# Trends on U.S. Cyber Security Event Notifications and its Implications

Ye-Eun Byun, Ick-Hyun Shin, Kook-Heui Kwon, Sang-Woo Kim*
*Korea Institute of Nuclear Nonproliferation and Control (KINAC)
e-mail : more2pro@kinac.re.kr, ihshin@kinac.re.kr, vivacita@kinac.re.kr

**Abstract**

When cyber attacks are discovered in nuclear facilities, licensees are required to notify regulatory organizations for quick action. This also helps regulatory organizations to strengthen regulatory capabilities for cyber security. Currently the U.S. issued the final draft rule for Cyber Security Event Notifications. Domestic regulatory activities being at an early stage for cyber security need to implement law for Cyber Security Event Notifications. Since the current laws are focused on the aspect of safety, they are in need of more specific laws for cyber security.

## 1. Introduction

It is important for licensees and applicants to prevent, respond to, and quickly report cyber attacks. Also if cyber attacks are discovered, licensees and applicants should notify regulatory organizations to promptly take action on that incident. Recently, the Nuclear Regulatory Commission (NRC) tried to institute a rule for Cyber Security Events Notifications (CSEN) for nuclear facilities. Now draft final of 10 Code of Federal Regulations (CFR) Part 73 and Regulatory Guide 5.83 were issued and received some feedbacks [1]. This rule is expected to improve the NRC's ability to response to cyber attacks and enable NRC to effectively evaluate potential cyber threats. On the other hand, Korea is on the first step to making these regulatory laws for nuclear facilities. These regulatory laws are all based on the amended Act on Physical Protection and Radiological Emergency (APPRE) Enforcement Decree. This paper will outline the implications for domestic regulatory activities of the NRC's efforts to CSEN.

## 2. NRC's efforts to CSEN

### *2.1 Backgrounds*

The NRC published its cyber security event notification requirements as part of the rules pertaining enhanced weapons in the Federal Register (76 FR 6200) for public comment in February of 2011. After bifurcation from the enhanced weapons rule in 2014, the NRC's effort to make the CSEN requirements began to speed up [1]. Currently the NRC is attempting to add CSEN requirements for nuclear power reactor facilities to 10 CFR 73.77. The NRC's recent rule which include section 73.54 (Protection of Digital Computer and Communication Systems and Networks) does not contain these materials.

### *2.2 Cyber Security Event Notifications*

According to the draft final regulatory guide 5.83, licensees subject to the provisions of 10 CFR 73.54 are required to notify the NRC Headquarters Operations Center via the Emergency Notification System (ENS). According to the regulations, there are three time frames in which notifications must be given one-hour, four-hour, and eight-hour according to the urgency of a cyber attack. [2]

.


(Figure 1) Classification of Notification

2.1.1 One-hour notifications

After the discovery of a cyber attack, licensees are required to notify the NRC within one hour. A cyber attack can be defined as anything that adversely impacts safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications). Such attacks also include anything that compromises support systems and equipment resulting in an adverse impact to safety, security, or emergency preparedness functions (SSEP) within the scope of 10 CFR 73.54.

These are examples of one-hour notification.

- a cyber attack that adversely impacts the normal operation of the facility through the unauthorized use of digital computer and communication systems and networks
- a cyber attack that adversely impacts the capability to shut down the reactor and maintain it in a safe shutdown condition, remove residual heat or control the release of radioactive material
- a cyber attack that adversely impacts the capability to detect, delay, assess, or respond to malevolent activities [2]

2.1.2 Four-hour notifications

After discovery of a cyber attack, licensees are required to notify the NRC. Notifications must be made if it was an attack that could have caused an adverse impact to safety-related or important-to-safety functions, security functions,

or emergency preparedness functions (including offsite communications); or that compromised support systems and equipment resulting in adverse impact to SSEP functions within the scope of 10 CFR 73.54. These contain attacks that are discovered or manifested on a Critical Digital Asset (CDA), Critical System (CS) or on a protected network but couldn't cause an adverse impact to SSEP functions because they were detected and mitigated or were not successfully executed.

These are examples of four-hour notification.

- a cyber security event that resulted in unauthorized access to a CDAs and/or CSs services
- an unauthorized transmitter or unauthorized portable media was attached or connected to a CDA, and cyber security controls indicates the presence of malware or unauthorized activity had occurred
- a cyber attack that caused an adverse impact to a CDAs and/or CSs confidentiality, integrity or availability, but no SSEP functions have been adversely affected [2]

2.1.3 Eight-hour notifications

Licensees are required to notify the NRC within eight hours after receipt or collection of information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack against digital computer, and communication systems and networks that fall within the scope of 10 CFR 73.54.

These are examples of eight-hour notification.

