Response to Public Comments on Draft Regulatory Guide (DG)-5061 "Cyber Security Programs for Nuclear Power Reactors" Proposed Revision 1 of Regulatory Guide (RG) 5.71

On March 3, 2022, the NRC published a notice in the *Federal Register* (87 *FR* 12208) that Revision 1 to Draft Regulatory Guide, DG-5071, Proposed Revision 1 of RG 5.71, was available for public comment, reference Docket ID NRC–2021–0143, The public comment period ended on April 3, 2022. The NRC received comments from the organizations listed below. The NRC has combined the comments and NRC staff responses in the following table:

Comments were received from the following individuals/companies and can be found in Agency Document Access Management Systems (ADAMS):

Comments Ameren-#	A. Lowery Ameren - Callaway Energy Center Email: alowry@ameren.com ADAMS Accession No. ML22124A082
Comments Kinectrics-#	Gary Locklear Kinectrics Cyber Security Programs for Nuclear Power Reactors Fuquay Varina, NC 27526 gary.locklear@kinectrics.com Phone: 919 306 4946 ADAMS Accession No. ML22124A078
Comments NEI-#	Richard Mogavero Senior Project Manager, Nuclear Security & Incident Preparedness Nuclear Energy Institute (NEI) www.nei.org 1201 F Street, NW, Suite 1100 Washington, DC 20004 P: 202.739.8174 rm@nei.org ADAMS Accession No. ML22124A079 (duplicate of ML22124A081)
Comments NuScale-#	Director, Regulatory Affairs NuScale Power, LLC, www.nuscalepower.com 1100 NE Circle Blvd., Suite 200 Corvallis, Oregon 97330 Office 541.360-0500 ADAMS Accession No. ML22125A007

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
Ameren-1	General	It is confusing that section C of the Reg Guide body and Appendix C both have sections numbers that start with C. Then, in the template in Appendix A, the C is dropped when referring to guidance from section C of the Reg Guide body. Suggest eliminating the C from the section numbers in the Reg Guide body. The first part of the Appendix A template basically requires doing everything in section 3.3 of the main Reg Guide section C. Following template sections sometimes repeat the language from the Reg Guide body and sometimes refer back to other sections of the body. This makes it difficult to read through the resulting Cyber Security Plan and determine what is being done. It would be necessary to always keep a copy of the Reg Guide in hand in order to determine what is required by the Cyber Security Plan if the template is used. Suggest incorporating the Reg Guide language into the Appendix A template so that a stand-alone Cyber Security Plan document is created from the template.	NRC staff agrees in part and disagrees in part with this comment. We agree that clarification is needed when referring to sections in Section C Staff Regulatory Guidance and sections in Appendix C. Any text within RG 5.71 referring to text in Section C Staff Regulatory Guidance is written as "RG 5.71, Staff Regulatory Guidance, Section <section number>" where section number is the applicable section number). As an example, RG 5.71, Staff Regulatory Guidance, Section C.4.1 is used to refer to text in section C.4.1 of the Staff Regulatory Guidance. When referring to text in Appendices A, B, or C the text is written as "Appendix <name>.<section number>" where name is A, B, or C and section number is the applicable section number. For example, a reference to Section 3.2 of Appendix C is written as Appendix C.3.2. The RG was reviewed to verify consistency of the text and updated accordingly. The NRC staff does not agree with the suggestion to incorporate the Reg Guide text in Appendix A. Not all of the text in Section C Staff Regulatory Guidance is necessary or useful in the Appendix A which is used by licensees as a template for cybersecurity plans. No change was made in the RG based on this part of the comment.
Ameren-2	Glossary	Critical digital Asset (CDA) – This definition is incomplete and would result in any digital device in a critical system being considered a CDA. When systems are evaluated, all system functions are examined and if ANY of these are SSEP functions, then the system is classified as a critical system. There could be stand-alone digital devices in this system, however, that only perform non-SSEP functions. These devices would not be classified as CDAs, even though they are digital components in a critical system. The definition needs to include bounding criteria regarding the digital device performing / supporting / protecting a SSEP function.	The NRC staff agrees with the comment. The text for the definition of CDA has been changed in the RG to use the definition in NEI 08-09, revision 6. This definition is as follows – "critical digital asset (CDA) 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 cyberattack would result in an adverse impact to a SSEP Function."

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
Ameren-3	Glossary	Attack vector and attack pathway – These definitions do not align with the industry use of these terms. While the term threat / attack vector is used extensively throughout several NRC approved NEI documents, the only place this term has been defined is in NEI 10-09. While this document was not approved by the NRC and is generally not used by the industry, the industry has adopted its terminology for pathways and attack vectors as these were not defined elsewhere. This document states: For the purposes of implementing cyber security plans, pathways that introduce vulnerabilities are associated with the following attack vectors: 1) Direct Network Connectivity 2) Wireless Network Capability 3) Portable Media and Equipment 4) Supply Chain 5) Direct Physical Access Licensees have developed their justifications for addressing security controls using this definition. Per NEI 08-09 section 3.1.6 (and Reg Guide A.3.1.6), not implementing a security control may be justified by demonstrating the attack vector does not exist. The industry understanding is that these justifications are based on evaluating the pathway rather than the method and while the results may typically be the same, this could be considered a change in philosophy. The best solution could be to move away from the attack vector term and simply focus on evaluating the threat the security control protects against and determining whether that threat exists for the specific CDA. This could then be addressed by eliminating either the method or the pathway. In any case, this is an item that needs to be addressed. If the NRC position is that the industry needs to be specifically evaluating the attack mechanism and not the pathway, then this is a change in philosophy that	NRC staff agrees in part and disagrees in part with this comment. The NRC staff agrees, as the commenter noted, NEI 10-09 was not approved for use by the NRC. NRC staff also agrees with the comment that the text on page 21 was contradictory. It incorrectly stated that attack vector is a delivery mechanism or vulnerability/exploit has been corrected to state that an attack vector is a delivery mechanism and vulnerability/exploit. The NRC staff disagrees with the comment that evaluating the pathway is sufficient in addressing security controls in accordance with NEI 08-09 section 3.1.6. During the approval of Addendum 1 of NEI 08-09 and during NRC inspections, the NRC staff and inspectors have repeatedly clarified that attack vector and attack pathway are not synonymous and this clarification has been documented in the revised RG released for public comment in RG 5.71, Staff Regulatory Guidance, Section C.3.3. and Appendix A.3.1.6, and in the attack vector and attack vector definitions in the glossary. The original version of RG 5.71 used the word “pathway” in the context of “communication pathway”. The original RG 5.71 also used the terms “pathway” and “attack vector” in distinct, different contexts. The original text of RG 5.71, Staff Regulatory Guidance, Section C.3.3 and Appendix A.3.1.6 used the term attack vector to help determine the selection and application of security controls. Pathways can be circumvented so considering only a pathway for mitigating cyberattack can result in insufficient analysis. Therefore, attack vectors analysis should be used for applying security controls, not simply pathway analysis. Licensees must demonstrate that the associated attack vectors (delivery mechanism and vulnerability/exploit) do not exist. Accordingly, understanding the intent of a control is important when evaluating if an alternative approach to addressing the attack vector will effectively mitigate the threat. Understanding the intent of the control will enable effective evaluation of the alternate approach to mitigating the threat

