoring, and documenting the use of maintenance tools used to maintain CDAs. • Controlling maintenance tools associated with CDAs to prevent improper		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.		X	X		See Class A.2 Basis.

Ctrl	Control	Common	Apply to CDA	Alternate	Not Applicable	Class A.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class A.3 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.1 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.2 Basis	Common	Apply to CDA	Alternate	Not Applicable	Class B.3 Basis
						modifications. Maintenance tools include, for example, diagnostic and test equipment and mobile devices such as laptops. • Checking and documenting media and mobile devices, such as laptops, containing diagnostic, system, and test programs/software for malicious code before the media or mobile device is used in/on CDAs. • Controlling the removal of maintenance equipment by one of the following: o Retaining the equipment within the licensee control so that unauthorized access to the maintenance equipment or systems is prevented. o Obtaining approval from an authority authorizing removal of the equipment from the licensee control. o Verifying that there is no licensee security related or SGI information contained on the equipment and validating the integrity of the device before reintroduction into the licensee control. If unable to verify/validate the integrity of the device, then sanitize or destroy the equipment. • Employing automated or manual mechanisms to restrict the use of maintenance tools to authorized personnel; employs manual mechanisms where CDAs or support equipment (e.g., laptops) cannot support automated mechanisms.																				

[BLANK PAGE]

APPENDIX E – NEI 13-10 FREQUENTLY ASKED QUESTIONS

Question 1: Does the expression “Safety functions” in Section 3 include important-to-safety?

Answer: Section 3 was revised in NEI 13-10, Revision 6, to clarify the term Safety functions.

Question 2: How does augmented quality apply to NEI 13-10?

Augmented quality CDAs such as Fire Protection and SBO perform Important-to-Safety functions but must be screened through these criteria to be classified as Indirect. Section 3 was revised in NEI 13-10, Revision 6, to clarify the term Safety functions.

Question 3: Can a site’s accident analysis be used to inform the screening in Section 3.1?

Answer: Yes. However, since the site’s accident analyses are based on CDA failure, it may not cover conditions or events that would be caused by the cyber compromise of the CDAs. The events caused by a cyber compromise go beyond simple failure and may include full or partial loss of control of the CDA, malfunctioning of the CDA, generation of false/misleading data by the CDA, suppression of valid alarm indications or generation of false alarm indications by the CDA and even autonomous operation of associated plant equipment by the CDA. . One way to cover the conditions resulting from the cyber compromise of a system/CDA is by performing an analysis to demonstrate how the consequences resulting from a cyber compromise of the BOP system or CDA are:

- Bounded by the current accident or other analysis;

- Mitigated by the plant operators by applying their training and operating experiences to ensure that the abnormal plant conditions caused by cyber compromised of BOP are within the safety boundary; and,

- Ensure that the safety instruments that perform safety functions are isolated from the BOP CDAs so that the cyber compromise of the BOP CDAs would not adversely impact the safety CDAs or systems from performing their functions.

Based on the above, a cyber compromise of the BOP CDAs does not lead to adverse impact to the safety CDAs or systems. Therefore, time required to detect and mitigate the cyber compromise of BOP CDAs before adverse impact to safety CDAs or systems need not be determined. The heater drains bridge controller example in Appendix C of NEI 13-10 provides an example that relies on Chapter 15 accident analysis when screening CDAs.

Question 4: Can wireless technologies be used with non-direct CDAs?

Answer: In general the answer is ‘no’ because to implement the baseline protections provided in Section 5 of NEI 13-10 to streamline the protection of Indirect CDAs, the Indirect CDA must meet the baseline criteria including the following:

- The Indirect CDA and any interconnected assets do not have wireless internetworking communications technologies

- The Indirect CDA and any interconnected assets must be "air gapped" or protected by a deterministic isolation device

The CSP section 3.1.6 process allows licensees to propose alternative countermeasures to any technical controls provided in the CSPs. However, because the above two criteria have been determined to eliminate the threat and attack vectors associated with wired and wireless communications, many of the technical security controls specified in CSP are addressed by the above criteria. Therefore, for a CDA to be classified as an indirect or BOP CDA, the CDA must comply with these two criteria.

