

July 23, 2020

Mr. Russell Felts
Acting Director, Division of Physical and Cyber Security Policy
Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Endorsement of NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with the Balance of Plant," dated July 2020, by August 30, 2020

Project Number: 689

Dear Mr. Felts:

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

Accordingly, the Nuclear Energy Institute (NEI),³ on behalf of its members, is submitting the attached white paper proposing changes to NEI 10-04 and NEI 13-10 for NRC review and endorsement. The attached white paper addresses the NRC comments in its letter dated July 14, 2020.⁴ The changes in this white paper improve the screening of digital computer and communication systems and networks associated with the

¹ ADAMS Accession No. ML12194A532

² ADAMS Accession No. ML17240A002

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

⁴ ADAMS Accession No. ML20195B113

Mr. Russell Felts

July 23, 2020

Page 2

balance of plant (BOP) at nuclear power reactors. The BOP will remain within scope of the NRC's cyber security rule and other related NRC requirements.

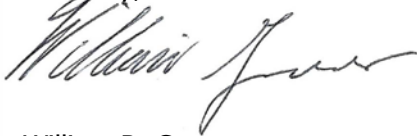
The intent of this white paper is to clarify the screening of Cyber Security Program digital assets associated with BOP and does not change the scoping of digital assets that impact plant reactivity for inclusion into the Cyber Security Program, as required by 10CFR 73.54(a)(1). BOP digital assets that do meet the definition for important-to safety functions in the BOP (whose compromise would result in an unplanned reactor shutdown or transient with the generated megawatts being reduced to zero within 15 minutes) do need to be further screened in NEI 13-10 to determine what cyber security protections are needed.

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

NEI requests that the NRC review and endorse the NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Balance of Plant," dated July 2020, by August 30, 2020. While each licensee must review changes to their Commission- approved Cyber Security Plan in accordance with the requirements of 10 CFR 50.54(p), NEI requests that the NRC's review confirm that the changes proposed in this white paper do not decrease the effectiveness of the cyber security plan provided in NEI 08-09. If any revisions to this document are desired, please include suggested wording and the technical data to support the proposed change(s).

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

Sincerely,

A handwritten signature in black ink, appearing to read "William R. Gross", written over a light blue horizontal line.

William R. Gross

Attachment

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

1 INTRODUCTION

1.1 PURPOSE

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

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

The enhancement to the guidance documents will ensure the BOP CDAs remain within scope of the NRC’s cyber security rule and other related NRC requirements; and, align the implementation of cyber security requirements with requirements applicable to non-nuclear generators.

1.2 BACKGROUND

Title 10 of the Code of Federal Regulations (CFR), Part 73, “Physical Protection of Plants and Materials,” § 73.54, “Protection of Digital Computer and Communication Systems and Networks,” requires power reactor licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the design basis threat as described in § 73.1, “Purpose and scope.” Through implementation of the cyber security plans and programs required by § 73.54, the industry has identified several lessons learned that warrant an assessment and revision of the guidance in NEI 10-04, Revision 2, and NEI 13-10, Revision 6. This white paper describes proposed changes to NEI 10-04, Revision 2 and NEI 13-10, Revision 6, that would support more efficient performance of cyber security program activities and oversight and promote consistent implementation of the requirements of 10 CFR 73.54.

2 DISCUSSION

When the cyber security rule (10 CFR 73.54) was initially issued, it did not extend to the BOP. In 2010, the NRC expanded the scope of the cyber security rule to cover the BOP to ensure a single regulator (the NRC) for cyber security at Nuclear Power Plants (NPP). In response, the Federal Energy Regulatory Commission (FERC) issued Order No. 706-B to clarify that the BOP systems and equipment within an NPP that are not within the scope of 10 CFR 73.54 are subject to compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standard approved in Order No. 706.

NEI 10-04 and NEI 13-10 were developed to be generally aligned with the NERC CIPs that were in place at that time. However, since that time, the NERC CIPs have evolved to

incorporate a graded approach based upon risk-based impact to the Bulk Electric System (BES). NEI 10-04 and 13-10 currently require application of cyber security controls regardless of the loss of the generator's impact on the BES. This paper seeks to incorporate the same risk-based methodology into the NRC's cyber security program to ensure licensees are protecting BOP assets at a level commensurate with the plant's risk to the reliability of the BES associated with non-nuclear generators.

In NRC SECY 10-0153, the NRC staff identified the SSCs in the BOP that have a nexus to radiological health and safety are those that could directly or indirectly affect reactivity of an NPP and are therefore within the scope of important-to-safety functions described in the cyber rule. That wording was captured in current cyber security program guidance, NEI 10-04, and has resulted in a considerable number of digital assets being identified as in scope.

Each licensee has interpreted the meaning of affecting reactivity contained in the current definition of a BOP CDA in NEI 10-04 differently. The interpretation by licensees of the meaning of 'affecting reactivity' has varied from 'any transient resulting in >20% reactor thermal power change' to the conservative position of 'any uncontrolled change in reactor thermal power.' The result of the more conservative interpretation was the incorporation of more digital assets under the Cyber Security Rule beyond what non-nuclear generation facility covers under the current NERC Critical Infrastructure Protection (CIP) Standards. Also, the NERC CIP standards have migrated from a fixed set of protection standards for applying cyber controls to the application of cyber controls based upon the level of impact the facility has on the BES.

The licensees with a conservative interpretation, under the proposed guidance, will be able to reduce the number of BOP CDAs covered by the Cyber Security Rule that truly do not result in the separation of the unit from the BES. The reduction in the number of BOP CDAs will allow the focusing of a licensee's resources on BOP CDAs that have a significant impact on the facility and BES. All licensees will be able to credit the protection provided by their Protective Area, as well as the BOP CDAs that are protected by being in isolated networks or behind a one-way deterministic device. Crediting these protections will allow the nuclear industry Cyber Security Programs to align to the same level of protection the non-nuclear generators apply under the current NERC CIP Standards.

The current NERC CIP Reliability Standard 002-5.1a and Glossary of Terms Used in NERC Reliability Standards defines when a BES Cyber System or Asset has an impact to the BES within 15 minutes of the system or asset being compromised. The Glossary of Terms defines a transient period and adding the 15 minutes time period to the definition in the NEI documents imposes the intended level of risk outlined in the NERC requirements. Defining the time period of the transient will not alter the underlying nuclear safety of the definition of BOP CDAs. The statements within NEI 10-04, Revision 2, and NEI 13-10, Revision 6, that define a BOP system or BOP CDA will need to be amended to incorporate the statement; **"with the generated megawatts being reduced to zero within 15 minutes."** The statement of what is considered to have an impact on the BES based upon an unplanned reactor shutdown or transient, provides clarification that is consistent with guidance in the NERC CIP Reliability Standards.

