Development of Institutional Basis for Physical and Cyber Security Event Notification Regulation in Nuclear Facilities

Jiyoung Han [a], Suhui Park [a], Seulwoo Bang [a], Yongmin Kim [a*]
[a]*Department of Radiological Science, Daegu Catholic University, Rep. of Korea*
[*]*Corresponding author: ymkim17@cu.ac.kr*

***Keywords :** Nuclear facility, Security Incident, Nuclear Facility, Reporting of Treats

1. Introduction

In the Rep. of Korea, the "Act on Physical Protection and Radiological Emergency" (hereinafter the 'Radiological Emergency Act'), together with its Enforcement Decree and Enforcement Rule, provides the overarching legal framework governing physical protection and electronic intrusions (cybersecurity) in nuclear facilities[1-3]. Among these, Article 11(Reporting) of the Act and Article 6(Report) of its Enforcement Rule stipulate the reporting obligations of nuclear licensees in the event of a threat occurring at nuclear facilities.

However, the legislation is limited to prescribing the targets and content of reporting, without establishing detailed regulatory notices on the reporting procedures, timing, or the specific categories of incidents that must be reported, in contrast to the "Nuclear Safety Act," under which the "Notices on Reporting/Disclosure of Accidents/Failures at Nuclear Facilities" stipulate the targets and reporting times for accidents and failures related to radiation exposure[4-5].

In recent years, the Republic of Korea has experienced a series of security incidents involving breaches of physical protection systems and cyber intrusions [6]. Representative cases include the 2021 cyberattack against the Korea Atomic Energy Research Institute (KAERI) and the 2014 hacking incident targeting Korea Hydro & Nuclear Power Co., Ltd. (KHNP). Comparable events have also been reported internationally, such as the 2019 drone intrusion at the Palo Verde Nuclear Generating Station in the United States and the 2017 ransomware infection at the Chernobyl Nuclear Power Plant in Ukraine, thereby underscoring the necessity of establishing clear and detailed reporting procedures to ensure effective responses and adequate support measures in the event of a threat. To develop a domestic regulatory notice on threat reporting, this study conducted a comparative analysis of the domestic Act and U.S. 10 CFR Part 73, examined policy directions for institutional improvement, identified key points of notification with assigned priorities, and proposed notification and reporting procedures and forms.

2. Methods

2.1 *Comparative Analysis of the Act on Physical Protection and Radiological Emergency and U.S. 10 CFR Part 73[7]*

In the United States, physical protection incidents are addressed under U.S. NRC 10 CFR Part 73 (Physical Protection of Plants and Materials), whereas in the Rep. of Korea, both physical protection and radiological emergency preparedness are regulated together under the Act on 'Radiological Emergency Act'.

The U.S. NRC addresses notification requirements for physical security events and cybersecurity events separately under 10 CFR Part 73, specifically in Section 73.77 (Cyber Security Event Notifications) and Section 73.1200 (Notification of Physical Security Events), thereby defining distinct categories of threats. Physical security covers intrusions, theft, and other physical attacks on nuclear facilities, equipment, and nuclear material, whereas cybersecurity covers hacking attempts, remote access attempts, and other attacks targeting digital systems. Each regime maintains an independent risk assessment and response strategy, and events are classified according to specified reporting deadlines, including those requiring notification within 15 minutes, within 1 hour, and within 4 hours. The comparative analysis is summarized in Table I.

Table I: Comparative Analysis

	Act on Physical Protection and Radiological Emergency	10 CFR Part 73 73.77 73.1200
Scope	Physical protection and radiological emergency	Physical security and cyber security
Reason for Reporting	In the event of a security system breach, intrusion, or other incident; system compromise; or abnormal signs	Explicit cases such as external threats, perimeter breaches, unauthorized access, network intrusion, and unauthorized access to systems
Reporting Deadline	Must be reported without delay	Depending on the incident, reporting deadlines are specified as 15 minutes, 1 hour, or 4 hours
Applica	Nuclear licensees and	High-risk security-

ble Entities	users	related facilities and transport management facilities, etc.

In the United States, reporting requirements for physical protection events and cybersecurity events are addressed separately; however, considering the organizational structure of the Nuclear Safety and Security Commission and the geographic accessibility associated with the territory of the Republic of Korea, establishing separate regulations appears to lack sufficient justification. Therefore, in Korea, while distinguishing between the types of physical protection and cybersecurity events, it is necessary to develop a regulatory notice that applies a unified reporting procedure to both, similar to the reporting provisions under the "Nuclear Safety Act" [4-5].

