Cybersecurity Inspections Lessons Learned

Public Meeting (Closed)

February 15, 2024
10:00 A.M. – 12:00 P.M.

Tammie Rivera, Cybersecurity Specialist
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

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

Topics

- Key Messages
- Background
- 2023 Top 3 Trends (MTM Violations & Cross-Cutting Aspects)
- Observations
- Lessons Learned & Insights
- Next Steps
- Q & A

Key Messages

- This meeting focuses on cybersecurity baseline inspection activities conducted during CY 2023.
- Staff identified lessons learned and trends from the 2023 cybersecurity inspections.
- This effort will support identification of any actions needed to ensure efficiency and effectiveness of future inspections.

Background

- Objectives of IP 71130.10
  1. *To provide assurance that digital equipment associated with safety, security, or emergency preparedness (SSEP) functions are adequately protected against cyber-attacks in accordance with (10 CFR) 73.54 and the licensee's approved cyber security plan (CSP).*

  2. *To verify that CSP changes and reports are in accordance with 10 CFR 50.54(p).*

Inspection Procedure 71130 Attachment 10, “Cyber Security,” (ML21155A209)

Background (continued)

- Inspection Requirements

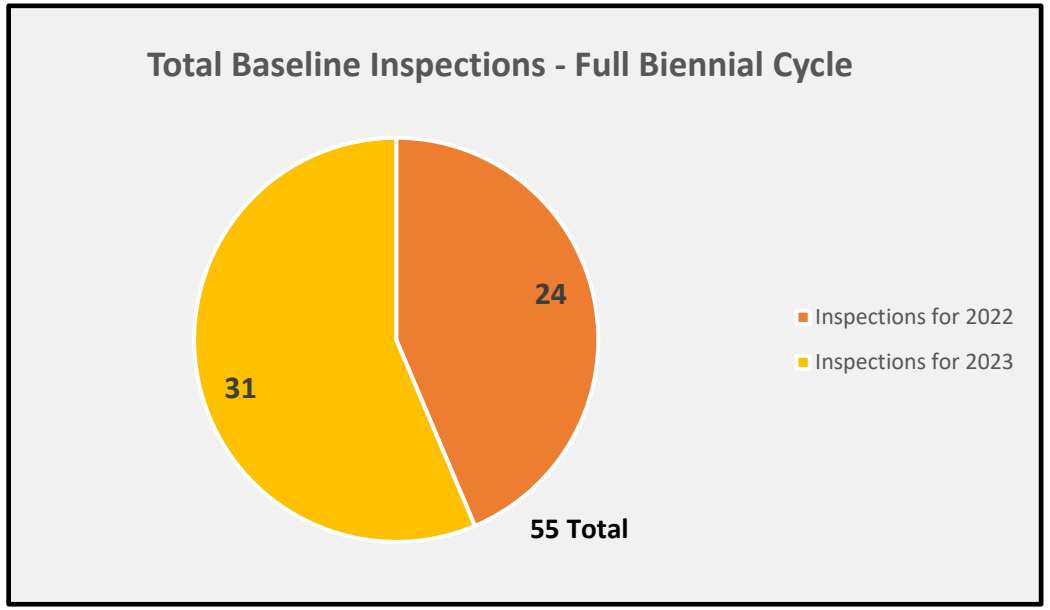
Excerpt from IP 71130.10, page 2:

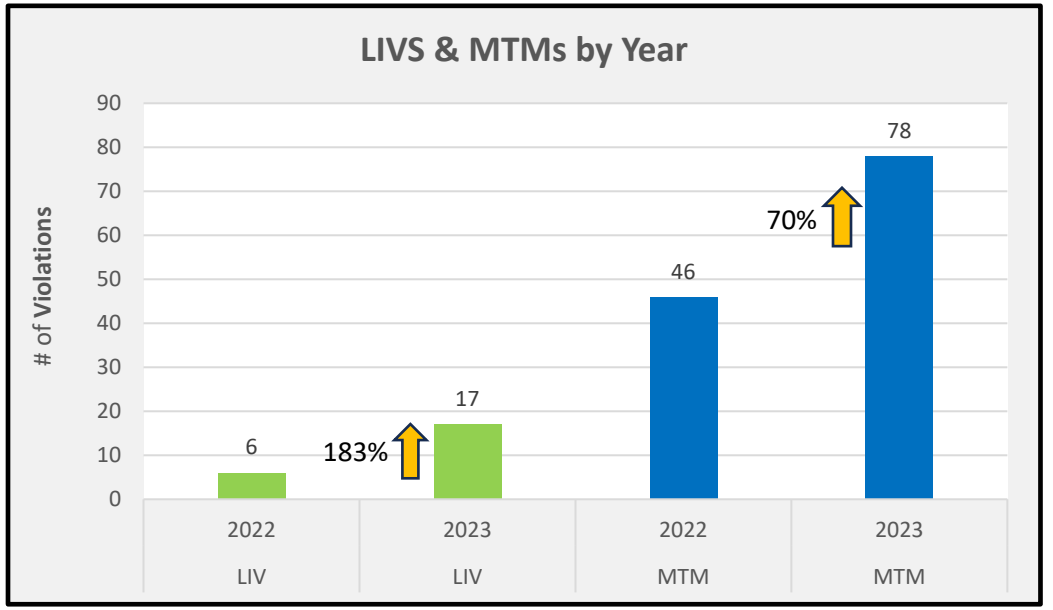
  - This inspection requirement range for completion is as follows:
    - minimum of three inspection requirements,
    - nominal four inspection requirements, and
    - maximum, based on unusual circumstance, or special considerations, five inspection requirements.

