

**U.S. NUCLEAR REGULATORY COMMISSION STAFF'S FEEDBACK AND OBSERVATIONS REGARDING NEI'S WHITE PAPER FOR "REMEDICATION OF VULNERABILITIES IDENTIFIED IN CDAS"**

**SPONSOR INFORMATION**

**Sponsor:** Nuclear Energy Institute

**Sponsor Address:** 1201 F St., NW, Suite 1100  
Washington, DC 20004-1218

**Project Number:**

**DOCUMENT INFORMATION**

**Submittal Date:** August 30, 2022

**Submittal Agencywide Documents Access and Management System (ADAMS) Accession No.:** ML23072A063

**Purpose of the White Paper:** The Nuclear Energy Institute (NEI) stated that the purpose of this white paper, "Remediation of Vulnerabilities Identified in CDAs", is to provide guidance to licensees to evaluate vulnerability notifications and potential remediation actions including, but not limited to, application of security patches. Furthermore, NEI intends for the guidance to assist licensees in determining and documenting the technical basis, justifying that a CDA is adequately protected.

**Action Requested:** NEI requested the U.S. Nuclear Regulatory Commission (NRC) staff's feedback and observations regarding the information discussed the white paper.

**FEEDBACK AND OBSERVATIONS**

The NRC staff is making no regulatory findings on this white paper and nothing herein should be interpreted as official agency positions.

The NRC staff's feedback and observations are focused on information related to the following regulatory requirements from Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communication Systems and Networks":

- Paragraph 54(a)(1) requires that 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.
- Paragraph 54(a)(2) requires that the licensee shall protect the systems and networks identified in paragraph (a)(1) of this section from cyber attacks that would: (i) Adversely

impact the integrity or confidentiality of data and/or software; (ii) Deny access to systems, services, and/or data; and (iii) Adversely impact the operation of systems, networks, and associated equipment.

- Paragraph 54(b)(2) states, in part, that to accomplish this, the licensee shall: Evaluate and manage cyber risks.

## 1.0 EXECUTIVE SUMMARY AND INTRODUCTION

### 1.1 General Observations

- The Executive Summary does not completely describe the purpose and objectives of the rule and the CSP (Cyber Security Plan). The summary states that "...10 CFR 73.54 provides requirements for, and licensee Cyber Security Plan provides measures for incident response and recovery from cyber attacks." However, 10 CFR 73.54 additionally requires that licensees implement and maintain a Cyber Security Plan that describes how equipment that performs SSEP functions, which if compromised would adversely impact the SSEP function, will be protected through the evaluation of risks. This requirement is addressed by evaluating and mitigating vulnerabilities and when necessary, remediating the equipment and systems to evaluate and manage those risks per 10 CFR 73.54.
- The final sentence in the Executive Summary states, in part, "...to mitigate the vulnerability attack pathways." The NRC has defined attack pathways and attack vectors as separate terms in its guidance in Regulatory Guide 5.71. However, these terms appear to be used interchangeable throughout the white paper. If NEI proposed to use those terms in a manner other than as the agency has previously defined, it should clearly articulate that in its own guidance.
- The introduction states, in part, that, "...this addendum (Addendum 5), did not completely address acceptable methods to remediate those vulnerabilities." However, the NRC did not understand this to be part of the intent of Addendum 5, as licensees' cyber security plans in section E.12, "Evaluate and Manage Cyber Risk," require them to address vulnerabilities using the information and remediation actions provided in the appropriate vulnerability notice.

## 2.0 EVALUATION OF ATTACK VECTORS

### 2.1 General Observations

- Terminology used in a manner different than previously defined either by the NRC or in approved NEI guidance should be clearly defined. For example, the term malware is specifically defined in Regulatory Guide 5.71 but appears to be used in a different manner in the white paper without providing a unique definition.

