Contribution ID: **271** Type: **Interactive Content Presentation**

Good Practices for Creation of a Computer Security Regulation for the Nuclear Industry

The nuclear industry is changing. Industrial Control Systems and physical security systems are evolving from analog to digital equipment. There is a proliferation of microprocessors and operating systems throughout the system. Equipment that was traditionally connected via dedicated, hardwired connections and used proprietary protocols are now networked using more traditional Internet Protocols (IP). Although these systems were historically isolated, they are now being integrated with traditional information technology systems. We must now consider these systems from an integrated perspective. Threat actors are increasingly exploiting this integration to compromise key assets in other industries. These same tactics could be used to target and exploit similar systems at nuclear facilities.

The need for state regulation of computer security of the nuclear industry is clear. This will require computer security professionals to be part of a larger group to create and revise these regulations. Historically, they may not be familiar with the regulation development process and international good practices. This paper will provide a description of the beginning of this process.

The goal of regulation is to create an effective and efficient computer security program at sites which have nuclear material and radioactive sources. It is intended to provide clear requirements for the operators to follow. These requirements also provide clear expectations for the regulator to perform assessments at each site. The regulation will be used to create consistency between each operators'computer security programs. The regulation also provides guidance and technical background where appropriate.

The IAEA's NSS 17 (Computer Security at Nuclear Facilities) provides important guidance. Key sections of a computer security regulation will include, but are not limited to:

- The legal basis for the regulation
- Organization and management of computer security programs
- Roles and responsibilities for the regulator and operators
- Other involved organizations (law enforcement, national intelligence capabilities)
- Ensuring and prioritizing confidentiality, integrity and availability
- Design Basis Threat
- Account and user management
- Asset identification and characterization
- Identifying vulnerabilities and managing risk
- Provisions for the protection of Industrial Control Systems and Physical Protection Systems
- Understanding network topology and enforcing separation of communications by function and sensitivity
- Intrusion detection and prevention
- Incident response and recovery
- Training and awareness programs

The creation and revisions of computer security regulations is a critical process and must be carefully managed. The regulation must be properly organized to be easy to understand and implement by the operator. It must use normative language for clarity. They also must clearly define the role of the regulator and provide transparent expectations of their assessment of operators. Requirements must be clearly separated from recommendations, good practices, and background material. Requirements must also be clearly enumerated to facilitate communications between the operator and regulator. Only by being measurable can requirements be assessed. Regulators and operators must form a partnership where impacts of policy can be openly discussed. Operators must be included early and often in the creation of these regulations. Each requirement carries a cost that will ultimately be paid by the consumer of the energy generated.

The developers of the regulation must clearly understand the impact and burden on both the regulator and the operators. The operator must implement the requirements, and the regulator must assess the effectiveness of the implementation by the operators. This can cause significant and sudden impact and burden includes both manpower and costs. A plan to acquire additional funds will be needed and the lead time for that funding and the hiring of new personnel. One suggested approach is to pilot the implementation and assessment of a draft regulation with the regulator and a selected operator. This allows a more agile and quick regulation development process than the normal regulation enactment and revision process. This can be as simple as tabletop exercises, or full implementation of draft regulations. Another option is to utilize a phased approach to regulation enactment and requirements. Requirements can be added over time. Regulatory items that start

as recommendations can become requirements over time. This allows operators to grow their computer security program in a phased effort over a longer time period. Before, during development and after development, there is a need for frequent and honest conversations between operators and regulators must continue. This will drive the successful implementation and revision processes.

State

United States

Gender

Male

Authors: Mr WHITE, Gregory (LLNL); Mr BROMBERGER, Seth (LLNL)

Presenter: Mr WHITE, Gregory (LLNL)

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