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		needs to be communicated. If the intent is just to evaluate the threat and it is acceptable to justify that the threat does not exist by elimination of either the pathway or method, then section A.3.1.6 (and the NEI documents) should be revised accordingly. To add further confusion, the second paragraph on page 21 indicates that an attack vector is a delivery mechanism or vulnerability/exploit. The attack vector definition, on the other hand, only says it is the mechanism and can be used to exploit a vulnerability.	posed by the attack vector.
Ameren-4	Page 22	Under the information to collect when following the CDA identification process, clarification is needed to explain what is meant by "developmental and evaluation-related assurance requirements".	The NRC staff agrees with this comment. The text in the RG 5.71, Revision 1, Staff Regulatory Guidance Section C.3.1.3 was changed (new text is underlined) as follows: • "developmental and evaluation-related assurance requirements <u>to be used by licensees for verifying the design, implementation, and testing of security functionality in products received in acquired devices.</u>"
Ameren-5	Page 28, A-6	The language for implementing alternative controls when a security control cannot be implemented does not align with A.3.1.6, which uses more recently agreed upon language also reflected in NEI 08-09 Addendum 1. A new bullet was added which states " Apply the security controls described in Appendices B and C to this guide, based on the maximum consequences of a successful cyber attack on the CDAs in terms of plant safety and security". This terminology is vague and does not seem to align with the methodology used for protecting safety and security functions.	The NRC staff agrees in part and disagrees in part with this comment. The NRC staff agrees that the text in RG 5.71, Revision 1, Appendix A.3.1.6 is not identical to text in NEI 08-09, Addendum 1. However, although the language is not identical, the NRC staff does not believe that the new language in Appendix A.3.1.6 contradicts the language in NEI 08-09, Addendum 1. The NRC staff agrees that the language quoted by the commenter is new language in RG 5.71, Staff Regulatory Guidance Section C.3.3. Consistent with language in Staff Regulatory Guidance Section C.3.2, a licensee may implement a graded approach for the application of security controls taking into account the consequences resulting from a successful cyber-attack. The NRC staff has added language stating that the application of security controls should be based on the maximum consequences of a successful cyber-attack to address a lesson learned from cybersecurity inspection

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
			violations where a cross cutting aspect of conservative bias was used in applying security controls. In some cases, this conservative approach has resulted in a licensee applying security controls that did not address the potential maximum consequences resulting from a successful cyber attack. The NRC staff does not agree that this new language is vague. The concept of a graded, consequence-based approach to the application of cybersecurity controls is discussed throughout this RG. The use of the "maximum consequence" language is to remind licensees that their application of cybersecurity controls should address the most risk-significant consequences resulting from a successful cybersecurity attack. This approach is consistent with the language in Staff Regulatory Guidance Section C.3.2.1. Section C.3.2.1 states: "Functions are protected commensurate with their safety and security significance through the determination and use of appropriate security levels. The security level defines the degree of security needed to protect the function, based on the consequences to plant safety and security from loss or impairment of the function due to cyberattacks. This is an example of a consequence-based, graded approach for risk-informed security." The NRC staff has determined that the language quoted by the commenter should also be added to Appendix A.3.1.6.
Ameren-6	Page 37, A-8	The final bullet under integrating the cyber security program into the physical security program discusses periodically exercising the entire security force using multiple realistic scenarios combining both physical and cyber simulated attacks. This requirement would better fit in a physical security Reg Guide as the cyber security organization does not have control over exercising the entire security force. Additionally, in physical security drills, it makes more sense to simulate a cyber attack simply as a failed or compromised piece of equipment that should be assumed to be lost. Cyber security incident response drills and physical attack drills typically follow	The NRC staff agrees with the comment. The bullet item has been deleted from RG 5.71, Revision 1, in Staff Regulatory Guidance Section C.4.1 and in Appendix A.3.2.

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		different timelines and use different response teams, making integration into a single drill impractical. Response to a cyber attack would be integrated with physical security as they are a member of the CSIRT. However, in a physical attack, security would simply be dealing with lost equipment and their response would likely not be impacted by the relatively longer timeline of the CSIRT determining the cause of a cyber attack and recovering a system. The NRC is currently soliciting input regarding integration of cyber security into Force On Force drills, and this is a more appropriate way to drive this particular item.	
Ameren-7	Page 40	In the first paragraph, clarification is needed regarding the meaning of " This effectiveness analysis should provide key information about the results of previous policy and acquisition decisions".	The NRC staff agrees with this comment. The following underlined text was added to RG 5.71, Revision 1, Staff Regulatory Guidance Section C.4.1.2 for clarification - "This effectiveness analysis should provide key information about the results of previous policy and acquisition decisions. This should include, but is not limited to, information on corrective actions implemented pertaining to the cybersecurity program and the enrollment of newly installed plant equipment in the cybersecurity program."
Ameren-8	Page A-2	Under A.3, the reference to 10 CFR 73 Appendix G seems unnecessary as the cyber event reporting was placed in 10 CFR 73.71. Any cyber event causing one of the criteria in Appendix G to be met would also be included as a reportable event in 10 CFR 73.71.	The NRC staff agrees that both entries are unnecessary, and the following change (strikethrough for deleted text) has been made to the text in RG 5.71, Revision 1, Appendix A.3 – [Licensee/Applicant] will also report any cyberattacks or incidents at [Site] to the NRC, as required by 10 CFR 73.71, "Reporting of Safeguards Events." ~~and Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73, "Physical Protection of Plants and Materials."~~
Ameren-9	Page A-9	Section A.4.1.1 could be interpreted to require the verification of every security control on every CDA every year. This would be a time consuming and resource intensive effort that would provide little benefit. Discussions with the NRC determined this was not the intent and this was meant more as a review of the effectiveness of the program based controls and to ensure	The NRC agrees in part and disagrees in part with this comment. We agree yearly verification of every control on every CDA is not necessary. We have communicated with licensees that they could use operational and management controls in Appendix C of RG 5.71 with ongoing monitoring of CDAs employing a consequence-based, graded approach. An example of ongoing monitoring would be whitelisting

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		ongoing monitoring of CDAs was occurring. This section should be re-worded to clarify the intent, or possibly be treated as an introduction section for the following sections or integrated into section A.4.1.2.	applications on a CDA that would notify a SIEM when a change is made on the CDA. Another example is verifying the configuration of a CDA in a vital area whenever the CDA is accessed by maintenance staff. We will add the following clarifying text (new text is underlined) to RG 5.71, Revision 1, Appendix A.4.1.1 "[Licensee/Applicant] performs periodic assessments to verify that the security controls implemented for each CDA remain robust, resilient, and effective throughout the life cycle. The CST verifies the status of these security controls [on at least an annual basis] or in accordance with the specific requirements for each security control, as described in Appendices B and C, whichever is more frequent. <u>An example of an acceptable alternate for verification of a security control at a specific periodicity would be whitelisting applications on a CDA that would notify a SIEM when a change is made on the CDA. Another example of an acceptable alternate is verifying the configuration of a CDA in a vital area whenever the CDA is accessed by maintenance staff.</u>" The staff disagrees with the suggestion to integrate Appendix A.4.1.1 into Appendix A.4.1.2. The purpose of licensee activities in Appendix A.4.1.1 is to periodically verify that the implemented security controls remain in place and function correctly to ensure security against a cyber-attack. The purpose of licensee activities in Appendix A.4.1.2 is to verify that the implemented security controls remain effective in addressing evolving threats and newly identified vulnerabilities.
Ameren-10	Page A-10	In the second paragraph of A.4.2, clarification is needed to explain the intent of "address safety, reliability, and security engineering activities".	The NRC staff agrees with this comment. The intent of the control is for the licensee to determine what configuration control activities are applicable for devices when a plant is decommissioned. However, the NRC staff agrees that the text quoted by the commenter is unclear. Accordingly, the NRC staff have revised the text in the second paragraph of RG 5.71, Revision 1, Appendix A.4.2 to state: "During the retirement phase while fuel is onsite, the [design control and configuration management procedures, or other

