# A Study on the Recent Tendency of Cyber Security Regulation for the Nuclear Fuel Cycle Facilities

Siwon Kim

Korea Institute of Nuclear Nonproliferation and Control, 1534 Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea

swkim@kinac.re.kr

## 1. Introduction

The cyber security regulations for nuclear facility in Unites States are based on the federal regulation 10 CFR 73.54[1] issued in 2009. The 10 CFR 73.54 requires licensee to protect their computers and information systems from cyber attacks that could lead to the theft or diversion of nuclear materials and the radiological sabotage. The NRC provides an acceptable approach and methodology for meeting the requirements for satisfying these demands through RG 5.71[2]. Also, NEI issued the NEI 08-09 to inform the licensee of the details necessary to satisfy 10 CFR 73.54 and RG 5.71.

The above-mentioned laws and guides have been applied to Nuclear Power Plants (NPPs) and it is difficult to apply them fitly to nuclear facilities other than NPPs. So, the regulations appropriate to the characteristics of each facility are needed. The purpose of this paper is to review the regulatory trends in US nuclear Fuel Cycle Facilities (FCFs) and provide the information on the differences from existing regulatory requirements for NPPs.

## 2. Cyber Security Regulation for the FCFs

As mentioned in the introduction, regulatory measures are being developed for nuclear FCFs in the United States. The draft federal regulation 10 CFR 73.53 [3] was proposed in March 2016, and will be finally issued in the first half of 2017 after several public meetings [4]. In addition, draft regulatory guides document DG-5062 [5] was developed as a detailed guide to support 10 CFR 73.53, and is undergoing formal comment period for rulemaking. When 10 CFR 73.53 is finally issued, the licensee submits the CSP within six months and will implement the CSP to satisfy the rule for 18 months.

This section provides the information about how the cyber security regulatory requirements for the nuclear FCFs are structured and how they differ from existing regulatory requirements of the NPPs.

### *2.1 Cyber Security Regulation Trends in FCFs*

The draft regulatory guide for FCFs, which has been developed to date, requires details such as organization, asset identification, defense in depth, security controls, periodic review, and event reporting and records in the same manner as the regulatory guide for nuclear power plants. The draft guide states that the target assets for applying regulatory requirements are not Critical Digital Assets (CDAs) but Vital Digital Assets (VDAs). It also required that assets are protected from cyber attacks that could cause a consequence of concern on FCFs. These consequences of concern are classified into the four types in the table below [5].

Table 1. Consequences of Concern[5]

| Type | Type Name |
|---|---|
| 1 | Latent - Design-Basis Threat |
| 2 | Latent - Safeguards |
| 3 | Active - Safety |
| 4 | Latent - Safety and Security |

In the US, Special Nuclear Materials (SNMs) are classified into three main category [6] according to the risk as shown in the table 2. The consequences of concern are different for each category. Types 3 and 4 can occur commonly to all categories. Type 1 can occur only in Category I FCF, and Type 2 can occur only in Category II FCF.

Security controls should be applied to identified VDAs. At this time, different security controls are applied depending on what type of consequence of concern on the FCF when the asset is compromised,

Table 2. Safeguard Categories of SNM[6]

| Category | Category Name |
|---|---|
| I | Strategic SNM |
| II | SNM of moderate strategic significance |
| III | SNM of low strategic significance |

as a result of a cyber attack. Above all, 48 security controls are commonly applied irrespective of the consequences of concern. Thereafter, 79, 85, and 105 security controls are additionally applied depending on the consequence of concern type. If two or more consequences of concern can be occurred, apply all security controls for each type. Subsequent fulfillment of requirements such as periodic review, incident reporting, and records will satisfy all CSPs. After that, if all of the requirements for periodic review, incident reporting, and records are satisfied, all CSPs are completed [5].

### *2.2 Differences from Regulation for NPPs*

The cyber security regulations for FCFs are similar to those currently applied in NPPs, but they differ in several points. This section describes these major differences.

First of all, the assets that could adversely affect the safety, security, or Emergency Preparedness (EP) function were selected for protection in NPP [2], but EP function were excluded and safeguard function was added in consideration of facility characteristics that FCFs treats large quantities of nuclear materials and there is no fission reaction in the FCFs. In addition, the name of the assets to be protected is named as VDA instead of CDA.

Secondly, in RG 5.71, the principle was to apply all applicable security controls for each CDA, and to apply alternative controls instead of unavailable security controls. However, after the CDA identification, the licensee applied a graded approach that grouped the CDAs according to the characteristics and consequences of each asset and applied the security controls differentially through NEI 13-10. Reflecting this experience, in the regulatory guide for FCF, the possible consequences of concern for each facility have been predetermined and security controls to be applied for each consequence of concern are assigned. There are also common security controls, and it is allowed that a way to group the VDAs by their characteristics and apply the same set of security controls [5].

Finally, the concept of Temporary Compensatory Measures (TCMs) was introduced. After completing the implementation of the security controls, if the intended method does not meet the performance specification of the security control, the licensee may instead implement the TCM. The TCM is an interim solution to allow the operation of the VDA while performing long-term measures required to adequately implement and validate the security controls [5].

## 3. Conclusion

So far, this paper has reviewed the cyber security regulatory trends of US nuclear FCFs and provided information on how they differ from regulations on NPPs. Follow-up study is to analyze in detail the differences between security control groups that apply to the four consequence of concern types and to identify which security controls are applied differently in Category I, II, and III facilities. Through this, the key elements, which convert deterministic approach into a consequence-based approach in NRC's existing regulation, can be analyzed.

## REFERENCES

[1] U.S. Nuclear Regulatory Commission, "Protection of Digital Computer and Communication Systems and Networks," Title 10, Code of Federal Regulations, Part 73, Section 54, Dec. 2015.

[2] U.S. Nuclear Regulatory Commission, "Cyber Security Programs for Nuclear Facilities," Regulatory Guide 5.71, Jan. 2010.

[3] U.S. Nuclear Regulatory Commission, "Require-ments for Cyber Security at Nuclear Fuel Cycle Facilities," Draft Title 10, Code of Federal Regulations, Part 73, Section 53, Oct. 2016.

[4] U.S. Nuclear Regulatory Commission, Public Meeting Presentation Material, "Discussion of Draft Proposed Rule Text for Fuel Cycle Cyber Security," May 2016.

[5] U.S. Nuclear Regulatory Commission, "Cyber Security Programs for Nuclear Fuel Cycle Facilities," Draft Regulatory Guide DG-5062, Jan. 2017.

[6] U.S. Nuclear Regulatory Commission, "Safeguard Categories of SNM," https://www.nrc.gov/security/domestic/mca/snm.html Feb. 2017.