WILLIAM R. GROSS
Director, Incident Preparedness

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

NUCLEAR ENERGY INSTITUTE

October 29, 2021

Ms. Sabrina Atack
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 Nuclear Energy Institute 10-04, "Identifying Systems and Assets Subject to The Cyber Security Rule," Revision 3

Project Number: 689

Dear Ms. Atack:

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 address the security controls provided in their cyber security plans (CSPs) with two exceptions. The two exceptions were:

1) Section 2.2, "Security Systems," Revision 2 did not include all of the security systems that are within the scope of the cyber security rule
2) Section 2.4, "Support Systems and Equipment," Revision 2 did not include all the digital systems and equipment that provide a pathway to critical systems (referenced digital test and maintenance equipment (M&TE) for safety and safety-related systems whose connections to critical systems may not be permanent)

Lessons learned through the implementation of cyber security programs over the last few years have indicated that guidance improvements were necessary to enhance clarity, enable efficient and consistent program implementation, and to support NRC oversight activities. Accordingly, the Nuclear Energy Institute (NEI)[2], on behalf of its members, submitted four white papers proposing changes to NEI 10-04, Revision 2, and NEI 13-10, "Cyber Security Control Assessments, Revision 6 for NRC review.

[1] Agencywide Document Access and Management System (ADAMS) Accession No. ML12194A532

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

By letters dated May 19, 2020 (for Emergency Preparedness (EP) related changes)[3], August 14, 2020 (for Balance of Plant (BOP) related changes)[4], August 28, 2020 for Safety-Related and Important-to-Safety related changes)[5], and June 30, 2021 (for Physical Security related changes)[6], the NRC stated that they reviewed the white papers based on NRC regulations and guidance, and based on their reviews, the staff concluded that the methods in the white papers for identifying and protecting critical digital assets were consistent with NEI 08-09, Revision 6.

The attached NEI 10-04, Revision 3, incorporates the changes discussed in the four white papers and reviewed by the NRC. In addition, NEI has made the following conforming and non-substantive changes to improve clarity and flow of the document:

1) Throughout the document, made the Safety-Related and Important-to-Safety wording consistent
2) In Section 1.2 made changes to capture restructuring changes to Sections 4 and 5
3) In Section 2.2, added Access Authorization as #11, vice #2 as indicated in the security white paper for ease of integrating the new number in licensee procedures
4) In Section 4, added a BOP section for consistency with the other SSEP function discussions (Safety-Related and Important-to-Safety functions, Security functions, and Emergency Preparedness functions)
5) In Section 5, reorganized the section for flow and to group each of the SSEP area discussions
6) Added new Appendices C&D to include the EP scoping analysis and flowchart
7) Made other editorial changes and changes to the revision history

With respect to the first NEI 10-04 exception, the NRC staff stated Revision 2 did not include all of the security systems that are within the scope of the cyber security rule. Revision 3 to NEI 10-04 addresses this concern by deleting wording in Section 2.2 which noted four programs (performance evaluation program, access authorization (AA) program, insider mitigation program, and corrective action program) not being within the scope of the cyber security rule. This section was replaced in Revision 3 and now states that consistent with 10 CFR 73.54(a), 10 CFR 73.54(b), and their CSP, licensees are required to perform an analysis and determine those digital assets that, if compromised, would cause an adverse impact to SSEP functions and thus require protection. Additional information pertaining to AA digital assets was also added and noted as a system to be evaluated. Therefore, NEI believes this exception can be removed.

With respect to the second NEI 10-04 exception, the NRC staff stated Revision 2 did not address a staff comment related to digital systems and equipment that provide a pathway to critical systems, specifically, digital test and maintenance equipment. This issue was addressed in Security Frequently Asked Question (SFAQ) 16-03, "Treatment of Digital Maintenance and Test Equipment," dated March 8, 2017.[7] The SFAQ discusses which digital M&TE need to be in scope of the licensee's CSP, and which M&TE do not. The

[3] ADAMS Accession No. ML20129J981
[4] ADAMS Accession No. ML20209A442
[5] ADAMS Accession No. ML20223A256
[6] ADAMS Accession No. ML21140A140
[7] Exempt from public disclosure in accordance with 10 CFR 2.390

guidance in SFAQ 16-03 will be incorporated into the next revision of NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," which is planned for 2022. A footnote has also been added in NEI 10-04, Section 5, "Methodology for Identifying Critical Digital Assets," that indicates the SFAQ will be incorporated into NEI 08-09. Therefore, NEI believes this exception can be removed.

Based on the discussion above, NEI requests that the NRC review and endorse NEI 10-04, Revision 3, dated October 2021, without any exceptions, by December 2021. If any revisions to this document are desired, please include suggested wording and the technical data to support the proposed changes(s).

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

Sincerely,

William R. Gross
Attachment

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

NEI 10-04 [Revision 3]

Identifying Systems and Assets Subject to the Cyber Security Rule

October 2021

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

NEI 10-04 [Revision 3]

Nuclear Energy Institute

Identifying Systems and Assets Subject to the Cyber Security Rule

October 2021

Nuclear Energy Institute 1201 F Street, N.W., Suite 1100, Washington, DC 20004

ACKNOWLEDGEMENTS

This document was initially prepared by the nuclear power industry for use in commercial nuclear power reactors to comply with United States federal regulations.

Contributors to this manual include:

Janardan Amin	Luminant Power
Sandra Bittner	Arizona Public Service Company
Cynthia Broadwell	Progress Energy
Steve Carr	FPL/NextEra Energy, Inc.
Mike Chandler	Southern California Edison Company
Michelle Davidson	STP Nuclear Operating Company
Jeff Drowley	Exelon Corporation
Nathan Faith	American Electric Power Company
Teri Fox-McCloskey	Nebraska Public Power District
Glen Frix	Duke Energy Corporation
Jan Geib	South Carolina Electric & Gas Company
Matt Gibson	Progress Energy
Bob Gill	Duke Energy
William Gross	NEI
Steve Hetrick	FPL/NextEra Energy, Inc.
Martin Hug	NEI
Glen Kaegi	Exelon Corporation
Walter Lee	Tennessee Valley Authority
Susan McPherson	Progress Energy
Brian Miles	NextEra Energy
Monica Ray	Arizona Public Service Company
Robin Ritzman	FirstEnergy Corp.
Donald Robinson	Dominion Generation
Bill Rucker	FPL/NextEra Energy, Inc.
Michael Schaub	Constellation Energy
Geoff Schwartz	Entergy Nuclear Operations
Paul Serra	Dominion Generation
James Shank	PSEG Services Corporation
Michael Slobodien	Entergy Nuclear Operations
Laura Snyder	Tennessee Valley Authority
Jack Southers	PSEG Services Corporation
Robert Stubbs	Southern California Edison Company
Joseph Taraba	Exelon Corporation
Douglas Walker	Exelon Corporation
John Yacyshyn	Exelon Corporation
Brad Yeates	Southern Nuclear Operating Company
David Young	FPL/NextEra Energy, Inc., NEI

NOTICE

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

Nuclear Energy Institute 1201 F Street N.W., Suite 1100, Washington, DC 20004

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

EXECUTIVE SUMMARY

The NRC Cyber Security Rule 10 CFR 73.54 defines the digital computer and communications systems and networks to be protected using the following language:

(a) Each licensee subject to the requirements of this section shall 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.
  (1) The licensee shall protect digital computer and communication systems and networks associated with:
    (i) Safety-related and important-to-safety functions;
    (ii) Security functions;
    (iii) Emergency preparedness functions, including offsite communications; and
    (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

On October 21, 2010, the NRC issued Staff Requirements Memorandum (SRM) COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," to clarify the NRC position on structures, systems, and components in the balance of plant with respect to the NRC's Cyber Security Rule. The SRM states: "The Commission has determined as a matter of policy that the NRC's cyber security rule at 10 CFR § 73.54 should be interpreted to include structures, systems, and components in the Balance of Plant that have a nexus to radiological health and safety at NRC-licensed nuclear power plants."