The current NERC CIP Reliability Standard 002-5.1a defines how digital assets are categorized

based on their impact to the BES and NERC CIP Reliability Standard 003-7, Security Management Controls, identifies what cyber security controls are applied based upon the level of risk to the BES.

The current criterion in NEI 13-10 will need to be modified to identify the level of risk to the BES and will be divided into three categories of LOW, MEDIUM and HIGH. The criteria for HIGH plants is defined as a loss of greater than 3000 MWe to the BES; the criteria for MEDIUM plants is defined as a loss of greater than 1500 MWe to the BES or meeting specific exceptions (as outlined in Section 3.2 of this document); and the criteria for LOW plants is that it does not meet the criteria of MEDIUM or HIGH.

Per NERC Standard IRO-008-2, Reliability Coordinator Operational Analyses and Real-Time Assessment, the Reliability Coordinator (i.e., MISO, PJM) will perform and maintain the analyses related to the three categories above, as well as the specific exceptions for MEDIUM plants. A Reliability Coordinator will notify impacted Transmission Operators and Balancing Authorities of system operating limits or Interconnection Reliability Operating Limits (IROLs). The NPPs are notified or can obtain information through Nuclear Plant Interface Requirements (NPIRs) (also referred to as Service Level Agreement) which is required under the NERC Standard NUC-001-3, Nuclear Plant Interface Coordination. Thus, each NPP (this includes sites with multiple plants) should have already been notified under their NPIR of their category and whether they meet any of the specific exception criteria and will be notified by their Transmission Operator should there be an issue in the future.

The application of the CIP categories (LOW, MEDIUM or HIGH) to NEI 13-10 will result in most NPP's Cyber Systems fitting into the LOW Impact category, however, some NPPs may fit into the MEDIUM or HIGH Impact categories. Therefore, consistent with NERC CIP Standards, most BOP CDAs would be protected by the following current NRC required programmatic controls contained in NEI 08-09, Revision 6 and other NRC required processes:

- CIP - Cyber Security Awareness; NRC - Control E.9, Training
- CIP - Physical Security Controls; NRC - Control E.5, Physical Protection
- CIP - Electronic Access Controls; NRC - Air gapped or isolated by a deterministic device
- CIP - Cyber Security Incident Response; NRC - Control E.7, Attack Mitigation and Incident Response
- CIP - Transient Cyber Assets and Removable Media malicious code risk mitigation: NRC - PMD Program – D.1.19, Access Control for Portable and Mobile Devices
- CIP - Declaring and responding to CIP Exceptional Circumstances; NRC - Emergency Operating Procedures, Abnormal Operating Procedures, Emergency Preparedness Plan and Physical Security Plan - Required by NRC regulations

NPPs fitting into the MEDIUM or HIGH Impact category will need to apply the cyber security controls found in criteria a through g of NEI 13-10, Revision 6, Section 5, Baseline Cyber Security Protection Criteria (Baseline Controls) to BOP CDAs.

Based upon the comparison of the current NERC CIP Standards to the cyber security controls of NEI 13-10, Section 5, Baseline Cyber Security Protection Criteria; the NEI 08-09, Appendix E programmatic controls; and other programmatic processes required by other regulatory requirements for an NPP licensed under 10 CFR 50, the Industry believes the CIP Reliability Standards for MEDIUM and HIGH impact BES Cyber Assets are met as noted above, and the current NEI 13-10, Section 5.1 additional controls would not be needed for the BOP-Scram/Trip CDAs and thus, Section 5.1 can be deleted.

The Baseline Controls of Section 5, a through g would be applied to any BOP CDAs, whether LOW, MEDIUM, or HIGH Impact categories, that are not air gapped or isolated by a deterministic isolation device, or not within the PA.

3 REGULATORY BASIS FOR CHANGE

3.1 CHANGES TO NEI 10-04, REVISION 2

For cyber security control purposes, the category of BOP was created based upon an agreement between the FERC and NRC. FERC issued Order No. 706, which specified Critical Infrastructure Protection (CIP) Reliability Standard to safeguard critical cyber assets. Order No. 706 specifically exempted “facilities regulated by the NRC” from these requirements.

The electric power industry’s implementation of the cyber rule over the last ten years have found that NERC’s CIP Reliability Standards have become more risk informed. Today’s NERC guidance is based upon risk-based impact to the bulk electric system that is outlined in CIP 002- 5.1a, Cyber Security – Bulk Electric System (BES) Cyber System Categorization and Glossary of Terms Used in NERC Reliability Standards. A BES Cyber Asset has been defined as:

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

To ensure consistency with the NERC CIP Reliability Standards, clarification is needed as to what constitutes an “unplanned reactor shutdown or transient.” For a Generator Owner/Operator, it is an event that results “generated megawatts being reduced to zero within 15 minutes.” Providing clarification of what constitutes an unplanned reactor shutdown or transient does not reduce the level of cyber security protection required by each NPP Cyber Security Plan or 10CFR73.54.

In summary, it was determined from this evaluation process that:

1. This change does not delete or contradict any of the regulatory requirements. This change does

not decrease the safeguards effectiveness of the Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and/or Cyber Security Plan.

2. This change does not decrease the overall level of Cyber Security system performance as described in paragraph (a) through (h) of 10 CFR 73.54 to provide reasonable assurance of protection against the design basis threat of radiological sabotage as stated in 10 CFR 73.1(a).
3. This change does not decrease the overall level of Cyber Security system performance needed to protect with the objective of reasonable assurance against the design basis threat of radiological sabotage as stated in 10 CFR 73.1(a).

The change is described in sufficient detail. There is also a sufficient description of how requirements are implemented through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks. Site-specific conditions that affect how the licensee implements Commission requirements have also been evaluated.

3.2 CHANGES TO NEI 13-10, REVISION 6

For cyber security control purposes, the category of BOP was created based upon an agreement between FERC and NRC. FERC issued Order No. 706, which specified CIP Reliability Standard to safeguard critical cyber assets. Order No. 706 specifically exempted “facilities regulated by the NRC” from these requirements. It was later determined that this exemption created a potential gap between NRC and FERC cyber security requirements as they apply to NPPs because the NRC staff interpreted the agency’s cyber security regulation, 10 CFR 73.54, published in March 2009, to require the protection of digital systems that, if compromised, could directly or indirectly result in radiological sabotage.”

