Contribution ID: **164** Type: **Paper**

The making of performance-based regulations

Canada is enhancing its Nuclear Security Regulations to be more performance-based. In removing prescriptive language from the regulations for a new performance-based one, the Canadian Nuclear Safety Commission (CNSC) needs to amend several key supporting documents, in particular the Design Basis Threat (DBT).

This paper will demonstrate the need for ensuring a collaborative approach across all areas of security, when developing modern regulations and regulatory documents that will provide expectations on how to nuclear facilities from evolving threats.

Addressing New Technology
How do we predict what security measures are needed when new technology is yet to be developed? Several vendors have submitted proposed designs to the CNSC for review of potential small modular reactors. CNSC must clearly understand the technology, the categorization of nuclear material to be used, the use of the reactor, any waste produced by the reactor, and the site where this technology will be located. Regulatory requirements for protecting the nuclear material from theft and the facility from sabotage must incorporate a security risk assessment and security by design.

Incorporating Cyber Security
How do we capture cyber security requirements and incorporate them into regulations that are heavily based on physical security? Physical security specialists must work with systems engineering specialists to ensure that the DBT includes the various cyber threats that could impact the operations of a nuclear facility. New regulations must include input from cyber experts. Requirements for protection of nuclear facilities must incorporate computer security measures. Security evaluations must include a cyber Threat and Risk Assessment that will consider the risk of cyber-essential assets being compromised.

Analyzing Evolving Threats
How do we ensure that security requirements will be adequate to allow licensed nuclear facilities to protect against the Design Basis Threat? CNSC has taken a different approach to amending the existing DBT. Staff decided early on that a collaborative approach across all areas of security was needed. An 8-member project team was created to ensure a robust process is followed to reach a defendable product. Phase 1 –Analysis involves the collection of data. Phase 2 –Development is the review of data and intelligence analysis. Phase 3 –Consultation includes reaching out to licensees through a classified workshop. Phase 4 –Approval consists of presenting the new DBT to the Commission for publication.

State

Canada

Gender

Male

Primary author: Mr POIRIER, Yves (CNSC)

Presenter: Mr POIRIER, Yves (CNSC)

Track Classification: PP: Design basis threat and threat assessment: prevention and protection