However, an exception can be made for certain radio-based communication devices, which may be considered non-direct CDAs, if the following conditions are met:

- These devices support certain security functions,
- Licensees already have accounted for potential compromise of the CDAs,
- These devices are isolated from other networks and other systems or equipment, and
- The consequences of their cyber compromise can be detected and independent alternate means are available to perform that communication function.

Therefore, the licensee may evaluate these devices based on, but not limited to, their functions, capabilities, connections, and configurations to identify them as indirect CDAs.

Question 5: What does the expression, "where technically feasible" mean?

Answer: This expression does not apply to the required security controls specified in the licensee's cyber security plans and thus does not apply to Direct CDAs. This expression only applies to the security controls listed in Section 5 of NEI 13-10 in regards to BOP CDAs. If the currently installed BOP device is capable of implementing the control, the control should be implemented. If the currently installed BOP device is not capable of implementing the control, the control need not be implemented and an alternate need not be documented. Licensee should document the control disposition (i.e., implemented, or not implemented because not technically feasible). This answer is based on a NERC FAQ on CIPs-002-009, which describes:

> Technical feasibility refers only to engineering possibility and is expected to be a "can/cannot" determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by the Responsible Entity. The Responsible Entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards.

Therefore, technically feasible means the CDA has integral functionality, including hardware and software, to enable it perform some or all the functions specified in the control specification. For example, if a CDA supports no passwords and has no user account functionality then account management is not technically feasible for that CDA. If a CDA has that functionality but to use it this capability must first be configured, then account management is technically feasible for

that CDA. For the BOP CDAs, the licensee will need to implement the baseline criteria and selected security controls provided in the bottom of Section 5.

Question 6: Is additional criteria required for screening complex CDAs or to limit certain CDAs from being classified as Indirect?

No. Classification of a CDA as Indirect is based on satisfying the criteria and is not dependent on the complexity of the CDA.

The ability to detect cyber compromise prior to adverse impact to Safety, Security, or EP functions may be easier to implement and document for simple CDAs vs Complex CDAs. Because simple CDAs may have limited and defined functional capabilities, the simple CDAs may have a small attack surface and limited potential consequences. Therefore, the indirect CDA determination of a simple CDA can be justified and documented by showing that various existing plant procedures and engineering and reliability measures, which the licensees has already implemented to address abnormal behavior of the controller, provide adequate detection and remediation prior to any adverse impact to Direct CDAs, or Safety or Security functions.

The objective of Indirect assessment is to address cyber security requirements by ensuring that there is no adverse impact to Direct CDAs, or Safety or Security functions due to cyber compromise. This method focuses on securing the associated function/s through detection and mitigation. In effect this method must assume the CDA is compromised and must then provide documented assurance that the compromise cannot adversely impact the associated Direct CDAs, or function/s. Direct assessment provides a fundamentally different approach to protecting the same functions by implementing controls focused on preventing a compromise of the CDA.

Indirect assessment is not dependent on the complexity of the CDA. It is only dependent on the ability to detect and mitigate adverse impact to Direct CDAs, or the function. A complex CDA may have a relatively easy method of detecting and mitigating adverse impact. For example, the only function of the Plant Computer may be to provide an indication of thermal power to ensure the plant is operating within Tech Spec limits. A compromise can be detected and mitigated by alternate indication that is readily available through alternate detectors and because adverse impact can only occur indirectly through manual Operator action. In this case, indirect assessment of the Plant Computer provides a relatively easy and reliable method of preventing adverse impact to the function through detection and mitigation.

A complex CDA that has a large number of functional capabilities that are incorporated into the CDA by means of its software and may support a number of interfaces and peripheral devices may have many potential consequences due to cyber compromise. The indirect CDA determination may not reduce the effort compared to addressing each the security controls required of a Direct CDA. CDAs may be associated with multiple SSEP functions. The indirect assessment must address detection and mitigation prior to adverse impact of all SSEP functions. For non-complex CDAs, that have multiple SSEP functions, it may be easier to identify the CDA as Direct.