The electric power industry’s implementation of the cyber rule over the last ten years has evolved and NERC’s CIP Reliability Standards have changed. Today’s NERC guidance is based upon risk-based impact to the bulk electric system that is outlined in CIP 002-5.1a, Cyber Security – Bulk Electric System (BES) Cyber System Categorization and Glossary of Terms Used in NERC Reliability Standards. A BES Cyber Asset has been defined as:

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

To ensure consistency with the NERC CIP Reliability Standards, clarification is needed as to what constitutes an “unplanned reactor shutdown or transient” based upon the NERC’s CIP Reliability Standards. For a Generator Owner/Operator, it is an event that results “generated

megawatts being reduced to zero within 15 minutes.”

The requirements of NERC CIP Reliability Standard 002-5.1a and NERC CIP Reliability Standard 003-7, Security Management Controls, affects how BOP CDAs are categorized for their impact to the BES and what cyber security controls are applied based upon the level of risk to the BES. The current criterion in NEI 13-10 will need to be modified to identify the level of risk and will be divided into three categories of LOW, MEDIUM and HIGH to classify an NPP. The criteria for MEDIUM and HIGH are defined (see below), and the criteria for LOW is any NPP that is not MEDIUM or HIGH.

The criteria under CIP Reliability Standard 002-5.1a for MEDIUM and HIGH use the same criteria except a MEDIUM impact is a loss of greater than 1500 MWe to the BES and a HIGH impact is a loss greater than 3000 MWe. The criteria are as follows:

- Aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding the MWe loss 1500 or greater in a single Interconnection.
- Determined through system studies that a unit must run in order to preserve the reliability of the BES.
- BES Cyber Systems for those generation facilities that have been identified as critical to the derivation of Interconnection Reliability Operating Limits¹ (IROLs) and their associated contingencies. IROLs may be based on dynamic system phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and Automatic Voltage Regulator response.
- BES Cyber Systems for Special Protection Systems and Remedial Action Schemes that may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed.

¹ Interconnection Reliability Operating Limits (IROLs) is defined by the NERC Glossary of Terms as “A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System.”

The cyber security controls outlined in CIP Reliability Standard 003-7 were used to identify which cyber security controls are to be applied to BOP CDAs and BOP-Scram/Trip CDAs. The application of the CIP categories to NEI 13-10 resulted in most NPP’s BES Cyber Systems fitting into the LOW impact category. These NPPs will identify their BES Cyber System CDAs as “BOP CDAs.” An NPP whose BES Cyber Systems meet the MEDIUM or HIGH impact criteria on the BES will identify their BES Cyber System CDAs as “BOP-Scram/Trip CDAs.”

BOP CDAs would need at the least the cyber security controls required for a LOW impact category BES Cyber Asset applied (e.g., CIP 003-7, Physical Security, Electronic Access, Cyber Security Incident Response, Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation and Declaring and Responding to CIPP Exceptional Circumstances). The BOP CDAs would be protected by the current NRC required programmatic controls contained in NEI 08-09,

Revision 6 and other NRC required processes. The following is a comparison of CIP controls to NRC required controls that meet or exceed the NERC CIP Standards:

- Cyber Security Awareness; Control E.9, Training
- Physical Security Controls; Located in the PA or VA or protected per Control E.5, Physical Protection
- Electronic Access Controls; Air gapped or isolated by a deterministic device
- Cyber Security Incident Response; Control E.7, Attack Mitigation and Incident Response
- Transient Cyber Assets and Removable Media malicious code risk mitigation: PMD Program; D.1.19, Access Control for Portable and Mobile Devices; D.1.19, Access Control for Portable and Mobile Devices
- Declaring and responding to CIP Exceptional Circumstances; Emergency Operating Procedures, Abnormal Operating Procedures, Emergency Preparedness Plan and Physical Security Plan; Required by NRC regulations

BOP-Scram/Trip CDAs will need the controls required for a MEDIUM and HIGH impact BES Cyber Asset applied. These can be addressed by applying criteria a through g of the NEI 13-10, Revision 6, Section 5, Baseline Cyber Security Protection Criteria (Baseline Controls).

Below is a comparison of the CIP Reliability Standards required in CIP Reliability Standard 003-7 for MEDIUM and HIGH impact to BES Cyber Assets to the NEI 13-10 Section 5 Baseline Cyber Security Protection Criteria, the NEI 08-09, Appendix E programmatic controls and other programmatic processes required by other regulatory requirements for an NPP licensed under 10 CFR 50:

- Personnel and Training (CIP-004)
 - Baseline control (a) requires that the CDA be in the Protected Area (PA) or Vital Area (VA), or protected per control E.5, Physical Protection. These controls exceed the requirements of CIP-004 by denying terminated personnel physical access to a CDA on which they may have an account. Unescorted access to the PA meets or exceeds the CIP-004 requirements.
 - The common programmatic control E.4, Maintenance, meets or exceeds the requirements of CIP-004.
 - The common programmatic control E.7, Attack Mitigation and Incident Response, meets or exceeds the requirements of CIP-004.
 - The common programmatic control E.8, Cyber Security Contingency Plan (Continuity of Operations), meets or exceeds the requirements of CIP-004.
 - The common programmatic control E.9, Training, meets or exceeds the requirements of CIP-004.
- Electronic Security Perimeters including Interactive Remote Access (CIP-005)
 - Baseline control (a) requires that the CDA be in the Protected Area (PA) or Vital Area (VA), or protected per control E.5, Physical Protection. These controls exceed the requirements of CIP-005 by denying physical access to a CDA. Unescorted access to the PA meets or exceeds the CIP-005 requirements.
 - Baseline control (b) requires that the CDA and any interconnected assets do not have wireless technologies. The control meets or exceeds the requirements of CIP-005

which assumes that the CDA has some level of two-way communications with the internet.

