	A	B	C	D	E	F
1	NRC Staff Comments on NEI 10-04 Revision 2 dated April 2012					
2	#	Section	Page	NEI 10-04 Text	Proposed Change(s)	Comment(s)
3	1	1.2	2	Licensees must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs that must be protected.	Change text to read as follows: "Licensees must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs that must be protected in accordance with the requirements set forth in 10 CFR 73.54."	
4	2	2.1	3	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.	Correct text as follows: "In the context of 10 CFR 73.54, identifying ~~A~~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."	
5	3	2.1.1	4	(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.	General comment: Include references to 10 CFR 54.4(a)(2) and (a)(3)	
6	4	2.1.2	4	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.	Include the following sentence to this paragraph: 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).	In addition to the clarification provided in Staff Requirements Memorandum (SRM) COMWCO-10-0001 and SECY 10-0153 concering important to safety systems, Chapter 7 of NUREG 0800 "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" provides criteria for determining non-safety systems that qualify as importantant to safety. Examples include systems that are necessary to maintain diversity and defense-in-depth for performing safety functions, such as the diverse actuation system and non-safety displays.
7	5	2.1.2	4	First paragraph of the section	Add as the last sentence to the first paragraph: "At a minimum, licensees should identify any systems that are credited in their facility licensing basis for the purpose of complying with NRC regulations and/or General Design Criteria."	In addition to the clarification provided in Staff Requirements Memorandum (SRM) COMWCO-10-0001 and SECY 10-0153 concering important to safety systems, Chapter 7 of NUREG 0800 "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" provides criteria for determining non-safety systems that qualify as importantant to safety. Examples include systems that are necessary to maintain diversity and defense-in-depth for performing safety functions, such as the diverse actuation system and non-safety displays.
8	6	2.1.2	4	Additionally, on October 21, 2010, the NRC issued Staff Requirements Memorandum (SRM) COMWCO-10-0001, "regulations of Cyber Security at Nuclear power Plants," to clarify NRC poisitions on structures, systmes, and compoennts in the balnce of plant with respect to NRC's Cyber Seucrity Rule. The SRM states: "The Commission has determined as a matter of policy that the NRC's cyber seucirty rule at 10 CFR 73.54 should be interpreted to include structures, systems,a nd components in teh Balance of Plant that have a nexus to radiological health and safety at NRC-licensed nuclear power plants."	Add the following statement to the end of this paragraph: "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 reacitivty of an NPP, and are therefore within the scope of important-to-safety functions described in 10CFR 73.54(a)(1)."	
9	7	2.1.2	5	Last paragraph / listing of section 2.1.2	Add to the list: "Licensee formal communications to the NRC (e.g., responses to Generic Communications or NRC Orders)."	Another source for identification of potential systems to protect may be found in generic communications (including responses) and/or NRC Orders. These systems would likely be identified in other documentation, but it may not hurt to list those sources here.

	A	B	C	D	E	F
1	NRC Staff Comments on NEI 10-04 Revision 2 dated April 2012					
2	#	Section	Page	NEI 10-04 Text	Proposed Change(s)	Comment(s)
10	8	2.2	5	These computer systems are not a part of the physical protection system, and may not satisfy the requirements of 10 CFR 73.54(b)(1).	Change text to read as follows: These computer systems are not a part of the physical protection system~~,~~ ~~and may not satisfy the requirements of 10 CFR 73.54(b)(1).~~	The staff does not agree with the wording used in this case, and that it could be misleading in cases where such systems may be within the scope of 10 CFR 73.54.
11	9	2.2	5	These systems may, however, be important for the protection of the public health and safety under certain conditions, and licensees should consider the extent to which information stored in these computers is used in the decision making process for reinstating UAA/UA.	Change text to read as follows: These systems may, however, be important for the protection of the public health and safety under certain conditions, and licensees should consider the extent to which information stored in these computers is used in the decision making process for reinstating UAA/UA consistent with 10 CFR 73.56. Under such conditions, these systems may be within the scope of 10 CFR 73.54.	Under certain circumstances the compromise of these computer systems can adversly impact the UA/UAA re-instatement determination of an individual. Therefore these systems may be within the scope of 10 CFR 73.54. However, if licensees implement measures that eliminate the use of these computer systems as a sole source of data verification for making UA/UAA determinations for these certain circumstances, these computer systems may be out of the scope of 10 CFR 73.54.