The purpose of NEI 10-04 is to provide guidance on the identification of digital computer and communication systems and networks subject to the requirements of 10 CFR 73.54.

DOCUMENT REVISION HISTORY

Revision 1
NEI 10-04, Revision 1 incorporates the NRC's clarification of the scope of the Cyber Security Rule with respect to SSCs in the balance of plant. Section 2.3 on EP systems has been clarified. A new section has been added to provide guidance on the identification of Critical Digital Assets.

Revision 2
NEI 10-04, Revision 2 incorporates changes to Revision 1 principally in Sections 2.2, "Security Systems," and Section 2.3, "Emergency Preparedness Systems, Including Offsite Communications." Conforming changes were made in Section 4, "Methodology for Identifying and Classifying Plant Systems," to align with the changes in Sections 2.2 and 2.3. Section 5, "Methodology for Identifying Critical Digital Assets," was enhanced to address the consideration of "pathways" as used in the definition of CDA found in NEI 08-08, Revision 6.

Revision 3
NEI 10-04, Revision 3 incorporates NEI white paper guidance for the identification and protection of digital assets associated with Safety-Related, Important-to-Safety, Balance of Plant, Security, and Emergency Preparedness functions. Section 5, "Methodology for Identifying Critical Digital Assets," was updated and reorganized to include detailed screening guidance for Important-to-Safety systems and equipment and Balance of Plant important-to-safety systems and equipment.

TABLE OF CONTENTS

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

IDENTIFYING SYSTEMS AND ASSETS SUBJECT TO THE CYBER SECURITY RULE

1 INTRODUCTION

The purpose of NEI 10-04 is to provide guidance on the identification of digital computer and communication systems and networks subject to the requirements of 10 CFR 73.54.

1.1 Overview of Scoping for the NRC Cyber Security Rule

The NRC Cyber Security Rule requires the identification of digital computer and communications systems, equipment and networks associated with Safety-Related and Important-to-Safety functions, Security functions, Emergency Preparedness functions including offsite communication (SSEP), and support systems and equipment which, if compromised, would adversely impact SSEP functions. NEI 10-04 uses guidance from available references to support the identification of assets meeting the criteria of 10 CFR 73.54. In summary, the following functional references and rationale are used as a basis for the conclusions in this document.

1. Safety-Related and Important-to Safety functions can be determined from each plant's Current Licensing Basis (CLB)[1] documents (e.g. Final Safety Analysis Report, licensing commitments[2], etc.)

2. Security functions necessary to prevent significant core damage and spent fuel sabotage are identified based on criteria described in 10 CFR 73.55. Site-specific commitments can be identified in licensee Physical Security Plans.

3. Emergency preparedness functions, including offsite communications necessary to respond to a radiological emergency are described in 10 CFR 50.47 (b) and Appendix E to Part 50. Site-specific commitments can be found in licensee Emergency Plans.

For the purposes of Cyber Security, the term "Support System and Equipment," are systems and equipment which, if compromised, would adversely impact safety-related, important-to-safety, security, or emergency preparedness functions.

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

[1] Current Licensing Basis documents (CLB): The set of documents that specify the licensing requirements and commitments that form the basis used by the U.S. Nuclear Regulatory Commission (NRC) to license a nuclear power plant or a standard plant design.

[2] Licensing commitment is a commitment specified in the plant CLB (e.g., a commitment to apply specific design criteria to an item or to implement the licensing guidance provided by the NRC in a Generic Letter or Regulatory Guide).

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 megawatts[1] being reduced to zero within 15 minutes should be identified as BOP CDAs.

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

1.2 Use of NEI 10-04

The Cyber Security Rule requires 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 10 CFR 73.1. Licensees must analyze digital computer and communication systems and networks associated with SSEP functions and identify those assets that must be protected in accordance with the requirements set forth in 10 CFR 73.54.

NEI 10-04 provides the following guidance to aid licensees in identifying the assets that must be protected against cyber attacks up to and including the design basis threat.

Section 2, "Identification of Systems Subject to the NRC Cyber Security Rule," provides general guidance and references that may be used to identify plant systems associated with SSEP functions, and related support systems and equipment that may be subject to the Cyber Security Rule.

Section 4, "Methodology for Identifying and Classifying Plant Systems," provides criteria that may be used to screen plant systems to determine whether the systems should be analyzed in accordance with 10 CFR 73.54 (b)(1) of the Cyber Security Rule. Those plant systems that fall under the Cyber Security Rule are referred to as Critical Systems.

Section 5, "Methodology for Identifying Critical Digital Assets," provides guidance for identifying those digital assets associated with the function of the systems identified using the guidance in Section 4 that must be protected from cyber attacks. These digital assets are referred to as Critical Digital Assets (CDAs).

2 IDENTIFICATION OF SYSTEMS SUBJECT TO THE NRC CYBER SECURITY RULE

The NRC Cyber Security Rule requires the protection of digital computer and communication systems and networks from cyber attacks up to and including the design basis threat as described in 10 CFR 73.1. Licensees must protect assets associated with: safety-related and important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety-related, important-to-safety, security, or emergency preparedness functions.

This section provides general guidance references that may be used to identify plant systems associated with SSEP functions, and related support systems and equipment that may be subject to the Cyber Security Rule. Section 4 of this document provides a methodology for identifying plant systems.

2.1 Safety-Related and Important-to-Safety Systems

In the context of 10 CFR 73.54, identifying assets associated with Safety-Related and Important-to-Safety functions requires a consideration of those non-Safety-Related systems and equipment that can affect Safety-Related and Important-to-Safety functions.

The identification of Safety-Related (SR) systems and equipment has already been performed by each licensee in support of the requirements of 10 CFR 50 Appendix B and other program requirements. Many sites' classification procedures have included criteria that identifies systems and equipment as SR that do not perform SR functions. This has occurred to allow support of certain programmatic requirements typically applicable to SR systems and equipment. This was done so that sites did not need to create separate Quality Assurance (QA) programs specific to these systems and equipment. Examples of this equipment could include electrical equipment powered from 1E Safeguard power supply, instrumentation classified under Regulatory Guide (RG) 1.97, and equipment with environmental or seismic qualification.

2.1.1 Safety-Related

Regulations defining "Safety-Related" functions are well established in the Code of Federal Regulations.

10 CFR 50.2 defines Safety-Related structures, systems, and components as follows:

> Safety-Related structures, systems and components means those structures, systems and components that are relied upon to remain functional during and following design basis events to assure:
> (1) The integrity of the reactor coolant pressure boundary;
> (2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
> (3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in 10 CFR 50.34(a)(1) or 10 CFR 100.11 of this chapter, as applicable.

10 CFR Part 54 describes NRC requirements for license renewal applicants. The requirements of 10 CFR 54.4 describe the scope of equipment within the scope of the license renewal rule. Specifically, 10 CFR 54.4 requires the following:

(a) Plant systems, structures, and components within the scope of this part are-
(1) Safety-related systems, structures, and components which are those relied upon to remain functional during and following design-basis events (as defined in 10 CFR 50.49(b)(1)) to ensure the following functions:
(i) The integrity of the reactor coolant pressure boundary;
(ii) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
(iii) 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 of this chapter, as applicable.

In addition to the 10 CFR 50.2 definition, SR systems and equipment also include any other systems and equipment whose postulated failure during the Design Bases Events (DBEs) could prevent satisfactory accomplishment of the SR function described above.

2.1.2 Important-to-Safety

The identification of Important-to-Safety systems and equipment is based on regulatory guidance contained in Generic Letter 84-01, NRC Use of the Terms, "Important-to-Safety" and "Safety-Related;" 10 CFR 50.49; and 10 CFR 54.4 (a)(2) and (a)(3).