- In the middle of page 2, a section states, in part, “With respect to these channels...” It is unclear whether the intent is to use the term “channels” interchangeably with “attack pathways,” or if channels refer to another term that is not defined within this white paper, such as attack vectors.
- On the top of page 3, a section states, in part, “When assessing a vulnerability, the licensee should account for how exploitation is possible (i.e., attack vector) because environmental factors that prevent inbound network traffic such as standalone, or air-gapped, networks or use of data diodes limit an attacker’s ability to remotely exploit certain types of vulnerabilities or take command and control.” An attacker as defined by the design basis threat will almost certainly not rely on only one vulnerability to get into a system, especially when the target is a nuclear security or safety system. Bypassing a CVE because it was screened out due to solely an attack vector metric is seldomly acceptable.
- The final section states, in part, that, “Ultimately, it’s the actions taken by an attacker (or malware) after exploitation occurs, that determines impact to safety, security, and emergency preparedness functions.” We agree with this statement as the actions that are taken by an attacker is the unknown. Vulnerability management programs, as stated in Section C.13.1 “Threat and Vulnerability Management” of RG 5.71, are intended to ensure the technical and operational elements of a licensee’s defensive strategy are sufficiently protected against known threats, vulnerabilities, and attack methods. Cybersecurity professionals do not know what actions an attacker and sometimes malware will initiate after exploitation, even when a network is sufficiently protected.

### 3.0 CONSIDERATIONS OF THE DESIGN BASIS THREAT

#### 3.1 General Observations

- The staff disagrees with the statement that, “The capabilities of a nation-state actor are ‘beyond design basis threat.’” The design basis threat affirmatively defines a range of attacks and capabilities against which a nuclear power plant must be prepared to defend against, without focus on the identity, sponsorship, or nationality of the adversaries.
- The staff disagrees in part with the statement, “During vulnerability analysis, the focus is preventing exploitation of a vulnerability that affects detecting the compromise prior to actions being taken to protect the SSEP function or a direct CDA.” During the process of vulnerability analysis, the focus is preventing exploitation of a vulnerability. The staff disagrees that vulnerability management is dependent on detection of compromise.
- Regarding the section “Indirect CDAs” on page 3, when speaking on Indirect CDAs, NEI 13-10, Appendix F, Guidance for Application of NEI 08-09 Appendix E Controls to Indirect, EP, and BOP CDAs for E.12 states that, “...this control (E.12) is addressed by NEI 13-10 Section 5 (e) and (g) and plant-wide program to address the threat and vulnerability notifications received from credible sources are screened, evaluated, mitigated and dispositioned in accordance with the CSP.” There is no mention that Indirect CDAs receive an exception for vulnerability screening and analysis. Vulnerability

analysis of Indirect CDAs should be addressed on a case-by-case basis. Indirect CDAs are at times connected to Direct CDAs and licensees must maintain awareness of whether a newly identified vulnerability has the potential to open a pathway to a CDA that impacts Safety or Security functions.

- Regarding the section on the bottom of page 3 that lists various questions, the staff disagrees on their intent. Licensees should consider these questions when implementing separate controls apart from vulnerability management during the initial assessment process. For example, detection is required per D.5.2 “Host Intrusion Detection System (HIDS)” and E.3.4 “Monitoring Tools and Techniques”. In addition, numerous other NEI 08-09 controls mention statements such as, “Monitors and records physical access to the CDA to timely detect and respond to intrusions.” Licensees cannot credit security controls already required to be implemented to address NEI 08-09 Addendum 5 and E.12.
- The staff disagrees with the statement in this section that states, in part, “When evaluating impact for an individual vulnerability, only the following need to be considered:...” This statement indirectly screens out vulnerabilities that could be addressed generically and is not fully inclusive of the aspects licensees must consider. Additionally, the staff disagrees with the focus on the proposed approach on the ability to detect compromise, as detection is unrelated to the vulnerability management program’s purpose of evaluating and mitigating vulnerabilities.
- Regarding the statement, “This is not a consideration for isolated CDAs,” the staff is unclear how the white paper defines isolated CDAs.
- For defense-in-depth (DiD), the staff agrees in part with the statement that, “Maintaining defense-in-depth (DiD) is a requirement of a licensee’s cyber security plan and was codified by the 2009 Power Reactor Security Requirements rulemaking, 10 CFR 73.54(c)(2). The NRC delineated specific requirements during the rulemaking period as to how DiD is achieved and to clarify the unique differences with DiD for 10 CFR 73.54 and 10 CFR 73.55, as well as distinguish DiD from the traditional design engineering concept of Nuclear Power Plant (NPP) operations.” This is true, but incomplete. In addition to this statement, the final rule was developed to ensure that the measures used to protect digital computer and communications systems and networks remained effective and continue to provide reasonable assurance. This section addresses the requirements in 73.54 (d) related to the cyber security program. The evaluation and management of cyber risk strengthens the DiD model. Having other layers in the DiD model doesn’t remove the need to evaluate and manage cyber risks.
- The white paper mentioned the six aspects to adequate and effective DiD. However, the staff disagrees with the white paper’s narrow application of these attributes to vulnerability management, rather than as general attributes of risk management.
- The “Note” at the bottom of page 5 states, in part, “This does not change the requirement to address vulnerabilities below a CVSS score of 7.0 for CDAs and a CVSS score of 4.0 for defensive architecture.” The use of “below” appears to be a

