NEI 10-04 [Revision 2]

Identifying Systems and Assets Subject to the Cyber Security Rule

July 2012

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

NEI 10-04 [Revision 2]

Nuclear Energy Institute

Identifying Systems and Assets Subject to the Cyber Security Rule

July 2012

Nuclear Energy Institute, 1776 I Street N. W., Suite 400, Washington D.C. (202.739.8000)

ACKNOWLEDGEMENTS

This document has been 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.

[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.

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 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 and important-to safety functions are defined in each plant's licensing basis documents (e.g. Final Safety Analysis Report and in the Plant Technical Specifications).

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 introduction of the term "Support System and Equipment," as related to SSEP functions is a new classification unique to the NRC Cyber Security Rule. These are systems and equipment which, if compromised, would adversely impact safety, 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. 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.

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 a set of questions 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 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).

Appendices A and B provide an example categorization of plant systems using the guidance in this document. These examples were derived principally from Maintenance Rule documentation and are not comprehensive. Licensees must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs that must be protected.

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, 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 not just safety and important-to-safety systems, but those non-safety related systems that can affect safety functions, including those systems that can impact reactivity. An identification of safety-related and important-to-safety systems has been made by licensees and can be found in their current licensing and design basis documentation.

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.

2.1.2. Important-to-Safety

Each licensee has, over time, developed a working application of the term important-to-safety in their licensing basis. Licensees should rely on their site-specific application in the identification of important-to-safety systems. Systems that perform important-to-safety functions should include those that are required to maintain diversity and defense-in-depth for safety functions (e.g., the diverse actuation system and credited diverse display systems). Licenses may have identified important-to-safety systems during renewal under the criteria in 10 CFR 54.4 (a)(2) and (a)(3).

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.

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 and important-to-safety systems include but may not be limited to:

a) FSAR
b) UFSAR
c) Design Basis documents
d) Technical Specifications
e) Licensee commitments with respect to RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants"
f) Maintenance Rule documentation
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.

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).

Additional requirements in 10 CFR 73.55 require licensees to, in part:

a) Establish, maintain, and implement a performance evaluation program;
b) Establish, maintain, and implement an access authorization program;
c) Establish, maintain, and implement an insider mitigation program; and
d) Use the site corrective action program to track, trend, correct and prevent recurrence of failures and deficiencies.

Licensees may use digital computing systems to facilitate the implementation of these other requirements in 10 CFR 73.55. These systems, however, are not a part of the onsite physical protection system, are not associated with the capability 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, and the failure or compromise of these information systems cannot lead to a radiological sabotage event. Accordingly, these systems are not within the scope of 10 CFR 73.54.

During the NRC's review of NEI 10-04 for endorsement, the NRC staff raised a concern regarding the cyber security status of the industry data-sharing mechanism, currently provided by the Personnel Access Data System (PADS). The concern regards a specific case for reinstatement of Unescorted Access Authorization/Unescorted Access (UAA/UA).

Subsequently, NEI issued System Administrator Bulletin 2012-02 to address the issue raised by the staff. The Bulletin requires the licensee companies to integrate actions consistent with the guidance in the Bulletin into their site procedures. These actions are designed to ensure that the PADS is not the sole source of information for making UAA/UA determinations. The guidance in the Bulletin will be incorporated into Revision 4, NEI 03-01, "Nuclear Power Plant Access Authorization Program." These actions ensure that the compromise of the PADS system would have no adverse impact on the access authorization program and, as the result, the PADS system remains out of the scope of 10 CFR 73.54.

Assets that must be analyzed in accordance with the requirements of 10 CFR 73.54(b)(1) include but are not limited to those associated with:

Security Systems

Physical barriers

1. Active Vehicle Barrier System [10 CFR 73.55(e)(10)(i)(A)]

Access controls

1. Access Control System and Devices
   [10 CFR 73.55(e)(8), (e)(9), (g)(1), (g)(4), (g)(5), (g)(6)]

Search programs
1. Metal Detection System [10 CFR 73.55 (h)(3)(i)]
2. Explosive Detection System [10 CFR 73.55 (h)(3)(i)]
3. X-ray Search System [10 CFR 73.55 (h)(3)(i)]

Detection and assessment systems
1. 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)]
2. 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)]
3. Illumination Systems [10 CFR 73.55 (i)(6)]

Communication requirements
1. Communications Systems [10 CFR 73.55 (j)]

Response requirements
1. Interdiction and Neutralization Systems (e.g., Remotely Operated Weapons System (ROWS)) [10 CFR 73.55 (k)]

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

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.

