A Study on the Current Status of the Domestic Regulatory Frame for Localization Measures of Insider Threat Prevention

Chan Kim[a*]
[a]Physical Protection Division, Korea Institute Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Yuseong-gu, Daejeon 34054
Corresponding Author: ckim@kinac.re.kr

1. Introduction

The 2020 NTI Nuclear Security Index and its final report addresses the progress of nuclear security over the past eight years, which has been monitored since 2012, such as the decrease in the number of countries with nuclear material and the introduction of a new system to prevent theft of nuclear material or sabotage using it. However, the report also indicates that critical vulnerabilities in key areas such as insider threat prevention, security culture at facilities, and cyber security are beginning to emerge [1].
In this paper, current status of domestic insider threat prevention measures and localization of overseas regulatory framework and programs for domestic NPP sites will be discussed.

2. NTI Nuclear Security Index 2020(Sabotage)

The indicator, 2.3 Insider Threat Prevention, of Sabotage Index Category 2. Security and Control Measures considers the sub-indicators below to be essential for reducing vulnerabilities to insider threats and tries to quantify from the score of 1 to 5.

2.1 (2.3.1) Personnel Vetting:

Countries receive the scores depending on whether national guideline specify that security personnel are subject to the following checks: drug testing, background checks, and psychological or mental fitness checks.

2.2 (2.3.2) Frequency of Personnel Vetting:

Countries receive the scores depending on how frequently security or other personnel with access to nuclear material areas are vetted at specified intervals.

2.3 (2.3.3) Reporting:

Evaluates whether domestic regulations or licensing conditions specify that personnel must report suspicious behavior to an official authority.

2.4 (2.3.4) Surveillance:

Evaluates whether the domestic regulations or license conditions require constant surveillance of areas with nuclear material; and/or vital area, when they are occupied using either a two-person surveillance system or a technological surveillance system.

2.5 (2.3.5) Insider Threat Awareness Program:

Evaluates whether the domestic regulations or license conditions require a nuclear-specific insider threat awareness program for all personnel involved in the operation and management of nuclear facilities.

As for the Insider Threat Prevention indicator, only 14 of the 47 countries evaluated for the Sabotage Index scored more than 73, 13 countries including Republic of Korea scored a medium range of 34-66 points, and 20 countries with a low score range of 0-27 points. The result informed the current situation of the countries around the world on the action for the prevention of insider threats.
In the Nuclear Security Sabotage Index, ROK scored 45 points for Insider Threat Prevention indicator, and it was revealed as one of the low-scoring items along with the Nuclear Security Culture indicator (25 points). This Insider Threat Prevention indicator of ROK scored 64 points in 2016 and 45 points in 2018 and 2020, and the score has fallen and stayed the same for the past four years.

3. Current Status of Domestic Insider Threat Prevention Measures

3.1 Definition in the APPRE (Act on Physical Protection Radiological Emergency)

In the current Act on Measures for the Protection of Nuclear Facilities, Etc. and Prevention of Radiation Disaster (Abbreviation: Act on Prevention of Radiation Disaster), "threats" are defined as below, but there is no mention of "insiders" and differentiated description of threat caused by insiders.

Article 2 (Definition)
6. The term "threat" means any of the following:
a) Sabotage;
b) Electronic infringement;
c) Using nuclear materials to harm human life and bodies or inflict damage on property or the environment;
d) Acquiring of nuclear materials to compel individuals, corporations, public institutions, international organization, or nations to commit a specific act;

3.2 Absence of a Fitness-for-Duty (FFD) Program

The NRC requires certain nuclear facilities to have fitness-for-duty programs to provide reasonable assurance that nuclear facility personnel are trustworthy, will perform their tasks in a reliable manner, are not under the influence of any substance, legal or illegal, that many impair their ability to perform their duties, and are not mentally or physically impaired from any cause that can adversely affect their ability to safely and competently perform their duties. In 1989, the NRC published requirements for FFD Programs in 10 CFR Part 26. These regulations required nuclear power plant licensees to implement a FFD Program for all personnel having unescorted access to the protected areas of their facilities and other personnel with particular type of access. [3]

Currently, the FFD's operation details for employees of nuclear power plant and partner companies are not included in the nuclear operators' physical protection regulations. According to the current physical protection regulations of nuclear operator, only the duties and responsibilities for personnel in charge of security and protection, as well as managing the scope and history of personnel after hiring are specified, but a program that manages illegal acts, suspicious behaviors, and psychological situations, appears to be absent.

3.3 Nuclear Security Culture Awareness

There is no FFD program as described above, nor are there any state-level nuclear security culture assessments and security responsibilities/duties training courses. According to the aforementioned NTI 2020 Nuclear Security Report and its Sabotage Index, ROK's Nuclear Security Culture score was calculated to be 25 points, which is lower than that of Insider Threat Prevention indicator, which has remained unchanged since 2016. And this score is almost at the bottom, among 47 countries evaluated for sabotage index.

In terms of actual implementation, cases of access violations and security violations are quite frequent, and this is because there are no strong penal provisions against such violations have not been established so far. Recently, comprehensive measures to prevent recurrence of security violations have been established and begun to implement since last year.

4. Localization Measures on Domestic NPP Sites

4.1 Referring to Overseas Case

Considering the highest scores in the Insider Threat Prevention indicator of the UK (100 points/1st) and the USA (91 points/2nd), it seems to be of great help for the localization of their regulatory system and implementing programs. Since the information of 10 CFR 73.55 is public, referencing it will be no difficult. In the case of UK CPNI, It's OK to say program, HoMER (Holistic Management of Employment Risk) and other insider threat management guidelines have been developed and utilized in a variety of ways. Those aforementioned programs and guidelines are partially confidential, regulator-level of cooperation and consultation to acquire the sensitive information of those programs will be needed. Also, in order to properly adopt and localize such regulatory system and programs, it seems urgent to research overseas references and review the apply plans at the level of regulatory agencies and facilities.

4.2 Complementing DBT(Design Basis Threat)

Currently, insider threat-related setup conditions in DBT are very simple, and those of the most sites are applied to the same level and scope. In such a state, the threat response scenario-in particular, the insider-related incident response scenario is inevitably more vulnerable. If it is possible to collect data on potential insider threat factors and actions based on the above-mentioned FFD program and behavior monitoring program, more specific quantification of the current DBT insider threat factors will be available.

5. Conclusion

Since ROK does not have adequate measures to prevent and respond to insider threats under the current laws and regulatory systems, there is an urgent need to supplement it.
To settle the insider threat mitigation program in a way that best suits the domestic situation, it has to be considered such as U.S. case that the federal law (10 CFR 73.55) mandated insider threat reduction program, or UK's systematic insider reduction program through regulatory agencies such as CPNI under MI5.
The result of a survey conducted by the KINAC Physical Protection division from 2019 to 2020 aimed at diagnosing the level of awareness and implementation of nuclear security culture among the workers at NPP sites, showed that there was a slight increase in the four survey areas over the two years: 1) comprehensive awareness of nuclear security, 2) management system, 3) leadership behavior, and 4) worker behavior. As such, if individual workers' awareness of nuclear security is improving than in the past, after the legal/regulatory framework is systematically established and implemented to the sites, the prevention of insider threats will be more effective.