Question 7: What are acceptable methods of detecting and mitigating cyber compromise to satisfy Section 3?

Examples of potential detection and mitigation prior to impact include:

- Detection prior to use. An example of detection prior to use may be Operations verifying alternate indications prior to taking a manual action. This method eliminates the need to continuously monitor for compromise if a quality check is done prior taking actions that would adversely impact the SSEP function.

- Tech Spec and TRM surveillance may provide acceptable detection and frequencies for associated CDA functions. This is acceptable for some of the most important CDAs and may be a method that could also be implemented for other CDAs if supported by justification that the detection frequency will provide sufficient time to mitigate adverse impact to the SSEP function.

- The time to detect may be infinite if it can be shown that there is never an adverse impact. Some CDAs may be "associated" with an SSEP function or may "impact" an SSEP function, but may not be capable of "adversely impacting" the SSEP function. In this case the answer should explain why there is no adverse impact and therefore an infinite time to detect. Generally "N/A" should not be used, but if it is used then it must be supported by an explanation as to why it is N/A.

- IDS may be an acceptable method of detection, but justification is required to show how this would permit mitigation prior to impact.

Question 8: Can CDAs associated with Security functions be classified as Indirect?

Yes. An example is a Security System HVAC unit. In this example the HVAC unit is a support system to the Security Computer. If this CDA is compromised it can result in overheating condition and subsequent failure of the Security Computer thereby adversely impacting the security functions of the Security Computer. The example documents that the temperature increase in the room can be detected and methods of mitigating this condition can be implemented before the functions of the security computer are adversely impacted. This meets all of the Indirect screening criteria in Section 3.

APPENDIX F – GUIDANCE FOR APPLICATION OF NEI 08-09 APPENDIX E CONTROLS TO INDIRECT, EP, AND BOP CDAS

This Appendix provides a consistent method for addressing NEI 08-09, Appendix E, cyber security controls for Indirect, EP, and BOP CDAs and provide a specific accounting of each control to demonstrate compliance with Section 3.1.6 of the cyber security plan (CSP).

This Appendix addresses the NEI 08-09, Appendix E, cyber security controls for CDAs not identified as direct by using alternative security controls that achieve the same objectives and purpose as the controls specified in Appendix E of the CSP by confirming that alternative security measures mitigate the threat/attack vector the control is intended to protect. In accordance with Section 3.1.6, the following are used as alternative security controls to address the Appendix E controls:

- The analysis which demonstrates the CDA is not direct,
- The implementation of the baseline cyber security protection criteria provided in Section 5, and
- Addressing the Appendix E controls using the table below.

1 TABLE DESCRIPTION

Each Appendix E control is assigned to one of the following three categories. The table describes how the control is addressed in accordance with Section 3.1.6 of the licensee's CSP.

Technical – Security controls in NEI 08-09, Appendix E, that are recognized as Technical and are not Operational & Management (O&M) in NEI 13-10.

These controls are already addressed by the applicable baseline controls cyber security protection criteria provided in Section 5. No additional implementation is required for individual CDAs, unless the technical control is relied upon to accomplish the detection criteria for indirect CDA's.

This is based on the general description in NEI 13-10, Section 3, that recognizes that selected controls from NEI 08-09, Appendix E, are technical and those security controls are addressed by taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety Related, Security, or EP functions and implementing the specific controls in Section 5 of NEI 13-10. These controls are specifically identified in NEI 13-10 Appendix D, Table A.3 and include E.1.3, E.1.6, E.3.3, E.3.4, E.3.6, E.3.7, E.3.8, E.3.9, and E.4.2

Addressed – These cyber security controls are already specifically addressed by existing controls identified within NEI 13-10. For example, E.5 "Physical and Operational Environment Protection" is already addressed in Section 5 of NEI 13-10 by criteria (a).

Controls that are already addressed will be implemented according to NEI 13-10 guidance.

Where applicable guidance is established in NEI 13-10, this will be implemented for consistency and to eliminate duplicate or conflicting requirements.

Addressed Programmatically – NEI 08-09, Appendix E, controls that do not fall into either of the above categories.