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.

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, security, or emergency preparedness functions. Support systems as equipment to be protected include those required to provide a stable environment conducive to the operational requirements of systems associated with SSEP functions or that, if compromised, would adversely impact system performing SSEP functions.

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) Fire protection systems
d) Secondary Power for Detection and Assessment Equipment
e) Support systems and equipment that are required to maintain diversity and defense-in-depth for safety functions (e.g., the diverse actuation system and credited diverse display 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).

Appendix A and B provide examples of plant systems that have been categorized during the development of this document using the questions in Section 4. The results are listed in Appendix A for a typical Pressurized Water Reactor (PWR) and Appendix B for a typical Boiling Water Reactor (BWR). These examples were derived principally from Maintenance Rule documentation and are not comprehensive. A site specific evaluation of systems must be performed.

CATEGORIZATION OF PLANT SYSTEMS

SAFETY

Is this system relied upon to remain functional during and following design-basis events (as defined in 10 CFR 50.49(b) (1)) to ensure:

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?

IMPORTANT-TO-SAFETY

1. Is this a non-safety related system whose failure could adversely impact any of the functions identified in the previous three "Safety Systems" questions?
2. Is this a non-safety related system that is part of the primary success path and functions or actuates to mitigate a transient that either assumes the failure of or presents a challenge to the integrity a fission product barrier?
3. Has operating experience or a probabilistic risk assessment shown that a non-safety related system function is significant to public health and safety?
4. Does the non-safety related system function to provide real-time or near-real-time plant status information to the operators for the safe operation of the plant during transients, and accidents?
5. Is this a structure, system, or component in the balance of plant that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient?
6. Is this a non-safety system required to maintain defense-in-depth and diversity requirements?

SECURITY

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

Is the system associated with or does it support functions identified in the Physical Security Plan or implementing procedures to satisfy the following:

Physical barriers

1. Does the system perform a function of the Active Vehicle Barrier System?

Access controls

2. Does the system perform a function to control access into protected and vital areas?
3. Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?
4. Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?
5. Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?
6. Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?

Search programs

7. Does the system perform a function for protected area searches (e.g. metal detection, explosive detection, X-ray)?

Detection and assessment systems

8. Does the system perform a function for intrusion detection?
9. Does the system perform a function associated with adversary assessment (including real-time and play-back video image system)?
10. Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?
11. Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?

Communication requirements

12. Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?

Response Requirements

13. Does the system perform a function for interdiction and neutralization?

Support Systems

14. Does the system provide secondary power for intrusion detection or alarm annunciation?
15. Does the system provide secondary power for alarm assessment?
16. Does the system provide secondary for non-portable communications?
17. Does the system provide secondary power for an active vehicle barrier system?

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 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

The section describes an acceptable method to consistently identify Critical Digital Assets (CDA). There are a number of sources from which the meaning of the terms "digital" and "Critical Digital Asset" can be either explicitly or implicitly deduced, including 10 CFR 73.54; NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6; Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," dated January 2010; Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2; IEEE 7-4.3.2-2003, and "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

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

- 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.

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;
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.

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

> 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).

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 and emergency preparedness).

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

APPENDIX A

EXAMPLE PRESSURIZED WATER REACTOR SYSTEMS

The table below reflects an example identification and categorization of systems for a generic Pressurized Water Reactor. This table is illustrative only and may be used to inform a site's understanding of the guidance in NEI 10-04. **A site must determine the specific categorization of their systems by conducting a site-specific analysis.**

Notes:

SR:	Safety Related
NSR/ITS:	Non-Safety Related/Important-to-Safety
SEC:	Security
EP:	Emergency Preparedness
Support:	Support system to SSEP
X:	The system satisfies the criteria for that column

