Sustainability in Competency and Capabilities

Capabilities and competencies are areas that require an ongoing level of focus. Many facets go into optimizing organizational sustainability, including human and financial resources, training and exercises, organizational turnover, and advanced knowledge retention, as well as the ability to collect and share lessons learned to address ongoing cyber security issues. As we look at how to address each of these areas individually, it is important to note that the cyber security threat landscape moves very fast, necessitating the need for clearly defined efforts to be flexible and rapidly evolve to meet the changing environment.

Participants who wish to give presentations are requested to submit an abstract of their work. Those abstracts will be reviewed as part of the selection process for presentations.

Identified areas to be considered

Management understanding and support of computer security is the first step in building a strong computer security program. Strategic and financial support is needed to drive a systematic approach to planning and implementation. There are many challenges with this topic, especially with governments and/or organizations who are maturing, maintaining, and improving their computer security programs. Further, the development of inspection or regulatory guides to assist in an improved knowledge base for both the regulator and operator will increase consistency in program implementation.

Training development models for computer security developed by government and commercial organizations are informative but lack specific analysis of the skills and training required for working in nuclear computer security. Organizations with nuclear security responsibilities must develop their own systematic approach to grow competent nuclear cyber security professionals. By using internal and external training and certification, as well as ongoing tabletop and hands-on exercises, the appropriate level of training can be provided to each employee's organizational role.

Knowledge, Skills, Abilities; Nuclear sector uses digital systems to monitor, operate, control, and provide security for the protection of information and operational technologies. Securing these digital systems for the health and safety of the public, while protecting the functions of safety, security, and emergency preparedness is paramount. Processes for current staff should be in place for an educational path to drive growth in knowledge, skills, and abilities. This process is becoming more challenging as computer security professionals are in great demand and the difficulty in replacing experienced and knowledgeable staff is resource consuming. Hiring and retaining computer security experts within these functional areas is critical.

Centers of Excellence (CoE) are promoted in many countries around the world. Activities covered by these CoE support the national and international nuclear sector including operators, suppliers, vendors and, to some extent the CoEs can benefit the development and sustainability of regulatory capacity. Some countries are missing such CoEs, and in some countries the existing CoEs may not be mature enough to support the regulatory capacities. This can be achieved by providing training, sharing of information and good/best practices, cooperation, and research and development initiatives. International or regional CoEs initiatives could also be used to sustain regulatory capabilities.

Technical Support Organization or Computer Security Technical Authority cooperates with governments and nuclear organizations who need computer security technical assistance, providing support to both regulators and operators. The TSO provides advice in the areas of computer security inspections, incident response, and training as needed. Not all countries have this capability and establishing a TSO, could provide strength in implementation for those

structures as identified in IAEA guidance TDL005 Incident response Planning at Nuclear Facilities. The structures are comprised of:

- National Competent Authorities
- Technical Authorities
- Operators

National working groups (NWG) facilitate ongoing implementation of computer security requirements in the nuclear sector to address cyber security issues. NWGs are focused on safety and security, and the protection of sensitive nuclear information and digital components in systems regulated by the respective government agencies. The NWG collects and shares lessons learned from the continued development and refinement of the nuclear cyber security guidance and inspections, and the implementation for the state computer security strategy. The NWG informs changing trends in cyber security, best practices, the regulatory environment, and state-level initiatives. NWG composition is of programs leaders and senior cyber security program management, who provide executive guidance to the NWG. Terms of reference will need consider interaction between regulators and licensees when engaging on topics as part of the working group.