WILLIAM R. GROSS
Director, Incident Preparedness
Facility Security Officer

1201 F Street NW, Suite 1100
Washington, DC 20004
P: 202.739.8123

wrg@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

April 20, 2021

Ms. Shana R. Helton
Director, Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Industry Comments on Draft Inspection Procedure 71130.10, "Cyber Security"

Project Number: 689

Dear Ms. Helton:

The Nuclear Energy Institute[1] (NEI) and our members appreciate the opportunity to provide comments on Draft Inspection Procedure (IP) 71130.10, "Cyber Security," for consideration by the U.S. Nuclear Regulatory Commission (NRC) staff. At this time, the NRC has completed the first cyber security program inspection at most power reactor facilities, including a subsequent review of corrective actions implemented to address inspection issues. The draft procedure provides an opportunity to enhance the inspection process through the incorporation of lessons learned from this first cycle of inspections.

Our suggested changes are directed at making the inspection process more performance-based and effective. At a high level, NEI recommends that the staff:

- **Enhance the cyber security program performance metrics**. As written, the metrics described in the draft IP are focused on a more efficient inspection process; however, utilities focus their energy on metrics that monitor program health to drive performance improvement. Consider revising the proposed metrics to monitor areas with the most substantial value added to the health of the cyber program.
- **Eliminate redundancy with other inspection activities**. Inspection efficiency can be improved by eliminating inspection elements that are redundant with other inspections. This includes elements of inspection activities that review Corrective Action Programs, and evaluations made pursuant to the requirements of 10 CFR 50.54(p). Other potential areas of inspection overlap should also be identified and eliminated.

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

- **Ensure the IP resource estimate matches the actual inspector complement and "hours on site."** It is important that the estimate reflect the best available information to promote a more effective process for both the inspection team and the licensee. Industry experience has shown that during some cyber security inspections, the cyber inspection team complement has been exceeded through the inclusion of NRC observers or individuals in training, causing inefficiencies for both the licensee and NRC inspection team. The IP should clearly indicate that individuals beyond the designated NRC inspection team should not perform inspection-related activities.

Our detailed comments may be found in the attachment to this letter.

If you have any questions or require additional information, please contact Rich Mogavero, at (202) 739-8174 or rm@nei.org, or me.

Sincerely,

William R. Gross

Attachments:

1) Industry Comments on Draft Inspection Procedure 71130.10, "Cyber Security"

c: Mr. James D. Beardsley, NSIR/CSD, NRC
NRC Document Control Desk

Comments

U.S. Nuclear Regulatory Commission
DRAFT INSPECTION PROCEDURE 71130.10

Page	Section	Proposed Change/ New Language	Comment/ Justification
1	01.01	~~To provide assurance that the licensee's digital computer and communication systems and networks associated with safety, security, and emergency preparedness (SSEP) functions, are adequately protected against cyber attacks…~~ To verify the licensee is satisfying the performance-based objectives of the cyber security rule in accordance with its NRC-approved cyber security plan.	The cyber security rule requires licensees, not inspectors, to provide high assurance of adequate protection against cyber attacks. For this reason, the inspection objectives should be for NRC inspectors to verify licensees are satisfying performance-based objectives of the cyber security rule.
1	01.01	Change: …associated with Safety, Security….to …associated with Safety-Related, Important-to-Safety, including BOP important to safety, Security, ….	To be consistent with NEI white papers on SR/ITS and BOP ITS. The word 'safety' is unclear in this context, the Rule uses Safety Related. Given the distinction between Important-to-Safety and BOP important to safety, it is not clear how this distinction is to be made in this document.
1	01.02	~~To provide assurance that CSP changes and reports support nuclear safety and security.~~ To verify that CSP changes and reports are in accordance with 10 CFR 50.54(p).	The IP should be clarified. 10 CFR 50.54(p) provides the framework to ensure that changes do not decrease the effectiveness of the program.
2	02.01	Change "to reduce the number of…" to "to clarify the process for identification of…"	Editorial