- Baseline control (c) requires that the CDA be air gapped or isolated by a deterministic device. The control meets or exceeds the requirements of CIP-005 which assumes that the CDA has some level of two-way communications with the internet.
- Physical Security Controls (CIP-006)
 - Baseline control (a) requires that the CDA be in the PA or VA, or protected per control E.5, Physical Protection. These controls meet or exceed the requirements of CIP-006 in denying physical access of unauthorized individuals to a CDA.
 - Refer to Attachment 5, Comparison of NERC CIP 006-6, Cyber Security – Physical Security of BES Cyber Systems, for MEDIUM Impact Cyber Assets to Nuclear Industry Cyber Security Controls, for a more detailed comparison.
- System Security Management (CIP-007)
 - Baseline control (a) requires that the CDA be in the PA or VA, or protected per control E.5, Physical Protection. These controls meet or exceed the requirements of CIP-007 in denying physical access of unauthorized individuals to a CDA.
 - Baseline control (b) requires that the CDA and any interconnected assets do not have wireless technologies. The control meets or exceeds the requirements of CIP-007 which assures that logical access cannot be establish outside of the facility.
 - Baseline control (c) requires that the CDA be air gapped or isolated by a deterministic device. The control meets or exceeds the requirements of CIP-007 which assures that logical access cannot be establish outside of the facility.
 - Baseline control (d) requires that the CDA be protected under the Access Control for Portable and Media Devices. These control meets or exceeds the requirements of CIP-007 by ensuring portable and media devices are scanned prior to being used on a CDA.
 - Baseline control (e) requires that the CDA be evaluated and documented to ensure:
 - Baseline security criteria remain in place and effective.
 - No new pathways or vulnerabilities are created.
 - No change in the CDA to make it Direct.
 - E.12, Evaluate and Manage Cyber Risk, controls are applied.The controls meet or exceed the requirements of CIP-007 which ensures that the CDA vulnerabilities are addressed in a timely manner.
 - Baseline control (g) requires that the CDA is reviewed periodically to ensure security posture is maintained and effective. The control meets or exceeds the requirements of CIP-007.
 - The common programmatic control E.7, Attack Mitigation and Incident Response, meets or exceeds the requirements of CIP-007.
- Incident Reporting and Response Training (CIP-008)
 - Control E.7, Attack Mitigation and Incident Response, control and the Corrective Action Program meet or exceed the requirements of CIP-008.
 - Refer to Attachment 7, Comparison of NERC CIP 008-6, Cyber Security – Incident Reporting and Response Planning, for MEDIUM Impact Cyber Assets to Nuclear Industry Cyber Security Controls, for a more detailed comparison.

- Recovery Plans (CIP-009)
 - The CDA is protected by the following procedures
 - Emergency Operating Procedures
 - Abnormal Operating Procedures
 - Emergency Preparedness Plan
 - Physical Security Plan
 - Engineering Change Program
 - Work Management Program
 - Corrective Action ProgramThese procedures and program ensure the continuity of operation which meets or exceeds the requirements of CIP-009.
- Configuration Change Management and Vulnerability Assessments (CIP-010)
 - Baseline control (a) requires that the CDA be in the PA or VA, or protected per control E.5, Physical Protection. These controls meet or exceed the requirements of CIP-010 in denying physical access of unauthorized individuals to a CDA.
 - Baseline control (d) requires that the CDA be protected under the Access Control for Portable and Media Devices. These controls meet or exceed the requirements of CIP-010 by ensuring portable and media devices are scanned prior to being used on a CDA.
 - Baseline control (e) requires that the CDA be evaluated and documented to ensure:
 - Baseline security criteria remain in place and effective.
 - No new pathways or vulnerabilities are created.
 - No change in the CDA to make it Direct.
 - E.12, Evaluate and Manage Cyber Risk, controls are applied.The controls meet or exceed the requirements of CIP-010 which ensure that the CDA's configuration is tracked and maintained to protect the asset.
 - Baseline control (f) requires that the CDA be periodically checked to ensure that the asset is capable of performing its intended function. The control ensures the CDA configuration is maintained to meet or exceed the requirements of CIP-010.
 - Baseline control (g) requires that the CDA is reviewed periodically to ensure security posture is maintained and effective. The control meets or exceeds the requirements of CIP-010.
- Information Protection (CIP-011)
 - Baseline control (a) requires that the CDA be in the PA or VA, or protected per control E.5, Physical Protection. These controls meet or exceed the requirements of CIP-011 in denying physical access of unauthorized individuals to a CDA.
 - Baseline control (b) requires that the CDA and any interconnected assets do not have wireless technologies. The control meets or exceeds the requirements of CIP-011 which assures that information cannot be downloaded outside of the facility.
 - Baseline control (c) requires that the CDA be air gapped or isolated by a deterministic device. The control meets or exceeds the requirements of CIP-011 which assures that information cannot be establish outside of the facility.
 - Baseline control (d) requires that the CDA be protected under the Access Control for Portable and Media Devices. These controls meet or exceed the requirements of CIP-011 by ensuring portable and media devices are controlled and scanned prior to being used on a CDA.

- Baseline control (e) requires that the CDA be evaluated and documented to ensure:
 - Baseline security criteria remain in place and effective.
 - No new pathways or vulnerabilities are created.
 - No change in the CDA to make it Direct.
 - E.12, Evaluate and Manage Cyber Risk, controls are applied.
The controls meet or exceed the requirements of CIP-011 which ensures that the information on a CDA is maintained properly.
- Baseline control (f) requires that the CDA be periodically checked to ensure that the asset is capable of performing its intended function. The control ensures the CDA configuration is maintained to meet or exceed the requirements of CIP-011.
- Baseline control (g) requires that the CDA is reviewed periodically to ensure security posture is maintained and effective to protect the information. The control meets or exceeds the requirements of CIP-011.
- The common programmatic control E.1, Media Protection, meets or exceeds the requirements of CIP-011.
- Declaring and Responding to CIP Exceptional Circumstances
 - The CDA is protected by the following procedures
 - Emergency Operating Procedures
 - Abnormal Operating Procedures
 - Emergency Preparedness Plan
 - Physical Security Plan
 - Engineering Change Program
 - Work Management Program
 - Corrective Action ProgramThese procedures and programs ensure the continuity of operation which meets or exceeds the requirements of being able to declare and respond to events that are similar to the CIP exceptional circumstances.

Based upon the comparison of the current NERC CIP Standards to the cyber security controls of NEI 13-10, Section 5, Baseline Cyber Security Protection Criteria; the NEI 08-09, Appendix E programmatic controls; and other programmatic processes required by other regulatory requirements for an NPP licensed under 10 CFR 50, the Industry believes the CIP Reliability Standards for MEDIUM and HIGH impact BES Cyber Assets are met as noted above. The current NEI 13-10, Section 5.1 additional controls that were added based upon NERC CIP Standards in 2012 are not needed for the BOP-Scram/Trip CDAs as shown by the comparison above and thus, Section 5.1 can be deleted. The text in Section 5.1 is replaced with “Deleted.”

The Baseline Controls of Section 5, a through g would be applied to BOP CDAs that are not air gapped or isolated by a deterministic isolation device, and not within the PA.

Aligning the cyber security controls that are applied to BOP CDAs and BOP-Scram/Trip CDAs to be consistent with the current NERC CIP Reliability Standard does not constitute a reduction in protection but makes NPPs similar to other Generator Owner/Operators on the BES. Modifying cyber security protection for assets that impact the reliability BES does not compromise the level of cyber protection for those CDAs that are within the scope of 10CFR73.54.

In summary, it was determined from this evaluation process that:

1. This change does not delete or contradict any of the regulatory requirements. This change does not decrease the safeguards effectiveness of the Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and/or Cyber Security Plan.
2. This change does not decrease the overall level of Cyber Security system performance as described in paragraph (a) through (h) of 10 CFR 73.54 to protect with the objective of reasonable assurance against the design basis threat of radiological sabotage as stated in 10 CFR 73.1(a).
3. This change does not decrease the overall level of Cyber Security system performance needed to protect with the objective of reasonable assurance against the design basis threat of radiological sabotage as stated in 10 CFR 73.1(a).

