Updating and Optimizing Existing Regulations

Competent Authorities are subject to both internal and external forces that drive the need to update or optimize existing regulations or establish new regulations. External forces include but are not limited to changes in the threat-risk developments, technological advances, political considerations, and industry/public acceptance.

Internal forces include but are not limited to the development of capacity (i.e., competencies and/or capabilities) of the competent authority, identification of adverse trends in licensee performance or attributes associated with cyber-attacks, new methods and procedures for inspections, and agreements with other organizations within the nuclear security regime (e.g., National Cyber Security Centre).

While regulations do unavoidably need sufficient flexibility to address an evolving threat landscape, it is not trivial to determine the effectiveness of regulations. The main requirement for regulatory updates is the need to strike a balance between current and stable regulations and updates to meet protection demands for cybersecurity. The level of regulatory effort has focused upon the development and maintenance of implementation guides focused on regulatory effectiveness and efficiency.

The computer security capabilities and competencies with the analysis of trends (supported by collaboration between the competent authority and owners/operators) will lead to maturity that will drive change to demonstrate regulatory compliance through inspections.

Identified needs/questions to be addressed

• How do regulators balance between change and stability? For example, do trends in cyber-attacks/campaigns demand increasing the frequency of regulatory updates? Is the regulatory framework sufficient in ensuring licensees evolve protections to keep pace with increasing adversary capabilities? Is it sufficient to only update guidance?
• What is a good trade-off between keeping requirements current and keeping some level of stability to include industry/public acceptance? For example, describe how a competent authority reviews and updates different types of regulation: regulatory rules vs. updates to implementation guidance.
Hierarchy of regulatory instruments (Conventions, Act, decree, rule, guide).
• How can we measure the effectiveness of a regulatory framework (e.g., continual improvement of inspections, risk-informed performance-based approaches, etc.)**?**
• How important is the level of incident reporting? For example, discussion on mandatory vs. voluntary reporting requirements (incident reports) Why or why not?
• Research and analysis (metric\lessons learned) to support inspections or inspectors? For example, providing actionable intelligence for inspectors to improve knowledge and performance. Describe support tools or processes to evaluate cybersecurity.
• Describe methods or techniques to determine whether regulation is sufficiently clear, comprehensive, succinct, or implementable? For example, incident reporting covers new technologies (e.g., Private Cloud Services storing sensitive nuclear information) or new reactor technologies (e.g., high-temperature gas-cooled reactor, molten salt reactors).