2	02.02	…including one Safety-Related or Important-to-Safety and one security….	The use of 'safety' is too vague and not defined in regulatory space. Use terms from Rule or NEI white papers on SR/ITS and BOP. It is not clear if BOP is part of this specific inspection section guidance with respect to configuration management.
3	03.01.a	Change "Ongoing assessments and monitoring" to "Ongoing monitoring and assessment"	Editorial
3	03.01.a	"at the frequency specified in individual controls" OR within the evaluated alternate control frequency	This proposed change reflects consistency in how industry applies the controls.
3	03.01.b	"Vulnerabilities that pose a risk to SSEP functions are mitigated" OR evaluated	This proposed change allows industry to perform an evaluation without having to 'patch' all vulnerabilities.
3	03.01.c	Change, "effectiveness analysis" to "effectiveness evaluation".	NEI 08-09, Section 4.4.3.1 is titled, "Effectiveness Analysis" however, the words used in subsequent paragraphs refer to the effort as an "effectiveness evaluation".
4	03.01.a	~~The assessment process verifies the licensee implements cyber security controls at the frequency specified in individual controls.~~ Security assessments verify security-related activities and actions occur at the frequency specified in security controls.	Security controls are security-related activities or actions carried out by a licensee (administrative controls) or by a critical digital asset (technical controls). Typically, a technical control is already implemented through system functionality (e.g., Group Policy setting) so it only may be necessary to verify that certain activities or actions occur at the specified frequency. (e.g., password expires after maximum password age).
4	03.02.a	Defense-in-depth protective strategies have been implemented, documented, and are maintained to ensure the capability to detect, delay, respond to, and recover from cyber-attacks on CDAs ~~in near real-time~~. The ~~defensive strategy~~ Cyber Security Plan establishes controls to ensure that the licensee can detect, delay, respond to, and recover from malware and cyber-attacks. The controls may differ for the different cyber security defensive levels. Licensees may have implemented near real-time automatic detection mechanisms to capture logs and to generate alarms~~, as~~	As described in NEI 08-09, Addendum, timely detection can be demonstrated through the use of near real time automated capabilities, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway. 'malware' and delay should be removed from throughout the inspection procedure to align with the Rule.

		~~necessary~~, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway (e.g., supply chain testing). Provide defense-in-depth ~~protective strategies~~ through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the program. ~~"Defense-in-depth protective strategies must provide high assurance of adequate protection against adverse impact to SSEP functions resulting from cyber attacks, which could adversely impact the integrity or confidentiality of data or software, deny access to systems, services, or data, and adversely impact the operation of systems, networks, and associated equipment to protect against the DBT."~~	NEI 08-09 Section 4.3, The defensive strategy ... implements the cyber security controls in accordance with the CSP.... 10 CFR 73.54(e)(2)(i) - timely detection and response to cyber attacks... The CSP Section 4.3 also does not use the words "in near real-time" following "CDAs". As this is a 'Performance based requirement' per 2.2.7 of the CSP. Consider re-wording to "To demonstrate the performance of this requirement, review the (provide)…" Also, the wording "protective strategies" is not within the section of the CSP. Recommend removing. This paragraph conflates many distinct elements of 10 CFR 73.54. More importantly, it provides no meaningful guidance to the inspector. Recommend it be removed.
4	03.02.b	"Verify that the licensee maintains controls and elements to ensure boundary protection for the cyber security levels and ensures that integrity of data is maintained."	This verification statement should reference the applicable section of the CSP.
4	03.02.b	"The defensive architecture has been implemented, documented, and is maintained to protect ~~critical digital assets~~ CDAs that have similar cyber risks…"	Editorial
5	03.02.b	"Analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber-attacks to preserve the intended function of plant systems, structures, and components within the scope of the cyber security rule and account for these conditions in the design of the program."	The cyber security rule requires licensees, not inspectors, to analyze digital computer and communications systems and networks… Recommend rewording for the inspector to 'verify' this inspection element.