Generic Letter 84-01 was developed in response to a concern raised by the Utility Safety Classification Group; specifically, that the term Important-to-Safety was used in various regulatory documents, yet it was not defined. The Utility Safety Classification Group claimed that Important-to-Safety should be considered equivalent in meaning to Safety-Related. The Generic Letter refuted this claim; however, the Generic Letter did not go so far as to provide a definition. The Generic Letter 84-01 stated:

> *NRC regulatory jurisdiction involving a safety matter is not controlled by the use of terms such as "safety-related" and "important to safety," and our conclusion that pursuant to our regulations, nuclear power plant … licensees are responsible for developing and implementing quality assurance programs for … plant operation which meet the more general requirements of General Design Criterion 1 for plant equipment "important to safety,"…*
>
> *…normal industry practice is generally acceptable for most equipment not covered by Appendix B within this class. Nevertheless, in specific situations in the past where we have found that quality assurance requirements beyond normal industry practice were needed for equipment "important to safety," we have not hesitated in imposing additional requirements commensurate with the importance to safety of the equipment involved. We intend to continue that practice*

Although Generic Letter 84-01 did not result in adding an Important-to-Safety definition within 10 CFR 50.2, it did state that current industry practice has been acceptable and additional quality assurance requirements will be imposed if determined otherwise. Over the past 40 years this can be seen in the issuance of various regulatory guidance and regulations including RG 1.155, "Station Blackout" (SBO), 10 CFR 50.63, "Loss of All Alternating Current Power," GL 83-28, "Required Actions Based on Generic Implications of Salem ATWS Events," 10 CFR 50.62, "Anticipated Transient Without SCRAM (ATWS)," 10 CFR 50.48, "Fire Protection," 10 CFR 50.49, "Environmental Qualification," including certain post-accident monitoring equipment in RG 1.97 and applicable provisions in Appendix A to Part 50, "General Design Criteria for Nuclear Power Plants."

Additionally, on October 21, 2010, the NRC issued Staff Requirements Memorandum (SRM) COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," to clarify the NRC position on structures, systems, and components in the balance of plant with respect to the NRC's Cyber Security Rule. The SRM states: "The Commission has determined as a matter of policy that the NRC's cyber security rule at 10 CFR § 73.54 should be interpreted to include structures, systems, and components in the Balance of Plant that have a nexus to radiological health and safety at NRC-licensed nuclear power plants." SECY 10-0153 contains the NRC staff response to the SRM. The SECY identifies the staff interpretation of the SRM as "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 10 CFR 73.54(a)(1)."

By letter to NEI dated January 5, 2011 (ADAMS Accession Number: ML103550480) the NRC provided Cyber Security Plan language to clarify the scope of systems that have a nexus to radiological health and safety. The letter states, in pertinent part:

> "In order to meet the Commission's policy decision, the following change is needed to the cyber security plans that are currently under review:
>
> > "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.""

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.

BOP SSCs may have been designed and built with normal industrial quality and may not meet the standards in Appendix B to 10 CFR Part 50. Licensees are not required to generate

paperwork to document the basis for the design, fabrication, and construction of BOP equipment not covered by Appendix B. Instead, it is the intent to ensure that each licensee's cyber security program protect those BOP SSCs that could result in an unplanned reactor shutdown or transient.

References to aid in identifying Safety-Related, Important-to-Safety, and BOP important-to-safety systems include but may not be limited to:

a) FSAR
b) UFSAR
c) Design Basis documents
d) Deleted
e) Licensee commitments with respect to RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants"
f) Deleted
g) Licensee formal communications to the NRC (e.g., responses to Generic Communications or NRC Orders)

2.2 Security Systems

Exercise caution when documenting security systems. Some physical protection equipment or systems may contain safeguards information (SGI) or security related information (SRI). Documentation created during assessments must be reviewed in accordance with site or corporate procedures to identify if the material should be classified as SGI.

The cyber security and physical security programs are intrinsically linked and must be integrated to satisfy the physical protection program design criteria of 10 CFR 73.55(b). These criteria are provided in 10 CFR 73.55 (b)(3), which requires: the physical protection program be designed to prevent significant core damage and spent fuel sabotage; that the program ensure that the capabilities to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1, are maintained at all times; and that the program provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program.

In the implementation of the licensee's protective strategy, security officers may use digital technologies, such as firearm scopes and distance range finders. Licensees must analyze these devices but need not classify them as CDAs if the licensee analysis demonstrates that a cyber attack on the device cannot adversely impact an SSEP function.

Accordingly, digital computer and communication systems and networks that should be analyzed include physical barrier systems, target sets, access control systems, search program systems, detection and assessment systems, communications systems, and response systems to ensure the requirements of 10 CFR 73.55 (b)(3) are maintained. Support systems and equipment that should be analyzed include those assets described in 10 CFR 73.55 necessary to satisfy the requirements of 10 CFR 73.55 (b)(3). Backup power supplies for the intrusion detection system and video image recording system are examples of support systems and equipment. In general, these systems may be found in the licensee's protective strategy developed in accordance with

Appendix C to 10 CFR Part 73, Section II, "Nuclear Power Plant Safeguards Contingency Plans," section (B)(3)(c)(v).

Consistent with 10 CFR 73.54(a), 10 CFR 73.54(b), and their CSP, licensees are required to perform an analysis and determine those digital assets that, if compromised, would cause an adverse impact to SSEP functions and thus require protection. 10 CFR 73.55(b)(7) requires licensees maintain an Access Authorization program in accordance with 10 CFR 73.56. Paragraphs 10 CFR 73.56(m) and (o) require licensees ensure the confidentiality and integrity of Access Authorization (AA) system data. For these reasons, AA digital assets and/or software, and the data contained within those assets and/or software, must also be analyzed in accordance with 10 CFR 73.54(b)(1). NEI 13-10 provides additional guidance licensees may use when analyzing AA digital assets.

The following are the security functions that must be protected against adverse impacts from the radiological sabotage cyber attack:

1. Physical barriers
2. Access controls
3. Search programs
4. Detection and assessment systems
5. Communication requirements
6. Response requirements

Example list of the systems to be evaluated but not limited to:

1. Active Vehicle Barrier System [10 CFR 73.55(e)(10)(i)(A)]
2. Access Control System and Devices
   [10 CFR 73.55(e)(8), (e)(9), (g)(1), (g)(4), (g)(5), (g)(6)]
3. Metal Detection System [10 CFR 73.55 (h)(3)(i)
4. Explosive Detection System [10 CFR 73.55 (h)(3)(i)]
5. X-ray Search System [10 CFR 73.55 (h)(3)(i)]
6. Intrusion Detection Systems
   [10 CFR 73.55 (b)(3)(i), (e)(7)(i)(B), (e)(8)(ii), (e)(9)(ii), (g)(1)(i)(B), (i)(1)]
7. Assessment Systems (including real-time and play-back/recorded video images) [10 CFR 73.55 (b)(3)(i), (e)(7)(i)(C), (i)(1), (i)(5)]
8. Illumination Systems [10 CFR 73.55 (i)(6)]
9. Communications Systems [10 CFR 73.55 (j)]
10. Interdiction and Neutralization Systems (e.g., Remotely Operated Weapons System (ROWS)) [10 CFR 73.55 (k)]
11. Access Authorization [(73.56)]

Support Systems

1. Secondary Power for IDS/Alarm Annunciation [10 CFR 73.55 (e)(9)(vi)(A), (i)(3)(vii)]
2. Secondary Power for Assessment Systems [10 CFR 73.55 (i)(3)(vii)]
3. Secondary Power for Non-Portable Communications [10 CFR 73.55 (e)(9)(vi)(B), (j)(5)]
4. Secondary Power for Active Vehicle Barrier System [10 CFR 73.55 (e)(10)(i)(B)]

References to aid in identifying Security Systems include:

a) Physical Security Plan
b) Protective strategy

2.3 Emergency Preparedness Systems, Including Offsite Communications

Digital assets associated with the EP functions described below require analysis **(see table in Appendix C and flowchart in Appendix D)** for determining whether they are to be protected as CDAs. In doing so, the licensee must ensure the EP function can be performed and there is no adverse impact to the function. If a compromise or loss of the DA has no adverse impact to the licensee being able to perform the EP function then, the DA may not be required to be identified as a CDA.

