Contribution ID: **65** Type: **Interactive Content Presentation**

Cooperation Success Stories –Compliance to the new CSA N290.7 Canadian regulation

Emerging global threats are constantly evolving. The velocity of technology change within organizations is introducing different attack surfaces with new technologies and digital mobility. These along with increased regulation on cyber security is a challenge that many utilities and cyber security teams face for their security postures.

A new Cyber Security regulation, CSA N290.7 Cyber Security for Nuclear Power Plants and Small Reactor Facilities, was recently introduced and mandated by Canadian Nuclear Safety Commission (CNSC) for the nuclear power plants. Canadian nuclear utilities are starting to comply with this standard. The CSA N290.7 is a consensus-based standard developed with the participation of nuclear operators, the Canadian regulator, Canadian nuclear laboratories and key suppliers. The Standard addresses cyber security for the following computer systems and components: (a) systems important to nuclear safety; (b) nuclear security; (c) emergency preparedness; (d) Production reliability; (e) Safeguards; and (f) auxiliary assets or systems which, if compromised, exploited, or failed, could adversely impact item (a), (b), (c), (d) or (e).

The compliance timeline is different for each utility. Ontario Power Generator (OPG) is the largest energy generator in Ontario, where we are required to meet different regulatory requirements for different parts of power generation (i.e. Nuclear versus Renewable Generation cyber assets). OPG is the first utility that scheduled to meet compliance to the new CSA N290.7 regulation in November 2019. As the first Canadian utility, OPG has faced many challenges. In addition to complying with this new regulation, OPG has also addressed other emerging threats within cyber security.

A major issue has been addressing the supply chain third party risk. The information technology, and process control supply chain is complex, involves distributed system of interconnected networks, that is geographically dispersed and has many tiers of suppliers –from component manufacturers, to designers, integrators, and operators. This is not explicitly addressed in the current version of the Standard. OPG has worked closely with internal stakeholders and industry leaders to develop Cyber Security Provisions and incorporate these into contract Terms and Conditions. OPG has two levels of contract terms: baseline, and heightened requirements. The baseline requirements are applicable to all OPG's purchasing agreements covering requirements for service providers that provide assets or services on regulatory assets. The Terms and Conditions have been included in all new contracts since 2017. OPG has been successful in this program rollout where we have continuously enhanced the program while sharing good practices and broader experience to enhance nuclear security through international working groups information exchange –as well as incorporating lessons learned from our main stakeholders.

Gender

State

Canada

Authors: Ms MAHDIAN, Parisa (Ontario Power Generation); Mr BENJAMIN, Mike (Ontario Power Generation)

Presenters: Ms MAHDIAN, Parisa (Ontario Power Generation); Mr BENJAMIN, Mike (Ontario Power Generation)

Track Classification: CC: National nuclear security regulations