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
480V AC DISTRIBUTION SYSTEM	X	X			
6.9KV AC DISTRIBUTION SYSTEM	X	X			
AIR COMPRESSORS	X	X			
MAIN CONTROL BOARD	X	X			
RADIATION MONITORING SYSTEM	X	X		X	
125V DC DISTRIBUTION-CLASS 1E	X				
250V DC DISTRIBUTION SYSTEM	X				
AUXILIARY FEEDWATER SYSTEM	X				
AUXILIARY RELAY CABINETS	X				
CHEMICAL AND VOLUME CONTROL	X				
COMPONENT COOLING WATER	X				
CONTAINMENT COOLING SYSTEM	X				
CONTAINMENT ISOLATION VALVES	X				
CONTAINMENT LINER-PENETRATION	X				
CONTAINMENT PRESS./LEAK DET.	X				
CONTAINMENT SPRAY SYSTEM	X				
CONTAINMENT SYSTEM	X				
CONTAINMENT VACUUM BREAKER	X				
DIESEL FUEL OIL SYSTEM	X				
DIESEL GENERATOR SYSTEM	X				
DIESEL JACKET WATER SYSTEM	X				
DIESEL LUBE OIL SYSTEM	X				
DIESEL STARTING AIR SYSTEM	X				
EMERGENCY SAFEGUARDS SEQUENCER	X				
EMERGENCY SERVICE WATER SYSTEM	X				
ESSENTIAL CHILLED WATER	X				

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
EXCORE NUCLEAR INSTRUMENT	X				
HIGH HEAD SAFETY INJECTION	X				
INCORE NUCLEAR INSTRUMENT	X				
INSTRUMENT AIR SYSTEM	X				
ISOLATION CABINETS	X				
LOW HEAD SAFETY INJECTION &RHR	X				
MAIN STEAM SYSTEM	X				
MCB-ACP TRANSFER PANELS	X				
NSSS PROCESS INSTRUMENTATION	X				
PASSIVE SAFETY INJECTION	X				
PRESSURIZER	X				
REACTOR COOLANT PUMP AND MOTOR	X				
REACTOR COOLANT SYSTEM	X				
REACTOR PROTECTION SYSTEM	X				
REACTOR VESSEL AND INTERNALS	X				
UNINTERRUPTIBLE AC - CLASS 1E	X				
EMERGENCY AC LIGHTING SYSTEM		X	X	X	
EMERGENCY DC LIGHTING SYSTEM		X	X		
125V DC DISTRIBUTION SYSTEM		X			X
208/120 VAC DISTRIBUTION		X			
AIRBORNE RADIOACTIVITY REMOVAL		X			
ANNUNCIATOR SYSTEMS		X		X	
AUX EQUIP & RECORDER PANEL		X			
AUXILIARY CONTROL PANEL		X			
AUXILIARY RESERVOIR		X			
BOP PROCESS INSTRUMENTATION		X			X
BORON RECYCLE SYSTEM		X			
BORON THERMAL REGENERATION		X			
BRIDGE CRANES		X			
CATHODIC PROTECTION SYSTEM		X			
CIRCULATING WATER SYSTEM		X			
CONDENSATE MAKE-UP		X			X
CONDENSATE POLISHING DEMIN		X			
CONDENSATE SYSTEM		X			
CONDENSER		X			
CONDENSER VACUUM SYSTEM		X			
CONTAINMENT PURGE SYSTEM		X			
COOLING TOWER SYSTEM		X			
DEMINERALIZED WATER SYSTEM		X			
ELECTRO-HYDRAULIC CONTROL		X			
EMERGENCY SCREEN WASH		X			
EXTRACTION STEAM SYSTEM		X			
FEEDWATER SYSTEM		X			
FUEL CASK HANDLING CRANE		X			
GENERATOR EXCITER SYSTEM		X			

