Lessons Learned from the development of the First Nuclear Power Plant Cyber Security Program: Moving beyond risk

Eric Lee
US Nuclear Regulatory Commission
December, 10 2009

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Overview

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Background**
- **Development of Regulatory Guide 5.71 "Cyber Security Programs For Nuclear Facilities"**
- **Lessons Learned**

Background

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **The Nuclear Regulatory Commission**
  - **The NRC was created as an independent agency by the Energy Reorganization Act, signed into law October 11, 1974, which abolished the Atomic Energy Commission. The NRC, which took over the regulatory functions of the AEC, formally came into being on January 19, 1975. The Energy Research and Development Administration, also created by the Energy Reorganization Act, took over the other functions of the AEC and is now part of the Department of Energy.**
  - **The Nuclear Regulatory Commission regulates the civilian uses of nuclear materials in the United States to protect public health and safety, the environment, and the common defense and security. The mission is accomplished through licensing of nuclear facilities and the possession, use and disposal of nuclear materials; the development and implementation of requirements governing licensed activities; and inspection and enforcement activities to assure compliance with these requirements. It is not connected in any way with defense matters or nuclear weapons.**

Background

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cyber

- 2001 - NRC issued an advisory to power reactor licensees to enhance cyber security
- 2002 - NRC required power reactor licensees to implement Interim Compensatory Measures to enhance cyber security
- Design Basis Threat Order (2003)
- 2004 - NRC issued NUREG/CR-6847 “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants”
- 2005 - NEI 04-04 “Cyber Security Program for Power Reactors”
- 2009 – NRC issued 10 CFR 73.54 “Protection Of Digital Computer and Communication Systems And Networks”

RG 5.71

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **DG-5022 (2008)**
  - **Provided highly prescriptive guidance on selected few security controls**
  - **Based on risk analysis to select specific security controls**
  - **Received many comments**

- **RG 5.71 (Draft July 2009)**
  - **Provides cyber security program attributes and criteria for those attributes**
  - **Provides security controls based on NIST 800-53 and 82**

RG 5.71

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

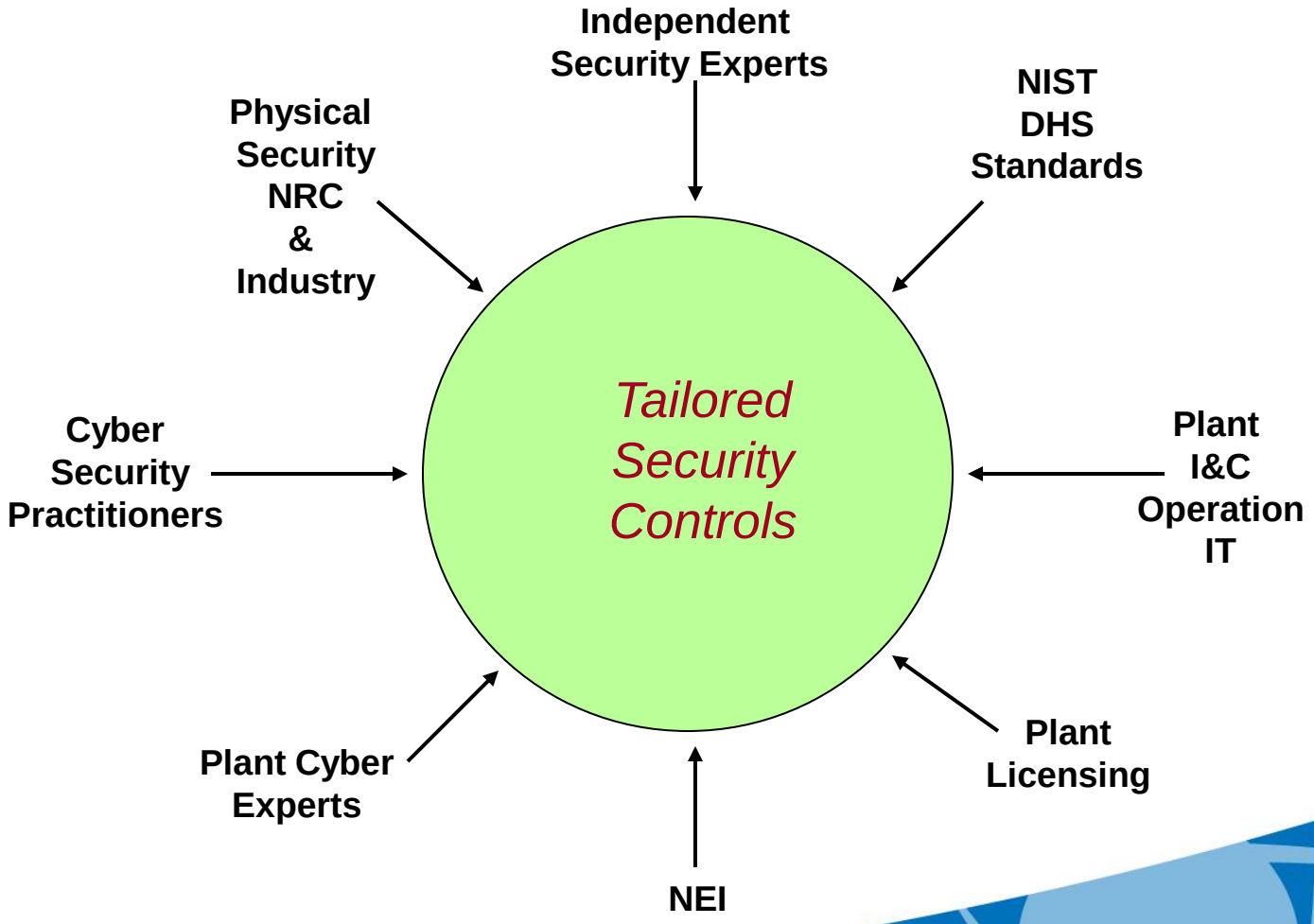
Summary of RG 5.71

- **Describes Cyber Security Team qualifications**
- **Describes how CDAs are identified**
- **Describes the defensive strategies**
  - **Defensive architecture**
  - **Describes minimum set of cyber security controls**
  - **Describes criteria for maintaining cyber security program**

- **Describes criteria for documentation for inspection**

Appendix A

RG 5.71


Independent Security Experts
Physical Security NRC & Industry
NIST DHS Standards
Tailored Security Controls
Cyber Security Practitioners
Plant I&C Operation IT
Plant Cyber Experts
Plant Licensing
NEI

Lessons Learned

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Forming a Team**
  - **Tailor security controls**
  - **Categorize system**
  - **Explain and defend Tailored security controls**

- **Reliability Engineering vs. Security Engineering**
  - **Compromise = failure (false)**
    - **Use of PRA**
    - **Use of FMEA**
    - **Pathways**
    - **Loss/degradation of integrity of control**
    - **Loss of confidentiality**

  - **Selecting vs. Appling Tailored Security Controls**
    - **Controls are overwhelming**
      - **Use of risk analysis**
      - **Select vs. Verify and Validate**

Lessons Learned

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Require regular re-assessments of effectiveness of program and controls**
- **Perform Penetration Tests to demonstrate program can resist real world challenges**
- **Add compensating measures to controls, for example:**

  ...for situations in which a CDA cannot support security function isolation, Licensee takes all of the following actions:
  • physically restrict access to the CDA/CS
  • monitors and records physical access to the CDA/CS to detect and respond to intrusions in a timely manner
  • Etc.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Questions?