The emergency preparedness systems within the scope of the cyber-security rule include digital computer, and communication systems and networks associated with measures needed for the protection of the public in the event of a radiological emergency. As used here, "measures" include emergency response actions described in the Emergency Plan to mitigate the consequences of the emergency and include, but are not limited to, emergency classification, formulation of protective action recommendations for the public, emergency notifications, and accident assessment.

The licensee is required to perform a documented analysis per 10 CFR 73.54(b)(1) to identify digital assets subject to protection per 10 CFR 73.54(c). The cybersecurity rule requirement of 10 CFR 73.54(b)(1) is to identify those assets that, if compromised, would adversely impact SSEP Functions. The licensee has an established Emergency Plan, independent of the Cyber Security Plan that identifies and describes the licensee's methods for maintaining emergency preparedness and responding to emergencies. These measures are evaluated using the criteria in NEI 10-04, Section 4, "Methodology for Identifying and Classifying Plant Systems," to demonstrate the licensee's capability to perform the function regardless of the failure mode (e.g., cyber attack, loss, or operational failure). This capability ensures that the licensee can detect a cyber compromise of an EP DA and an alternate method is adequately independent and diverse to fulfill the EP function. The ability to fulfill the EP function regardless of digital asset compromise is a key decision for determining whether the digital asset is required to be identified as a CDA. Adverse impact is focused on the EP function.

EXAMPLE OF ADEQUATE INDEPENDENT AND DIVERSE METHOD

a. Two methods would be considered adequately independent (diverse) if they do not rely on equipment that if compromised by cyber attacks would adversely impact both methods of performing the EP function (e.g., a PBX-based phone system vs. satellite phones, data obtained by MET tower vs. data obtained through a weather service, data obtained from SPDS vs. received via fax, etc.).

Since the cyber-security rule applies to the licensee, the rule requirements are applicable only to digital assets used to perform licensee emergency response functions. More specifically, these are the digital assets described in a licensee's Emergency Plan and implementing procedures as being required by the licensee emergency response organization personnel during a radiological emergency. For certain EP systems, licensees are not expected to implement cyber security

measures on equipment that is not under the licensee's sole custody and control. 10 CFR 73.54 requires licensees to ensure EP response functions are not adversely impacted due to a cyber attack. Licensees must be able to demonstrate the capability to perform emergency response functions even in cases where they may use equipment for which they do not have full custody and control and cannot reasonably implement cyber security protective measures. The following guidance should be considered when making scoping determinations.

- Emergency response capabilities must be maintained. Some of the 16 planning standards of 10 CFR 50.47(b) apply to *emergency preparedness* activities while others govern *emergency response* capabilities. To the extent that a digital asset serves only as a means to perform an emergency preparedness activity (e.g., to track qualification of emergency response organization personnel), it would generally be exempt from 10 CFR 73.54. However, if the licensee's Emergency Plan or implementing procedures requires the emergency response organization to use this digital asset during a radiological emergency (e.g., to confirm the qualification of response teams prior to their dispatch from the operations support center), the asset may be subject to 10 CFR 73.54.

- Systems for both onsite and offsite communications should be considered. Although 10 CFR 73.54(a)(1)(iii) is explicitly applicable to offsite communications, other communications capability such as data and voice communication systems between the control room and the licensee's emergency response facilities, the licensee's means for initiating augmentation of the emergency response organization, the communication systems for implementing protective actions in-plant and within the owner controlled area, and other similar onsite communications may be encompassed under 10 CFR 73.54.

- Backup capabilities should be considered. 10 CFR 50, Appendix E requirements call for reliable primary and backup communications capabilities for certain emergency response functions. In general, licensees have also established backup capabilities for other functions as a matter of prudency (e.g., accident assessment). Digital means of implementing primary and backup communications, to include communication systems and networks, are to be protected from cyber attacks in accordance with 10 CFR 73.54 and the licensee's and applicant's NRC-approved Cyber Security Plans. Licensees may consider backup capabilities when addressing cyber security controls in accordance with the Cyber Security Plan. It is important to recognize that the Commission's regulations place emphasis on prudent risk reduction measures, but does not require dedication of resources to handle every possible accident that can be imagined.

- ANS is not subject to 10 CFR 73.54. Although most licensees have established an Alert and Notification System (ANS) for their EPZs, they have done so as an agent of the affected State(s). The NRC regulations in 10 CFR 50, Appendix E require that the licensee demonstrate that the ANS capability is in place, but assign responsibility for activation of the system to State and local authorities. Although the NRC has established a capability requirement for the ANS in Appendix E, FEMA has the responsibility for establishing design criteria for an ANS and for evaluating the design of the ANS against the design criteria. FEMA has not established cyber-security design criteria for an ANS.

  In addition, it is important to recognize that ANS sirens only direct a population to turn

on radio and television for official information. Inappropriate activation of the ANS, or the inability to activate the ANS, will be immediately identifiable and resolved by State or local officials. These officials have backup alerting capabilities at their disposal (e.g., route alerting). Accordingly, the ANS is not subject to 10 CFR 73.54.

- Emergency declaration and notification capabilities shall be maintained. The implementation of cyber security controls must not adversely impact a licensee's ability to meet the emergency declaration and notification requirements and respective timeframes that are required by 10 CFR 50, Appendix E.

- ERDS is not subject to 10 CFR 73.54. NRC discussed the cyber security classification of the Emergency Response Data System (ERDS) in NRC letter from Richard P. Correia to Melvin M. Leach dated January 15, 2010 (Adams accession number ML100130359). The letter concluded that ERDS would not be considered to be within the scope of 10 CFR 73.54.

- Self-imposed requirements should be considered. A licensee may have additional self-imposed requirements identified in their Emergency Plan that were intended to address site-specific response needs (e.g., compensate for response constraint or vulnerability), and which are performed using a digital asset or communications system. These components will need to be evaluated to determine if they are subject to 10 CFR 73.54.

- In the case of scoping EP DAs/CDAs, the "alternate methods" are methods for performing the EP functions as required by the licensee's Emergency Plan. NEI 13-01, "Reportable Action Levels for Loss of Emergency Preparedness Capabilities," Rev. 0, defines the term method for accomplishing an EP function as follows:

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

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

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

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

These checks ensure the equipment is capable of performing its intended function and an appropriate response is initiated if the EP DA is compromised.

  - The methods for fulfilling the functions shall be adequately independent and diverse such that a single cyber attack will not adversely impact the licensee's capability to perform the EP function. Two alternate methods can both be digital if they are adequately independent, diverse, and not susceptible to the same cyber attack (e.g., a PBX-based phone system vs. satellite phones, data obtained by MET tower vs. data obtained through a weather service, data obtained from SPDS vs. received via fax, etc.).

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

10 CFR 50.47(a)(1)(i) requires a NRC finding that there is reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency before an initial operating license, or initial combined operating license is issued. The NRC considers the findings of the Federal Emergency Management Agency with regard to offsite preparedness and its own findings in making this determination. Subsequent to license issuance, the licensee is required by 10 CFR 50.54(q)(2) to follow and maintain the effectiveness of an Emergency Plan that meets the requirements in Appendix E to this part and, for nuclear power reactor licensees, the sixteen planning standards of 10 CFR 50.47(b). Accordingly, these sixteen planning standards correspond to the "emergency preparedness functions" identified in 10 CFR 73.54(a)(1); the licensee describes how they meet the planning standards in their Emergency Plans.

Table 2.3.1, below, lists the 16 emergency planning standards from 10 CFR 50.47(b), the associated planning standard functions, sources of additional information, and scope-related information. Digital assets that support the below listed emergency response functions will need to be screened for applicability to 10 CFR 73.54 in accordance with the requirements of 10 CFR 73.54 (b)(1). The guidance in this table does not relieve the licensee of the responsibility of assessing site-specific systems that may be used to support that function and that would be required during the response to a radiological emergency.