The change is described in sufficient detail. There is also a sufficient description of how requirements are implemented through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks. Site-specific conditions that affect how the licensee implements Commission requirements have also been evaluated.

4 PROPOSED CHANGES TO GUIDANCE

Based upon the revised requirements of the NERC CIP Reliability Standard 002-5.1a, two NEI documents are affected. The guidance in NEI 10-04, Revision 2, Identifying Systems and Assets Subject to the Cyber Security Rule, will need to (1) have the definition of BOP System Structures and Components (SSCs) to relate the current CIP Reliability Standard method for determining an asset, and (2) clarify what could directly or indirectly affect reactivity as it pertains to BOP CDAs. The sections with pages affected are:

- Section 1.1 (Overview of Scoping for the NRC Cyber Security Rule) page 1
- Section 2.1.2 (Important-to-Safety) page 5
- Section 5 (Methodology for Identifying Critical Digital Assets) Page 22

The guidance in NEI 13-10, Revision 6, Cyber Security Control Assessments, will need to have the definition of BOP Critical Digital Assets (CDAs) to relate the current CIP Reliability Standard method for determining an asset. The definitions of BOP system and assets should have the phrase, **“with the generated megawatts being reduced to zero within 15 minutes,”** appended to the end. The criteria for determining whether a CDA is a BOP or BOP-Scram/Trip will need to be modified. The cyber security controls that the BOP and BOP-Scram/Trip CDAs are to be assessed against will need to be amended based on whether the plant falls into the LOW, MEDIUM, or HIGH Impact NERC category. The sections with pages affected are:

- Section 3.2 (BOP CDAs) page 6
- Section 5 (Baseline Cyber Security Protection Criteria) page 11
- Section 5.1 (BOP CDAs That Could Cause a Reactor Scram/Trip) page 12
- Appendix A (Figures) page A-1

- Appendix B (Template) page B-6
- Appendix C (Examples) pages C-8, C18, C-29, C-36, C-44, C-52, and C-60

4.1 PROPOSED CHANGES TO NEI 10-04, REVISION 2

[Proposed changes in redline/strikeout]

- Section 1.1 (Overview of Scoping for the NRC Cyber Security Rule) page 1

NEI 10-04 utilizes the licensee's Current Licensing Basis (CLB) to ascertain important-to-safety functions in the context of the NRC Cyber Security Rule. With regard to balance of plant (BOP) systems, however, the NRC has provided additional guidance on how these systems relate to the important-to-safety function under the Rule. **Additionally, the NERC CIP Reliability Standard 002-5.1a and Glossary of Terms Used in NERC Reliability Standards defines when a Bulk Electric System (BES) Cyber System or Asset has an impact to the BES within 15 minutes of the system or asset being compromised. The Glossary of Terms defines a transient period and adding the 15 minute time period to the definition in the NEI documents establishes an acceptable level of risk that is consistent with the NERC requirements.** Particularly, the NRC has clarified that, for the purposes of the NRC Cyber Security Rule, systems or equipment performing important-to-safety functions include structures, systems, and components in the balance of plant that have a nexus to radiological health and safety or could directly or indirectly affect reactivity.

Specifically, SSCs in the BOP that could result in an unplanned reactor shutdown or transient **with the generated megawatts¹ being reduced to zero within 15 minutes should be identified as BOP CDAs.**

¹The units of "megawatts" refers to megawatts electric unless identified differently.

- Section 2.1.2 (Important-to-Safety) page 5

Accordingly, the scope of the cyber security rule at 10 CFR 73.54 includes SSCs in the Balance of Plant out to the first inter-tie with the offsite distribution system that could result in an unplanned reactor shutdown or transient. **An "unplanned reactor shutdown or transient" consistent with the definitions in NERC's CIP Reliability Standards, is defined as an event that results in the generated megawatts being reduced to zero within 15 minutes.**

- Section 5 (Methodology for Identifying Critical Digital Assets) Page 22

b) Important-to safety functions in the Balance of Plant whose compromise would result in an unplanned reactor shutdown or transient **with the generated megawatts being reduced to zero within 15 minutes;**

4.2 FINAL LANGUAGE TO NEI 10-04

- (Last paragraph on page 1)

NEI 10-04 utilizes the licensee's Current Licensing Basis (CLB) to ascertain important-to-safety functions in the context of the NRC Cyber Security Rule. With regard to balance of plant (BOP) systems, however, the NRC has provided additional guidance on how these systems relate to the important-to-safety function under the Rule. Additionally, the NERC CIP Reliability Standard 002-5.1a and Glossary of Terms Used in NERC Reliability Standards defines when a Bulk Electric System (BES) Cyber System or Asset has an impact to the BES within 15 minutes of the system or asset being compromised. The Glossary of Terms defines a transient period and adding the 15 minutes time period to the definition in the NEI documents imposes the intended level of risk outlined in the NERC requirements. Particularly, the NRC has clarified that, for the purposes of the NRC Cyber Security Rule, systems or equipment performing important-to-safety functions include structures, systems, and components in the balance of plant that have a nexus to radiological health and safety or could directly or indirectly affect reactivity and could result in an unplanned reactor shutdown or transient with the generated megawatts¹ being reduced to zero within 15 minutes should be identified as BOP CDAs.

¹The units of "megawatts" refers to megawatts electric unless identified differently.

- (First full paragraph on page 5)

Accordingly, the scope of the cyber security rule at 10 CFR 73.54 includes SSCs in the Balance of Plant out to the first inter-tie with the offsite distribution system that could result in an unplanned reactor shutdown or transient. An "unplanned reactor shutdown or transient" consistent with the definitions in NERC's CIP Reliability Standards, is defined as an event that results in the generated megawatts being reduced to zero within 15 minutes.

- (At the bottom of page 22 and top of page 23)

A digital device should be identified as a Critical Digital Asset (CDA) if it performs:

- a) SSEP functions or whose compromise would adversely impact a SSEP function;
- b) Important-to safety functions in the Balance of Plant whose compromise would result in an unplanned reactor shutdown or transient with the generated megawatts being reduced to zero within 15 minutes;
- c) Support functions (e.g., primary or back-up power, HVAC, fire protection, etc.) whose compromise would adversely impact a SSEP function; or
- d) Network boundary isolation, protection, or detection/prevention monitoring functions for CDAs as described in Section 4.3, "Defense-in-Depth Protective Strategies," of the licensee's Cyber Security Plan.