This category addresses the Appendix E controls for the non-direct CDA by using the programmatic approaches. Where possible, these Appendix E security controls are addressed by the existing plant programs to fulfill the control objectives.

2 USE OF THE TABLE

The table below describes how licensees have addressed the NEI 08-09, Appendix E, controls for non-direct CDAs. Licensees must modify the table to provide specific procedure/documentation references where required. The modified table may then be used in conjunction with documentation specified in Section 3 of NEI 13-10 to document non-direct CDA compliance to the NEI 08-09 Appendix D and E controls

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.1.1	Media Protection Policy and Procedures (SGI, Non-SGI and 2.390)			X	For SGI and SRI information, the licensee's information protection is addressed by [Insert site specific procedure reference] which address the 10CFR73.21 and 10CFR2.390 program.
E.1.2	Media Access			X	Same as E.1.1
E.1.3	Media Labeling/Marking	X		X	Same as E.1.1
E.1.4	Media Storage			X	Same as E.1.1
E.1.5	Media Transport			X	Same as E.1.1
E.1.6	Media Sanitation and Disposal	X		X	Same as E.1.1
E.2.1	Personnel Security Policy and Procedures			X	This control is addressed by complying with the requirements of 10CFR73.56. [Insert site specific procedure reference.]
E.2.2	Personnel Termination/Transfer			X	This control is addressed by complying with the requirements of 10CFR73.56 along with the work controls and Human Resources personnel termination/transfer procedures. [Insert site specific procedure reference.] Additionally, per the licensee's cyber security policy and the termination/transfer procedures, the site ensures that logical access to CDAs is revoked for individuals who no longer require access to the CDAs.
E.3.1	System and Information Integrity Policy and Procedures			X	The licensee's system and information integrity is addressed by [Insert site specific procedure reference.]
E.3.2	Flaw Remediation			X	This control is addressed by the plant wide flaw remediation procedure. [Insert site specific procedure reference.] Note: This may be a combination of procedures.

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.3.3	Malicious Code Protection	X			*Technical Control* – addressed by NEI 13-10 Section 5 This security control is addressed by alternative cyber security controls as described in Section 3.1.6 of licensees' cyber security plans by the following: • Taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security, or EP functions. • Implementing the baseline controls cyber security protection criteria specified in Section 5 that are deemed to be adequate and this control is not required unless malicious code protection mechanisms are relied on for detection of a cyber compromise of the CDA.
E.3.4	Monitoring Tools and Techniques	X			Same as E.3.3
E.3.5	Security Alerts and Advisories			X	This control is addressed by the site vulnerability management procedure, [insert site specific procedure reference] that monitors credible sources for vulnerability/threat updates and implements corrective actions or mitigating measures in a reasonable timeframe once new applicable vulnerabilities/threats have been identified.
E.3.6	Security Functionality Verification	X			Same as E.3.3
E.3.7	Software and Information Integrity	X			Same as E.3.3
E.3.8	Information Input Restrictions	X			Same as E.3.3
E.3.9	Error Handling	X			Same as E.3.3
E.3.10	Information Output Handling and Retention			X	Same as E.1.1
E.3.11	Anticipated Failure Response		X(f)		Addressed by NEI Section 5(f).

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.4.1	System Maintenance Policy and Procedures			X	This requirement is addressed by plant-wide maintenance policies and procedures. [Insert references to site maintenance procedures, IT procedures, Interface agreements etc.]
E.4.2	Maintenance Tools	X	X(d)		*Technical Control* – addressed by NEI 13-10 Section 5 (d)
E.4.3	Personnel Performing Maintenance and Testing Activities			X	This control is addressed by complying with the requirements of 10CFR73.56, the training qualification program, the work control program, and the IT maintenance procedures. [Insert site specific procedure reference.]
E.5.1	Physical and Operational Environment Protection Policies and Procedures		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a).
E.5.2	Third Party/Escorted Access		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a).
E.5.3	Physical & Environmental Protection		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a).
E.5.4	Physical Access Authorizations		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a).
E.5.5	Physical Access Control		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a).
E.5.6	Access control for Transmission Medium		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a).
E.5.7	Access Control for Display Medium		X(a)		The security control is addressed by implementing the baseline security control as specified in NEI 13-10 Section 5 (a).