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
			procedural processes] continue to apply to remaining CDAs that affect safety-related and important-to-safety, security, or emergency preparedness functions." The NRC staff has determined that this revised text provides greater clarity.
Ameren-11	Appendices B and C	The addition of the "Control Intent" sections provide useful information regarding the threat the control is intended to protect against which then aids in the development of appropriate alternate controls.	The NRC staff agrees with the comment. No changes were made to the RG based on this comment.
Kinectrics-1	General	The use of the term's 'safety' and 'safety-related' does not reflect a consistent scope. For example, on page 7, second paragraph, 2nd last sentence, the sentence contains '….maintenance equipment for safety and safety-related systems….' Since it is referring to 73.54, it can only mean safety-related and important-to safety. But in the last paragraph on page 7, 1st sentence, it reads '….loss of degradation of safety, security, and emergency preparedness (SSEP) functions….'. In this sentence it must mean safety-related and important-to-safety. The document needs to reflect a consistent use of terms to avoid user confusion. The industry has expended significant cost implementing 73.54 cyber security requirements due to inconsistent use of terms and using terms without providing a clear understanding of their meaning and scope. The term 'adverse impact' has a similar inconsistent use. The term as used in 3.1.3 1st paragraph, clearly indicates that adverse impact is related to radiological sabotage, i.e., significant core damage and therefore has the potential to adverse impact public health and safety. However, in the Definition section, 'adverse impact' makes no mention of radiological sabotage or core damage or impact public health and safety. The document text should be corrected to assure that use of the term 'adverse impact' is clearly and consistently connected with protecting the health and safety of the public.	The NRC staff agrees in part and disagree in part with this comment. The NRC staff agrees that when referring to SSEP functions as defined in 10 CFR 73.54, the first S in SSEP represents safety-related and important-to-safety. The text in the RG has been updated to consistently use the words "safety-related, important-to-safety" throughout the RG for the first "S" in SSEP. This includes updating RG text to replace "safety" with "safety-related and important-to-safety" where appropriate in regard to SSEP. The NRC staff disagrees with the comment regarding the definition of adverse impact. The NRC cybersecurity rule requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against a cyber-attack up to and including the design basis threat for radiological sabotage in 73.1. Protecting against this DBT would require a licensee to prevent significant core damage and spent fuel sabotage. Therefore, it is correct to say in Staff Regulatory Guidance Section C.3.1.3 that one possible consequence of adequately protecting CDAs includes radiological sabotage resulting in significant core damage. The NRC staff notes that the definition of adverse impact in the Glossary does reference radiological sabotage. No change was made to the RG based on this part of the comment. The NRC staff as a policy does not reference whitepapers in RGs. The NRC staff may reference NEI guidance documents. In this RG we have referenced NEI 10-04, Revision 3,

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		Important-to-Safety – While the term is used throughout the RG no guidance is provided that reflects the Important-to-Safety NRC accepted NEI Whitepaper guidance. Recommend including in this RG CDA scoping discussion.	"Identifying Systems and Assets Subject to the Cyber Security Rule."
Kinectrics-2	Section C.3.1	The 2nd sentence of this section should provide the overall guidance, scope, and concern of this RG. As the document is written, a safety-related DA would be required to be a CDA even though a compromise would NOT adverse impact the SSEP function. This position is included in the 'adverse impact' definition for 'support items', but is not allowed for non-support DA. This creates an unnecessary inconsistency.	It is unclear what the commenter means when stating that this section "should provide the overall guidance, scope, and concern of this RG." The scope of this RG is set forth in RG 5.71, Section A, "Purpose," and the first paragraph of Staff Regulatory Guidance Section C of this RG. As stated in Staff Regulatory Guidance Section C.3.1, a CDA is, in part, any digital asset that if compromised would adversely impact a safety-related or important-to-safety function. If a digital asset cannot compromise a safety-related or important-to-safety function, it is by definition not a CDA. Conversely, as the NRC staff understands the term, a safety-related digital asset is by definition a digital asset that if compromised would adversely impact a safety-related or important-to-safety function and therefore must be classified as a CDA. The NRC staff disagrees with the commenter's definition of adverse impact. See response to Kinectrics-1 regarding adverse impact. No change was made to the RG based on this comment.
Kinectrics-3	Section C.3.1.3	The following leads into the identification of critical systems, i.e. 'However, it may be difficult for a licensee to identify CDAs without first conducting a wider assessment of all the systems within the facility. This 'assumption' is unwarranted given that existing plants have historically identified their safety related systems and equipment items. Also, because the NRR has an important-to-safety QA inspection program that identifies 'important-to-safety' systems and equipment items. New plant designs also identify regulatory related equipment items as part of their classification and categorization process.	The NRC staff disagrees with this comment. The purpose of the sentence quoted by the commenter is merely to acknowledge that licensees may have hundreds of systems and possibly thousands of digital assets that affect the operation of their plant. Consistent with the language in 10 CFR 73.54 (b)(1), a licensee must analyze digital computer and communication systems and network to identify those CDAs that must be protected against a cyber-attack. One of the reasons for this wider assessment is to reduce the potential burden on the licensee by having them identify and only protect CDAs. The NRC disagrees that identifying and analyzing critical

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		This 'critical system' guidance placed an unnecessary burden on utilities, without providing any value. In many cases it has added additional burden to maintain a CS list. Such a list has no related regulatory requirements, nor is it needed for an effective CSP, i.e., without having a CS list does not adversely impact the CSP. Example: a single CDA in a non-safety-related system, due to interfaces with a safety-related system/function, may cause the non-safety-related system on the critical system list. Strongly recommend removing 'critical systems' from this document discussion. If the system starting point guidance remains, recommend that it should be clearly stated that this is a method to grossly identify potential plant systems that may contain CDAs and may be useful for identifying CDA's. Recommend not providing a term to describe these plant systems, i.e., Critical System, after that paragraph but focus on the remainder of the CSP apart from systems reference. This is consistent with the need to focus on performing and protecting SSEP functions. Additionally, many areas of 73.54 are NOT plant systems, e.g., ATWS, SBO, EP, BOP, and DAs included strictly due to interfaces, etc. Recommend deleting Figures 3 & 4 and related discussion and change some labels on Figure 5, e.g., upper left box becomes 'Licensee's Systems'.	systems places an unnecessary burden on a licensee. A critical system is either a system that directly supports an SSEP function or supports CDAs that directly supports an SSEP function. These are precisely the types of systems and assets that must be analyzed and protected in accordance with the cybersecurity rule. The NRC staff agrees that identifying critical systems is a starting point for identifying CDAs. For this reason, the NRC does not agree with eliminating the discussion of critical system from the RG or eliminating or revising Figures 3, 4, and 5. No change was made to the RG based on this comment.
Kinectrics-4	Glossary	Adverse Impact – See previous discussion on Use of Adverse Impact.	The NRC staff disagrees with this comment. This comment is identical to portions of the comment in Kinectrics-1 above discussing "adverse impact". The NRC staff reiterates the relevant portion of its response to the comment in Kinectrics-1 addressing adverse impact. No change was made to the RG based on this comment.
Kinectrics-6	Glossary	Critical digital asset (CDA) - 'A component of a critical system that consists of or contains a digital device….'	The NRC staff agrees with the comment. See response to Ameren-2. The NRC staff has adopted the definition of CDA

