Nuclear Supply Chain Security

Kim Lawson-Jenkins
Cybersecurity Branch
Office of Nuclear Security and Incident Response

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

NRC Cybersecurity Regulation and Guidance

- Title 10 Code of Federal Regulation 73.54, “Protection of Digital Computer and Communication Systems and Networks”

- Regulatory Guide 5.71, Revision 1, “Cybersecurity Programs for Nuclear Power Reactors”

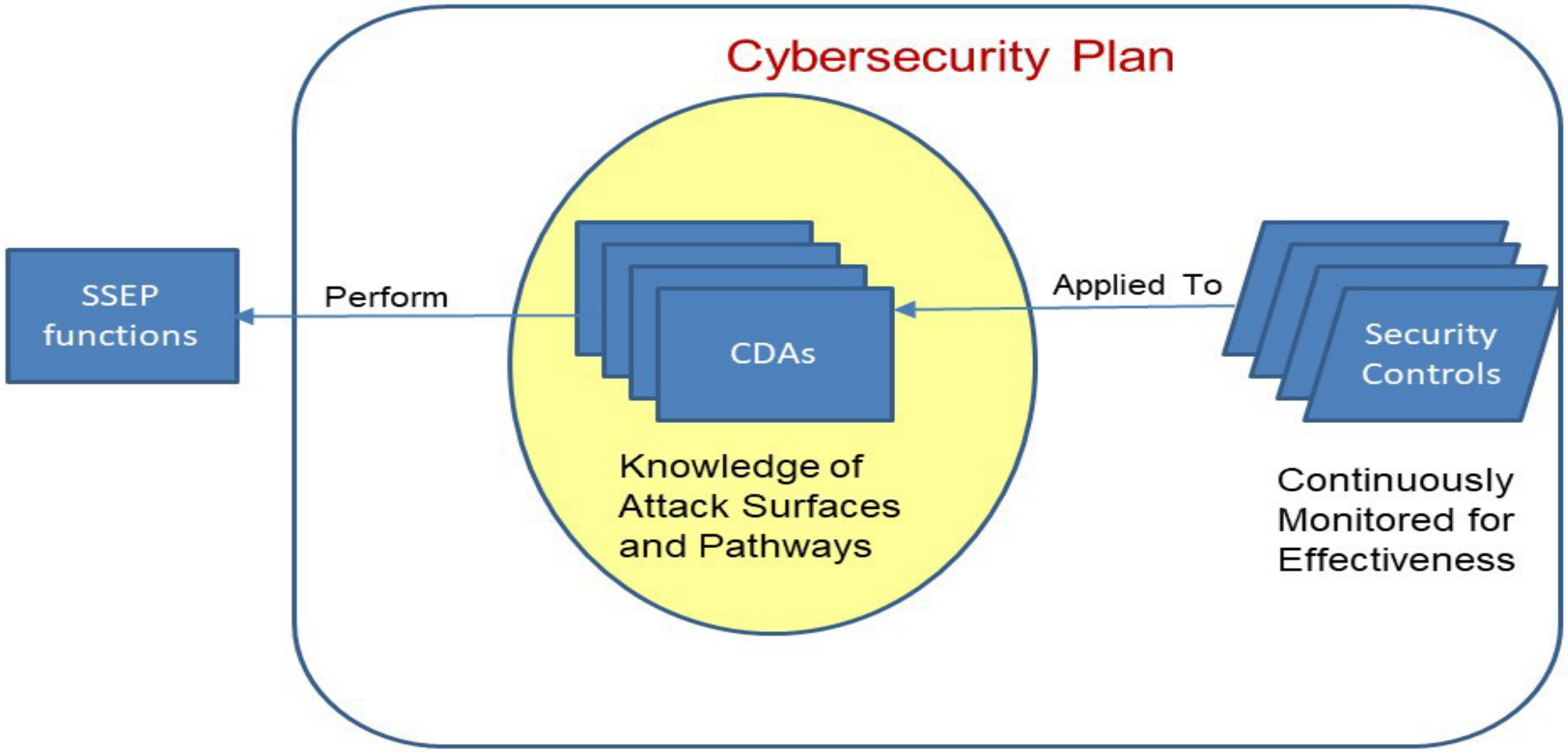
- Title 10 CFR 73.110 – Proposed New Regulation – “Technology-Inclusive Requirements for Protection of Digital Computer and Communication Systems and Networks”

