Regulatory Trends in Cyber Security Event Monitoring and Detection for Nuclear Facilities

Seongyeol Oh[a]*, JaeKwan Park[a], Jae-Gu Song[a], Yonggu Lee[a], Ju Hyung Song[a], Inhye Hahm[a], Young Jun Lee[a]
[a]*Korea Atomic Energy Research Institute, 111, Daedeok-daero 989 Beon-gil, Yuseong-gu, Daejeon 34057, Korea*
*Corresponding author: seongyeol@kaeri.re.kr
*Keywords : Nuclear cyber security, Event monitoring, Detection, Regulatory requirement

1. Introduction

Cyber security monitoring and detection at a nuclear facility is not a single technology but a function assembled from several controls: defining what is monitored, generating and protecting event records, identifying intrusions and anomalies, linking the result to alerting, response and notification, and confirming that the monitoring capability remains effective. Because these controls sit in different families, verifying them individually does not establish that the overall function operates.

A requirement to detect and respond is long standing: 10 CFR 73.54 (2009) requires the cyber security program to be designed to "apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks," and 10 CFR 73.77 (2015) links detection to a reporting duty through one-, four- and eight-hour notifications and a written follow-up report within 60 days.

This paper examines how that function is expressed in documents issued or revised between 2021 and 2026 in the United States [1-3], the IAEA guidance [4], Canada [5], the United Kingdom [6] and Korea [7, 8].

2. International Trends in Monitoring Regulation

2.1 Demonstration of Detection Capability

The reviewed guidance addresses how detection capability can be demonstrated. NEI 08-09, Revision 7, Addendum 2, Section 2.1 [3] provides that "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," and asks whether it was placed "at a location where it can detect cyber attacks and permit the licensee to respond and eliminate the cyber attacks before an adverse impact to the SSEP function" (Safety, Security and Emergency Preparedness). Inspection Procedure 71130.10 [9] records the same forms. RG 5.71, Revision 1 [1] calls for detection of cyber attacks and their indicators on Critical Digital Assets (CDAs) and along attack pathways, and for automated tools to support near-real-time event analysis.

IAEA and CSA documents also address the information needed to support detection. IAEA NSS 17-T [4] states that detection activities "include ensuring that there is adequate data monitoring in place to support detection through the collection and preservation of information related to possible incidents." CSA N290.7:21 [5] requires event monitoring controls that "maintain a record of relevant CEA events" (Cyber Essential Assets), and a note to the same clause states that, where a device is not capable of generating or retaining logs, "alternate means of identifying events should be considered."

The three approaches to demonstrating detection described above in NEI guidance were already included in the 2017 Addendum 2 [10] and are retained in Revision 7 [3]. Detection along an attack pathway allows protection to be assessed where a CDA cannot host a monitoring agent, provided the alternative detection and response capability is justified. This is an alternative means of implementation, not an exemption from the protection requirement. NEI Addendum 2 provides assessment questions on whether the selected detection method allows response before an adverse impact on SSEP functions. Applying these criteria requires the licensee to justify detection timing and response against the relevant plant conditions and attack scenarios. Further clarification of how such evidence is developed and evaluated could improve consistency in regulatory application.

2.2 Centralized Monitoring and Security Operations Centers

Centralized monitoring is explicitly addressed in the reviewed guidance. Addendum 2 to NEI 08-09, Section 4.1 permits a licensee to "utilize a Security Operations Center (SOC) as a component of their detection, monitoring and response implementation," and provides that logs sent to it should be protected "in transit and at rest" and that, where a third party provides the SOC, a service level agreement "or similar document" should outline "the lines of demarcation between the licensee and the service provider." RG 5.96, Revision 0 [2] states that "the Defensive Cyber Security Architecture (DCSA) may consider support for a cybersecurity operations center (CSOC)," defines SOC and CSOC as synonymous and discusses security information and event management (SIEM) capabilities, and notes that the licensee may require an analysis to determine "whether the CSOC provides access to attack pathways due to interactions between the monitored systems and the CSOC." IAEA NSS 17-T treats it as an option: the computer security team's activities "might include staffing a security operations centre for the monitoring and assessment of potential computer security incidents…". SyDP 7.5 of the ONR Security Assessment Principles [6] names no centre but asks for "effective management structures" for "detecting, reporting, responding to and handling cyber security incidents"; its cyber posture tables (Annexes H to J) are not published. None of these makes a particular organizational form a requirement.

SOC use is an optional implementation already addressed in earlier industry guidance [10]. RG 5.96

discusses its contribution to the defensive architecture together with the possibility that interactions with monitored systems introduce attack pathways [2]. The significance is that the monitoring connection itself becomes part of the security assessment. Existing requirements for asset identification, monitoring and control effectiveness continue to apply [1-3]. However, further guidance would have to state how a licensee demonstrates that a centre covers the assets its plan protects, and what monitoring remains at the plant when central support is unavailable.

2.3 Verification at the Design Stage

The reviewed documents explicitly address verification during design. IAEA NSS 17-T provides that requirements be "provided in sufficient detail to allow design decisions to be made, the design to be verified and design changes to be evaluated" and that system risk management should include "verification at each step of the design of the computer security measures." CSA N290.7:21 places the same obligation in its lifecycle clause: at preliminary design "cyber security requirements shall be verified," with verification and validation continuing through commissioning. The ONR Security Assessment Principles [6] express it as an outcome: dutyholders should ensure their operational and information technology is secure and resilient to cyber threats "by integrating security into design, implementation, operation and maintenance activities"; consistently, the principles "do not specify particular processes but describe what good cyber security will look like."