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		The definition is inconsistent since it implies that a DA in a critical system, (see other discussion on 'Critical System), makes it a CDA. This definition adds confusion to the use of 'Critical Systems and is reflected in how the industry's addresses 'Critical Systems'. Recommend a different definition that includes the DA function and potential adverse impact. See Section C.3.1, 1st paragraph, 2nd sentence for CDA recommended text.	in NEI 08-09, Revision 6.
Kinectrics-7	Glossary	Defense-in-Depth – Only applies to components. Doesn't it also apply to the function(s) to be performed?	The NRC agrees with this comment. The word function was added to the definition. The definition with the revised (underlined text is added) text is – "Defense-in-depth An approach to security in which multiple levels of security and methods are deployed to guard against failure of one component, function, or level."
Kinectrics-8	Glossary	Balance of Plant – Does not agree with the BOP scope added to the original cyber rule via the SECY letter under the 'affects reactivity' umbrella and addressed in the NEI BOP NRC accepted White paper. Recommend including in this RG scoping section.	It is not clear to the NRC staff what is meant by this comment. The NRC staff understands that the commenter does not agree with including balance of plant within the scope of the cybersecurity rule. The NRC Commission as a matter of policy has determined that digital systems within the balance of plant are within the scope of the rule. Associated with this decision, the NRC has determined that NEI 10-04, Revision 3, "Identifying Systems and Assets Subject to the Cyber Security Rule," is acceptable for use for addressing balance of plant issues for implementing the cybersecurity rule. It is not clear to the NRC staff what change the commenter wants made to this RG's scoping section. No change was made to the RG text based on this comment.
NEI-1	General	Based on the significant changes proposed in NEI 10-04, Revision 3 and NEI 13-10, Revision 7, the NRC should consider delaying issuance of RG 5.71 until the NRC completes the review and approval of both NEI documents.	The NRC agrees with this comment. NRC RG 5.71, Revision 1, cites NEI 10-04, Revision 3 and NEI 13-10, Revision 7 throughout the RG and lists the revised NEI documents in the References section.
NEI-2	General	The document uses "safety" and "safety-related" interchangeably throughout document; the industry recommends revising RG 5.71 for consistency with the NRC-approved NEI White Paper focused on the	The NRC agrees with this comment that "safety" and "safety-related" were used interchangeably throughout document. See response to Kinectrics-1 for the RG change made to address this issue identified in this comment.

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		identification and protection of digital assets associated with Safety-Related (SR) and Important-to-Safety (ITS) functions.	
NEI-3	Applicability	There is a comma at the end of the sentence causing confusion to the reader. Did the NRC intend on providing additional information? Or should this be a period?	The NRC staff agrees with this comment. The comma at the end of the sentence has been replaced with a period.
NEI-4	7	RG 5.71, Revision 1 should note that NEI 08-09 and the associated Addendums have been found to be acceptable for use by the NRC.	The NRC staff agrees with this comment. Section B, Background, of this RG has been updated to state that NEI 08-09 and the associated addendums have been found acceptable for use by the NRC.
NEI-5		The comment letter submitted by the commenter did not contain a comment number 5.	No response is required.
NEI-6	7	Although noted later in document, the Background Section should state that NEI 13-10 has been found to be acceptable for use by the NRC.	The NRC staff agrees with this comment. A sentence has been added in the Background section that NEI 13-10 has been found acceptable for use by the NRC.
NEI-7	General	NEI 08-09, Addendum 1, contained changes based on nuclear plants being in a "production environment," these changes do not appear to be captured in this revision of RG 5.71.	The NRC staff agrees with the comment that changes made in NEI 08-09, Addendum 1, based on nuclear plants being in a "production environment" are not reflected in RG 5.71, Revision 1. The text in NEI 08-09, Addendum 1, specifically addresses concerns performing vulnerability scans in a production environment. The NRC also agrees that vulnerability scans should not be performed if the scan could have an adverse impact on the operation of the plant. In such a case, the NRC recommends that the vulnerability scan be performed prior to the CDA being put into a production environment or during a plant outage. The text in RG 5.71, Revision 0, always allowed for vulnerability scans or assessments to be performed throughout the life cycle of a CDA's use in a plant. This includes prior to placing the CDA in a production environment and during plant outages. The original text also takes into account potential technology changes in the future that may allow certain types of vulnerability scans to be performed that will not affect the performance of the CDA. The NRC has determined that the existing language in RG 5.71, Revision 0, adequately addressed the comment's concern about conducting vulnerability scans in a production environment. Therefore, the corresponding text in

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
			RG 5.71, Revision 1, was not changed based on this comment.
NEI-8	14	Bullet should read "characterization of threats to the facility as specified in RG 5.69" with applicable reference to the guide. To the second bullet in the final set of bullets in Section C.3 just prior to Section C.3.1, add "… as specified in RG 5.60"	The NRC staff agrees with the comment, but notes that the commenter incorrectly references RG 5.60 instead of the correct RG 5.69. The NRC staff has modified the text of the second bullet in RG 5.71, Revision 1, Staff Regulatory Guidance Section C.3.1 as follows (new text is underlined) • characterization of threats to the facility, as specified in NRC RG 5.69 NRC RG 5.69 has been added to the Reference section of the RG 5.71.
NEI-9	19	This revision of RG 5.71 does not address that the Federal Energy Regulatory Commission's (FERC) has incorporated a graded approach to cyber security and has revised needed cyber security controls for generators accordingly. This should be addressed within the Balance of Plant (BOP) sections within the document. This would also include discussing the 15-minute shutdown guidance in the NRC approved NEI White Paper focused on the identification and protection of digital assets associated with Balance of Plant functions.	The NRC staff agrees with the comment and has made the suggested change in RG 5.71, Revision 1, Staff Regulatory Guidance Section C.3.1.3 based on the latest version of NEI 10-04. RG 5.71 Staff Regulatory Guidance Section C.3.1.3 is where the NRC provides guidance on balance of plant. The NRC agrees that FERC has developed a graded approach to cybersecurity and has established cybersecurity controls for generators of electricity to the grid. NRC licensees are subject to the cybersecurity rule. Therefore, the NRC did feel it was necessary to address or provide guidance on FERC's actions that are unrelated to the NRC's cybersecurity rule.
NEI-10	19	Page 19 and Figures 4 and 5, as well as other parts of the document, state BOP criteria as "and" and "or." This should be consistent throughout Document Should be "and"	The NRC staff agrees with the comment but changes in Figures 4 and 5 have made the comment moot. The NRC staff has revised the language in RG 5.71, Revision 1, Staff Regulatory Guidance Section C.3.1.3, and elsewhere in the RG as appropriate to state that identification of CDAs include BOP digital assets that if compromised could affect reactivity and result in an unplanned reactor shutdown or transient. The NRC has revised both Figures 4 and 5 of the RG to remove the words "affects reactivity or" and replaced those words with "BOP causes a plant trip." As a practical matter all reactor trips affect reactivity. Reactivity is affected when power is affected. Therefore, if a BOP CDA causes a reactor trip, the reactor trip will affect

