Cybersecurity Inspection Insights

ROP Public meeting

July 13, 2023

Cybersecurity Inspection Insights

Purpose

- Share cybersecurity inspection lessons learned and insights to recommend enhancements to the overall inspection process
- Support NRC efforts to develop examples to improve clarity for minor/more-than-minor (MTM) criteria

Cybersecurity Inspection Insights

Observation

- Frequency of violations during cybersecurity inspections outpace other inspections by at least a factor of 3*
  - Cybersecurity: 15 NCV Green findings per 1000 hours of inspection
  - Others: 1-5 NCV Green findings per 1000 hours of inspection
- Two main factors through discussions with regional inspectors/ branch chiefs
  - All performance deficiencies impact the security cornerstone and require analysis as an issue of concern
  - There are limited cybersecurity examples of minor violations to aid in minor/MTM determination

* Shared by NSIR at NEI Cybersecurity Implementation Workshop

Cybersecurity Inspection Insights

Recommendations

- Enhance cybersecurity issue screening criteria
  - Consider operational impact of issue
  - Provide an offramp to analyze an issue of concern prior to classifying as a performance deficiency
- Provide additional cybersecurity minor/MTM examples (currently being addressed by NSIR)

Cybersecurity Inspection Insights

Screening Criteria

- When assessing an issue of concern as a performance deficiency the following questions could help determine if further screening is necessary and a violation is warranted
  - Does a deficient implementation of the control reveal an exposure to a known exploited vulnerability to allow an adversary to attack the site, which would result in an adverse impact?
  - Would the CDA fail in a manner that does not impact the SSEP function?
  - Was compliance to the security control documented in the site's device or system assessment? (Was a good faith effort made to address the control?)
    - Has the CDA been assessed as a non-direct CDA? (Is the control required control for Indirect CDAs?)
    - Has the site provided substantiation that supports their assessment (vendor guidance, standards, etc.)?
    - Was the assessment performed according to the site's procedural guidance?
  - If the control was addressed through alternative means or controls, was substantiation provided per CSP 3.1.6?
  - Were the other controls in the control family implemented per NEI guidance? (Defense in Depth applied)
  - If the site has self-identified a performance deficiency, was it entered into the site's Corrective Action Program?

Cybersecurity Inspection Insights

Minor/MTM Examples

- Additional cybersecurity examples would be beneficial to describe when a performance deficiency does/does not adversely affect the security cornerstone (discussed by NSIR staff)
- Identify where inspectors may have had difficulty screening an issue as minor/MTM during the current inspection cycle

Cybersecurity Inspection Insights

Summary

- Inspection execution is an evolving process and criteria used to evaluate issues should be reviewed and enhanced when appropriate
- Cybersecurity inspection findings are an outlier (high) in the number of findings per 1000 hours of inspection
- The current SDP criteria in IMC 0609 and IMC 0612 treats all cybersecurity performance deficiencies as violations
- Additional screening criteria earlier in the process may provide an off ramp for inspection issues that have no adverse impact
- More examples of minor violations for cybersecurity issues would address some of the inspection challenges that regional inspectors and branch chiefs have identified. (NSIR is currently addressing)
- NEI through the Cybersecurity and ROP task forces are eager to assist in providing recommendations and supporting enhancements to the cybersecurity inspection program