2.2 Institutional Directions for Improving Security Event Notification

Following the comparative review of U.S. NRC regulations, the study examined the domestic legal and institutional framework to identify areas requiring improvement in the security event reporting system. Through this analysis, several key directions for institutional enhancement were derived.

First, the study emphasized the need to introduce a differentiated event classification and reporting framework that reflects the threat level, potential impact, and intent of the incident. Second, it highlighted the importance of clarifying the legal definition of the "time of event recognition," which serves as the basis for determining reporting deadlines. Third, the study underscored the necessity of standardizing written reporting requirements in order to ensure procedural consistency across licensees. Finally, the scope of the definition of security events was proposed to be expanded, thereby encompassing potential vulnerabilities in addition to actualized threats. These methodological steps were intended not only to strengthen the clarity and consistency of reporting obligations, but also to establish a comprehensive security management framework tailored to domestic conditions.

2.3 Establishing Reporting Requirements and Event Prioritization

As part of the methodological process, the study also reviewed the common mandatory elements required for security incident reporting. These elements include: (i) basic information such as the time of occurrence and discovery, location, and reporter details; (ii) an incident overview, including the type, cause, and sequence of events; (iii) the scope of impact; (iv) the current response status, including initial actions and notification to external agencies; and (v) future plans, such as recovery schedules and preventive measures. The detailed items under each category were examined to systematically organize the reporting requirements. Furthermore, in order to determine incident priorities, the study referenced NRC regulations to classify incidents according to risk levels, which were then applied to establish reporting time categories within the proposed notice.

2.4 Reporting procedures and forms

The reporting procedure in the event of a security incident is stipulated as follows: identification of the incident, classification and priority assessment, collection of key information, notification to the relevant authorities, implementation of initial response measures and preservation of evidence, and post-incident analysis accompanied by the submission of a follow-up report. The format of the follow-up report has been partially adapted from the template prescribed under the Nuclear Safety Act [4-5].

3. Results

Through this study, a draft notice was designed to be composed of the purpose, definitions, reporting subjects, and reporting methods and procedures. Reportable incidents are categorized into physical protection incidents and electronic intrusion incidents, with verbal reporting deadlines established according to the severity and criticality of the event. The incident classification and verbal reporting deadlines were established with reference to NRC 10 CFR 73.77 and 73.1200. Some of the reportable events classified under these regulations are as follows.

- within 15 minutes: when a hostile action is imminent or has occurred
- within 1 hour: such as theft of spent nuclear fuel, unauthorized operation of a reactor, or cases that have a direct impact on nuclear safety, security, or emergency response functions
- within 4 hours: such as unauthorized entry into vital areas, attempts to bring in prohibited items, or cyberattacks that could potentially have an adverse impact

The reporting methods and procedures follow those prescribed in the existing Nuclear Safety Act of the Republic of Korea, requiring the submission of a written report following a verbal report.

4. Conclusions

This study developed a draft regulation specifying notification requirements in the event of threats to nuclear facilities in the Republic of Korea. To achieve this, comparative analyses of domestic and international laws, examination of relevant case studies, identification of institutional improvement measures, specification of reporting items, and classification of incidents were undertaken. The draft regulation derived from this research can serve as a foundation for the future enactment of an official notice and is expected to contribute to the establishment and effective operation of a comprehensive domestic security incident reporting system.

Acknowledgement

This work was supported by the Korea Institute of Nuclear Nonproliferation and Control (KINAC) through a research service project.

REFERENCES

[1] Nuclear Safety and Security Commission(NSSC), Act on Physical Protection and Radiological Emergency(Act No. 18664)
[2] Nuclear Safety and Security Commission(NSSC), Enforcement Decree of the Act on Physical Protection and Radiological Emergency(Presidential Decree No.34449)
[3] Nuclear Safety and Security Commission(NSSC), Enforcement Regulation of the Act on Physical Protection and Radiological Emergency(Ordinance of the Prime Minister No.2000)
[4] Nuclear Safety and Security Commission(NSSC), Act on Nuclear Safety(Act No. 20553)
[5] Nuclear Safety and Security Commission(NSSC), Notices on Reporting/Disclosure of Accidents/Failures at Nuclear Facilities(NSSC notice No. 2025-4)
[6] S. W. Kim, An Analysis on the Cyber Accident for the Cybersecurity Policy Making at the Nuclear Facilities, Proceedings of the 2017 Winter Conference of the Korean Institute of Communications and Information Sciences, 2017.
[7] Nuclear Regulatory Commission, 10 CFR 73 Physical Protection of Plants and Materials