5	03.02.d	~~User Identification and Authentication~~ Evaluate Changes to the Identification and Authentication Controls	NRC has already inspected this element during previous implementation inspections. Recommend it be reworded to “evaluate changes to the identification and authentication controls”.
5	03.02.d	The licensee has established access controls to limit and to control the access to CDAs, as prescribed by the CSP. The licensee has established policies and procedures as required by the CSP (e.g., NEI 08-09, Appendix D, Section 1, “Access Control,” and Section 4, “Identification and Authentication” or Regulatory Guide 5.71, Appendix B.4, “Identification and Authentication.”). The licensee also has policies and procedures for the removal of personnel from having access when their job functions no longer require access and the periodic review of the access authorization list.	All other inspection requirements appropriately defer to "in accordance with the CSP", however, item 03.02.d specifically mentions NEI 08-09, App D, Sec 1 and Sec 4 or RG 5.71, App B.4. Although NEI 08-09 is the common standard for all Cyber Security Plans, it is more appropriate to reference the licensees CSP directly as the standard in which they are being inspected. Specific guidance documents should be listed as examples, considering that the licensee's CSP could theoretically commit to something different.
5	3.02.d	“The licensee also has policies and procedures for ~~the removal of personnel from having access when their job functions no longer require access and~~ the periodic review of the access authorization list.”	Proposed change to align with NRC-approved Cyber Security Plan., (Appendix D, Section 1.2)
6	03.02.a	Verify that the licensee maintained the defensive architecture, its capability to detect, ~~to~~ respond to, and ~~to~~ recover from cyber ~~security threats~~ attacks.	The cyber security rule requires licensees to protect its digital systems and networks against cyber attacks.
6	03.03.a	Delete: ~~“They also include requirements to assess and configure CDAs for safety-related components”.~~	Sentence is redundant to context of this section and the overall topic of CDAs. As written, it seems to imply that SR CDA’s may not be consistent with rule scope and are treated differently. If the intent is to point out that SR items in general (not just CDAs) get special treatment, then clarity may be needed.
6	03.03.a	“Design Changes or Replacement Equipment”	NRC has already reviewed this element as part of the implementation inspections. The inspector should (could) review changes to systems to ensure the CSP was followed.
7	03.03.c	Verify that the licensee has implemented appropriate supply chain and services acquisition controls for changes and/or replacement CDAs.	Editorial

7	03.04.a	General Comment / Question	Consider removing verification of CSP changes from the scope of this IP, if it is redundant to other NRC inspections.
9	03.06	General Question	If Performance Metrics are selected by the licensee and the data provided is not complete or is not completed within a quarterly periodicity, what is the jeopardy or penalty? ○ Will Performance Metrics be declined and defaulted back to a full inspection? OR ○ Will "partial credit" be granted or considered for the data that was provided? OR ○ Will "extra penalty" be assessed (more penalty than otherwise assessed if a full inspection)? What is the threshold for determining whether or not the information was provided completely, and the team be reduced by one contractor?
9	03.06.a	Specificity needed on which aspects of the inspection that 'Performance Testing' may replace.	Section 71130.10-03 states that performance testing or metrics may allow other sections of the procedure to be waived. Sections 03.01a, 03.01b, 03.02a, 03.02b, 03.02d, 03.02e, 03.03a and 03.03b state that: "Information to complete this inspection step may be provided by the results of licensee performance testing." However, Section 03.06a states: "The planned performance and function testing is anticipated to demonstrate Inspection Requirements 03.02.a, 03.02.b, 03.02.c, and portions of 03.01.a, 03.01.b, 03.01.c, 03.02.d, 03.03 a, and 03.03.b. If the performance test(s) demonstrate implementation of these performance requirements, although not required, the inspection team may still elect to sample the requirements listed, above."

			The following information would provide valuable insight to licensee's inspection preparation and response activities: • Which portions of 03.01.a, 03.01.b, 03.01.c, 03.02.d, 03.03 a, and 03.03.b are subject to replacement per Section 03.06a? If contingent upon the design of functional testing approach, what specific criteria will be considered? • Section 03.02e implies that performance testing is an option, although this section is not listed at the forward of Section 03.06a. Is performance testing of the PMMD program subject to the exclusions described in Section 03.06? • Section 03.06a lists 03.01c and 03.02c, although these sections do not contain the statement that " Information to complete this inspection step may be provided by the results of licensee performance testing."
10	03.06.b	Clarify the impact on Inspectors/Contractors for the inspection when adequate performance metrics are provided.	Is this meant to say "by a contractor"? Or some other version? Section 03.06b states: If the following data is provided completely to the inspection team during the RFI submission, the inspection team shall be reduced by a contractor. Section 71130.10-04 states: The estimated time to complete the inspection procedure direct inspection effort is 70 hours (with a range of 63 to 77 hours) per site and will consist of one week of direct inspection effort with contractor support. This inspection is planned to be conducted as a team inspection. The team shall consist of two regional inspectors and two contractors. When a licensee elects to demonstrate an authentic and realistic performance and function test of the cyber security network configuration, the opportunity could provide inspectors a more efficient way to evaluate the licensee’s defensive architecture and selected