- Draft Regulatory Guide 5075, “Establishing Cybersecurity Programs For Commercial Nuclear Plants Licensed Under 10 CFR Part 53”

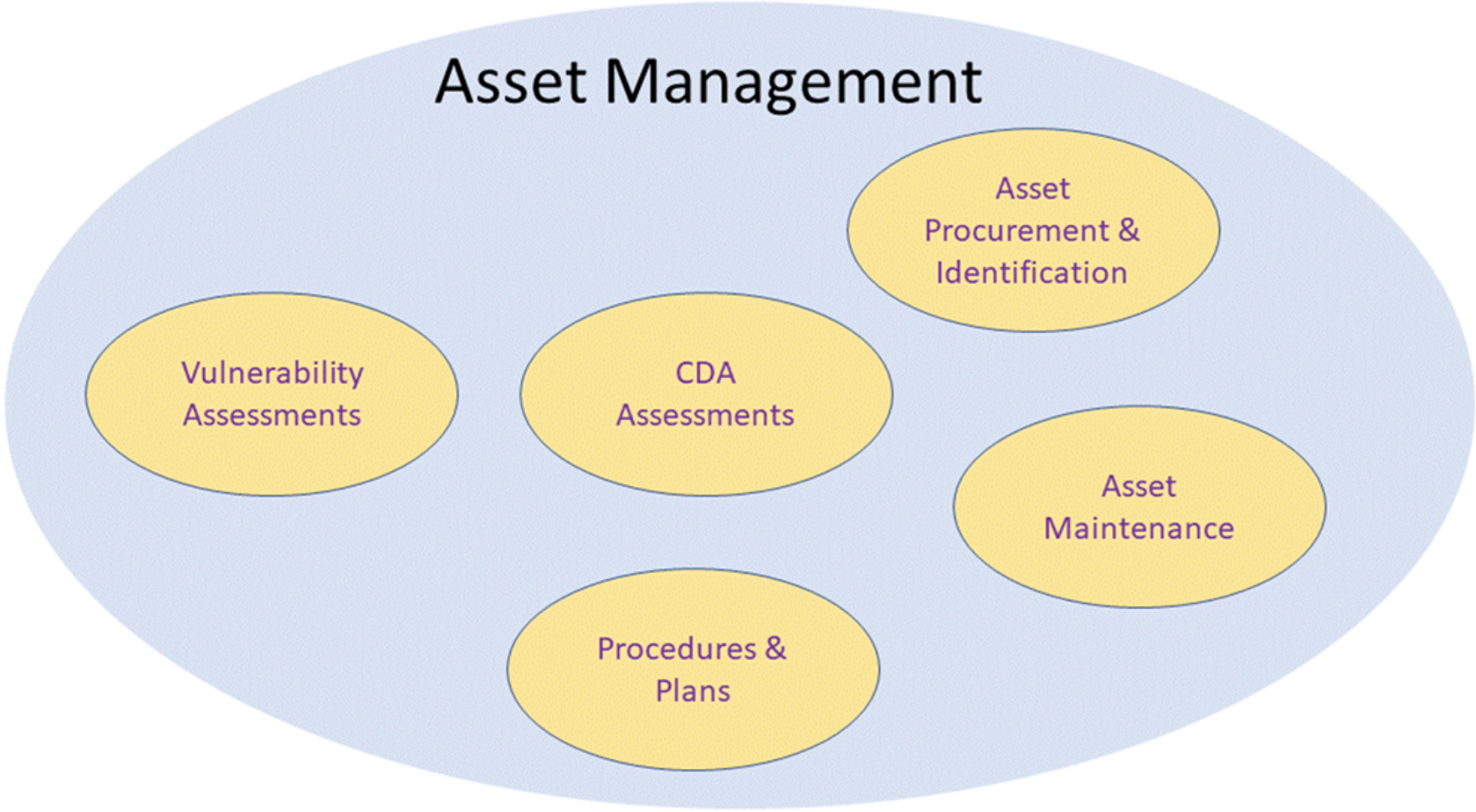
Three Questions for a Nuclear Regulator

- Can the facility operate safely?
- Can the facility operate securely?
- How is it verified that the facility is operating safely and securely?