4.3 PROPOSED CHANGES TO NEI 13-10, REVISION 6

- Section 3.2 (BOP CDAs) page 6

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 **a transient with the generated megawatts¹ being reduced to zero within 15 minutes?**

¹The units of “megawatts” refers to megawatts electric unless identified differently.

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 **including what is defined by the NERC’s CIP Reliability Standards as an event that results in the generated megawatts being reduced to zero within 15 minutes.** 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 identify 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~~ **is** 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 in Section 3.3, 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)~~ **that can result in the generated megawatts being reduced to zero within 15 minutes.** 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: (facilities with LOW Impact on the BES) are associated with the administrative controls of:**

- **Cyber Security Awareness; Control E.9, Training**
- **Physical Security Controls; Control E.5, Physical Protection**
- **Electronic Access Controls; Air gapped or isolated by a deterministic device**
- **Cyber Security Incident Response; Control E.7, Attack Mitigation and Incident Response**

- **Transient Cyber Assets and Removable Media malicious code risk mitigation: PMD Program; D.1.19, Access Control for Portable and Mobile Devices**
- **Declaring and responding to CIP Exceptional Circumstances; Emergency Operating Procedures, Abnormal Operating Procedures, Emergency Preparedness Plan and Physical Security Plan; Required by NRC regulations**

Based upon the risk to the Bulk Electric System (BES) that some stations may possess, all or a portion of the BOP CDAs may be classified as BOP-Scram/Trip CDAs (facilities with MEDIUM or HIGH Impact on the BES) due to meeting one of the following criteria:

- **Aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding the loss of 1500 MWe or greater in a single Interconnection.**
- **Determined through System studies that a unit must run in order to preserve the reliability of the BES.**
- **BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of Interconnection Reliability Operating Limits¹ (IROLs) and their associated contingencies. IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and Automatic Voltage Regulator response.**
- **BES Cyber Systems for Special Protection Systems and Remedial Action Schemes that may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed.**
- **BOP CDAs that are not air gapped or isolated by a deterministic isolation device, or not within the PA.**

¹ Interconnection Reliability Operating Limits (IROLs) is defined by the NERC Glossary of Terms as “A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System.”

Those BOP CDAs that are classified BOP-Scram/Trip CDAs will have the Baseline Cyber Security Protection Criteria discussed in Section 5 applied to protect the assets at the same level as the FERC regulated Generator Operators/Owners.

~~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.~~

- Section 5 (Baseline Cyber Security Protection Criteria) page 11

Where a licensee chooses to credit these baseline cyber security controls for an Indirect, BOP-**Scram/Trip**, 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-**Scram/Trip** CDA or Indirect CDA may be considered to be adequately protected from cyber attacks if all of the following baseline criteria are met

- Section 5.1 (BOP CDAs That Could Cause a Reactor Scram/Trip) page 12

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):-~~

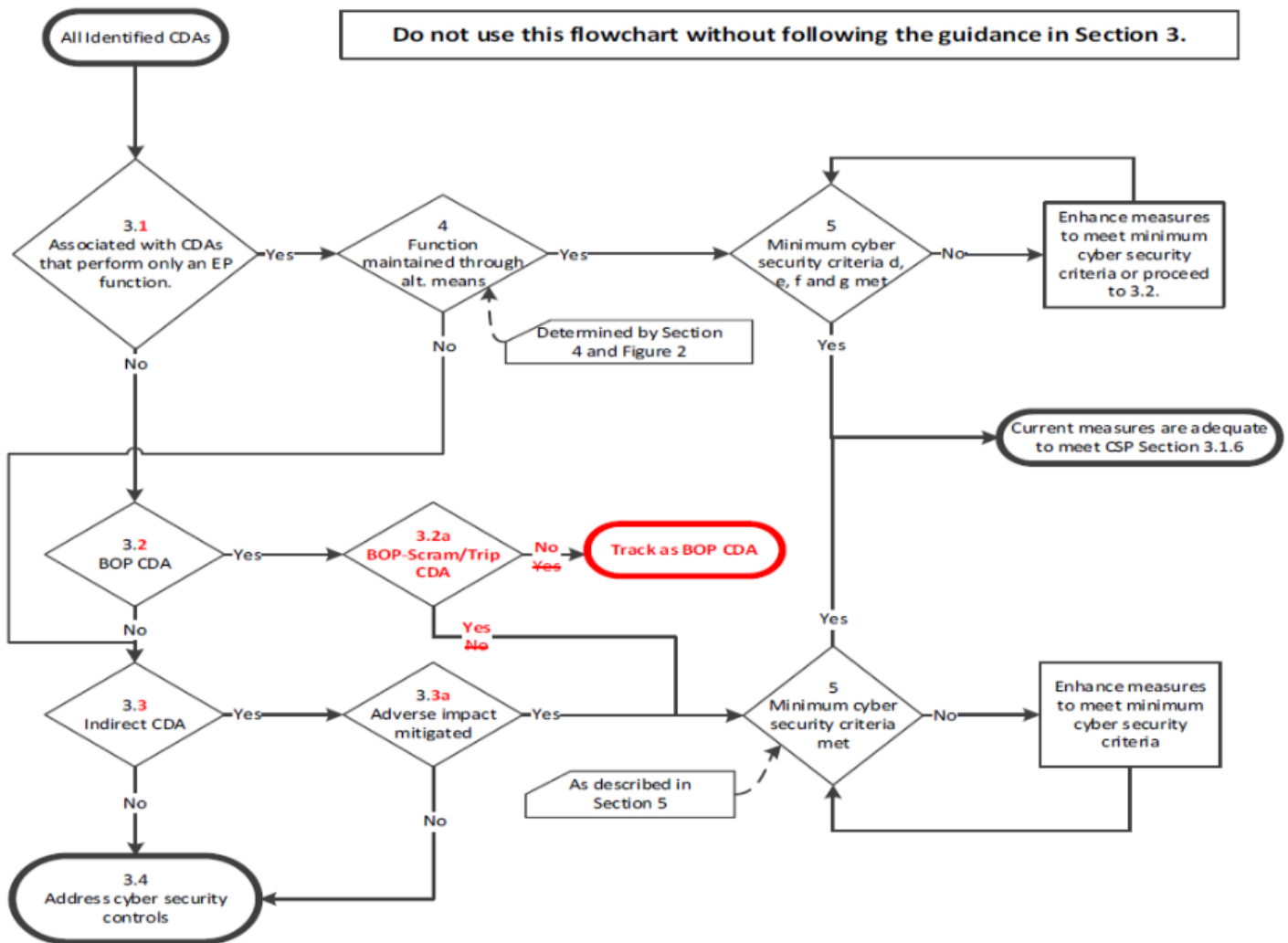
~~D.1.2, "Account Management" D.1.6, "Least Privilege"~~

~~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"~~

- Appendix A (Figures) page A-1



- Appendix B (Template) page B-6

2.0 Figure 1, Box 3.2 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 **as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.**

2.1 Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.