typographical error, and the staff notes that licensees are required to address vulnerabilities with a CVSS score of 7.0 or above and a score of 4.0 or above for defensive architecture in accordance with NEI 08-09 Addendum 5

- The section on the top of page 7 states, in part, “Having such a breadth of DiD technical and administrative controls allows Licensees to demonstrate with a high assurance that a vulnerability will not be exploited and adversely impact an SSEP function.” The staff agrees that a licensee’s CSP does provide “a breadth of technical and administrative controls”. However, these controls are used synonymously to achieve DiD, which vulnerability management is a part of. A vulnerability management program is an element within the broader scope of DiD implementation and not the other way around.

#### 4.0 EQUIPMENT PAST END OF SUPPORTED LIFE

##### 4.1 General Observations

- Addendum 2 of NEI 08-09 is mentioned within the white paper in this section. Addendum 2 provides approaches to implement the cyberattack detection, response, and recovery elements of the Rule and CSP. Specifically, this addendum provides the actions that are performed after the assessment and analysis of the vulnerability management program. The staff recommends that the acts of detect, respond, and eliminate (DRE) be described and implemented separately from the requirements for vulnerability management to avoid conflating them.
- Whitelisting is mentioned within this section as well. As stated before in our response, other controls that are already required should not be used as a means of mitigation for a vulnerability. Vulnerabilities need to be assessed and analyzed as an independent entity. Whitelisting and other forms of host intrusion detection systems (HIDS) are other controls separate from the vulnerability management control.
- Security testing is mentioned on page 9 within this section. The white paper states, in part, “If security testing has been performed on the system or test system, it can be considered as part of remediation of the vulnerabilities.” The staff is unclear whether the white paper is referring to physical or logical security testing. Specific logical/technical security testing would be a factor in the contribution towards a remediated vulnerability. Additionally white security testing might highlight vulnerabilities, vulnerabilities would only be mitigated through a licensee’s actions taken after the results from the testing have been analyzed.
- The staff agrees that the section, “Mitigations for End-of-Life Equipment,” outlines a reasonable approach to addressing CDAs that no longer receive vendor-supplied patches following their end-of-life.

