Analysis of Current Status of Cyber Security Regulation in U.S. NRC

In-hyo Lee *
Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Daejeon, Republic of Korea 34101
**Corresponding author: lih9103@kinac.re.kr*

1. Introduction

In 2009, U.S. NRC legislated 10 CFR 73.54 "Protection of Digital Computer and Communication Systems" to regulate cyber security in nuclear facilities [1]. After that, RG 5.71 "Cyber Security Programs for Nuclear Facilities" was published in 2010, suggesting detailed guidelines to satisfy 10 CFR 73.54 [2]. Licensees are able to implement cyber security on their facilities referring to RG 5.71.

About 10 years passed since the RG 5.71 was first published and insights or lessons learned from regulatory activities such as approval of cyber security plan (CSP), implementation of Milestone 8, and cyber security inspections are accumulated. Therefore, these insights or lessons learned may be reflected in regulatory guides and the draft version of regulatory guides was published in February 2022 with revisions 1 (DG-5061) [3].

This paper discusses and analyzes the major changes between RG 5.71 and DG-5061, and the backgrounds and reasons for those changes are also discussed.

2. Overview of RG 5.71

RG 5.71 is composed of four chapters which are INTRODUCTION, DISCUSSION, REGULATORY POSITION, IMPLEMENTATION, and APPENDIX A, B, and C. In this chapter, the brief contents of RG 5.71 are discussed mainly focusing on REGULATORY POSITION. Also, the structures of RG 5.71 are shown in Fig. 1.

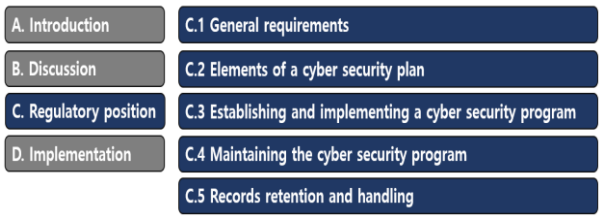

Fig. 1. Structure of RG 5.71

2.1 General Requirements

In this section, key requirements that the licensee must follow such as providing high assurance that digital computer systems are protected against cyber-attacks are described.

2.2 Elements of Cyber Security Plan

To protect digital computer systems from cyber-attacks, the elements of a cyber security plan that satisfies the cyber security program of the licensee are described.

2.3 Establishing and Implementing a Cyber Security Program

This section explains how the licensee establishes and implements a cyber security program. The cyber security program could consist of defensive architecture and security controls.

2.4 Maintaining the Cyber Security Program

To maintain the cyber security program, the licensee shall evaluate and manage cyber risk by establishing a security life cycle for critical digital assets (CDAs) that contains the following elements in Table I.

Table I: Elements of Security Life Cycle

No.	Elements
1	Continuous monitoring and assessment
2	Configuration management
3	Change management
4	Security impact analysis of changes and environment
5	Effectiveness analysis
6	Ongoing assessment of security controls and programs effectiveness
7	Vulnerability scans/assessments
8	Change control
9	Security program review

2.5 Records Retention and Handling

The licensee shall retain all records and supporting technical documentation by 10 CFR 73.54(h). To maintain records or supporting technical documentation so that inspectors can evaluate any of the cyber security elements is provided one acceptable method in RG 5.71. Those records could be digital records that log files, audit files, and non-digital records that capture and record.

3. Major Changes in DG-5061

3.1 Scopes

The applicable scopes of the regulatory guides were nuclear facilities in RG 5.71, however, in the case of DG-5061, the regulatory guides are applied only limited to nuclear power reactors. So, the regulation scope became clear. Furthermore, in DG-5061, it was changed that power reactor applicants and licensees who are in the development phase of digital safety systems also use the regulatory guides, wherever, in RG 5.71, the regulatory guides were applied to operating reactors.

3.2 Changes by Sections

The descriptions of key changes by sections can be summarized in Table II.

Table II: Newly Inserted Parts in DG-5061 Comparing with RG 5.71

Sections	Descriptions	Notes
C3. Establishing and Implementing a Cyber Security Program	- To use risk insights of DBT when developing and maintenance of cyber security programs (e.g. threat information, the likelihood of adversary success, and the resulting level of consequences of the threats) - Considerations of establishing a cyber security program (e.g. characterization of facility functions, threats to a facility, specification of requirements, etc.)	Newly inserted
C3.1.2. Define Roles and Responsibilities and Form the Cyber Security Team	- Additional roles and responsivities of CST: reviewing and evaluating the implementation of procurement procedures	Newly inserted
C.3.2 Defense-in-Depth Protective Strategies	- Elements of defense-in-depth protective strategy: defensive architecture and defensive strategy	Newly inserted
C.3.2.1 Security (deleted) Defensive Architecture	- Additional characteristics of defensive architecture - Incorporating analog communication within the defensive architecture is one example of digital isolation - Data communication between systems within the same security levels should be protected	Newly inserted
C.3.3 Security Controls	- Analysis should be reproducible and consistent	Newly inserted
C4.2.1 Configuration Management	- Security assessment of a CDA can be changed if any configuration changes occur - Also, be documented	Newly inserted

3.3 Discussions

The DG-5061 may be changed by the accumulated lesson learned and the backgrounds of the changes may be inferred.

If new vulnerabilities are founded or the environment of CDAs is changed, the cyber security of licensees' facilities will have to be re-evaluated. Because the evaluation process may be performed with a risk-based approach, the risk assessment may be emphasized. Also, since cyber threats may come from the supply chain, the R&R of the cyber security team in the procurement process may be added in DG-5061.

Another is the importance of documentation. To maintain the quality of cyber security, reproducibility and consistency may be important. The written document of a series of cyber security activities may assure quality, reproducibility, and consistency. On the other hand, for objective and fair inspections the documentation may be emphasized.

4. Conclusions

From the comparison analysis, useful insights were obtained. They were (1) importance of risk analysis, (2) importance of documentation, and (3) Importance of understanding of facilities and digital computer systems.

The lessons learned from the regulation experience were reflected in DG-5061, properly. So, further studies are needed to fully understand the background and apply it to domestic nuclear facilities.

REFERENCES

[1] U.S. NRC, Protection of Digital Computer and Communication Systems and Networks (10 CFR 73.54), 2009.
[2] U.S. NRC, Cyber Security Programs for Nuclear Facilities (RG 5.71, Rev. 0), 2010.
[3] U.S. NRC, Cyber Security Programs for Nuclear Power Reactors (DG-5061, Rev. 1), 2022.