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
GENERATOR GAS SYSTEM		X			
GENERATOR ISOLATED PHASE BUS		X			
GENERATOR SYSTEM		X			
GLAND SEAL AND STEAM SEAL		X			
GROSS FAILED FUEL DETECTION		X			
HEAT TRACING SYSTEM		X			
HEATER VENTS, DRAINS		X			
HYDROGEN SEAL OIL SYSTEM		X			
LOAD FREQUENCY CONTROL		X			
METAL IMPACT MONITORING		X			
NEW FUEL HANDLING SYSTEM		X			
PA SYSTEM		X			
POLAR CRANE SYSTEM		X			
POST ACCIDENT HYDROGEN SYSTEM		X		X	
POST ACCIDENT SAMPLING SYSTEM		X		X	
PROCESS COMPUTER		X		X	
REACTOR COOLANT PUMP VIBRATION		X			
REACTOR MAKE-UP WATER SYSTEM		X			
REFUELING SYSTEM		X			
ROD CONTROL SYSTEM		X			
ROD DRIVE COOLING SYSTEM		X			
ROD POSITION INDICATION SYSTEM		X			
SCREEN WASH SYSTEM		X			
SEISMIC MONITORING SYSTEM		X		X	
SITE FIRE DETECTION SYSTEM		X		X	
SITE FIRE PROTECTION SYSTEM		X			
SPENT FUEL POOL CLEANUP		X			
SPENT FUEL POOL COOLING SYSTEM		X			
SPENT FUEL SYSTEM		X			
STARTUP AND AUX TRANSFORMER		X			
STEAM CYCLE SAMPLING		X			
STEAM DUMP SYSTEM		X			
STEAM GEN. CHEMICAL ADDITION		X			
STEAM GENERATOR		X			
STEAM GENERATOR BLOWDOWN		X			
TURBINE SYSTEM		X			
TURBINE-GENERATOR LUBE OIL		X			
UNINTERRUPTIBLE AC SYSTEM		X			
ACCESS CONTROL SYSTEM			X		
CLOSED CIRCUIT T.V. SYSTEM			X		
INTRUSION DEVICES			X		
NORMAL AC LIGHTING SYSTEM			X		
PHYSICAL SEARCH SYSTEM			X		
SECURITY COMMUNICATION SYSTEM			X		
SECURITY COMPUTER SYSTEM			X		

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
SECURITY FENCING AND GATES			X		
SECURITY LIGHTING SYSTEM			X		
SECURITY POWER SYSTEM			X		
EMERGENCY COMMUNICATIONS				X	
EMERGENCY OFF-SITE FACILITY				X	
METEOROLOGICAL & ENVIRONMENTAL				X	
PABX SYSTEM				X	
TECHNICAL SUPPORT CENTER				X	
DIESEL FUEL OIL STORAGE BLDG					X
HVAC AUXILIARY BUILDING					X
HVAC CONTROL ROOM AREA					X
HVAC DIESEL BUILDING					X
HVAC DIESEL FUEL OIL BLDG					X
HVAC EMERG. SERV. WTR. STRUCT.					X
HVAC FUEL HANDLING BUILDING					X
NITROGEN SUPPLY/BLANKETING					X
NORMAL SERVICE WATER SYSTEM					X
OIL DRAINS SYSTEM					X
REACTOR COOLANT SAMPLING					X
CHEMICAL DRAINS SYSTEM					
ACID & CAUSTIC SYSTEM					
AUXILIARY BOILER FUEL OIL					
AUXILIARY BOILER/STEAM SYSTEM					
AUXILIARY STEAM CONDENSATE					
CARBON-DIOXIDE SUPPLY SYSTEM					
CHEMICAL STORAGE BLDG.					
CHLORINE BLDG. & SHED					
CIRCULATING WATER TREATMENT					
COMPRESSED GAS STORAGE					
COOLING TOWER BLOWDOWN					
COOLING TOWER MAKE-UP					
EXHAUST HOOD SPRAY					
FILTER BACKWASH STORAGE & TRAN					
GASEOUS WASTE PROCESSING					
HVAC ADMINISTRATIVE BLDG					
HVAC RADWASTE BUILDING					
LIGHTNING PROTECTION SYSTEM					
LIQUID WASTE PROCESSING					
LUBE OIL STORAGE & TRANSFER					
NONESSENTIAL CHILLED WATER					
OILY WASTE COLLECT & SEPARATOR					
OXYGEN SUPPLY SYSTEM					
PA SYS - OUTSIDE POWER BLOCK					
POTABLE WATER SYSTEM					
RADIOACTIVE EQUIPMENT DRAINS					