In Korea, the April 2027 amendment extends the approval obligation for information-system security regulations to construction-permit and standard-design-approval applicants [7]. Early review is useful because logging functions, time synchronization and collection paths can be incorporated more readily during design than through later modifications. However, design review alone cannot demonstrate performance in the installed configuration. Equipment configurations, staffing and external services may remain unresolved, so the review can confirm that monitoring requirements are specified and testable while identifying matters requiring later confirmation. For regulatory application, the design-stage submittal can distinguish the monitoring functions addressed by the design from assumptions to be confirmed during commissioning.

Table I: Comparison of monitoring-related provisions

Source	Detection evidence	Centralized monitoring	Design verification
US NRC, NEI	Automated, manual or attack-pathway demonstration	SOC/CSOC optional; connection risks assessed	CSP with licence application; relevant design features reviewed
IAEA NSS 17-T	Data collection and preservation	SOC optional	Design verification; commissioning validation criteria
UK ONR SyAPs	Outcome-based requirements	Detection and response management	Security integrated into design
Canada CSA N290.7	Event records or alternative identification	SOC/SIEM; graded by significance	Requirements verified at preliminary design
Korea RS-015, Act	Monitoring, detection and effectiveness evaluation	Central record management; integrated analysis	Approval scope extended to design applicants from Apr. 2027

3. Monitoring Regulation in Korea

KINAC/RS-015 [8] gives the detailed controls under Article 9(1)4 of the Act. Its Revision 2 (December 2023) states in its revision summary that it reflects domestic inspection experience and recent overseas revisions, naming RG 5.71 (2023) and IAEA NSS 17-T (2021). Counterparts exist across the five functions: (1) collection, in the time-based correlation of audit records across multiple CDAs; (2) detection, in the monitoring of CDAs and the blocking of abnormal and unauthorized connections; (3) analysis and response, in the consolidated analysis of logs from automated tools and the immediate alerting of incident responders; (4) notification, in the reporting of incidents to the regulatory body; and (5) sustainment, in bypass prevention, periodic checks of the monitoring systems, and an effectiveness evaluation performed at the periodicity the standard sets or, where none is set, at least each planned outage. Audit records are also to be centrally manageable, and log review, analysis and reporting integrated and automated. Where a CDA cannot support a control, a documented justification with an alternative measure is required.

RS-015 requires monitoring and effectiveness evaluation but does not enumerate alternative detection methods in the same way as NEI Addendum 2. Further guidance could clarify how these existing requirements support facility-specific demonstrations of detection capability and sustained effectiveness. As to design-stage verification, the amendment of the Act promulgated on 31 March 2026 (Act No. 21520, effective 1 April 2027) [7] extends the approval obligation to applicants for a construction permit for a power, research or fuel cycle facility (Nuclear Safety Act, Arts. 10, 30, 35(1)), for a standard design approval (Art. 12), and for a construction and operating permit for a radioactive waste management facility (Art. 63); a new Article 9(2) makes an approval granted to a standard design approval applicant effective until that approval expires, while allowing the regulator to order correction or supplementation within that period. This extends the opportunity to review monitoring provisions before construction, while their implementation and performance remain subject to subsequent confirmation.

4. Conclusions

Monitoring requirements are common to the frameworks examined. The documents reviewed

highlight demonstration of detection capability, centralized monitoring as an optional implementation whose connections are considered in security assessment, and verification during design. Recent documents retain or further specify provisions already present in earlier guidance. The domestic standard requires monitoring and detection and the central management of records, but names no organizational form; the amended Act extends the approval obligation for information-system security regulations to construction-permit and standard-design-approval applicants from April 2027.

For small modular reactors this is a change of emphasis rather than a new category of requirement: multiple modules and shared facilities affect the unit to which records and events are attributed, reduced staffing affects which form of detection can be credited, and fleet-level monitoring brings the attack pathway analysis into scope. Future work will derive stage-specific review items, submittals and acceptance bases for the five functions and test them against a standard design submittal.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Regulatory Research Management Agency for SMRS (RMAS) and the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea (No. 1500-1501-409).

REFERENCES

[1] U.S. NRC, Cybersecurity Programs for Nuclear Power Reactors, RG 5.71, Rev. 1, 2023 (ADAMS ML22258A204).
[2] U.S. NRC, Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed under 10 CFR Part 53, RG 5.96, Rev. 0, 2026 (ML25232A008).
[3] Nuclear Energy Institute, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09, Revision 7, Apr. 2025, Addendum 2 (ML25107A191).
[4] IAEA, Computer Security Techniques for Nuclear Facilities, Nuclear Security Series No. 17-T (Rev. 1), Vienna, 2021.
[5] CSA Group, Cyber Security for Nuclear Facilities, CSA N290.7:21, Toronto, 2021.
[6] ONR, Security Assessment Principles for the Civil Nuclear Industry, 2022 Edition, Version 1, 2022.
[7] Act on Physical Protection and Radiological Emergency, Act No. 21520, Korea, promulgated 31 Mar. 2026, effective 1 Apr. 2027.
[8] KINAC, Security for Computer and Information Systems of Nuclear Facilities, KINAC/RS-015, Rev. 2, 2023.
[9] U.S. NRC, Cybersecurity, Inspection Procedure 71130.10, 2021 (ML21271A106).
[10] Nuclear Energy Institute, Addendum 2 to NEI 08-09, Revision 6, Cyber Attack Detection, Response and Elimination, July 2017 (ML17212A634).