Ongoing Monitoring and Assessment White Paper

Tanvir Siddiky
CSB/DPCP/NSIR

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Overview of the Paper

- The purpose of the paper is to provide licensees guidance and examples on OM&A activities and changing control periodicity
- Provides basis and guidance of 9 categories from NEI 08-09 section 3.1.6 for implementing an alternate periodicity
- The paper presents examples and some guidance, but it lacks clarity, justification and proper basis for alternate periodicity
- NEI intends to incorporate the feedback from this white paper into NEI 08-09 Rev 7; therefore, the white paper was not considered for approval for use

Previous Public Meeting with NEI

- Attack vectors can be mitigated by applying additional security controls
- Continuously staffed vs continuously surveilled
- Password change periodicity can be extended under certain conditions and event (Termination, job function change etc.)
- Additional capabilities of SIEM
- Adverse impact to SSEP functions and safety issue
- NIST 800-63 standard
- Transfer of alternate periodicity from one CDA to another
- Examples provided are not primary basis rather an additional justification

Feedback for NEI

- Alternate periodicity must meet the intent of the original control periodicity.
  - For example, the intent of password control periodicity (NEI 08-09 D.4.3) is to prevent unauthorized access due to password theft or password cracking. If an alternate password change periodicity is used, complete justification needs to be provided to show that the intent was met by the extension
- Alternate periodicity in lieu of implementing the original periodicity must mitigate the consequences of the threat/attack vector the control is intended to protect.
  - For example, if SIEM is being credited for detecting rogue devices and rogue device scanning periodicity (NEI 08-09 D.1.18) is extended beyond agreed upon time, explanation and basis of justification need to be provided regarding how the new periodicity mitigates the threat/attack vector

Feedback for NEI

- If OMA activities are aligned with regularly scheduled maintenance due to nuclear safety risk, other measures need to be considered as well. This alone should not be a justification of frequency extension. Equipment that can't be shut down due to nuclear safety risks, the periodicity may be extended not to exceed 24 months or refueling outage whichever one is sooner.

- More guidance is needed to take credit for continuously staffed and surveilled locations for altering password change periodicity. Security/operations personnel need to have documented instructions and training that the specific control is intended to mitigate. Camera recordings need to be reviewed regularly.

Feedback for NEI

NEI's proposal regarding extension of password change periodicity-

- CDA has no network connection (Public meeting discussion), or
- Remote attack pathways have been considered and addressed (Public meeting discussion)

And **one of the** following is applied:

- CDA is in a locked and alarmed cabinet (Page 9 example 3)
- CDA is under key controlled program limited to the critical group (Page 9 example 3)
- CDA is in a continuously manned or surveilled area (Page 4 and public meeting discussion)

This approach is not sufficient as it introduces gap in mitigating the consequence of the attack vector.

Feedback for NEI

- Crediting SIEM- Availability of New Technologies
  - SIEM technical capability documentation needs to be provided
  - The implementation must include periodic verification of the effectiveness and continuing function of the technology
  - SIEM generated security logs, events, access control lists etc need to be periodically reviewed
  - E.3.1 (System and information integrity) and E.3.4 (monitoring tools and techniques) should be implemented on the new technology

Feedback for NEI

- If a generally accepted standard such as NIST is credited for alternate periodicity justification, then the standard needs to be followed completely and not only certain sections.
- Regarding sections on Industry operating experience and experience with security control, it is not acceptable to cite the potential for human performance or procedural compliance errors as a sole justification for extending the original control periodicity.
- Sections on Benchmarking and Audits/Assessments lack adequate guidance.
- The staff reviewed the white paper under the assumption that the examples provided in the white paper are illustrative and are not all-inclusive. Additional detail and justification would be needed to extend the frequency including the length of the frequency and potential backstops for event-based frequency

QUESTIONS AND COMMENTS

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment