Consideration on Preventive and Protective Measures Against Insider Threats at R.O.K. Nuclear Facilities

Seungmin Lee*, Jungho Lee and Moonsung Koh
Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Yuseong-gu, Daejeon, Korea
*Corresponding author: seungmin@kinac.re.kr

1. Introduction

The term 'adversary' is used to describe an individual or group performing or attempting to carry out a malicious act. An adversary may be categorized as an insider and outsider. The term 'insider' is specifically used to describe an adversary with authorized access to a nuclear facility, a transport operation or sensitive information [1]. Insiders are able to take advantage of their access rights and knowledge of a facility to bypass dedicated security measures. They can also threaten cyber security, safety measures, and material control and accountancy (MC&A). Insiders are likely to have the time to plan their actions. In addition, they may work with an external adversary who shares their objectives. Because of these reasons, the IAEA published "The Implementing Guide Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8" to help Member States better understand this potential threat posed by insiders [2].

This paper focuses on the current status of measures used to prevent, detect and respond to potential insiders at nuclear facilities in the Republic of KOREA. Measures against insiders are then analyzed based on IAEA guidelines.

2. The current status of preventive and protective measures at R.O.K. Nuclear Facilities

In this chapter, the preventive and protective measures against potential insiders at nuclear facilities, especially nuclear power plants, will be reviewed.

2.1 The general approach to implementing comprehensive measures against potential insiders

A potential insider problem must be approached in a different way than that of the outsider. An outsider attack can only be addressed once they occur. However, there are several factors associated with an insider protection system that reduce the likelihood of their presence (as well as elements that detect and prevent insider malicious actions). An insider protection approach can be broken into several sequential phases, as shown in Figure 1.

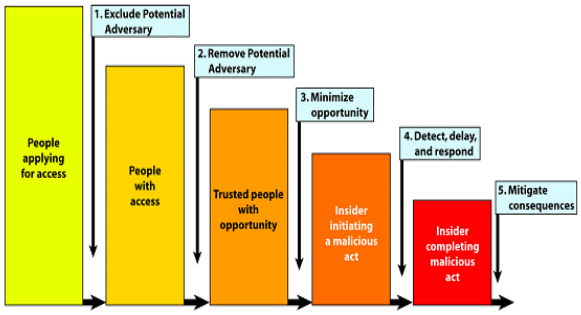

Figure 1. Steps for preventive and protective measures against potential insiders

The term "preventive measures" is used to describe the means to remove minimize possible insider threats. The term is used to describe measures that deter, detect, and delay a malicious act by an insider. Protective measures should be coordinated with the overall contingency plans at a facility.

2.2 The current status of preventive and protective measures at Nuclear Facilities in the R.O.K.

Many regulators and facility operators attended a 'Workshop about Preventive and Protective Measures against Insider Threats at Nuclear Facilities of R.O.K.' held on July 2015. All participators discussed the current status of preventive and protective measures against the potential insiders. In the R.O.K, various measures are used at nuclear facilities to prevent and protect against insider threats; however, this paper will discuss only some general information about this topic because of security issues.

Information that can be given in this paper includes background checks for facility operators. Staff at facilities must periodically attend refresher programs on security education and awareness. All employees at nuclear facilities must be given an annual medical. Some employees such as reactor operators must complete a drug screening and be given a psychological assessment. If an employee has received a positive assessment, they are issued a clearance status and given an identification badge. Badge inventories and records are maintained by using an 'access control system.' Visitor control procedures are applied to ensure that only appropriately cleared individuals gain access to

security areas and facilities. Unescorted access onto the site and into the facilities is granted to employees and contractor personnel who have an authorized photo badge. Facility operators use strict procedures to ensure that when people arrive at a location to do a critical job, they are scheduled to do the job and are the appropriate people to do it. And they use a quality assurance program. A formal QA program will help deter an insider, and by strictly defining the work process, can minimize insider opportunities.

Facility operators use a variety of measures to detect, delay and respond to malicious acts. Metal detectors and X-ray machines are installed at entrances to areas where insiders could bring in prohibited items such as weapons. Metal and radioactive material detectors are also installed at exits at restricted areas. Material control and accounting (MC&A) programs are in place to detect loss or removal of material from authorized storage locations. They provide an audit trail to detect responsible parties. If significant amount goes missing (larger than the reasonably expected measurement error of the instruments) or if an item is discovered missing during a physical inventory of items, then a contingency plan in advance is put into action immediately. A response plan to protect the populace in the event of sabotage has also been prepared. These contingency and response plans are rehearsed often and are kept up to date to ensure that they will be effective if needed.

2.3 Analysis of the measures against the insider

The IAEA published “The Implementing Guide Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8” to provide information on the prevention and protection against insiders. This guide recommends a general measure against insiders. The approach discussed in this study uses this guide.

As mentioned in the previous chapter, various preventive and protective measures are used against a potential insider threat. Most measures are useful, but some measures are insufficient--based on international standard. The vulnerability can be improved with new regulations.

3. Conclusions

An insider threat is a great risk to a security system because of the access, authority, and special knowledge that someone within a facility possesses. Therefore, it is imperative that effective measures be taken to prevent insider incidents. A combination of preventive and protective measures offers the best solution to mitigating rogue elements within a facility. These include employee screening process, security awareness education, physical protection systems, and policies and procedures ensuring appropriate handling and controls of attractive target materials. Unfortunately, some state measures are insufficient--based on international standards. This vulnerability can be dealt with through the use of well managed and evolved regulations.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, Vienna (2014).
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, Vienna (2011).