Table 2.3.1 Scoping Considerations for Emergency Preparedness Functions

Planning Standard	Planning Standard Functions	Additional Information	10 CFR 73.54 Scoping Guidance
10 CFR 50.47(b)(1)	Assignment of emergency response responsibilities. The response organization has the staff to respond and augment on a continuing basis (24-hour staffing) IAW the Plan.	Supporting requirements are found in Sections IV.A.1 – 8 of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.A of NUREG-0654 and the licensee's Emergency Plan.	Not within scope of 10 CFR 73.54; no digital asset or communications considerations.
10 CFR 50.47(b)(2)	Process ensures that on-shift emergency response responsibilities are staffed and assigned.	Supporting requirements are found in Sections IV.A.2.a, b, and c; IV.A.3 and 9; and IV.C of Appendix E to 10 CFR Part 50.	Not within scope of 10 CFR 73.54; no digital asset or communications considerations.
10 CFR 50.47(b)(2)	Process for prompt augmentation of on-shift staff is established and maintained.	Informing criteria are found in Section II.B of NUREG-0654 and the licensee's Emergency Plan.	Communications systems used to callout augmented ERO members.
10 CFR 50.47(b)(3)	Arrangements for requesting and using offsite assistance have been made.	Supporting requirements are found in Sections IV.A.6 and IV.A.7 of Appendix E to 10 CFR Part 50.	Communication systems used to request the offsite support.
10 CFR 50.47(b)(3)	State and local staff can be accommodated at the EOF in accordance with the Emergency Plan.	Informing criteria are found in Section II.C of NUREG-0654 and the licensee's Emergency Plan.	Communications systems used to communicate with the offsite support while they are onsite.

Planning Standard	**Planning Standard Functions**	**Additional Information**	**10 CFR 73.54 Scoping Guidance**
10 CFR 50.47(b)(4)	A standard scheme of emergency classification and action levels is in use.	Supporting requirements are found in Sections IV.B and IV.C of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.D of NUREG-0654 and the licensee's Emergency Plan.	Systems used in the process of classifying emergency conditions; this does not include individual EAL indications. Systems used to transmit information that is used to make emergency classifications if the classification is done away from the control room.

Planning Standard	Planning Standard Functions	Additional Information	10 CFR 73.54 Scoping Guidance
10 CFR 50.47(b)(5)	Procedures for notification of State and local governmental agencies are capable of completing initial notifications within 15 minutes of the declaration of an emergency. Administrative and physical means have been established for alerting and providing prompt instructions to the public within the plume exposure pathway. The public alert and notification system meets the design requirements of FEMA-REP-10 or is compliant with the FEMA approved Alert and Notification System (ANS) design report and supporting FEMA approval letter.	Supporting requirements are found in Sections IV.D.1 and IV.D.3 of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.E of NUREG-0654 and the licensee's Emergency Plan.	Communications systems used to notify OROs of an emergency declaration or PAR. Assets required to meet the licensee-specific evaluation criteria of Section II.E of NUREG-0654 and the licensee's Emergency Plan. The ANS is exempt from 10 CFR 73.54.
10 CFR 50.47(b)(6)	Systems are established for prompt communication among principal emergency response organizations. Systems are established for prompt communication to emergency response personnel.	Supporting requirements are found in Section IV.E.9 of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.F of NUREG-0654 and the licensee's Emergency Plan.	Assets required to meet the licensee-specific evaluation criteria of Section II.F of NUREG-0654 and the licensee's Emergency Plan.

Planning Standard	Planning Standard Functions	Additional Information	10 CFR 73.54 Scoping Guidance
10 CFR 50.47(b)(7)	EP information is made available to the public on a periodic basis within the plume exposure pathway EPZ.	Supporting requirements are found in Section IV.D.2 of Appendix E to 10 CFR Part 50.	Not within the scope of 10 CFR 73.54; not an emergency response function.
10 CFR 50.47(b)(7)	Coordinated dissemination of public information during emergencies is established	Informing criteria are found in Section II.G of NUREG-0654, NUREG-0696, and the licensee's Emergency Plan.	Assets required in meeting this function.
10 CFR 50.47(b)(8)	Adequate facilities are maintained to support emergency response.	Supporting requirements are found in Sections IV.E.1–4, IV.E.8 and IV.G of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.G of NUREG-0654, NUREG-0696, and the licensee's Emergency Plan.	Assets required to meeting the licensee-specific evaluation criteria of Section II.H of NUREG-0654 and the licensee's Emergency Plan.
10 CFR 50.47(b)(9)	Methods, systems, and equipment for assessment of radioactive releases are in use.	Supporting requirements are found in Sections IV.B and IV.E.2 of Appendix E. to 10 CFR Part 50. Informing criteria are found in Section II.I of NUREG-0654 and the licensee's Emergency Plan.	Assets required to meet the licensee-specific evaluation criteria of Section II.I of NUREG-0654 and the licensee's Emergency Plan.
10 CFR 50.47(b)(10)	A range of public protective action recommendations (PARs) is available for implementation during emergencies.	Informing criteria are found in Sections II.J.1–4, II.J.7–8, and II.J.10 of NUREG-0654 as well as Supplement 3 to NUREG-0654 and the licensee's Emergency Plan.	Assets required to meet the licensee-specific evaluation criteria of Section II.J of NUREG-0654 and the licensee's Emergency Plan.

Planning Standard	Planning Standard Functions	Additional Information	10 CFR 73.54 Scoping Guidance
10 CFR 50.47(b)(11)	The means for controlling radiological exposures for emergency workers are established.	Supporting requirements are found in Section IV.E of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.K of NUREG-0654 and the licensee's Emergency Plan.	Assets used in assessing emergency personnel radiation doses if use of those assets is described in the Emergency Plan or implementing procedures as being used during an emergency to staff response teams prior to dispatch from the OSC, and where the compromise of the assets could prevent a licensee from implementing response measures.
10 CFR 50.47(b)(12)	Arrangements are made for medical services for contaminated, injured individuals.	Supporting requirements are found in Sections IV.E of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.L of NUREG-0654 and the licensee's Emergency Plan.	Not within scope of 10 CFR 73.54; no digital asset or communications considerations.
10 CFR 50.47(b)(13)	Plans for recovery and reentry are developed.	Informing criteria are found in Section II.M of NUREG-0654 and the licensee's Emergency Plan.	Not within the scope of 10 CFR 73.54; not an emergency response function.

Planning Standard	Planning Standard Functions	Additional Information	10 CFR 73.54 Scoping Guidance
10 CFR 50.47(b)(14)	A drill and exercise program (including radiological, medical, Health Physics, etc.) is established. Full-scale drills and exercises are assessed via a formal critique process in order to identify weaknesses associated with an RSPS. Identified RSPS weaknesses are corrected.	Supporting requirements are found in Sections IV.F.1–2 of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.N of NUREG-0654 and the licensee's Emergency Plan.	Not within the scope of 10 CFR 73.54; not an emergency response function.
10 CFR 50.47(b)(15)	Training is provided to emergency responders.	Supporting requirements are found in Section IV.F.1 of Appendix E to 10 CFR Part 50. Informing criteria are found in Section II.O of NUREG-0654 and the licensee's Emergency Plan.	Assets required to track personnel training and qualification, if use of those assets is described in the Emergency Plan or implementing procedures as being used during an emergency to confirm qualification of response teams prior to dispatch from the OSC.
10 CFR 50.47(b)(16)	Responsibility for Plan development and review is established.	Informing criteria are found in Section II.P of NUREG-0654 and the licensee's Emergency Plan.	Not within the scope of 10 CFR 73.54; not an emergency response function.

2.4 Support Systems and Equipment

The NRC Cyber Security Rule requires protection from cyber attack assets associated with support systems and equipment which, if compromised, would adversely impact Safety-Related, Important-to-Safety, Security, or Emergency Preparedness functions. Support systems and equipment to be protected include, for example, those required to provide an environment to assure the operational requirements of systems performing SSEP functions or provide motive force (e.g., pneumatic, hydraulic, electrical) for the required performance of SSEP functions.

Separately, other systems and equipment that do not directly support the operational requirements of the SSEP function, but, if compromised, would adversely impact systems and equipment performing SSEP functions, are to be evaluated for protection. For example, malfunction or operation of a non-Safety-Related system or equipment whose failure during the DBE could prevent satisfactory accomplishment of a Safety-Related system or equipment performing a Safety-Related function.