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.5.8	Monitoring Physical Access		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a) and by taking credit for the existing physical security program and access controls.
E.5.9	Visitor Control Access Records		X(a)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (a) and by taking credit for the existing physical security program and access controls.
E.6	Defense-In-Depth		X(c)		The security control is addressed by implementing the baseline controls cyber security protection criteria as specified in NEI 13-10 Section 5 (c).
E.7.1	Incident Response Policy and Procedures			X	This control is addressed by the site maintenance, corrective action program, configuration management (that are updated to address cyber security) and incident response procedures, [Insert site specific procedure reference.] These generic procedures apply to CDAs generally. No additional policy requirements for non-direct CDAs.
E.7.2	Incident Response Training			X	Incident response training applies to CDAs in general. [Insert site specific procedure reference.] Additional training may be needed to deal with the wide range of technically and functionally-diverse non-direct CDAs.
E.7.3	Incident Response Testing and Drills			X	Incident response testing and drills that apply to CDAs in general. [Insert site specific procedure reference.] Additional testing and drills may be needed to deal with the wide range of technically and functionally-diverse non-direct CDAs.

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.7.4	Incident Handling			X	Incident handling protocols apply to CDAs in general. [Insert site specific procedure reference.] Additional incident handling protocols may be developed to deal with the wide range of technically and functionally-diverse non-direct CDAs.
E.7.5	Incident Monitoring			X	Incident monitoring applies to CDAs in general. [Insert site specific procedure reference.] No additional incident monitoring is required for non-direct CDAs.
E.7.6	Incident Response Assistance			X	Incident response assistance applies to CDAs in general. [Insert site specific procedure reference.] No additional incident response assistance is required for non-direct CDAs.
E.8.1	Contingency Plan			X	Plant operating procedures provide contingencies for abnormal conditions. Maintenance procedures provide capabilities to recover the function of failed equipment. Contingency plans are developed in accordance with the CDAs function and/or capability when operating and maintenance procedures do not recover the function within the required timeframe to preserve the Safety, Security, or EP function. [Insert site specific contingency procedure reference.] No additional implementation is required for non-direct CDAs.
E.8.2	Contingency Plan Testing			X	Contingency plan testing is performed in accordance with the contingency procedure. No additional testing is required for non-direct CDAs.
E.8.3	Contingency Training			X	Contingency plan training is performed in accordance with the contingency procedure. No additional training is required for non-direct CDAs.

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.8.4	Alternate Storage Site/Location for Backups			X	Alternate storage locations are established in accordance with the contingency procedure. No additional requirements for non-direct CDAs.
E.8.5	CDA Backups			X	CDA backups are established in accordance with the contingency plan established in E.8.1. No additional requirement for non-direct CDAs.
E.8.6	Recovery and Reconstitution			X	Normal site maintenance, repair and recovery processes, which includes root-cause analysis when necessary, are sufficient (including necessary technical detail as appropriate) for the recovery of non-direct CDAs.
E.9.1	Cyber Security Awareness and Training			X	This control is addressed by the plant wide cyber security awareness and training. [Insert site specific procedure reference.] No additional training is required for indirect CDAs.
E.9.2	Awareness Training			X	This control is addressed by the plant wide cyber security awareness and training. [Insert site specific procedure reference.] No additional training is required for indirect CDAs.
E.9.3	Technical Training			X	This control is addressed by the plant wide cyber security technical training. [Insert site specific procedure reference.] When technical cyber controls are credited for the detection of a compromise, technical training must include specific material on the use of those capabilities for detecting the cyber compromises of non-direct CDAs. Additionally, for EP indirect CDAs, the facility personnel are trained to use the alternate methods for accomplishing the functions performed by the EP indirect CDAs.