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
			reactivity. Accordingly, including the phrase "affects reactivity" is redundant. The text changes in Figures 4 and 5 eliminated the need to change the word "or" to "and" in the figures.
NEI-11	18	Figure 3, BOP and ITS should not be under safety systems, this should be at a higher level.	The NRC staff agrees with this comment and modified Figure 3 to place BOP and ITS on the same level as the other systems in the figure.
NEI-12	21 Figure 5	There is no guidance in DG-5061 that discusses how this decision block should be interpreted. It appears to be redundant with the "Performs…" and "Supports…" decision blocks. Remove bubble "Affects Critical Assets, Functions and/or Pathways."	The NRC staff disagrees with the comment. There is text on page 21 that discusses "adversely affect SSEP functions or CSs or CDAs that perform SSEP functions" and "provide a pathway to a CS or CDA that could be used to compromise, attack, or degrade an SSEP function". The new text and addition to Figure 5 were based on lessons learned during discussion with licensees who made a distinction between devices that could "affect" critical assets, functions and/or pathways and devices that "supported" CDA and critical systems. If the effect could manifest in one of the conditions identified in 10 CFR 73.54 (a)(2) then the device that caused the effect should be identified as a CDA. No change was made in the RG based on this comment.
NEI-13	40	Section C.4.1.2 added a discussion on metrics; the NRC should consider clarifying that metrics are not required to address the control and are optional.	The NRC staff disagrees with this comment. The current text in RG 5.71, Revision 1, states: "It is possible for licensees to provide evidence of the effectiveness of their cyber security program without implementing cyber security metrics, and therefore, this guidance is presented as an option." This sentence has been moved to the beginning of the discussion on metrics to make clear that their use is optional.
NEI-14	Appendices B and C	NEI recommends the NRC eliminate Appendices B and C. Licensees should be free to use security control sets by NIST, NERC, IAES, ISO, IEE, IEC, or other credible external organizations. This will reduce prescriptiveness and increase efficiency in overall implementation. Remove Appendix B and Appendix C	The NRC staff disagrees with this comment. Regulatory guides provide one acceptable method licensees may use to comply with NRC regulatory requirements. Licensees are free to use any security control sets in the development of their cybersecurity plan. The NRC will review the security control sets to determine if the plan meets the requirements of 10 CFR 73.54 and adequately protects against a cybersecurity attack. Use of the security control sets in Appendices B and C in the RG is one acceptable way of implementing the requirements in 10 CFR 73.54. No change was made in the RG for to this comment.

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
NEI-15		The NRC should consider removing the prohibition for wireless communication associated with Safety- Related and Important-to-Safety systems and allow its use with appropriate cyber security controls.	The NRC staff disagrees with this comment. Cybersecurity programs in compliance with 10 CFR 73.54 must analyze, protect, and monitor computer systems. The defensive architecture in RG 5.71 uses a graded approach "that establishes formal communication boundaries (or security levels) in which defensive measures are deployed to detect, prevent, delay, mitigate, and recover from cyber attacks" and "systems requiring the greatest degree of security are located within the most secure level of the defensive architecture". To simplify and assure adequate implementation of the defensive architecture presented in RG 5.71, wireless communication associated with Safety- Related and Important-to-Safety systems is prohibited. Extensive and significant changes to the defensive architecture and cybersecurity plans would be needed to fulfill the requirement of adequate protection of safety-related and important-to-safety systems if wireless communication is permitted for these systems. The current version of the RG does not support these changes. No change was made to the RG based on this comment.
NEI-16	General	The term "Intent of Control" – was added to all controls. Where was this definition derived? The industry is concerned that this added wording will now create inspection concerns and unnecessary discussions between the "Control Intent" and the licensees cyber security program documents and procedures.	The NRC agrees that it added the section "Intent of Control" for each control to RG 5.71, Revision 1. A discussion of the intent of each control was added as a result of lessons learned from the cybersecurity inspections. These inspections indicated that licensees did not understand the intent of the original controls when alternate controls were selected for implementation. Not understanding the intent of the original control resulted in the selection of alternate controls that did not adequately address attacks and threat vectors addressed by the original control. Some stakeholders recognize the value of including the "Intent of Control" section in the RG (see, e.g., Comment Ameren-11). The NRC has determined that understanding the intent underlying the use of a particular security control is an essential and useful element in determining if the security control adequately addresses the threat it is being used to protect against. The information in the "Intent of Control" sections of the RG is derived from information in various NIST and IEC cybersecurity documents. The NRC has determined that including information on the

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
			intent of a control aids in the development of appropriate alternate controls. No change is made to the RG based on this comment.
NEI-17	Glossary	Many definitions were added to this document, examples being: • Attack Pathway • Attack Surface • Attack Vector • Portable Media Where did the definitions come from?	The NRC agrees with the comment. The new definitions were added to the document to clarify terms used in the RG. The definitions for Portable Media, Attack Pathway, and Attack Vector were terms used in the original version of RG 5.71. Portable Media is a tailored version of the definitions for removable media and portable storage device from the document Committee on National Security Systems (CNSS) Glossary (CNSSI 4009). The definitions for Attack Pathway and Attack Vector were generated by NRC staff. The definition for Attack Surface came from the NIST Computer Security Resource Center Glossary https://csrc.nist.gov/glossary/term/attack_surface. No change was made to the RG based on this comment.
NEI-18	Glossary	The definition of cyber attack changed; there are now three definitions, Rev 0, Rev 1, and NEI 08-09. The industry recommends using one consistent definition, that being the NEI 08-09 definition.	The NRC agrees that the definition of cyberattack in RG 5.71, Revision 0, RG 5.71, Revision 1, and NEI 08-09 are not identical. The NRC revised the definition of cyberattack in Revision 1 to include the term "adverse impact." Including this term directly ties the Revision 1 definition to 10 CFR 73.54. The NRC has not elected include the NEI 08-09 definition in the RG 5.71, Revision 1, because the NEI 08-09 definition does not include the term "adverse impact" consistent with the cybersecurity rule language. The NRC notes the two definitions are substantially the same. No change was made to the RG based on this comment.
NEI-19	Glossary	The definition of support system should note the change in the NRC approved NEI White Paper focused on the identification and protection of digital assets associated with Safety-Related (SR) and Important-to-Safety (ITS) functions.	The NRC disagrees with this comment. The RG cites NEI 10-04 revision 3 "Identifying Systems and Assets Subject to the Cyber Security Rule," and NEI 13-10, Revision 7, "Cyber Security Control Assessments". These documents, which supersede NEI White Paper focused on the identification and protection of digital assets associated with Safety-Related (SR) and Important-to-Safety (ITS) functions, do not contain changes for identification and protection of support systems for SR and ITS functions. No change was made to the RG based on this comment.
NEI-20	5. B.	A revision log should be added to RG 5.71, Revision 1	The NRC disagrees with this comment. A revision log is not a