			program elements. If the inspectors conclude that the licensee provided an effective, acceptable performance and function test, then the inspection may consist of one inspector and two contractors for one week. This resource reduction occurs because the satisfactory performance and function test provides reasonable assurance of site cyber security protection in the inspection areas identified in this procedure. Does performance and function testing potentially reduce the number of NRC Inspectors, or NRC Contractors needed for the inspection?
10	03.06.b	"If the following data is provided completely to the inspection team during the RFI submission, the inspection team shall be reduced by one contractor."	Editorial Also, this change in the number of contractors should be included in the 'Resource Estimate' section similar to performance testing regarding the reduction in NRC inspectors.
10	03.06.b	General comment	Many of the metrics do not seem to provide a good measure of how well a licensee is overseeing their own program. An intrusive, engaged, and well implemented program is more likely to identify usage of unauthorized PMD, undocumented configuration changes, and unnecessary ports or protocols. A site performing log analysis and periodic baseline configuration checks may identify more of these items during their reviews, while a site only relying on the engineering configuration management program may find less, but the metric would then indicate the site with the less rigorous program is doing a better job.
11	03.06.b.1	~~"number of days to disable and remove…"~~	Propose removing for consistency with NRC-approved Cyber Security Plan (Appendix D, Section 1.2).
11	03.06.b.1	Bullet 1	The Industry has a concern on the broadness of the phrase "violation of access control policy." It does not seem well defined and could result in lack of consistency among licensees even by referencing D1.1 controls and site-specific policy documents.

			If keeping, consider adding clarity. The Industry asks: What constitutes a “violation of access control policy?”
11	03.06.b.1	Bullet 2 ~~“number of days to disable and remove…”~~	The Industry questions the basis in using the number of days to disable and remove user credentials of employees. Generally, the industry does not issue individual user admin credentials to CDAs and when physical access has been revoked in accordance with Physical Security policy, all CDAs are properly protected via the isolation associated with Milestone 3. Disabling of individual user admin accounts would be addressed in the periodic account reviews as defined by the CSP. It seems to the Industry that there may be gap with the intent of this metric and how licensee’s manage access. With this metric ‘as is’ it would be challenging to assess the value it contributes to the performance of a licensee’s cyber program.
11	03.06.b.1	Bullet 3	The Industry is not clear what constitutes a “non-compliance incident of cyber security controls by third-party personnel.” The industry agrees licensees need to control visitors, contractors and other third-parties however, clarity and specifics on what constitutes the phrase as licensees treat third-party personnel the same as FTEs from a requirement standpoint. The Industry is looking for basis in making this a sperate activity, or metric.
11	03.06.b.1	Bullet 4	There is merit to measuring unauthorized PMMD connectivity, but the vast majority of plant CDAs are unable to support logging for it, which introduces a logistical challenge. There are few automated capabilities for reporting this on existing CDAs. The industry suggests dialogue as to monitoring areas where the NRC sees substantive value added to the health of a licensee’s cyber

			program and to limit areas where the logical constraints of obtaining the information are introduced.
12	03.06.b.3	Configuration Control Propose removal, or changed to state "Periodic review of auditable events shows that change management has been maintained (D2.6), Ongoing effectiveness review of Change Management indicates all have been done in accordance with the CSP (A4.4.3)"	Industry believes that E10.3 is being met thru D2.6 and A4.4.3.
12	03.06.b.2	Bullet 1	The metric implies that security flaws will be corrected and does not consider the allowance to disposition a flaw as not requiring remediation. Monitoring the number of failures/issues post-patching and flaw remediation suggests licensees are required to routinely install security patches on CDAs. The NEI 08-09 R6 Addendum 5 process along with existing security controls precludes the need to install security patches for most vulnerabilities. Also, it is unclear if the metric is assessing maintenance effectiveness (patch testing program) as opposed to security control effectiveness. The Industry suggests this metric be revised to monitor areas with more substantial value added to the health of the cyber program. For example, vulnerabilities that constitute a reduction of effectiveness and corrective actions needed to maintain adequate defense-in-depth.
12	03.06.b.4	Bullet 1	The Industry sees this metric as too high-level that it does not have much value to be reported on. The Industry's stance here is that any malware event making it past a licensee's boundary controls would most likely be associated with a corresponding NRC Event Notification, and potentially a PI&R inspection depending on the severity of the malicious code. It does not seem prudent to track as a quarterly metric.
12	03.06.b.4	Bullet 2	Consider removing.