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.9.4	Specialized Cyber Security Training			X	This control is addressed by the plant wide cyber security specialized cyber-security training. [Insert site specific procedure reference.] No additional training is required for indirect CDAs.
E.9.5	Situation Awareness			X	This control is addressed by the plant wide policies and procedures for situational awareness. [Insert site specific procedure reference.] No additional situational awareness is required for non-direct CDAs.
E.9.6	Feedback			X	This control is addressed by the plant wide policies and procedures for cyber security feedback. [Insert site specific procedure reference.] No additional feedback required for non-direct CDAs.
E.9.7	Security Training Records			X	This control is addressed by the plant wide policies and procedures for security training record keeping. [Insert site specific procedure reference.] No additional training records are required for non-direct CDAs.
E.9.8	Contacts With Security Groups and Associations			X	This control is addressed by the plant wide policies and procedures for incident response. [Insert site specific procedure reference.] No additional requirements for non-direct CDAs.
E.10.1	Configuration Management		X(e)		Addressed by NEI 13-10 Section 5(e).
E.10.2	Configuration Management Policy and Procedures		X(e)		Same as E.10.1.
E.10.3	Baseline Configuration			X	A baseline configuration is documented by entering the specific hardware, firmware/software (including patches and updates) and configuration setting information for the non-direct CDA into a site configuration management program and associated systems.
E.10.4	Configuration Change Control		X(e)		Same as E.10.1.

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.10.5	Security Impact Analysis		X(e)		Same as E.10.1.
E.10.6	Access Restrictions for Change			X	This security control is addressed by alternative security control as described in Section 3.1.6 of licensee's cyber security plan by the following: • Taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security, or EP functions. • Taking credit for implementing NEI 13-10 Section 5(a), 5(b), and 5(c). The corrective action program addresses discovered deviations. Detection of unauthorized changes is accomplished in accordance with E.3.4. • Conducting post maintenance testing to validate that changes are correctly implemented.
E.10.7	Configuration Settings			X	This security control is addressed by alternative security control as described in Section 3.1.6 of licensee's cyber security plans by the following: • Taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security or EP functions, • Taking credit for implementing Sections 3.1.3 and 3.1.5 and E10.3 of the CSP. • Conducting post maintenance testing to validate that changes are implemented correctly.

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.10.8	Least Functionality			X	This security control is addressed by alternative security control as described in Section 3.1.6 of licensee's cyber security plans by the following: • Taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security, or EP functions. • Taking credit for implementing Sections 3.1.3 and 3.1.5 of the CSP.
E.10.9	Component Inventory			X	This security control is addressed by alternative security control as described in Section 3.1.6 of licensee's cyber security plans by the following: • Taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security, or EP functions. • Taking credit for implementing NEI 13-10 Section 5(e) and CSP Sections 3.1.3, 3.1.5 and E.10.3 as specified above.
E.11.1	System and Services Acquisition Policy and Procedures			X	This security control is addressed by alternative security control as described in Section 3.1.6 of licensee's cyber security plans by: • Taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security, or EP functions and by implementing standard nuclear purchasing processes.
E.11.2	Supply Chain Protection			X	Same as E.11.1.
E.11.3	Trustworthiness			X	Same as E.11.1.

Control	Control Title	Technical	Addressed	Addressed Programmatically	Basis
E.11.4	Integration of Security Capabilities			X	This security control is addressed by alternative security control as described in Section 3.1.6 of licensee's cyber security plans by: • Taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security, or EP functions • Implementing the threat and vulnerability management program in accordance with NEI 08-09 Appendix E.3.2 and E.3.5. [Insert site specific procedure reference.] No additional requirements for non-direct CDAs.
E.11.5	Developer Security Testing			X	This control is addressed by taking credit for implementing measures to detect and mitigate the cyber compromise prior to adverse impact to direct CDAs or Safety, Security, or EP functions and by implementing standard nuclear purchasing processes [insert site specific procedure reference] that address: • Internal pre-operational testing, • Malicious code scanning when possible, and • Calibration / configuration program.
E.11.6	Licensee Testing			X	Same as E.11.5.
E.12	Evaluate And Manage Cyber Risk		X (e,g)		This security control is addressed by alternative security control as described in Section 3.1.6 of licensee's cyber security plans. As an alternate, this control is addressed by NEI 13-10 Section 5 (e) and (g) and plant-wide program to address the threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.

[BLANK PAGE]