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
RADIOACTIVE FLOOR DRAINS					
RADWASTE SAMPLING SYSTEM					
SECONDARY DRAINS SYSTEM					
SECONDARY WASTE TREATMENT					
SERVICE AIR SYSTEM					
SEWAGE DRAINS SYSTEM					
SEWAGE TREATMENT SYSTEM					
SITE GROUNDING SYSTEM					
SPENT FUEL CASK					
SPENT FUEL CASK DECON & SPRAY					
SPENT RESIN AND CONCENTRATES					
STORM DRAINS SYSTEM					
UPFLOW FILTER SYSTEM					
WASTE NEUTRALIZATION SYSTEM					
WASTE PROCESS ANALOG CONTROL					
WASTE PROCESS COMPUTER					
WASTE PROCESSING ANNUNCIATORS					
WASTE PROCESSING CONTROL BOARD					
SWITCHYARD SYSTEM					

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

APPENDIX B

EXAMPLE BOILING WATER REACTOR SYSTEMS

The table below reflects an example identification and categorization of systems for a generic Boiling Water Reactor. This table is illustrative only and may be used to inform a site's understanding of the guidance in NEI 10-04. **A site must determine the specific categorization of their systems by conducting a site-specific analysis.**

Notes:

SR:	Safety Related
NSR/ITS:	Non-Safety Related/Important-to-Safety
SEC:	Security
EP:	Emergency Preparedness
Support:	Support system to SSEP
X:	The system satisfies the criteria for that column

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
DIESEL GENERATOR SYSTEM	X				
DIESEL GEN FUEL OIL		X			
DG JKT WTR & DG DEMIN WTR		X			
4 KV AC DISTRIBUTION SYSTEM	X	X			
480V AC DISTRIBUTION SYSTEM	X	X			
208/120 VAC DISTRIBUTION SYS	X	X			
UNINTERRUPTIBLE AC SYS	X	X			
125 VDC BATTERY CHARGER SYS	X	X			
125 VDC BATTERIES & BAT DIST	X	X			
PROCESS COMPUTER				X	X
MAIN CTRL BOARD (RTGB)		X			
ANNUNCIATOR SYSTEMS		X		X	
AUX.CONTROL BOARD		X			
INSTR AIR	X	X			
RX VESSEL & INTERNALS	X				
NUCLEAR STM SUP SHUTOFF	X				
NEUTRON MONITORING SYSTEM	X				
REACTOR PROT SYS (RPS)	X				
CORE SPRAY SYSTEM (CS)	X				
STANDBY LIQUID CTRL (SLC)	X				
RESIDUAL HEAT REMOVAL SYS	X				
AUTO DEPRESSURIZATION	X				
HIGH PRESS COOLANT INJECTION (HPCI)	X				
DIESEL GEN SERV WTR SYS	X				
DIESEL GEN STRT AIR SYS	X				
250 VDC DISTRIBUTION SYSTEM	X				

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
STANDBY GAS TREATMENT SYS	X				
ROD CONTROL SYSTEM		X			
CNTRL ROD DRIVE HYDRL		X			
REACTOR WTR CLEAN-UP RWCU		X			
REACTOR RECIRCULATION SYS		X			
CONTAINMENT ATMOS. CTRL		X			
REACTOR CORE ISOL COOLANT		X			
REACTOR BLDG SAMPLING SYS		X		X	
POST ACCIDENT SMPL		X		X	
MAIN STEAM SYS (INC EHC)		X			
EXTRACTION STEAM SYSTEM		X			
MSR DRN & REHEAT STM		X			
AUXILIARY BOILER SYSTEM		X			X
FEEDWATER SYSTEM		X			
HTR DRN, MISC VENT&DRN		X			
COND & RET COND		X			
COND FLT DEMIN SYSTEM		X			
COND DEEP BED&OUT DEMI		X			
COND MAKE-UP (INC MWT)		X			
CONDENSER		X			
OFF GAS & CNDSR VACUUM		X			
CIRCULATING WATER SYSTEM		X			
SCREEN WASH SYSTEM		X			
INTAKE & DISCHARGE CANAL		X			
SERVICE WATER SYSTEM		X			
RX BLDG CLO COOL WTR SYS		X			
TURBINE SYSTEM		X			
TURBINE CTRL SYS (INC.TSI)		X			
TURBINE-GENERATOR LUBE OIL SYS		X			
GLAND SEAL & STM SEAL		X			
EXHAUST HOOD SPRAY SYSTEM		X			
GENERATOR SYSTEM		X			
GENERATOR EXCITER SYSTEM		X			
GENERATOR GAS SYSTEM		X			
STATOR COOLING WATER SYSTEM		X			
HYDROGEN SEAL OIL SYSTEM		X			
GENERATOR ISOLATED PHASE BUS		X			
24V DC BATTERY SYSTEM		X			
24V DC BATTERY CHARGER SYSTEM		X			
24/48V DC DISTRIBUTION SYSTEM		X			
DIESEL GEN LUBE OIL SYSTEM		X			
DIESEL GEN INTK/EXH SYSTEM		X			
SEISMIC MONITORING SYSTEM		X		X	
SERVICE AIR SYSTEM		X			
PNEUMATIC NITROGEN SYS		X			

