Contribution ID: **547** Type: **Paper**

Developing Computer Security Regulations for Radioactive Material and Associated Facilities

Radioactive material and associated facilities are vulnerable to cyber attack. Possible adversary scenarios include disabling or spoofing computer-based security systems to gain unauthorized access to radioactive material, to an associated facility, or to security-sensitive information; compromise of computer-based accounting and inventory systems to mask theft or diversion of radioactive material by insiders; and sabotage of computer-based safety or operational systems in order to cause the release of radiation. To counter such scenarios, many regulatory bodies are developing or considering the development of regulatory requirements for computer security, as recommended by current and forthcoming International Atomic Energy Agency (IAEA) guidance.

The paper presents a framework that regulatory bodies could use to undertake this process. The framework consists of a series of questions that the regulatory body could address in deciding whether and how to develop regulatory requirements for computer security, as well considerations that would go into addressing those questions. The questions addressed include:

(1) whether the regulatory body has the legal authority to impose computer security requirements;
(2) whether to impose computer security requirements as part of general security regulations or as separate requirements or by other means such as license conditions;
(3) what other competent authorities may need to be involved in the development and implementation of computer security requirements;
(4) whether to use a performance based, prescriptive or combined approach to computer security requirements;
(5) the types of adversary scenarios that the computer security measures implemented by operators should address;
(6) the types of computer security requirements that regulations might include;
(7) whether to vary the requirements based on practices (e.g. teletherapy versus industrial irradiator) or keep them generally applicable to all practices; and
(8) how the operator will be directed to document compliance with the resulting requirements, for example in the operator's security plan or in a separate computer security plan.

The paper also provides example regulatory provisions for different regulatory approaches to computer security. The result is a tool that can be used by regulatory bodies directly, in bilateral or multilateral regulatory development workshops, and in training on this topic.

Gender

Male

State

United States

Author: MORRIS, Frederic (Pacific Northwest National Laboratory)

Co-authors: Ms WEISE, Rachel (Pacific Northwest National Laboratory); DONNELLY, David (Pacific Northwest National Laboratory)

Presenter: MORRIS, Frederic (Pacific Northwest National Laboratory)

Track Classification: CC: National nuclear security regulations