Contribution ID: **83** Type: **Paper**

The relationship between Maturity and Regulatory Models (Prescriptive vs. Performance Based) for Cyber Security

In February 2013, US President Barack Obama, promulgated Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity", in which he directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure [1].

In response, NIST released its Cybersecurity Framework for use across all critical infrastructure sector on February 12, 2014 [2] which was revised on April 16, 2018 [3]. "The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles [3]".

The debate currently is how best to apply this in a heavily regulated sector, like that in which nuclear power plants operate. Three central questions require detailed consideration: (1) What is the role that the State and the competent authority play in progressing both competence and capabilities of licensees? (2) What type of regulation (prescriptive or performance-based) is most appropriate based upon both the organization and human resources available within the State? and (3) how is risk identified, assessed, evaluated and treated by both the State and the licensee?

This paper contemplates these questions and proposes potential directions and actions to cultivate maturity of organizations using the NIST framework as a reference. The focus will be on the transition from establishing a foundational level of maturity using a prescriptive based approach to an adaptive level of maturity relying upon performance based approaches.

References:

[1] United States Department of Energy, Use of the NIST Cyber Security Framework & DOE C2M2, https://www.energy.gov/sites/prod/files
of-NIST-Cybersecurity-Framework-DOE-C2M2.pdf

[2] United States National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, 12 February 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[3] United States National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, 16 April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

State

United Kingdom

Gender

Male

Primary author: STJOHN-GREEN, Mike (Mr)

Co-author: ROWLAND, Michael (Practical Reason Incorporated)

Presenter: STJOHN-GREEN, Mike (Mr)

Track Classification: CC: Information and computer security considerations for nuclear security