Licensees are required to identify and evaluate those digital assets associated with security support systems whose failure or compromise as the result of a cyber attack would result in an adverse impact to an SSEP function. While implementing the licensee's protective strategy, security officers may use digital technologies. Examples include but are not limited to: officer efficiency aids, firearm scopes, and distance range finders. These devices should be analyzed but need not be classified as CDAs if licensee analysis demonstrates that a cyber attack on the device cannot adversely impact an SSEP function. Please see Section 5 of NEI 10-04 for considerations in determining if a digital asset is a CDA.

The determination of support systems, networks, and equipment can be found in a site's current licensing and design basis documentation.

For example, support systems and equipment may include, but not be limited to, the following:

a) Electrical Power systems whether primary or backup
b) HVAC systems
c) Deleted
d) Secondary Power for Detection and Assessment Equipment
e) Diesel Generator lube oil systems

3 IDENTIFICATION OF SYSTEMS SUBJECT TO THE FERC ORDER

On October 21, 2010, the NRC issued Staff Requirements Memorandum (SRM) COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants." The SRM states: "The Commission has determined as a matter of policy that the NRC's cyber security rule at 10 CFR § 73.54 should be interpreted to include structures, systems, and components in the Balance of Plant that have a nexus to radiological health and safety at NRC-licensed nuclear power plants."

SECY 10-0153 contains the NRC staff response to the SRM. The SECY identifies the staff interpretation of the SRM as:

> "The staff determined that 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 10 CFR 73.54(a)(1). The staff also determined that SSCs in the BOP are under licensee control and could be in the protected area or in the owner controlled area. The electrical distribution equipment out to the first inter-tie with the offsite distribution system would be subject to the NRC's cyber security regulations. Based on this determination, the staff does not believe that there will be any SSCs in the BOP that will fall under NERC's CIP standards. However, there may be some SSCs that are not subject to either NRC's cyber security regulations or NERC's CIP standards because these SSCs do not directly or indirectly affect reactivity and do not affect grid reliability. Consistent with the MOA between NRC and FERC, the staff will continue to coordinate with FERC and NERC to share relevant operating experience and other related technical information on SSCs inside and beyond the scope of 10 CFR 73.54(a)(1)."

On March 10, 2011, the FERC docketed an "Order dismissing compliance filing" (134 FERC ¶ 6180) in response to a filing made by NERC regarding Order 706-B. In the March Order, the FERC determined:

> "Based on the NRC's November 26, 2010 letter, we find that the NRC's cyber security rule appears to cover all balance of plant, and no balance of plant at a U.S. nuclear power plant has been found to be subject to NERC's CIP Standards. Accordingly, we dismiss the compliance filing containing the Version 2 and 3 Implementation Plans as moot. However, if at a future time, it is determined that any of the systems, structures or components within a nuclear power plant's balance of plant are subject to NERC's CIP Standards, NERC must file with the Commission, within 90 days of such determination, an implementation plan for U.S. nuclear power plant owners' and operators' compliance with the then current version of the CIP Standards."

In accordance with the Memorandum of Agreement (MOA) with FERC, and the Memorandum of Understanding (MOU) with NERC, the NRC has agreed to share with FERC and NERC any information discovered during an inspection concerning digital assets that do not fall under 10 CFR 73.54 and that may be under the scope of requirements defined by NERC in its CIP Reliability Standards. This includes SSCs in the BOP categorized by a licensee as no longer important-to-safety, not directly or indirectly affecting reactivity at a nuclear power plant, or not

resulting in an unplanned reactor shutdown or transient. SSCs in the BOP out to the first inter-tie with the offsite distribution system that is not within the scope of 10 CFR 73.54 may be subject to NERC CIP Reliability Standards. During inspections, NRC may request licensees provide the NRC a list of such systems. In accordance with the MOA and MOU with FERC and NERC, respectively, and the SRM COMWCO-10-0001, the NRC can share this information with FERC and NERC for the determination of whether such systems are within the scope of NERC CIP Reliability Standards.

4 METHODOLOGY FOR IDENTIFYING AND CLASSIFYING PLANT SYSTEMS

This section provides a methodology for identifying and classifying plant systems to determine the regulatory categorization of those systems. The goal of this section is to provide the method used for screening plant systems to determine whether the systems fall under the NRC's Cyber Security Rule. Systems that fall under the Cyber Security Rule are referred to as Critical Systems (CS). A site-specific evaluation of systems must be performed utilizing the licensee's CLB.

CATEGORIZATION OF PLANT SYSTEMS

SAFETY-RELATED

Is this system relied upon to remain functional during and following DBEs to assure?

1. The integrity of the reactor coolant pressure boundary?
2. The capability to shut down the reactor and maintain it in a safe shutdown condition?
3. 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 purposes of this guidance, only systems are being considered. Systems are considered Safety-Related within the scope of the 10 CFR 73.54, if at least one of the system's design functions, as documented in the site's CLB, or other system design documents, is classified as Safety-Related.

IMPORTANT-TO-SAFETY

For purposes of this guidance, the Important-to-Safety equipment and functions are not specific plant systems but are typically part of existing plant systems and functions. Important-to-Safety equipment is Non-Safety-Related (NSR) equipment that is used to meet the CLB commitments to assure the integrity of the RCPB, the capability to shut down the reactor and maintain it in a safe shutdown condition (e.g., commitments for Fire Protection, SBO, ATWS and EQ).

See Section 5 for detailed screening of Important-to-Safety systems and equipment.

BALANCE OF PLANT IMPORTANT-TO-SAFETY

The scope of the cyber security rule in 10 CFR 73.54 has been interpreted by the NRC Commission to include 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.

See Section 5 for detailed screening of BOP important-to-safety systems and equipment.

SECURITY

Please see detailed guidance in Section 2.2 of NEI 10-04.

EMERGENCY PREPAREDNESS

Please see detailed guidance in Section 2.3 of NEI 10-04

SUPPORT SYSTEMS THAT COULD ADVERSELY IMPACT SSEP FUNCTIONS

1. Could the compromise of the support system have an adverse impact on a safety-related or important-to-safety function?
2. Could the compromise of the support system have an adverse impact on a security function?
3. Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?

5 METHODOLOGY FOR IDENTIFYING CRITICAL DIGITAL ASSETS

Appendix B of NEI 08-09, Revision 6 defines a Critical Digital Asset (CDA) as a digital computer, communication system, or network that is:[3]

- A component of a critical system (this includes assets that perform SSEP functions; provide support to, protect, or provide a pathway to Critical Systems); or
- A support system asset whose failure or compromise as the result of a cyber attack would result in an adverse impact to a SSEP Function.

The following interpretation is consistent across various sources and provides an approach for identifying those digital assets that are associated with SSEP functions and are required to be protected from cyber attacks in accordance with 10 CFR 73.54.

A digital asset may be identified as a programmable device (e.g., EPROM, microprocessor, etc.) that uses any combination of hardware, firmware and/or software to execute internally stored programs and algorithms, including numerous arithmetic or logic operations, without operator action. Solid state devices (e.g., electro-mechanical on/off devices, relays, hard-wired logic devices, circuit boards, etc.) that do not have firmware and/or software are not considered digital devices.

A digital device that communicates to a CDA need not be classified as a CDA simply due to the connectivity pathway. If the compromise of the digital asset can be used to compromise a CDA, then the digital asset should be classified as a CDA. Where cyber security controls, implemented in accordance with CSP Section 3.1.6 for the CDA, address the threats associated with the pathway (i.e., the attack vector no longer exists to the CDA), then the digital device does not need to be classified as a CDA.

Unless otherwise specified in this document as related to the guidance for identification of CDAs (e.g., where alternate methods that are adequately independent, and diverse are available to fulfill the function), a digital device should be identified as a 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, etc.) and, through analysis, demonstrate a compromise would adversely impact a SSEP function;
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.