- theft or suspicious loss of smart cards or other "two factor" authentification devices required for accessing a CDA or CS
- a website posting or notification indicating a planned cyber attack against the plant [2]

*2.3 24-hour Recordable Events*

Licensees are required to use their site corrective action program (CAP) to record vulnerabilities, weaknesses, failures and deficiencies in their cyber security plan as well as record notifications within twenty-four hours of their discovery [2]. With the site CAP, licensees could monitor any noticeable trends of current cyber attack by performing periodic evaluations and this could help to document, track, trend, correct and prevent recurrence of failures and deficiencies in their cyber security program [3]

*2.4 Notification Process*

After notification to the NRC Headquarters Operations Center via the ENS, licensees may include an event number and time which are given during the notification in the Licensee Event Report (LER). This is done in order to provide a cross-reference to the notification, making the event easier to trace. The NRC records all conversations with the NRC Operations Center. [2]

*2.5 Written Security Follow-up Reports*

The CSEN to the NRC Headquarters Operations Center requires submission of a written security follow-up report to the NRC within 60 days of the notification using the NRC form 366, "Licensee Event Report (LER)." Licensees should follow established procedures when submitting their follow up report. There are some cases which the NRC does not require written security follow-up reports as specified in draft final 10 CFR 73.77. [2]

**3. Implications for Domestic Regulatory Activities**

Based on the amended APPRE Enforcement Decree, the KINAC has helped the government develop cyber security frameworks. As part of continuing efforts to provide nuclear facilities cyber security frameworks, the KINAC has developed regulation standards (KINAC/RS-015).

*3.1 Report of the cyber security*

There are also some efforts to develop domestic SCEN requirements to respond to cyber accidents and evaluate ongoing suspicious activities for threat implications. What KINAC/RS-015 contains for report is a system of emergency connection and a report for emergency accidents. Licensees should arrange connection systems to respond and report quickly [5].

<Table 1> Current Domestic Legal System regarding Event Notifications

| Aspect of Cyber Security | Aspect of Safety |
|---|---|
| Report for Emergency Accident<br>- Materials for report | Object of Report |
| Response Support for Emergency Accident | Report Process<br>- Report<br>- Notification |
| | Level Assessment of accident<br>- Tentative Level Assessment of accident<br>- Level Assessment of Accident<br>- Composition and Operation of Assessment Commission |
| | Making Public of Information for Accident<br>- Making Public of Information to the people<br>-Making Public of Information to the overseas organization |
| | Inspection, Assessment, Management of accident<br>- Inspection and Response of Accident<br>- Management, Analysis and Assessment of data |

The Nuclear Safety and Security Commission (NSSC) amended the notice for Reporting and Making Public of accident and failure of nuclear facilities based on Nuclear Safety Act. This notice covers details of reporting and making public of licensees to the NSSC when nuclear

facilities occurs accident and failure during operation or handling with radiological materials. According to this notice, the object of report is divided by characteristic of nuclear facilities. Also there are three type of reporting time; within one-hour, four-hour, eight-hour.

For example, the accident that may cause the environmental pollution or that may be the threat to safety of radiation worker because of leak of the radiological materials should be reported within one hour. And the accident that is taken urgent action for safety operations of facilities because of fire in the facilities or generation of poisonous gas should be reported within four hours. One of the accidents that should be reported within eight hours is the accident taken urgent action for safety operations of facilities for natural disaster.

Licensees are required to report orally using available means of communication before the required deadline. After that, licensees should submit initial written reports with a given form. When the neighborhood registrations needs urgent evacuation for robbed, lost or leaked radiological materials, licensees should report immediately to the headquarters of the police controlling that area. [6]

**4. Conclusions**

To implement CSEN requirements is one of the ways to strengthen regulatory capabilities for cyber security of nuclear facilities. The U.S. is currently about to implement a final rule and Korea is faced with needs to make a rule to prevent digital computers, and communication systems and networks from cyber attacks. Since the current notification system is rather focused on the aspect of security, more specific regulations governing cyber security are needed. New regulations would allow better monitoring of cyber threats to nuclear facilities. It could also offer better protection of digital computers, and communication systems and networks associated with the SSEP function. Our future work will focus on specific ways to implement CSEN requirements in Korea.

**REFERENCES**

[1] NRC, Cyber Security Event Notification Final Rule, 2014
[2] NRC, DRAFT FINAL REGULATORY GUIDE 5.83
[3] NRC, DRAFT FINAL 10 CFR PART 73 RULE LANGUAGE
[4] NRC, 10 CFR Part 73
[5] KINAC, 원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준(KINAC/RS-015), 2014
[6] 원자력이용시설의 사고·고장 발생시 보고·공개 규정, 2014