Contribution ID: **297** Type: **Paper**

Developing a multi-year nuclear-cyber capability development training and education program

The cyber domain has evolved over the past thirty years from one that was primarily concerned with the protection of data confidentiality, integrity, and availability, to one that includes an integrated set of defensive technologies and processes in order to respond to the ever-advancing threats posed by skilled cyber actors. As the cyber threat actors have evolved their capabilities, it has required that defenders not only deploy defensive cyber capabilities and skilled cyber defense staff to handle these tools and data, but also extend their training and education programs to include all staff such that the entire organization is considered as part of the cyber defense team, identifying and reporting observations that may indicate that a cyber-attack has or is taking place.

The nuclear domain for this same thirty years has included programs to address the protection and nonproliferation of nuclear materials through programs for physical security protection, insider threat mitigation, nuclear material accounting and control, transportation security, protection from sabotage, and incident response. It is only in the past ten years that cyber-security has become a capability of concern, not only as applied to these existing security domains, but also by itself as the attack surface within a nuclear facility is large and includes interaction with a diverse multifunctional staff. To address these security concerns countries such as China and the United States have established nuclear security centers of excellence in support of developing capabilities that contribute to mitigating the overall risk of handling and using nuclear materials.

Over the past three years the US and China have been working together at the State Nuclear Security Technology Center (SNSTC) in Beijing, China to implement a multi-year nuclear-cyber capability development training and education program. This program was built using US NIST Special Publication 800-50 on building an Information Technology Security Awareness and Training Program that includes a basic curriculum allowing students to progress from awareness programs to training courses to specialized domain education, with all course materials derived from existing risk and threat assessments. These courses are being implemented at the Center of Excellence in Beijing that is a multi-building site modeled with common nuclear facility capabilities including physical security zones and associated protection technologies, a functional Central and Secondary Alarm Stations (CAS/SAS), a material processing facility, and a material storage vault. This infrastructure allows for all courses from awareness through advanced to be offered with a hands-on component.

This paper presents the co-developed capability development training program including a history of the courses conducted that informed the creation of the structural levels and how this information was mapped to China's existing operational training programs for completeness. Program course levels include awareness, basic training, intermediate-to-advanced training on specific topics, and educational initiatives in conjunction with national universities. Our paper also includes information on how we handled cultural issues in the development and delivering of nuclear-cyber courses and how these courses have benefited the overall US-China confidence building process within the nuclear-cyber community.

Keywords: Nuclear-Cyber, Training and Education, Multicultural Exchange, United States, China

Gender

Male

State

China

Authors: Mr ZONG, Bo; LIU, Xiaojun; Mr SPIRITO, Chris; Mr NICKERSON, Charles

Presenters: Mr ZONG, Bo; Mr SPIRITO, Chris

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