NRC Regulatory Guide (RG) 5.71 (RG 5.71) defines Adverse Impact as:

[3] M&TE has been addressed in SFAQ 16-03 and will be incorporated into future revisions of NEI 08-09

A direct deleterious effect on a CDA (e.g., loss or impairment of function, reduction in reliability, reduction in ability to detect, delay, assess or respond to malevolent activities, reduction of ability to call for or communicate with offsite assistance, and the reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency). In the case where the direct or indirect compromise of a support system causes a safety, important to safety, security or emergency preparedness system or support system to actuate or "fail safe" and not result in radiological sabotage (i.e., causes the system to actuate properly in response to established parameters and thresholds), this is not considered to be an adverse impact as it defined by 10 CFR 73.54(a).

Safety-Related/Important to Safety

This section provides a methodology for identifying and classifying plant equipment performing SR or Important-to-Safety functions to determine the regulatory categorization of equipment. The goal of this section is to provide the method used for screening plant equipment to identify digital SR or Important-to-Safety equipment that would fall under the NRC's Cyber Security Rule. Results of this screening process will identify digital equipment that is referred to as a CDA and those that will remain as a digital asset.

Identification of systems and equipment performing SR or Important-to-Safety functions is performed as follows. The classification steps are to be considered in the sequence presented and include the context from previous steps and tiers:

1. Identify under the Current Licensing Basis (CLB) the list of DBEs applicable to the system or equipment under consideration.
2. Identify systems and equipment that are credited in that DBE safety analyses for satisfying SR definition elements (i.e., maintain Reactor Coolant Pressure Boundary (RCPB), shutdown the reactor, maintain safe shutdown condition or the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11). Note that these systems and equipment are identified as SR.
3. Identify those systems and equipment that are required to support the functionality and operability (e.g. cooling water, lube oil, HVAC, electrical, etc.) of the systems and equipment identified in Step 2. Note that these systems and equipment are also identified as SR.
4. Identify any CLB commitments where a system or equipment is classified as SR. These systems and equipment are also determined to be SR under this guidance document.
5. Identify NSR systems and equipment that functionally interface (including digital pathways) with the SR systems and equipment. Determine if a compromise by cyber attack of the NSR system and equipment interfacing with the SR function could prevent or adversely impact the performance of the SR function, then identify the NSR equipment as a CDA for protection as a SR equipment.

6. If identified SR systems and equipment contain a digital component that if compromised could adversely impact the proper operation of the identified SR systems and equipment, then the digital component is a SR CDA. **(REPEAT STEPS 2 THRU 6 FOR EACH DBE IDENTIFIED IN STEP 1)**

7. Identify any NSR systems and equipment that are used to meet the CLB commitments to assure the integrity of the RCPB, the capability to shut down the reactor, or maintain it in a safe shutdown condition e.g., commitments for Fire Protection Program (FPP), SBO Analysis, ATWS Analysis and EQ Program. These systems and equipment are identified as Important-to-Safety.
    a. Identify systems and equipment required or credited in response to each of the following:
        i. For ATWS Analysis, identify systems and equipment required for complying with 10 CFR 50.62
        ii. For SBO Analysis, identify systems and equipment utilized in mitigating the SBO event per 10 CFR 50.63, and systems and equipment that support bringing the unit(s) to and maintain in safe shutdown.
        iii. For FPP, identify FP systems and equipment related to protecting systems and equipment required for bringing the unit(s) to and maintain in safe shutdown; and the FP systems and equipment (detection/suppression) used in response to a fire in areas containing SR equipment to comply with applicable fire protection requirements (10 CFR 50.48, 10 CFR 50 Appendix R, or GDC 3). These FP SSCs are important-to-safety systems and equipment.
        iv. For EQ (10 CFR 50.49), identify NSR electrical equipment whose failure under postulated environmental conditions could prevent satisfactory accomplishment of the SR function of electrical equipment; and certain equipment, per 10 CFR 50.49(b)(3) that must be qualified to perform a post-accident monitoring function in a harsh environment based on RG 1.97 Cat 1 and 2 classification.

8. Identify the systems and equipment that are credited or required to support the systems and equipment identified in Step 7. Identify these items as Important-to-Safety.

9. Identify NSR systems and equipment that functionally interface (including digital pathways) with the Important-to-Safety equipment. Determine if a compromise by cyber attack of the NSR equipment interfacing with the Important-to-Safety equipment could adversely impact the Important-to-Safety function, then identify the NSR equipment as a CDA for protection as an Important-to-Safety equipment.

10. If identified Important-to-Safety systems and equipment contain a digital component that if compromised by a cyber attack, could adversely impact the proper operation of the identified Important-to-Safety systems and equipment, the digital component is an Important-to-Safety CDA.

Security Support System Scoping Criteria

With respect to security support systems, this guidance provides a process for determining if an

alternate means exists to maintain the capability of performing the security function in the event of a cyber attack. If the security support system only supports a security function, there is an alternate means to support the security function, and the alternate means is documented in plant procedures and trained on, the analysis could show the digital asset is not a CDA. Specifically, plants should address the following questions in the analysis:

- Does the digital asset only perform a security support function?
- Can the support function the support system provides be addressed by an alternate means?
- Is there a means to identify that the digital asset performing the security support function is no longer functioning?
- Is there sufficient time to implement the alternate means of performing the support function, before the failure or compromise impacts the security function?
- Is the alternate means captured in plant procedures and trained on?

If the answer to all above questions are yes, then the analysis should be documented in the digital asset analysis and the security support system digital asset is not a CDA.

EP DA/CDA Scoping Criteria:

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

Licensees must ensure EP-only CDAs previously assessed by NEI 13-10 revisions, found acceptable for use by the NRC, include the analysis that demonstrates detection of a cyber compromise and identifies adequate alternate methods to perform required EP functions to be re-classified as DAs. The NEI 13-10 EP-only assessments previously performed should be maintained as records in accordance with the licensee CSP section 4.13, "Document Control and Records Retention and Handling," as evidence of the reclassifying determination. After completing the analyses (see the table and the flowchart), no further evaluation is required for EP-only DA/CDA identification unless there is a subsequent change to the DA or the EP function.

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

If the licensee has implemented alternate methods that are adequately independent and diverse to fulfill the Emergency Plan requirements, the impact from compromise or loss of the EP-only digital asset will not prevent execution of the EP function.

EP Scoping Criteria for Critical Digital Asset Determination:

1. Does the digital asset only perform an EP function as described in the sixteen planning

standards (Section 2.3)?
a. No; is not associated with the EP criterion, or is also relied on for safety-related, important-to-safety, or security functions. The asset must be screened for other functions (SSEP) in NEI 10-04.
b. Yes; proceed to #2

2. Is the EP-only digital asset interconnected with other non-EP CDAs such that the DA can be leveraged (e.g., via a cyber attack or compromise) to adversely impact the interconnected non-EP CDA (i.e., the attack vector exists and has not been mitigated through the implementation of cyber security controls implemented in accordance with CSP Section 3.1.6)?

Note: If the EP DA provides protection that is inherited by a non-EP CDA, the EP DA must be assessed to ensure the attack vector does not exist or has been mitigated through the implementation of cyber security controls.
a. No; proceed to #3
b. Yes; identify DA as CDA

3. If the digital asset is compromised due to a cyber attack, can the cyber compromise of the DA be detected in time so that the EP function(s) performed by the digital asset can be fulfilled as required by the associated planning standard(s)?
a. No; identify DA as CDA
b. Yes; DA is not a CDA. The EP Scoping Analysis template below may be used to document the basis that supports the non-Critical classification.

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

Analysis of the scoping criteria may be documented using the Table in Attachment C below, and an overall EP Flowchart can be found in Attachment D.

Other Notes:

Licensees should note the following:

1) The above guidance should not inhibit the licensee from designating a component with multiple digital devices or a network containing multiple digital devices as a single CDA. However, the licensee must justify that protective requirements of the Cyber Security Plan are satisfied for these configurations.
2) The licensee may find a single digital device type associated with more than one Critical System, and that these Critical Systems perform different SSEP functions (e.g., Safety-Related and Emergency Preparedness).

