U.S.NRC
Protecting People and the Environment

NRC Inspection Manual Chapter 0612 Appendix E – Minor Examples

Kim Lawson-Jenkins
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission

Overview

- IMC 0612 Appendix B – Issue Screening
- Updated and New Cybersecurity Minor Examples
- Next Steps

IMC 0612 Appendix B – Issue Screening

Is the performance deficiency More-than-Minor?

If the answer to **any** of the following questions is "yes," then the performance deficiency is More-than-Minor and is a finding. If the answer to all of the following questions is "no," then the performance deficiency is minor and is not a finding.

1. Could the performance deficiency reasonably be viewed as a precursor to a significant event?
2. If left uncorrected, would the performance deficiency have the potential to lead to a more significant safety concern?
3. Is the performance deficiency associated with one of the cornerstone attributes and did the performance deficiency adversely affect the associated cornerstone objective?

IMC 0612 Appendix B – Issue Screening

Defense in Depth considerations

- Capability to detect, respond to, and recover from cyber attacks
- Multiple layers of defensive security controls are placed throughout the system with the intent of providing overlapping defenses in the event that a control fails, or a vulnerability is exploited

Updated Cybersecurity Minor Example

- **NEI 08-09, Appendix A, Section 3.1.6 – Mitigation of Vulnerabilities and Application of Cyber Security Controls**

Application of Cyber Security Controls

NEI 08-09, Appendix A, Section 3.1.6 – Mitigation of Vulnerabilities and Application of Cyber Security Controls

A critical digital asset (CDA) was classified by the licensee as a direct CDA and the inspectors discovered that the licensee had inadequately implemented some of the technical controls in Appendix D of NEI 08-09, “Cyber Security Plan for Nuclear Reactors”. The issue addressed by this example is the misclassification of a CDA that results in inadequate protection against a cyber attack.

Minor if: Upon assessment, the CDA met the criteria for an indirect CDA in accordance with NEI 13-10 and all the required baseline controls were in place for an indirect CDA. The PD can also be minor if the CDA met the criteria for an indirect CDA in accordance with NEI 13-10 and alternate controls were in place that were commensurate to the required baseline controls.

MTM if: The PD is MTM if the required baseline controls for an indirect CDA were not in place, or the required Appendix D & E security controls were not in place for a direct CDA, or adequate alternate security controls were not in place for either indirect or direct CDA.

New Cybersecurity Minor Examples

- Baseline Configuration
- Ongoing Monitoring and Assessment
- Removal of Unnecessary Services and Programs
- Physical Access Control
- Evaluate and Manage Cyber Risk (Vulnerability Management)

Baseline Configuration

NEI 08-09, Appendix E, Section 10.3 – Baseline Configuration

The inspector performed a review of the cyber security control assessment for a CDA. The licensee failed to implement the cyber security control E10.3 “Baseline Configuration” which requires licensees to document and maintain an up-to-date, complete, accurate, and readily-available baseline for each CDA. When the inspector asked for the running configuration of software on the CDA, a discrepancy between the documented baseline configuration and the running configuration was identified.

Minor if: This is an isolated incident and the discrepancy between the baseline and running configuration was an incorrect parameter – such as a version number - related to software that did not impact the effectiveness of other security measures (e.g. vulnerability management). Missing attributes did not introduce a new vulnerability or an unmitigated vulnerability.

MTM if: The baseline configuration did not list software identified in the running configuration, the gap was not an isolated incident, or an incorrect version impacted the effectiveness of other security measures.

Ongoing Monitoring & Assessment

NEI 08-09, 4.4 Ongoing Monitoring and Assessment

The inspector performed a review of the cyber security control assessment for a digital device within the scope of 10 CFR 73.54. When performing verification of implemented security controls, the inspector identified a security control that should have been implemented on the digital device but was not. The inspector also determined that the licensee had provided no documented evidence verifying ongoing monitoring of the controls for the selected digital device.

Minor if: If an undetected or unauthorized change to a single security control would not result in a reduction in the effectiveness in the defense in depth protective strategy or there are no unmitigated vulnerabilities. An example would be a reboot of a CDA that resulted in an unneeded application or service running that had previously been disabled. If the running application or service did not introduce any known vulnerabilities required to be assessed per the vulnerability management policy, and other defense in depth measures – such as a SIEM identifying new traffic from a port used by the application – could mitigate the effect of the change, then the violation would be minor.

MTM if: The PD adversely affected the security cornerstone objective because failure to perform ongoing assessments of implemented cyber security controls does not provide adequate protection by not verifying that the cyber security controls implemented for CDAs remain in place throughout the life cycle of the CDA. Failure to perform ongoing assessments of cyber security controls also does not provide adequate protection for detecting unauthorized changes to data or software that could adversely affect SSEP functions.

Removal of Unnecessary Services & Programs

NEI 08-09, Appendix D, Section 5.1 Removal of Unnecessary Services and Programs

The inspector performed an initial review of the cyber security control assessment of an engineering workstation between security levels 3 and 4. The review found numerous unnecessary services installed and not disabled on the workstation.

Minor if: If the service or program does not introduce an unmitigated vulnerability on the device. An example would be Server Message Block (SMB) on a device where the operating system has been patched for the vulnerability.

MTM if: If the licensee has an unnecessary service or program and failure to implement this control would result in a reduction of the defense-in-depth protective strategy – such as not establishing an accurate baseline configuration, not adequately screening vulnerability notices or having the ability to detect an exploitable vulnerability, not having the ability to determine that the unnecessary service has been enabled or an unnecessary port in processing unidentified or unauthorized traffic, etc…

Physical Access Control

NEI 08-09, Appendix E, Section 5.5 Physical Access Control

The inspector performed a review of the cyber security control assessment and a walkdown of an x-ray machine located in a warehouse outside of the protected area. The review determined that insufficient physical security controls were implemented for the x-ray machine.

Minor if: The licensee can demonstrate functionality and adequate defense in depth protections to determine if the security function provided by the x-ray machine has been compromised prior to operation. Adequate alternate controls for a real-time intrusion protection (i.e., automated detection capabilities) to immediately facilitate dispatching security personnel to investigate and/or remediate a potential cyber security concern include a combination of the following - physically protecting the x-ray machine with serialized tamper seal tape, random security guard patrols, cameras monitored by Site Security 24/7 and/or testing to verify operability prior to use of searching packages/materials for contraband. See NEI 08-09 Appendix E.3.6 for the security control “Security Functionality Verification”.

MTM if: The licensee failed to implement or implemented inadequate alternate controls to prevent and detect a compromise of near real time detection of compromise of the security function of the x-ray machine.

Vulnerability Management

NEI 08-09, Appendix E, Section 12 Evaluate and Manage Cyber Risk (Vulnerability Management).

The inspector performed a review of the cyber security control assessment for a device within the scope of 10 CFR 73.54. The licensee stated that they were following NEI 08-09 Addendum 5 for their vulnerability management process. The inspector determined that the licensee had not adequately implemented vulnerability assessments.

Minor if: Vulnerability notices for applicable CDA software or firmware are tracked in the licensee's vulnerability management process using the periodicity specified in their cybersecurity plan but the inspection identified an isolated vulnerability not identified by the licensee.

MTM if: Review of vulnerability notices was based on limited input (i.e., not based on multiple credible sources) or incorrectly performing vulnerability assessments using CVSS as specified in NEI 08-09 Addendum 5.

Next Steps

- **July 30 – Comments resolved; updated section of the IMC is submitted to Office of Nuclear Reactor Regulations (NRR)**