The Big Picture



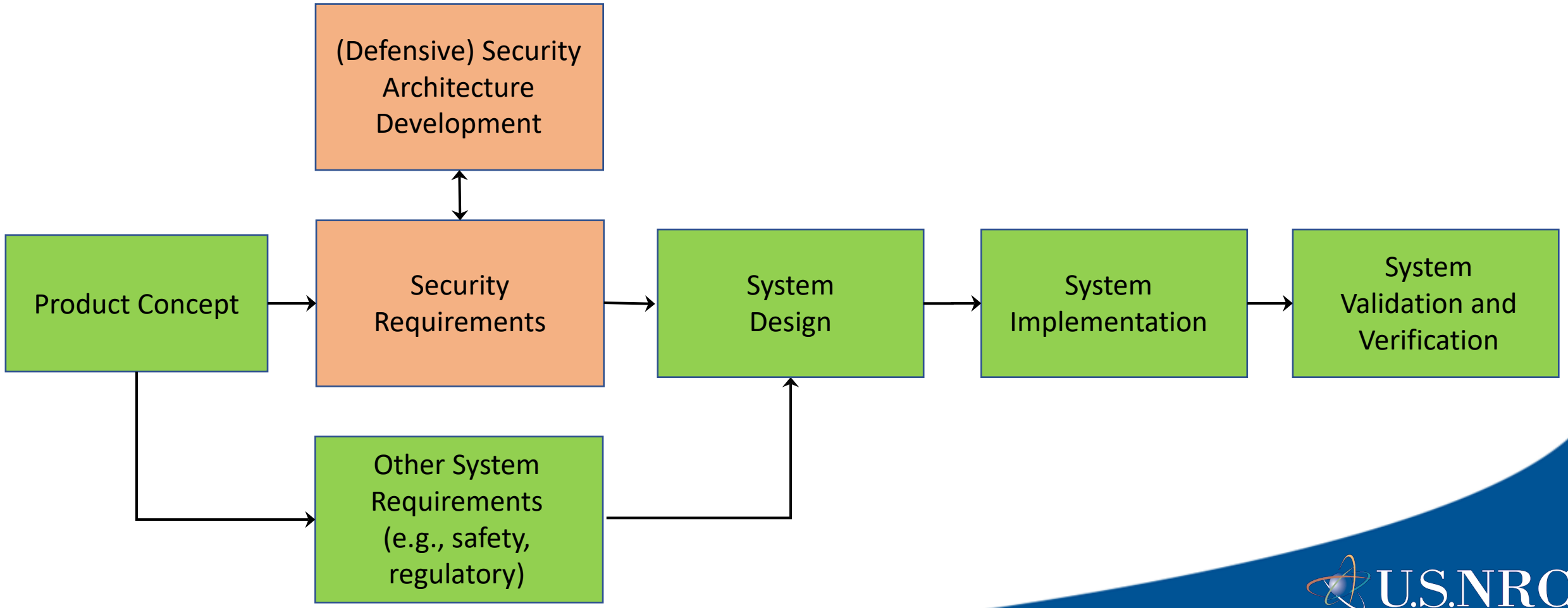
Knowing What You Have



Vendor Information for Asset Management

- Software bill of material
- Secure configuration information
- Maintenance information
- Identification of new vulnerabilities and mitigations
- “Normal” behavior and operation of equipment

Security By Design



Chain of Custody

Concluding thoughts…

- Cybersecurity requirements regarding supply chain are reviewed and approved by a regulator during licensing approval or amendment processes.
- A regulator's inspection program verifies the implementation of the approved cybersecurity requirements for a licensed facility.
- Supply chain security requirements should address the entire lifecycle of a device – manufacturing, procurement, testing, installation, operation, maintenance, and retirement.

Questions?

Thank you!