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

Appendix A. **[Deleted]**

Appendix B. **[Deleted]**

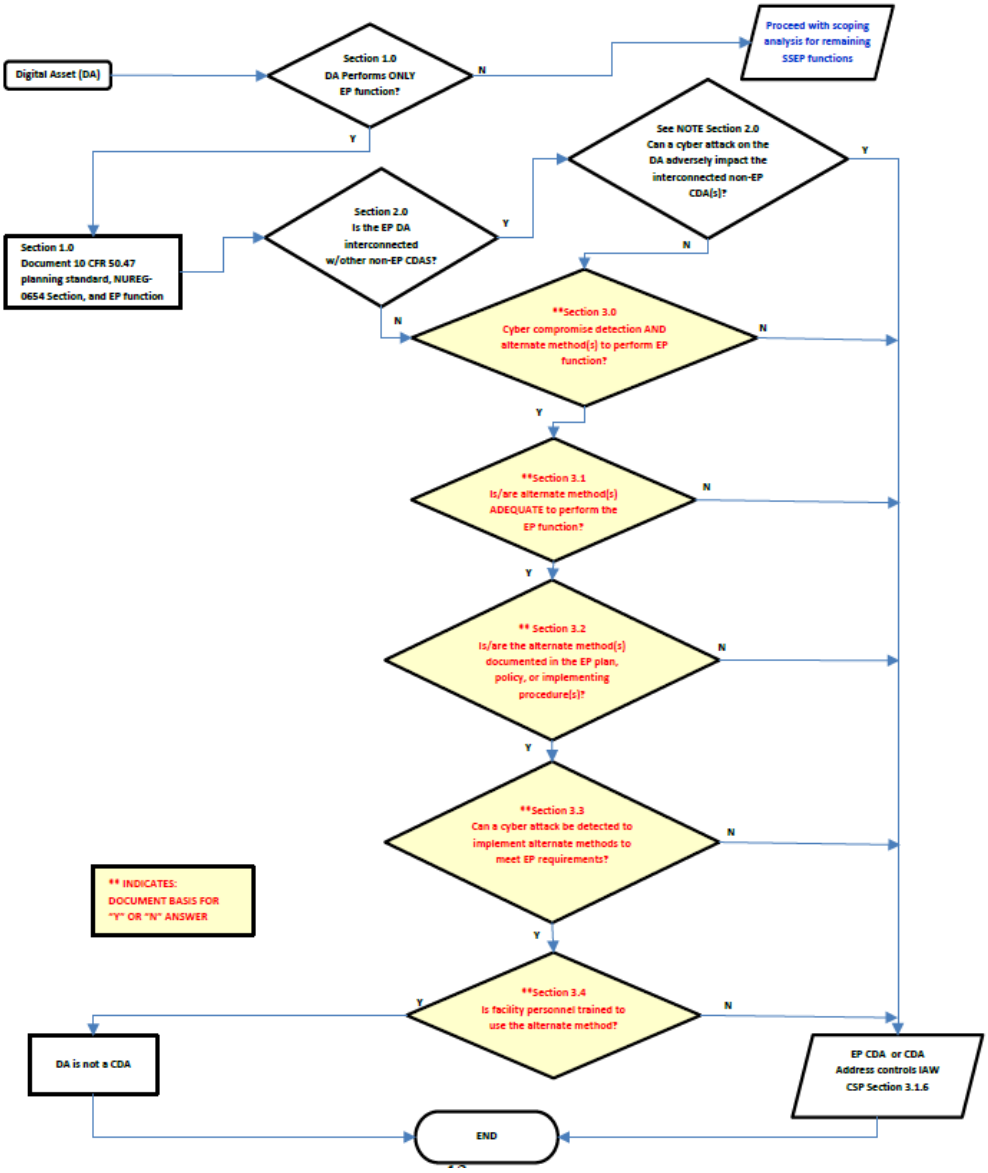
Appendix C.
EP Scoping Analysis

EP Scoping Analysis		
1.0	Does DA perform ONLY an EP-related or EP support systems and equipment function?	☐ YES ☐ NO
Note: The following guidance may be used for identification of EP CDAs associated with EP functions that are not otherwise also relied on for safety, important-to-safety, or security functions.		
If YES, document applicable 10 CFR 50.47 Planning Standard(s) below:		
If YES, document applicable NUREG -0654 Section(s) below:		
If YES, document the Emergency Planning function(s) below:		
IF YES, THEN proceed Step 2.0	IF NO, THEN proceed with scoping analysis for remaining SSEP functions	
2.0	Is the EP DA being assessed interconnected with other non-EP CDAs such that the DA can be leveraged (e.g., via a cyber attack or compromise) to adversely impact the interconnected non-EP CDA (i.e., the attack vector exists and has not been mitigated through the implementation of cyber security controls implemented in accordance with CSP Section 3.1.6)? Note: If the EP DA provides protection that is inherited by a non-EP CDA, the EP DA must be assessed to ensure the attack vector does not exist or has been mitigated through the implementation of cyber security controls.	☐ YES ☐ NO
	Note: Connectivity alone does not constitute a DA being identified as a CDA. For this question to be a YES, determine whether the DA could be leveraged to adversely impact another safety-related, important-to-safety, or security function AND if the interconnected CDA is not adequately protected from potential adverse impact. If the answer is NO, then the DA would be a CDA.	
IF NO, THEN proceed Step 3.0	IF YES, THEN the EP only asset is a CDA and requires controls provided in the licensee's CSP in accordance with Section 3.1.6.	
3.0	Can a cyber compromise of the DA be detected in time AND are alternate methods available for performing the intended EP function, including offsite communications, in time to fulfill the associated required EP standard(s)? **Document basis for YES or NO answer:**	☐ YES ☐ NO
IF YES, THEN proceed to Step 3.1	IF NO, THEN the EP only asset is a CDA and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	
3.1	Are one or more of the alternate methods administrative, non-digital, or if digital is it diverse and adequately independent? Document basis for YES or NO answer:	☐ YES ☐ NO
Note:		

1.) Two methods would be considered diverse and adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both methods of performing the EP function (e.g., a PBX-based phone system vs. satellite phones, data obtained by MET tower vs. data obtained through a weather service, data obtained from SPDS vs. received via fax, etc.). 2.) Administrative methods, including actions performed by personnel, can be considered as an alternate method provided it does not depend on the DA being assessed.		
IF YES, THEN proceed to Step 3.2	IF NO, THEN the EP only asset is a CDA and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	
3.2	Are the alternate methods documented? Document basis for YES or NO answer:	☐ YES ☐ NO
Note: The alternate methods must be documented in a plant plan, policy, or implementing procedure.		
IF YES, THEN proceed to Step 3.3	IF NO, THEN the EP only asset is a CDA and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	
3.3	Are there measures to detect a cyber attack on the DA so alternate methods can be implemented as required to meet the EP requirements to ensure the equipment can perform its intended function and an appropriate response initiated, if needed? Document basis for YES or NO answer.	☐ YES ☐ NO
Note: 1.) Specifically, a cyber attack that would prevent the EP-related equipment from performing its intended function can be detected and responded to prior to an adverse impact on the EP-related function during a radiological emergency. 2.) Measures for detection and response may be technical, procedural, or administrative, and could include periodic functional or availability testing (e.g., existing periodic operability tests performed on plant systems or equipment). The measures in place must include required EP equipment operational checks and the associated performance frequency established in the E-Plan or EP implementing procedures for the cyber security controls required periodicity checks to ensure the equipment can perform its intended function within the required EP timelines, if applicable, and an appropriate response initiated if the EP DA is compromised.		
IF YES, THEN proceed to Step 3.4	IF NO, THEN the EP only asset is a CDA and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	
3.4	Are appropriate facility personnel trained to use the alternate method? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN the EP DA is non-critical (i.e., DA is not a CDA).	IF NO, THEN the EP only asset is a CDA and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

Appendix D.
Identification of EP DA/CDA Flowchart
(Do not use the flowchart without following the guidance in Appendix C)



[THIS PAGE IS LEFT BLANK INTENTIONALLY]