			Licensees generally do not perform active or passive scanning of production CDAs due to operational concerns, which is acceptable per Addendum 1. This metric could challenge a licensee's ability to procure a tool, develop a process and create a metric to measure the number of days to deactivate user credentials of former employees via scans. The Industry suggests the removal of this metric as it further adds complexity to a low value assessment of the health of a licensee's cyber program. The Industry has come clarifying questions: 1. Should this be moved to Flaw Remediation defined by vulnerability evaluations not completed? 2. Does this refer to anti-virus activity as it is discussing scanning potentially infected files? The metric also discusses boundary device tasks. Does this refer to traffic control and detection?
13	03.06.b.5	Bullet 1	It is likely that this metric will not be applicable to most CDAs because most CDAs do not have native security capabilities, and therefore has limited ability to assess the health of the cyber program. This metric would require an effort to identify the population of CDAs with security capability and collect the data needed to report failures to test manually or through automated means security capabilities. This metric would significantly increase the level of effort during an inspection cycle, well over and above what could be reduced effort during an inspection.
13	03.06.b.5	Bullet 2	Does the use of the term 'respond' in this context, refer to the Section 4.6 of the CSP?
13	03.06.b.6	Software and Information Integrity	CDA software integrity is typically verified as part of a manual process when patches or functionality changes are required. Because this is a strictly manual process, this metric would significantly increase the level of

			effort during an inspection cycle, well over and above what could be reduced effort during an inspection.
13	03.06.b.7	Bullet 1	Consider removing or identify # of untrained personnel identified during the last 24 month assessment.
14	03.06.b.7	Bullet 2	This metric suggests staffing vacancies only are considered when a licensee is inspected. Furthermore, ensuring someone is assigned only is less than acceptable. Staffing personnel need to be both assigned and qualified. Acceptability is based on the completion of required activities and not directly tied to organizational positions. The Industry suggests the metric should be revised to clarify the minimum, acceptable and high-performance standards for staffing key positions in the program.
14	03.06.b.8	"~~number of unnecessary ports and protocols~~" should change to "Number of CDAs with a port or protocol that has been unevaluated"	Consider removing. Firewalls and other network appliances used to implement the site's defensive strategy are typically identified during cyber security control assessment process and typically don't change. There is low value in checking CDAs to verify firewall configurations have not changed and could be problematic operationally by introducing unneeded activity to a firewall or network just to obtain this data on the suggested frequency, as well as a significant resource challenge. It is the suggestion of the Industry to eliminate this metric and continue dialogue on one that would add value to the assessment of the health of the cyber program. Similar to the comment above about security functions, this metric may not be maintainable.
14,17	03.06.b & 71130.10-04		3.6.b says If the following data is provided completely to the inspection team during the RFI submission, the inspection team shall be reduced by **contractor**. The licensee will be informed of the NRC's decision to

			credit the performance metrics submission and of the reduction in **contractors** visiting the site… 7.1130.10-04 says the inspection will consist of **two regional inspectors and two contractors** but that satisfactory performance and function tests will modify the team to **one regional inspector and two contractors**. Does submission of performance testing and metrics reduce the number of regional inspectors or contractors?
17	71130.10-04	"The estimated time to complete the inspection procedure direct inspection effort is **70 hours (with a range of 63 to 77 hours) per site** and will consist of **one week** of direct inspection effort with contractor support."	Should the one week of "direction inspection effort" be understood as 40 hours at a licensee's site, or about 60% of the total budgeted hours? Section 71130.10-05 says the frequency of cyber inspections is one week every two years but the estimated time to complete the "inspection procedure direction inspection" effort is 70 hours per site (+/- 7 hours), or almost two weeks.