~~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”~~

IF YES, THEN Proceed to Step 3.2

IF NO, THEN END ASSESSMENT HERE.

- Appendix C (Example) pages C-8, C-18, C-29, C-36, C-44, C-52, and C-60

Modify each of the Examples to accommodate the changes of Appendix B (Template).

4.4 FINAL LANGUAGE FOR NEI 13-10, REVISION 6

- Section 3.2 starting on page 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 of 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 a transient with the generated megawatts¹ being reduced to zero within 15 minutes?
6. Is this a non-safety system required to maintain defense-in-depth and diversity requirements?

¹The units of “megawatts” refers to megawatts electric unless identified differently.

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 including what is defined by the NERC’s CIP Reliability Standards as an event that results in the generated megawatts being reduced to zero within 15 minutes. 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 identify 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 is 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 in Section 3.3, as described below.

The language added to the CSPs (and reflected in Question 5) includes a set of BOP CDAs that are of interest to FERC that can result in the generated megawatts being reduced to zero within 15 minutes. BOP CDAs (facilities with LOW Impact on the BES) are associated to the administrative controls of:

- Cyber Security Awareness; Control E.9, Training
- Physical Security Controls; Control E.5, Physical Protection
- Electronic Access Controls; The CDA and any interconnect assets are air gapped or isolated by a deterministic device
- Cyber Security Incident Response; Control E.7, Attack Mitigation and Incident Response
- Transient Cyber Assets and Removable Media malicious code risk mitigation: PMD Program; D.1.19, Access Control for Portable and Mobile Devices
- Declaring and responding to CIP Exceptional Circumstances; Emergency Operating Procedures, Abnormal Operating Procedures, Emergency Preparedness Plan and Physical Security Plan; Required by NRC regulations

Based upon the risk to the Bulk Electric System (BES) that some stations may possess, all or a portion of the BOP CDAs that can be classified as BOP-Scram/Trip CDAs (facilities with MEDIUM or HIGH Impact on the BES) due to meeting one of the following criterion:

- Aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding the loss of 1500 MWe or greater in a single interconnection.
- Determined through System studies that a unit must run in order to preserve the reliability of the BES.
- BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies. IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and Automatic Voltage Regulator response.
- BES Cyber Systems for Special Protection Systems and Remedial Action Schemes that may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed.
- BOP CDAs and any interconnected assets that are not air gapped or isolated by a deterministic isolation device, or are not within the PA.

Those BOP CDAs that are classified BOP-Scram/Trip CDAs will have the Baseline Cyber Security Protection Criteria discussed in Section 5 applied to protect the assets at the same level as the FERC regulated Generator Operators/Owners.

- Section 5 and 5.1 on pages 11 and 12

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 reasonable 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.

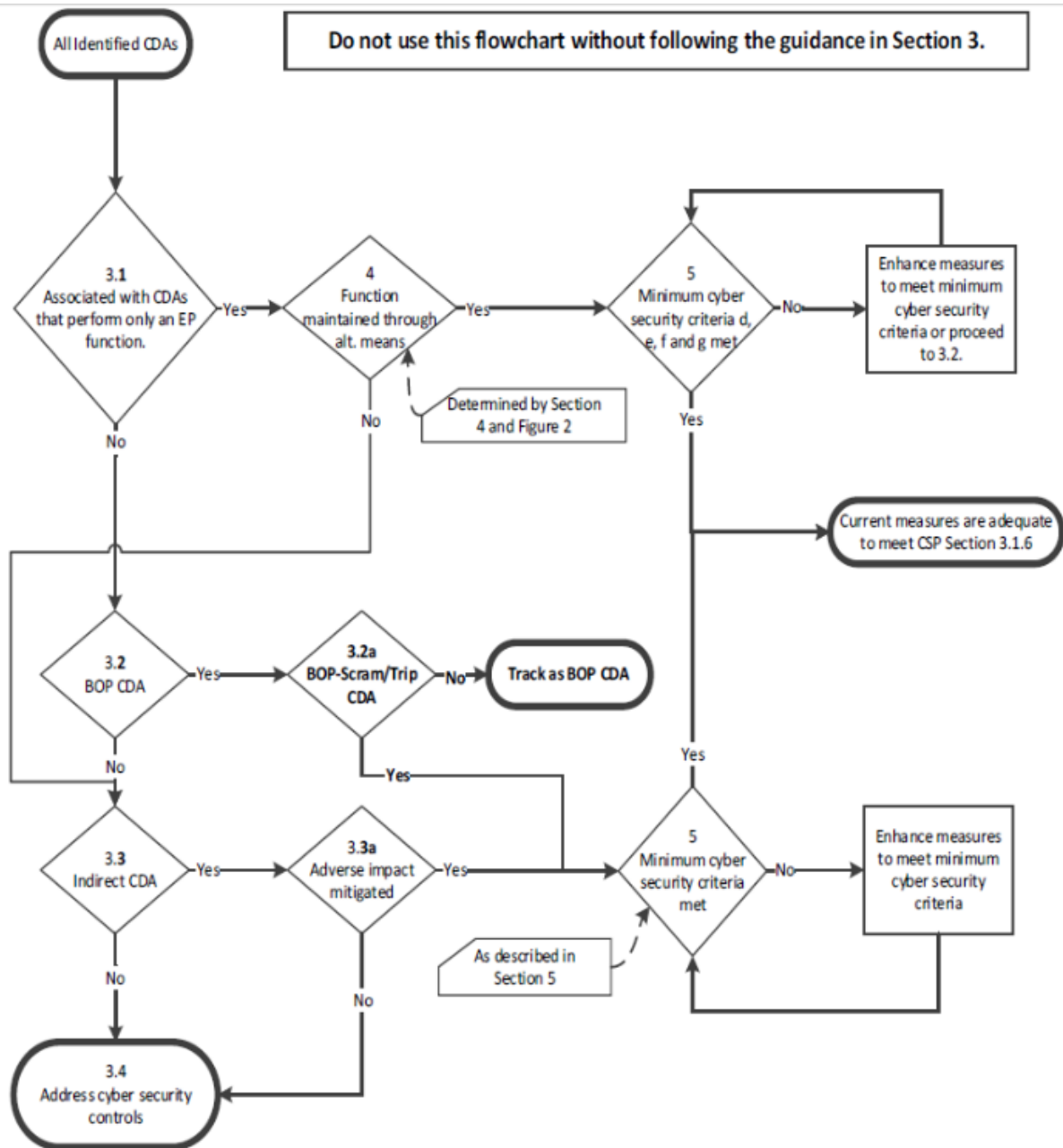
Where a licensee chooses to credit these baseline cyber security controls for an Indirect, BOP-Scram/Trip, or EP CDA, the licensee must confirm these baseline minimum controls criteria are met. EP CDAs may be considered to be adequately protected from cyber attacks if baseline criteria d, e, f, and g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

(Appendix A, page A-1)



(Appendix B, page B-6)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input type="checkbox"/> NO
<p><u>Note:</u> 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.</p>		
<p><u>IF YES, THEN</u> proceed to Step 2.1 <u>IF NO, THEN</u> proceed to Step 3.0</p>		
2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If YES	IF YES, THEN <u>Proceed</u> to Step 3.2	
If NO	THEN END ASSESSMENT HERE.	