  - Inspection teams considered the following special considerations during development of cybersecurity team inspection plans:
    - First biennial cycle completion using IP 71130.10
    - High number of inspection findings during the biennial cycle

Inspection Procedure 71130 Attachment 10, "Cyber Security," (ML21155A209)

Inspections and Violations





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

2023 Top 3 Trends

MTM Violations

Most commonly cited NEI 08-09[1] security controls:

1. Vulnerability Management (*E.12*)
2. Baseline Configuration (*E.10.3*)
3. Monitoring Tools and Techniques (*E.3.4*)

Cross-Cutting Aspects (CCAs)

Most commonly cited CCAs as described in NRC IMC 0310[2]:

1. Conservative Bias (*H.14*)
2. Resources (*H.1*)
3. Procedure Adherence (*H.8*)

[1] NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, Addendum 1 Markup dated 2017 (ML17079A423)
[2] IMC 0310, "Aspects Within The Cross-cutting Areas," (ML19011A360)

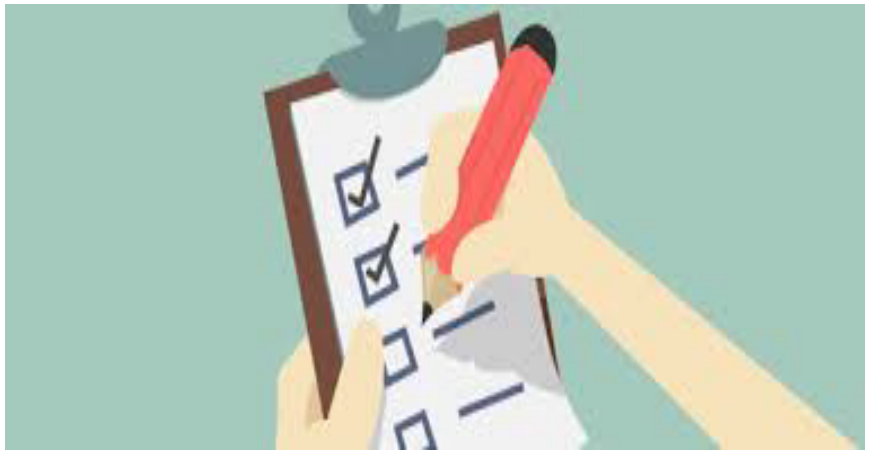
Observations

- Resources – Staffing and retention of well qualified cyber staff
- Training – properly trained staff and knowledge transfer (particularly, *specialized training*)
- Documentation – insufficient documentation (*i.e. CDA assessments and alternate controls*)
- Licensee cyber staff not thoroughly familiar with the requirements, guidance, or misinterpretation of the requirements

Lessons Learned

- A one-week inspection is challenging and resource intensive
- Inspectors have observed that the best performing sites and well-maintained cybersecurity programs have strong support from senior management
- Documentation still does not reflect the whole story
- Inspectors observed that some licensee staff lacked experience with regulatory requirements, background, and guidance related to the implementation of the cybersecurity program.

Insights



- Accurate and complete documentation improvement reduces the number of questions.

- The program is in the maintenance phase. Inspection focus on the defense-in-depth approach

- The NRC will continue to enhance the oversight program.

  - IMC 0612 Appendix E, "Examples of Minor Issues"

Next Steps

- An agency working group was established to evaluate alternate inspection procedure frequencies and team composition

- Reasons for establishing the working group:
  - Completing cybersecurity biennial inspections in one onsite week has been a challenge for regional inspection teams.
  - Inspection teams and licensee response teams need more time to address questions and disposition identified issues.

- The working group expects to present solutions that will gain efficiency and effectiveness

- The working group will develop recommendations for management consideration. Any proposed changes to the inspection procedure will be discussed at a later public meeting.

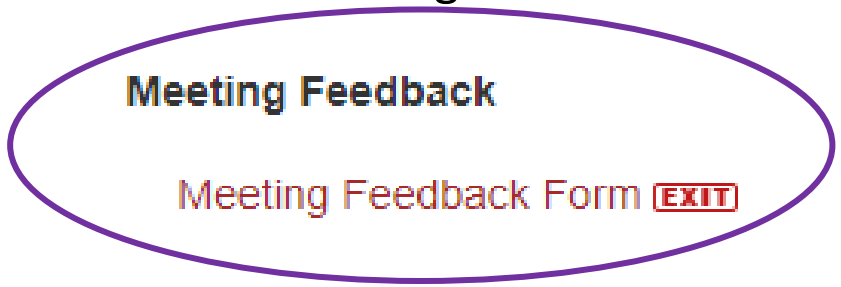
Questions & Discussion

Trends → Observations → Lessons Learned → Increase Efficiency

Submitting Meeting Feedback & POC

To submit feedback and comments please:

- Navigate to this meeting on the NRC Public Meeting Schedule
- Click the Meeting Feedback Form link



Meeting POC: Tammie Rivera

Tammie.Rivera@nrc.gov

Cyber Security Branch

Division of Physical and Cyber Security Policy

Office of Nuclear Security and Incident Response