12	10	2.2	6		Include the following within the list of Security Systems: Access Authorization 1. Access Authorization Computer Systems [10 CFR 73.56] If licensees implement measures that elimiate the use of these computer systems as a sole source of data verification for making UA/UAA determinations for these certain circumstances these computer systems may be out of the scope of 10 CFR 73.54.	The compromise of computer systems used to implement portions of the Access Authorization Program for managing data used for making UA/UAA determinations could have an adverse impact on licensee's ability to comply with 10 CFR 73.56 and the Insider Mitigation Program.
13	11	2.3	6-7	The emergency preparedness systems wihtin the scope of the cyber-security rule are those which, if compromised by a cyber attack, would prevent a licensee from implementing measures needed for the protection of the public in the event of a radiological emergency. Such sysetms and equipment include digital computer, and communication systems and networks associated with these measures.	Change text to read as follows: The emergency preparedness systems within the scope of the cyber-security rule ~~are those which, if compromised by a cyber attack, would prevent a licensee from implementing measures needed for the protection of the public in the event of a radiological emergency. Such sysetms and equipment~~ include digital computer, and communication systems and networks associated with ~~these~~ measures needed for the protection of the public in the event of a radiological emergency	
14	12	2.3	7	Licensees must be able to demonstrate the capability to perform emergency response functions even in cases where they may use equipment they for which they do not have full custody and control and cannot reasonably implement cyber security protective measures.	Correct text as follows: Licensees must be able to demonstrate the capability to perform emergency response functions even in cases where they may use equipment ~~they~~ for which they do not have full custody and control and cannot reasonably implement cyber security protective measures.	
15	13	2.3	7-8	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). Such systems should not be vulnerable to a particular cyber attack that would render more than one means inoperable or unreliable. Unless both the primary and the backup EP systems are vulnerable to the same mode of cyber-attack, only one of these EP systems need be considered under 10 CFR 73.54(b)(1). For example, a licensee's Emergency Plan may require the use of an Internet-based program for tracking, trending, and communicating emergency response data with a backup capability that uses analog public telephone lines. In the absence of a common mode cyber-attack that would simultaneously render both communications methods inoperable, only one of these systems would need to be protected as provided in 10 CFR 73.54. 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	Change text to read as follows: 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.	10 CFR 73.54 does not distinguish between primary and backup systems. In addition, the cyber security rule specifies the protection of digital assets making the comparison to analog systems unclear.

	A	B	C	D	E	F
1	NRC Staff Comments on NEI 10-04 Revision 2 dated April 2012					
2	#	Section	Page	NEI 10-04 Text	Proposed Change(s)	Comment(s)
16	14	Table 2.3.1	9	10 CFR 50.47(b)(2) Additional Information Column	Add IV.A.9" to the listing.	
17	15	Table 2.3.2	12	10 CFR 50.47(b)(11) Additional Information Column	Change "IV.E.1" to read "IV.E".	
18	16	Table 2.3.3	12	10 CFR 50.47(b)(12) Additional Information Column	Change "IV.E.5-7" to read "IV.E"	
19	17	2.4	14	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.	Change text to read as follows: 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 and those systems that, compromised, may adversely impact systems performing SSEP functions. This includes any systems that are either directly or indirectly connected to systems that perform SSEP functions.	The original text leaves out systems that perform maintanence and tests. These systems are very vulnerable to compromise as they are not typically physically bound to specific locations and thus are not afforded some of the physical security protective measures that other systems receive. This guidance also leaves out systems that are either directly or indirectly connected to systems that perform SSEP functions as stated in RG 5.71.
20	18	2.4	14	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	Change text to read as follows: 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) Maintanence and test digital equipment that are used to service, monitor, troubleshoot and/or install software on systems that perform a SSEP function f) Systems credited in the facility licensing basis for the purpose of complying with NRC regulations and/or General Design Criteria	NRC staff have seen systems, including safety systems, that have dedicated digital "maintenance" terminals and/or laptops. These devices are used for tasks like updating setpoints, troubleshooting the digital system and installing software patches. Although often not permanently connected to the plant system(s), these "maintenance" systems should be protected from cyber threats at a level commensurate with the systems that they service.
21	19	4	17	1. Is this a non-safety related system whose failure could prevent satisfactory accomplishment of any of the functions identified in the previous three "Safety Systems" questions?	Change text to read as follows: Is this a non-safety related system whose failure could adversely impact any of the functions identified in the previous three "Safety Systems" questions?	We should not limit this to prevent satisfactory accomplishment, but expand it to include any adverse impact including delaying or degrading the performance of safety functions.
22	20	4	17		Under important-to-safety, add the following: "6. Is this a non-safety system required to maintain defense-in-depth and diversity requirements?"	This is to ensure that systems such as the diverse actuation system are also protected from cyber attacks.