(Appendix C, page C-8)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input type="checkbox"/> NO
<p><u>Note:</u> 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.</p>		
<p><u>IF YES, THEN</u> proceed to Step 2.1 <u>IF NO, THEN</u> proceed to Step 3.0</p>		
2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If YES	IF YES, THEN <u>Proceed</u> to Step 3.2	
If NO	THEN END ASSESSMENT HERE.	

(Appendix C, page C-18)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input type="checkbox"/> NO
<p><u>Note:</u> 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.</p>		
<p><u>IF YES, THEN</u> proceed to Step 2.1 <u>IF NO, THEN</u> proceed to Step 3.0</p>		
2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If YES	IF YES, THEN <u>Proceed</u> to Step 3.2	
If NO	THEN END ASSESSMENT HERE.	

(Appendix C, page C-29)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input type="checkbox"/> NO
<p><u>Note:</u> 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.</p>		
<p><u>IF YES, THEN</u> proceed to Step 2.1 <u>IF NO, THEN</u> proceed to Step 3.0</p>		
2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If YES	IF YES, THEN <u>Proceed</u> to Step 3.2	
If NO	THEN END ASSESSMENT HERE.	

(Appendix C, page C-36)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<p><u>Note:</u> 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.</p>		
<p>IF YES, <u>THEN</u> proceed to Step 2.1</p>		
<p>IF NO, <u>THEN</u> proceed to Step 3.0</p>		
2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If YES	IF YES, THEN <u>Proceed</u> to Step 3.2	
If NO	THEN END ASSESSMENT HERE.	

(Appendix C, page C-44)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<p><u>Note:</u> 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.</p>		
<p>IF YES, <u>THEN</u> proceed to Step 2.1</p>		
<p>IF NO, <u>THEN</u> proceed to Step 3.0</p>		
2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If YES	IF YES, THEN <u>Proceed</u> to Step 3.2	
If NO	THEN END ASSESSMENT HERE.	

(Appendix C, Page C-49)

CDA Number: 1C34K0693 CDA Description: FIELDBUS COMMUNICATION MODULE BP #1/SL

The FCM1 OE Fieldbus Communications Module allows Fieldbus Modules (FBMs) to communicate with the CP60 control station via the redundant 10 Mbps Ethernet trunk Fieldbus. The FCM1OE converts 10 Mbps Ethernet signals used by the CP60 control station to 2 Mbps HDLC signals used by Fieldbus Modules (FBMs), and vice versa. The FCM1 OE also provides galvanic isolation between the 10 Mbps Ethernet trunk Field bus and the 2 Mbps module Field bus. The FCM1 OE modules are used in pairs for redundancy. A FCM1 OE (or pair of FCM1OE modules) can support up to 32 FBMs.

The communications modules perform the same function as the interface between the FBMs and CP60s via RS 485 and therefore can be assessed as a group.

(Appendix C, page C-52)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<p><u>Note:</u> 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.</p> <p>The purpose of the Digital Feedwater Control System (DFWCS) is to maintain adequate water level in the reactor vessel based on the demand requirements of the mode of operation to maintain adequate reactor core coverage over the entire power range of the reactor. This is accomplished by controlling the Motor Feed pump and Reactor Feed pump Turbines rate of flow to the vessel.</p> <p>The Fieldbus Communication Modules (FCMs) function is the interface field signals and communicate device between the FBMs and the Controllers (CP60s) of the Foxboro I/A platform. These devices are housed on the same rack as the FBMs.</p> <p>If the FCMs were compromised it could actuate or prevent an actuation as specified above that could result in a transient, and or Turbine/Reactor Trip. However, this result does not impact a Safety or Security function. The interfaces DFWCS has with other systems would not prevent or impact a safety function.</p> <ol style="list-style-type: none"> 1. The DFWCS is a non-safety related system whose failure does not adversely impact any of the functions identified in the three "Safety Systems" questions. 2. The DFWCS is a non-safety related system that is not 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. The DFWCS does not have an operating experience or a probabilistic risk assessment showing that a non-safety related system function is significant to public health and safety. 4. The DFWCS does not perform a 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. The DFWCS is 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 (1) an unplanned reactor shutdown or (2) a transient with the generated megawatts being reduced to zero within 15 minutes. 6. The DFWCS is a non-safety system that is not required to maintain defense-in-depth and diversity requirements. 		
IF YES, <u>THEN</u> proceed to Step 2.1		IF NO, <u>THEN</u> proceed to Step 3.0

April 2020

2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
If YES	<p>IF YES, THEN <u>Proceed</u> to Step 3.2</p> <ul style="list-style-type: none"> • The impact results in the loss of less than 1500 MWe in a single interconnection. • The Distribution System Operator has determined through System studies that the unit is not required to run in order to preserve the reliability of the Bulk Electric System. • The Distribution System Operator has reviewed the Interconnection Reliability Operating Limits (IROLs) and their associated contingencies, and has determined the unit is not critical to the IROLs. • The Distribution System Operator has determined for Special Protection Systems and Remedial Action Schemes that may be implemented to prevent disturbances of the unit would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed. • BOP CDA is isolated by a deterministic isolation device, and within the PA. 	
If NO	THEN END ASSESSMENT HERE.	

(Appendix C, page C-60)

2.0	Figure 1, Box 3.2 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 as to why the CDA will cause generated megawatts to reduce to zero within 15 minutes or less.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
<p><u>Note:</u> 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.</p>		
<p><u>IF YES, THEN</u> proceed to Step 2.1 <u>IF NO, THEN</u> proceed to Step 3.0</p>		
2.1	Figure 1, Box 3.2a Is the CDA a BOP-Scram/Trip CDA as described in Section 3.2? Document why the CDA meets the BOP-Scram/Trip Criteria in Section 3.2.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If YES	IF YES, THEN <u>Proceed</u> to Step 3.2	
If NO	THEN END ASSESSMENT HERE.	