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		identifying the significant changes, additions, and deletions made to Revision 0 of RG 5.71. The section "Reason for Revision" provides a very high-level summary of the RG update but does not identify the specific revisions. NIST SP800-53, Rev 4 provides a good example of such a log listing significant revisions.	part of the template used by the NRC for the revision of the RG. Additionally, licensees of currently operating nuclear power plants are not required to make changes based on the changes in this revised RG. Therefore, the NRC has determined that including a revision log would not serve any useful purpose. the need for a detailed log beyond the information provided in the Reason for Revision section is minimal. No changes were made to the RG based on this comment.
NuScale-1.	C.3.1.3, pg. 19	The phrase "directly or indirectly affect the reactivity of an NPP" is overly broad. Consider using the guidance in NEI 10- 04 "Loss of electrical output or reactor shutdown within 15 minutes." The broad guidance of "directly or indirectly affects reactivity" is not quantitative as even minor changes in secondary plant parameters (loss of a 5^{th} or 6^{th} point heater, etc.) while affecting reactivity have little or no impact on plant operation or on the electrical output of the plant. This broad definition has caused uncertainty and has led to expansion of assets defined as CDAs beyond what is required to ensure safety, security, and emergency preparedness (SSEP) functions or protection of the Bulk Electrical Supply (BES). This should be applied wherever reactivity or transient are used throughout the document. This will align with the text on page 20 and the revision of NEI 10-04 referenced on page 20 should be issued by the time this document is issued.	The NRC staff agrees in principle with this comment but has not adopted the suggested language. The following sentence, which adopts language from NEI 10-04, was added to the RG 5.71, Revision 1, in Staff Regulatory Guidance Section C.3.1.3: "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."
NuScale-2.	C.3.1.3, pg. 19	The word transient in "could result in an unplanned reactor shutdown or transient" is unquantified and the recommendation for "reactivity affect" in Comment 1 should be applied. Quantify "transient" similarly to reactivity change in Comment 1, using guidance similar to that in NEI 10-04 "Loss of electrical output or reactor shutdown within 15 minutes "to prevent overly broad classification of assets that do not have an impact on SSEP functions or the BES.	The NRC agrees in principle with this comment but has not adopted the suggested language. This comment is similar to the NuScale-1 comment. Accordingly, the NRC reiterates its response to the NuScale-1 comment.

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
NuScale-3.	C 3.1.3, pg. 21	The phrase "However, such systems are still vulnerable to cyber attack originating from internal sources" does not include the risk from malicious software or firmware inserted via the supply chain. Change wording to "However, such systems are still vulnerable to cyber attack originating from internal sources, or insertion from the supply chain."	The NRC agrees in principle with this comment but has not adopted the suggested language. The phrase "supply chain" has been added to the following underlined text in RG 5.71, Revision 1, Staff Regulatory Guidance Section C.3.1.3 – "However, such systems are still vulnerable to cyberattack originating from internal sources, such as inserting media into a system that has malicious code on it, supply chain, diagnostic systems, and other offline connections and access."
NuScale-4.	C 3.1.3, pg. 21	The phrase "In addition, because of the abundance of off-the-shelf devices and peripherals that support communications technology…" should include wireless and Internet of Things. Change wording to "In addition, because of the abundance of off-the-shelf devices and peripherals that support communications technology including wireless and Internet of Things (IoT) "	The NRC staff disagrees with this comment. The cited sentence in the RG mentions no specific examples and is technology neutral. No change was made to the RG based on this comment.
NuScale-5.	Pg. 55	Add SIEM to the list of Acronyms as it is used in the document. Add "SIEM" (Security incident and event monitor).	The NRC staff agrees in part and disagrees in part with this comment. The staff had added SIEM – Security Incident and Event Management. to the Acronyms section of RG 5.71, Revision 1. The acronym defined in the Acronym list is taken from the NIST on-line Computer Security Resource Center Glossary. Accordingly, the NRC has not adopted the commenter's suggested language for defining what the acronym SIEM means.
NuScale-6.	A.3.1.3, pg. 62	Phrase "[Licensee/Applicant]'s CST identified and documented CDAs that have a direct, supporting, or indirect role in the proper functioning of CSs" is overly broad and includes digital equipment that may not support an SSEP function in a CS. Change to "[Licensee/Applicant]'s CST identified and documented CDAs that have a direct, supporting, or indirect role in the proper functioning of a CSs SSEP function."	The NRC staff agrees with the comment and has used the suggested text in the RG 5.71, Revision 1, Appendix A.3.1.3.
NuScale-7.	A.3.1.6, pg. 64	The application of controls does not allow for a quantitative risk- based approach to control assignment.	The NRC staff disagrees with this comment. This RG does not utilize a specific assessment methodology for selecting and

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		This comment assumes NRC acceptance of EPRI TAM or similar assessment mechanism as a method of control assignment. This reflects current cyber security best practice vs application of controls regardless of effectiveness. Add a new bullet point: With respect to technical security controls, [Licensee/Applicant] used …the following for each CDA: • Apply an NRC-approved quantitative risk-based analysis of the CDA to apply the controls in Appendix B to RG 5.71 to CDAs, OR; • (New 1st bullet point) "implementing all of the security"	applying security controls. Appendix A is a template to be used by licensees to describe their CSPs and the guidance is one acceptable method for implementing a CSP. If a licensee chooses to use another method for applying security controls, the licensee can update Section 3.1.6 of their CSP with their chosen method. No change was made to the RG based on this comment.
NuScale-8.	A.4.1.3, pg. 67	Vulnerability scanning is of limited use in detecting attacks. Add real time monitoring to this section. This is supported by monitoring requirements throughout this revision of RG 5.71. Change section title to (or add new section that performs the same function) "Vulnerability Assessments, Scans and Monitoring." Add "[Licensee/Applicant] Employs real time monitoring of all CSs network traffic events and logs in real-time to analyze for changes in network communications or identified characteristics of a cyber-attack and maintains a current library of attack profiles. Automated collection and analysis of network traffic, CDA events and logs by a SIEM to provide notification to licensee in real time of security events and provide for incident response and forensic analysis."	The NRC staff partly agrees and partly disagrees with the comment. The NRC staff agrees that additional clarifying text identified in this comment should be added in the RG 5.71, Revision 1 but the NRC staff disagrees with the section of the RG suggested for the change. The new text is more suitable under section Staff Regulatory Guidance Section C.4.1 Continuous Monitoring and Assessment. The NRC staff disagrees with the actual wording of the new text. Some of the suggested text is too prescriptive for this RG however the following bulleted text has been added to Staff Regulatory Guidance Section C.4.1: • "automated collection and analysis of network traffic, CDA events, and logs to provide notification to licensee in real time of security events and provide for incident response and forensic analysis;"
NuScale-9.	A.4.2.4, pg. 70	The section does not address changes to the cyber risk environment. Add bullet point: "changes to the risk environment as	The NRC staff disagrees with this comment. The section already includes language that addresses changes to the overall cyber security program and plan implementation, which includes implementation of security controls to address