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
HYDROGEN SUPPLY SYS		X			
CARBON-DIOXIDE SUPPLY SYS		X			
FIRE PROTECTION SYSTEM		X			
FIRE DETECTION SYSTEM		X		X	
FIRE PROTECTION CO2 SYSTEM		X			
HYDROGEN WTR		X			
PROCESS RAD MONITORING SYS		X			
AREA RAD MONITORING SYSTEM		X		X	
AUGMENTED OFFGAS SYSTEM		X			
REFUELING SYS		X			
RX VESSEL SERV EQUIP		X			
SPENT FUEL SYSTEM		X			
FUEL POOL COOL SYSTEM		X			
PRIMARY CONT. (INC.LINER&PENE)		X			
BRIDGE CRANES		X			
NORMAL AC LIGHTING SYS			X		X
EMERGENCY DC LIGHTING SYS			X		X
SECURITY COMPUTER SYSTEM			X		
CARD READER/ACCESS CTRL SYS			X		
CLOSED CIRCUIT T.V. SYSTEM			X		
INTRUSION DEVICES			X		
SECUR FENCING,GATES, ACCESS PT			X		
PHYSICAL SEARCH SYSTEM			X		
SECURITY COMMUNICATION SYSTEM			X		
ERFIS COMPUTER SYS (INC. SPDS)				X	
METEOROLOGICAL & ENVIR				X	
START-UP AUX.&AUX XFMR		X			
HEAT TRACING SYSTEM		X			X
HVAC DIESEL GENERATOR BLDG		X			X
HVAC REACTOR BUILDING		X			X
HVAC CONTROL BUILDING		X			X
PA SYSTEM					X
RADWASTE SAMPLING SYSTEM					
TURBINE BLDG SMPL SYSTEM				X	
TUR BLDG CLO COOL WTR SYS		X			
CATHODIC PROTECTION SYSTEM					
TURNING GEAR SYSTEM		X			
SAMG DIESEL GENERATOR SYSTEM					
LIGHTNING PROTECTION SYSTEM		X			
MICROWAVE SYSTEM			X		
LUBE OIL STR & XFER SYSTEM		X			X
FUEL OIL SYSTEM		X			
HALON SUPPLY SYSTEM		X			
SEWAGE TREATMENT SYSTEM					
STORM DRAINS SYSTEM					

SYSTEM NAME	SR	NSR/ITS	SEC	EP	Support
OIL DRAINS SYSTEM					
RADIOACTIVE FLR DRN SYSTEM					
RADIOACTIVE EQUIP DRN SYS					
WATER TREAMENT (INC. CG,CS,CV)					
CHLORINATION (INC. CG,CS,CV					
SODUIM HYPOCHLORITE INJECT					
POTABLE WATER SYSTEM					
DEMINERALIZED WATER SYS					
CAUSTIC SYSTEM					
ACID SYSTEM					
SOLID WASTE PROCESSING					
LIQUID WASTE PROCESSING					
DRY SPENT FUEL STORAGE					
GANTRY CRANES					
24KV SWITCHYARD SYSTEM					