Review of the US Cyber Security Self-assessment Method From the Regulatory Perspective

Chaechang Lee*
Korea Institute of Nuclear Nonproliferation and Control, 1534, Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea
*chiching@kinac.re.kr

1. Introduction

Nuclear Safety and Security Commission (NSSC) and Korea Institute of Nuclear Nonproliferation and Control (KINAC), regulators for the ROK's nuclear facilities, developed and distributed a regulatory standard for the licensees' Cyber Security Regulation. Nuclear licensees have been phasing in and implementing procedures for the regulation to comply with the standard, KINAC/RS-015 [1].

As one of the activities of the regulation, nuclear facilities licensee shall carry out the continuous assessment of the cyber security controls at least at every overhaul period to validate that the security controls developed according to the cyber security controls of KINAC Regulatory standard (RS-015) are actually applied on the site and properly working. In addition, nuclear facilities licensee shall also evaluate whether the previously established cyber security controls are effectively working in continuously changing cyber threat and environment.

This paper presents how the U.S. nuclear licensees perform cyber security self-assessment and regulator's perspective to introduce and apply the method to the ROK's nuclear facilities. However, it does not represent the official position of regulatory body.

2. U.S. Cyber Security Self-Assessment

U.S. Nuclear Power Plant (NPP) licensees should assess the cyber security risk of nuclear safety systems, physical security systems, and emergency preparedness systems in accordance with Regulatory Guide (RG) 5.71 of Nuclear Regulatory Commission (NRC) [2]. NRC had contracted with the Pacific Northwest National Laboratory (PNNL) to develop a method to support this. Licensees can select their own practices and tools that are appropriate to them to collect information, estimate cyber security risk, and perform risk management activities.

NUREG/CR-6847 “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants” was originally a limited release document and withheld from public disclosure under 10 CFR 2.390. The USNRC released the document under FOIA/PA NO:2015-0209 [3]. Nuclear power reactor licensees can use the method to assess and manage cyber risk of any systems in their facilities.

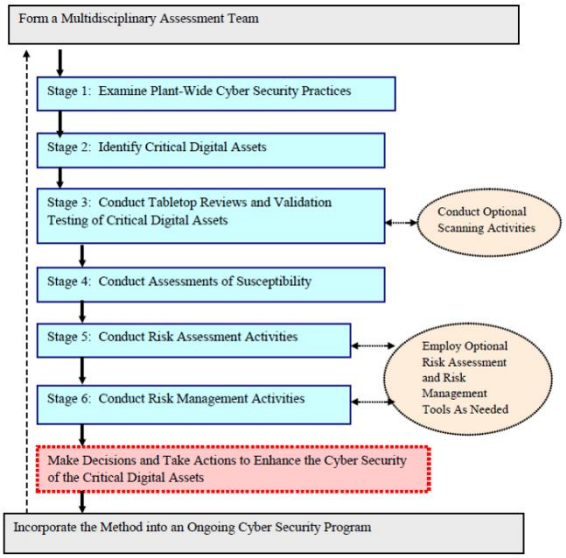

Fig. 1. Simple Flowchart for the Cyber Security Self-Assessment Method for U.S. NPP [3].

The method provides a systematic and phased approach that enables licensees to conduct a thorough self-assessment of cyber security at their respective facilities. And it allows the users a fair amount of latitude in selecting tools and techniques that work best for their specific needs. Figure 1 shows a six-stage process for the self-assessment approach.

3. Regulatory Point of View

This section describes from a regulator's perspective what the ROK's regulator and licensees should consider when introducing and applying the US cyber security self-assessment method.

First, all activities for self-assessment should be performed by the licensees, because it is the licensees that know best what systems affect the plant, how they are connected with each other, and what security constraints they have. Regulators can inspect that appropriate procedure is in place for the licensee to conduct self-assessment and that the composition of teams for self-assessment is appropriate and that the self-assessment process and results are reasonable.

Second, it is difficult for nuclear licensees to derive a high-risk score as an outcome through self-assessment. This could be evidence of a lack of their cyber security activities. Thus, rather than focusing on the results of the self-assessment itself, regulators should focus on whether the self-assessment has resulted on a reasonable basis through the appropriate process. This should ensure that the nuclear licensee's self-assessment is not to be a means to cover their cyber security vulnerabilities or exaggerate their cyber security activities in its facilities but to be a meaningful assessment.

Third, regulatory agencies should inspect that corrective action by the licensee against the results of the self-assessment is appropriate. The risk level derived from the results of the method should be mitigated through corrective action. While nuclear licensees are reviewing the cost-effectiveness of corrective action to deal with the risk, regulators can check its effectiveness to verify if corrective actions can lower the level of risk from which it was derived.

Finally, it is impractical to perform a self-assessment for all CDAs at once. The available time period is an overhaul, and the number of people is limited to three to seven. Therefore, the selection of critical systems and CDAs to apply the self-assessment method should be appropriate. Critical systems and CDAs that span several areas of security level in defense-in-depth strategy and can seriously impact on NPP if compromised should be chosen first.

4. Conclusion

The cyber security self-assessment method was specifically designed for cyber security evaluations of nuclear facilities. The method can be used by licensees to determine their cyber security posture. The licensees also can make their own method that are appropriate to them to collect information, estimate cyber security risk, and perform risk management activities.

REFERENCES

[1] KINAC, “Regulatory Standard – Security for Computer and Information System of Nuclear Facilities”, Oct. 2014.

[2] U.S. NRC, Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”, 2010.

[3] C. S. Glantz et al., NUREG/CR-6847 PNNL-14766, “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants”, Jul. 2004, Released under FOIA/PA NO:2015-0209.