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		documented in reports, alerts, and notices from the Critical Infrastructure Security Agency (CISA), CDA vendors or credible sources."	changes in the cyber risk environment. No change was made to the RG due to this comment.
NuScale-10.	B.1.1, pg. B-1	To follow current best practice, access control policy should establish a Zero Trust architecture where practicable per NIST SP 800-207. This will drive the security architecture to current best practice while decreasing burden for password management, portable device, and media control. Add as initial control element: "establishes a Zero Trust Architecture in CSs and CDAs to the extent practicable. For CSs and CDAs where Zero Trust is not achievable the policy will;"	The NRC staff disagrees with this comment. The NRC is currently engaged in a long-term effort exploring how a Zero Trust architecture could be applied in nuclear security. However, RG 5.71 currently illustrates a defensive architecture with security levels and boundary protection devices. Licensees can augment or completely replace the defensive architecture illustrated in RG 5.71, Revision 1, with a Zero Trust architecture. However, the accompanying CSP (Site specific Appendix A) and the set of security controls supporting the defensive architecture would have to be tailored. A future revision of RG 5.71 may include sufficient information – perhaps as an Appendix – to implement a Zero Trust architecture applicable for nuclear facilities but no changes were made to this RG based on the comment.
NuScale-11.	B.1.17, pg.B-9	Missing section number "as articulated in RG 5.71; Section numbers should be listed wherever RG 5.71 is referenced for clarity. Add section number: "…as articulated in RG 5.71, C.3.2" , employ throughout document for clarity.	The NRC staff agrees with the comment and added the section number to the identified text of the RG for clarity.
NuScale-12.	B.3.1, pg. B-17	This control intent does not add information to the reader beyond the title. Change control intent to read: "The intent of this control is to ensure the development, documentation, and deployment of policies and associated implementing procedures to address requirements of CDAs and communication protection controls that establish network segmentation and boundary protection and cryptographic rules."	The NRC staff disagrees with the comment. The intent of this control is for licensees to have policies and procedures that address the requirements of CDAs and communication protection controls. The NRC has determined that the suggested additional text would incorrectly limit the policy to requirements of CDAs and communication protection controls that establish network segmentation and boundary protection and cryptographic rules. For example, the new suggested text would not be applicable for the control Appendix B.3.22 Fail in a Known State. No change was made to the RG based on this comment.
NuScale-13.	B.3.2, pg. B-18	Add real-time CDA monitoring as alternate control. Add following as alternate control: "Employ real-time CDA configuration monitoring and blocking of	The NRC disagrees with this comment. The NRC has determined that real-time CDA monitoring is not required in this specific control, particularly given existing controls in RG 5.71, Revision 1. In Appendix C, security controls C.11.6,

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		modifications using an active cyber security monitoring system."	"Access Restrictions for Change," and C.11.7, "Configuration Settings," contain text for automated monitoring of configuration changes. No changes were made to the RG based on this comment.
NuScale-14.	B.3.3, pg. B-19	The control intent assumes the licensee uses the same security level numbering format as RG 5.71 :"… Levels 3 and 4 from all other levels." Add reference in RG: "…Levels 3 and 4 from all other levels as shown in RG 5.71 Figure 6."	The NRC staff agrees in part and disagrees in part with this comment. The NRC staff agrees that clarifying text should be added to the security control, but the staff disagrees with the location for making the update. The following underlined text is added to the Licensee/Applicant Activities section of the control instead of the Control Intent section of Appendix B.3.3. • "using physically separate network devices to create and maintain logical separation of Levels 3 and 4 from each other and from all other levels as shown in RG 5.71 Figure 6."
NuScale-15.	B.3.4, pg. B-19	Last bullet does not specify real time DOS monitoring. Add real-time monitoring to control language for last bullet: "employing monitoring tools to detect indicators of denial-of-service attacks against CDAs in real time."	The NRC staff disagrees with this comment. The purpose of the last bullet is to detect indicators of DoS attacks and to take defensive actions before the attack is fully launched. The NRC has determined that adding the words "real-time" provides no additional clarity to the existing language of this bullet. No changes were made to the RG based on this comment.
NuScale-16.	B.3.6, pg. B-20	Control element: "Employ cryptographic mechanisms to recognize changes to information during transmission and upon receipt, unless otherwise protected by alternate physical measures" does not reflect control system protocols and communications. Internal ICS communications are in general not encrypted and encryption decryption within control systems cannot be easily performed except in systems with advanced controllers. Either delete the control element or specify when practicable. If the control element is intended for non ICS internal data, the control should specify this. Change control element to read "Employ cryptographic mechanisms to recognize changes to information during transmission over insecure networks and upon receipt from insecure networks where practicable, unless otherwise protected by alternate physical measures."	The NRC staff disagrees with this comment. Nowhere in the RG is it implied or explicitly stated that the security controls in Appendix B apply only to ICS protocols. The controls are applied to CDAs that perform or support SSEP functions. If an ICS protocol now or in the future can support cryptographic mechanisms without negatively impacting SSEP functions, then the security control is applicable. Otherwise, an alternate control should be used as is done today in many operating NPPs. No changes were made to the RG based on this comment.

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
NuScale-17.	B.3.7, pg. B-20	Confidentiality is in general not a protected characteristic of ICS systems beyond Identifiers and authenticators (first bullet control element) since ICS systems rarely contain PII this control should specify security data. Reword Control Intent to read: "The intent of this control is to ensure that the confidentiality of security and personal identifying information data is maintained as the data is passed to or from CDAs."	The NRC staff disagrees with this comment. The concern of this control is not confidentiality of PII. The concern is confidentiality of transmitted data that might be intercepted and used by an adversary in a cyberattack. This may or may not be "security" data. For example, it may be configuration information for a CDA. No change was made to the RG based on this comment.
NuScale-18.	B.3.15, pg. B-23	ICS systems rarely use DNS data or Name Services; this control should specify that DNS services be removed or disabled except where required. External DNS requests should be rejected. See NIST SP 800-82 Rev 2. Change Control Intent and control to specify only for systems that use DNS. Change Control Intent to "For CDAs that use domain name services, ensure implementation and control of DNS services. Disable or remove DNS services in CDAs that do not use name resolution." Change Control to add control elements: • Disable DNS services or remove where practicable in CDAs that do not use name services. DNS services where required are configured to reject DNS queries to external domains.	The NRC staff disagrees with this comment. While critical systems containing industrial control technology rarely, if ever, use DNS, other systems at NPPs within the scope of 10 CFR 73.54 may use this service. This may be especially true of emerging technologies and systems. If CDAs do not require DNS, then the services should be removed based on security controls B.5.1 "Removal of Unnecessary Services and Programs" and C.11.8 "Least Functionality" in Appendices B and C in the RG. No changes were made to the RG based on this comment.
NuScale-19.	B.3.21, pg. B-25	Remove control, except for safety systems (these are covered in other standards). Diversity is difficult to obtain and is rarely implemented for non-safety systems / CDAs, while decreasing common vulnerabilities the inherent difficulties of implementing diverse control systems within a system make this control impractical and addition of control system architectures can add	The NRC staff disagrees with this comment. While certainly there are tradeoffs (negative and positive) in using diversity for security purposes, implementation of this security control is not limited to industrial control systems. It can be used for IT systems that support safety-related, important-to-safety, and security systems. Licensees have an option to implement an adequate alternate for this control. No change was made to the

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		attack surfaces and exploit sequences. Remove control. Delete control.	RG based on this comment.
NuScale-20.	B.4	This entire section does not use best practice in current cyber security. Add Zero Trust as a new control with the remainder of the controls in B.4 to be applied when a Zero Trust architecture cannot be achieved. New ICS upgrades and installations will often be able to select a Zero Trust architecture vastly increasing the security of the entire system, addition of this control will drive licensees to current best practice. Add new B.4 control as first control B.4.1 and renumber the rest with the addition of B.4.x: "Where Zero Trust cannot be achieved…rest of control B.4.1 implement a Zero Trust architecture as described in NIST SP 800-207." If control is added, update references to include NIST SP 800-207.	The NRC staff disagrees with this comment and has not adopted the suggested language. This comment is similar to the NuScale-10 comment. Accordingly, the NRC reiterates its response to the NuScale-10 comment. No change was made to the RG based on this comment.
NuScale-21.	B.4.2, pg. B-25	Add passphrases to second control element. Change second control element to read: "passphrases and passwords have length and complexity commensurate with the required security."	The NRC staff disagrees with this comment. A password is a string of characters an individual uses to authenticate their identity. This control is applicable also for specifically formatted passwords such as passphrases and PINs. No change was made to the RG based on this comment.
NuScale-22.	B.4.3, pg. B-28	Change password change requirement to reflect current best practice of not changing non-compromised sufficient passwords. Change of passwords that have sufficient complexity and have not been compromised does not add security and increases burden. Add the statement: "Passwords of insufficient complexity and lengths for required security due to operational or technical limitations are changed every [describe the periods for each class of system; for example, 30 days for workstations, 3 months for CDAs in the vital area], passwords should be updated whenever a valid threat indicates risk of compromise."	The NRC staff disagrees with this comment. The current text of RG 5.71, Revision 1, already allows licensees to utilize best practices when implementing their CSP. The NRC has determined that the proposed language is overly prescriptive and unnecessary. When this control cannot be implemented on a CDA, licensees have an option to implement an adequate alternate for this control. No change was made to the RG based on this comment.

