U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Options for Cyber Security Design Requirements for Power Reactors

April 9, 2015

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Scope

- **Discuss options for including cyber security design requirements for power reactors into NRC regulations**

- **Scope does not include any other cyber security initiatives, such as the NEI petition for cyber security rulemaking**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Objective

- **Provide an overview of potential options for including cyber security design requirements for power reactors into NRC regulations**

- **Solicit stakeholders feedback regarding the options for including cyber security design requirements**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Current Cyber Security Regulations & Guidance (1/2)

- **(2004) Publication of NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants"**
- **(2005) NRC endorsement of NEI 04-04, "Cyber Security Program for Power Reactors"**
- **(2009) Issuance of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"**
- **(2010) Publication of Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities"**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Current Cyber Security Regulations & Guidance (2/2)

- **(2010) NRC endorsement of NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors"**

- **(2011) Publication of RG 1.152, Revision 3, "Criteria For Use Of Computers in Safety Systems of Nuclear Power Plants." This revision deleted cyber security guidance under 10 CFR Part 50 to be consistent with programmatic requirements of 10 CFR 73.54**

- **(2013) NRC endorsement of NEI 13-10, "Cyber Security Control Assessments"**

Current Regulatory Framework

- **10 CFR 73.54 provides programmatic requirements for licensees and COL applicants to protect digital computer and communication systems and networks against cyber attacks**

- **The current regulatory framework requires licensees and COL applicants to submit a cyber security plan to be reviewed by the NRC**
  - Licensees and COL applicants are not required to submit design information addressing cyber security requirements for NRC review
  - For new reactors, the first opportunity for the NRC to inspect the implementation of the cyber security program is after the COL is issued
    - This typically occurs long after the referenced design certification is completed

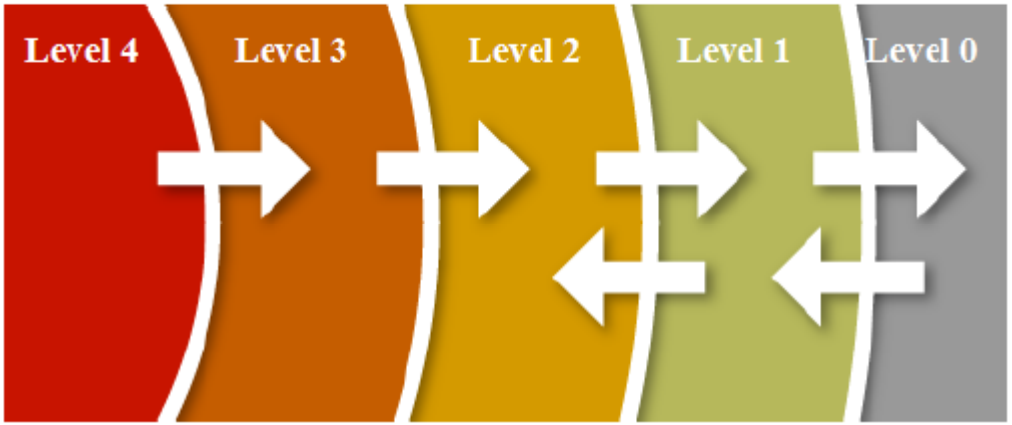
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ACRS Concerns (1/2)

- **The Advisory Committee on Reactor Safeguards (ACRS) has raised concerns regarding control of access to plant equipment and networks**
  - The ACRS has stated that control of access to critical plant systems should be reviewed as part of design certifications and COL application reviews
  - The ACRS has raised similar concerns regarding the licensing reviews of operating plant digital I&C upgrades

ACRS Concerns (2/2)

- **ACRS recommended uni-directional communication from Level 4 to Level 3, and from Level 3 to Level 2, to be enforced via a communication flow enforcement device (e.g., data diode)**
  - The design of this device would be reviewed during licensing
  - A recommended approach that is described in RG 5.71 is shown below



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Design Certification Applicants

- **Design certification applicants requested the NRC to review their cyber security design features as part of design certification application reviews**
  - GEH submitted ESBWR Cyber Security Program Plan
  - AP1000 submitted the AP1000 PMS Computer Security Plan
  - Aspects of both plans that addressed 10 CFR 73.54 were not reviewed since demonstrating compliance to 10 CFR 73.54 is the responsibility of the COL applicant.

- **NuScale requested NRC review cyber security features as part of their design certification applications**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Benefits of Cyber Security Design Requirements (1/3)

- International nuclear power plant standards (e.g. IEC 62859) recommend that cyber security requirements be defined as early as possible in the system development lifecycle

- Consideration of cyber security early in the system development lifecycle can improve both a system's ability to resist a cyber attack, and limit the adverse consequences of a successful attack on the system

Benefits of Cyber Security Design Requirements (2/3)

- **Incorporation of cyber security controls as part of the development of I&C systems is currently a voluntary measure**

- **Since design certification applicants are not required to address cyber security, COL holders must address the requirements of CFR 73.54 during later stages**
  - If a vulnerability exists within the installed design, the licensee would have to either modify the system or implement compensatory measures to mitigate the vulnerability
  - This is often less effective than developing a more secure and robust system that provides inherent protection against the vulnerability

Benefits of Cyber Security Design Requirements (3/3)

- **Cyber security design requirements could enable the NRC to review the applicant's/licensee's proposed cyber security measures earlier in the licensing process**
  - Cyber security design requirements will provide an added level of regulatory assurance for new reactor designs and for new safety I&C systems to be installed in operating reactors
  - COL holders and licensees would be able to reference the staff's safety evaluation on the cyber security design controls in their cyber security program

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Overview of Options: Option #1

- **Develop cyber security design requirements to complement the current programmatic cyber security regulations**
  - Applicable to DC and COL applicants, and licensees seeking approval of digital upgrades for safety and important to safety systems
  - Applicable for systems that perform safety and important-to-safety functions
- **Information demonstrating that cyber security controls were considered during the design of systems that perform safety and important-to-safety functions should be provided**
  - Results of cyber vulnerability assessments conducted for systems that perform safety and important-to- safety functions
  - Information on how identified vulnerabilities are mitigated and the cyber security design control(s) used to mitigate the vulnerabilities

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Overview of Options: Option #2

- **Develop regulations to require technical controls for information flow enforcement in design**
  - Applicable to DC and COL applicants, and licensees seeking approval for digital upgrades for safety and important-to-safety systems
  - Specific to the controls specified in Section B.1.4 of RG 5.71 (i.e., one-way, hardware-based data communication paths between Level 4 and Level 3, and between Level 3 and lower security levels of the cyber security defensive architecture)
  - The intent of this option is to limit the design review to the control of information flow between the security levels of the cyber security defensive architecture

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Overview of Options: Option #3

- **No change to the existing cyber security program**
  - Continues the current practice verifying the compliance of the licensees' operational cyber security program via inspection without conducting a cyber security design review of systems that perform safety and important-to-safety functions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary

- **A SECY paper is being considered to propose options for including cyber security design requirements for power reactors into NRC regulations**
  - Intended to address concerns raised by the ACRS and Design Certification Applicants

- **Three options are being considered:**
  1. Develop cyber security design regulations to complement the current programmatic cyber security regulations
  2. Develop cyber security design regulations to require hardware-based controls for information flow enforcement
  3. No action