#### 5.0 IMPLEMENTATION OF REMEDIATION

## 5.1 General Observations

- The staff disagrees with the approach proposed in the white paper that focuses on implementing controls such as physical security, configuration management, work control process, monitoring tools, and portable media protection as a means to address the attack vector a vulnerability is intended to exploit. An adequate way to address vulnerabilities is to examine what controls are in place and determine if one or more specific controls would preclude the vulnerability from being exploited. For example, a licensee cannot take credit for existing administrative and physical security controls to mitigate the attack vector that would exploit a vulnerability with a particular protocol. In that case, the physical security and work control processes would not address the attack vector that intends to exploit the vulnerability and detection would not mitigate the vulnerability either. Detection is an after-the-fact mechanism to mitigate the consequences of an attack. In both cases, neither the risk is being evaluated or managed and; therefore, this approach would not meet the requirements of the 10 CFR 73.54 which is to evaluate and manage the risk.
- Page 11 of this section which states, in part, “What security controls are currently in place that protect the CDA from exploitation of the vulnerability as described in the alert or notification document?” This is adequate if the licensee analyzes each vulnerability. In addition, the NRC does not accept statements such as “protected by the data diode” or “protected with physical security” as justification to not protect CDAs under a vulnerability management program.
- The staff disagrees with the statement on page 11 which states, in part, “A licensee should credit any security controls already in place that would prevent or detect an attacker (or malware) attempting to exploit a vulnerability (e.g., unescorted access authorization, behavioral observation program, physical access control, system monitoring, port blockers, control of portable media/file transfers, device whitelisting, security and operator rounds).” This is not adequate to meet the requirements for a vulnerability management program. The program must stand on its own and act as an independent layer of the DiD infrastructure. Controls mentioned in this sentence should already be in place per a licensee’s CSP.
- Regarding the statement at the bottom of page 11, the white paper states, in part, “To access the network, the attacker would need to connect a laptop to a network switch. The network switch is in a secured location. Port locks are installed on connected network cables plugged into the switch and port blockers are installed in all unused ports. Port security is enabled on interfaces (switch ports) in use and unused interfaces are administratively shutdown. The network is monitored and alerts when a “rogue” system is connected.” This implies that physical security is sufficient to address a network-based vulnerability. An attacker within the design basis threat will almost certainly not rely on one vulnerability to access a system. It will most likely be a well thought out, coordinated attack that might bring down a monitoring network before the vulnerability is exploited. Simply stating that physical security is sufficient to not address/analyze a vulnerability is not adequate.

- The staff disagrees in part with the statement at the bottom of page 11 which states, in part, “If a critical digital asset is not connected to a network, then an attacker would be unable to exploit any network-based vulnerabilities (those with the CVSS attack vector of “network” or “adjacent”) despite being vulnerable.” A laptop connected to the CDA would introduce the “adjacent” attack vector. A licensee’s PMMD program constitutes one layer within the DiD infrastructure. Vulnerability management adds another layer. Altogether these layers develop a DiD approach that decreases overall risk within a licensee’s network infrastructure.
- Regarding the statement at the top of page 12, the white paper states, in part, “When a licensee is unable to correct a vulnerability, the focus should be on other preventive or detective measures such as intrusion prevention or detection.” Being unable to correct a vulnerability is subjective and it may be different from site to site. NRC understands that bringing a system down for patching may cause adverse impact, but that should not mean that the licensee should discard the vulnerability because “detection” is in place. For example, an outage should provide the flexibility necessary for correcting a vulnerability.
- Regarding the statement on the top of page 12, the white paper states, in part, “A licensee must describe how the safeguards identified in the previous template question prevent or detect attempts to exploit the vulnerability in question in the context by which vulnerability exploitation is possible (i.e., attack vector). Security controls are safeguards that must be defeated by an attacker (or malware) to have an opportunity to exploit a vulnerability. If multiple (two or more) barriers must be defeated before an attacker could have an opportunity to exploit a vulnerability, then it can be concluded that security controls in place provide adequate DiD protection despite a critical digital asset still being vulnerable.” The staff believes this statement is too subjective as written, and could be incorrectly interpreted as allowing a licensee to utilize controls that are already in place and conclude that barriers exist so there would be no direct requirement to assess/analyze particular vulnerabilities.
- Regarding the statement in the middle of page 12, the white paper states, in part, “If a licensee fails to identify security controls in the second question above that would prevent or detect exploitation of the vulnerability (under consideration) or determines they are inadequate, then corrective action must be taken.” This statement is too broadly written. All licensees subject to 10 CFR 73.54 have a method of detection and prevention capability on their network. Furthermore, licensees are unlikely to conclude that their detection and prevention techniques are inadequate. Therefore, according to this logic, if the licensee has detection and prevention on their network and they deem their DiD protections are adequate, then corrective action for a vulnerability does not need to be taken. This would not meet the requirements of the Rule.
- Correcting a vulnerability when unable to do so is mentioned in various parts of the white paper. Being unable to correct a vulnerability is too subjective. Previous conversations between a licensee and the NRC have proven that identical vulnerabilities are treated differently depending on various factors. Throughout the white paper, there is a strong

emphasis on taking credit for controls that should already be in place in order to address the requirements of the vulnerability management program. The staff wants to ensure that this is not an adequate way to address vulnerabilities.