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
NuScale-23.	B.4.2, pg. B-28	Insert new control element for passphrases. New control element to read: “passphrases should contain four words separated by spaces or characters and are used in preference to passwords where practicable.”	The NRC staff disagrees with this comment. The recommended change is too prescriptive. RG 5.71, Revision 1, provides licensees with the discretion to formulate adequate passwords that comply with security requirements. No change was made to the RG based on this comment.
NuScale-24.	B.5.2, pg. B-32	This control is incomplete, as a host-based intrusion-detection system (HIDS) will only detect changes to the Host (Server or PC that it runs on). This control should be expanded to include Network Intrusion Detection (NIDS) and Security Incident and Event Monitoring (SIEM). These are standard components of a cyber-security monitoring system and allow for detection of anomalous network traffic and attacks that a server especially a compromised one will not detect or alert on. Add separate control B.5.3 to describe proper SIEM setup to include monitoring of all network traffic via the NIDS with compensating physical controls. Where not possible renumber controls to reflect.	The NRC staff disagrees with this comment. Security control B.5.2 was written specifically for a HIDS. Security functions typically performed by NIDSs and SIEMs are addressed in security control C.3.4 Monitoring Tools and Techniques in Appendix C of the RG. No change was made to the RG based on this comment.
NuScale-25.	B.5.4, pg.B-33	Control does not reflect current best practice. Add Zero Trust. Add new control element to emplace Zero Trust on CDAs and CDs where feasible.	The NRC staff disagrees with the comment. The NRC disagrees and has not adopted the suggested language. This comment is similar to the NuScale-10 comment. Accordingly, the NRC reiterates its response to the NuScale-10 comment. No change was made to the RG based on this comment.
NuScale-26.	C.1.2, pg.C-2	Control does not reflect current best practice. Establishment of Zero Trust provides for media protection and control. Add new control element to emplace Zero Trust on CDAs and CDs where feasible.	The NRC staff disagrees with the comment and has not adopted the suggested language. This comment is similar to the NuScale-10 comment. Accordingly, the NRC reiterates its response to the NuScale-10 comment. No change was made to the RG based on this comment.
NuScale-27.	C.3.3, pg. C-6	Control does not provide for continuous monitoring. Continuous monitoring of network communications, logs and events will provide for additional protection (detect) against malicious software (and firmware / hardware).	The NRC disagrees with this comment. Guidance on continuous monitoring is covered in security control C.3.4 Monitoring Tools and Techniques in Appendix C of the RG. No change was made to the RG based on this comment.

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		Add, as first control element: "Maintains a continuous monitoring system for CS and CDAs that provides for real-time analysis."	
NuScale-28.	C.8, pg. C- 22	Add forensics and evidence retention to control elements. Add control element: "Containment and eradication efforts to the extent practicable preserve forensic evidence of the attack, including but not limited to; data in memory, changes to software and firmware and storage media and preserve network information to analyze the attack."	The NRC staff agrees with this comment and has added the suggested text to Appendix C.8 of the RG.
NuScale-29.	C.8.4, pg. C-26	Add forensics and evidence collection and handling. Add control element: "Cyber security forensics and evidence retention - This includes knowledge of computer forensic and evidence gathering and retention, legal requirements for handling and transmission of evidence."	The NRC staff agrees with this comment and has added the suggested text to Appendix C.8.4 of the RG.
NuScale-30.	C.8.6, pg. C-27	Add reporting Cyber Security Incidents to CISA (this is now required by regulation). Add control element for licensee to inform CISA of cyber security attacks as required and consistent with site security program.	The NRC staff disagrees with this comment. The NRC does not have a regulatory requirement that licensees report cybersecurity incidents to CISA. The scope of this RG pertains to compliance with NRC regulations, not the requirements of another government agency. No change was made to the RG based on this comment.
NuScale-31.	C.10.4, pg. C-36	Add gathering and handling of evidence. Add gathering, retention, and handling of evidence to first control element.	The NRC staff agrees in part and disagrees in part with this comment. The NRC staff agrees that clarifying text regarding the gathering and handling of evidence should be added to RG 5.71, Revision 1. The NRC staff disagrees that this clarifying text should be added to Appendix C.10.4. The NRC staff has determined that the clarifying text should be added to Appendix C.10.10, "Roles and Responsibilities of the Cyber Security Specialist." The text in section Appendix C.10.10 in the RG was updated (new text is underlined) as follows: • "<u>gathers, handles, and</u> preserves evidence collected during cyber security investigations to prevent loss of evidentiary value;"
NuScale-32.	C.11.3, pg. C-41	Quarterly audits of baseline configurations are impractical and would be highly resource intensive (the	The NRC staff disagrees with this comment. The text in question is in square brackets. The NRC has used square

Commenter	Section	Specific Comment and Proposed Resolution	NRC Resolution
		audit would likely not finish before the next quarter starts) recommend changing to semi-annually. While feasible for the larger CSs the control does not establish the scope of the audits. Change audit frequency to semi- annually.	brackets in RG 5.71 to indicate that licenses are allowed to insert site-specific review periodicities for this control. Accordingly, licensees already have the ability to conduct quarterly audits of baseline configurations semi-annually or at other periodicities. Additionally, some licensees have implemented alternates – such as continuous monitoring for configuration changes – based on the impact of unauthorized configuration changes for some CDAs. No change was made to the RG based on this comment.
NuScale-33.	C.12.2, pg. C-46	The changing landscape of threats to ICS systems increasingly shifts to supply chain attacks from sophisticated adversaries. Recommend a robust supply chain risk management plan as described in NIST SP 800-161. Add as C12.2.1 "Establishes a Cyber Security Supply Chain Risk Management Program" as reflected in NIST SP 800-161.	The NRC staff agrees in part and disagrees in part with this comment. The NRC staff agrees to add NIST SP 800-161 to RG 5.71, Revision 1. The document has been added to Reference section of the RG. The NRC staff does not agree with adding guidance on establishing a supply chain risk management program in RG 5.71, Appendix C.12.2. Instead, the NRC staff has revised RG 5.71, Revision 1, Staff Regulatory Guidance, Section C: 3.3.3.1, "System and Service Acquisition," to include the following language: • "establishment of a cybersecurity supply chain risk management program based on the guidance found in NIST SP 800-161, 'Supply Chain Risk Management Practices for Federal Information Systems and Organizations'"