U.S.NRC
Protecting People and the Environment

Revision of RG 5.71
(Draft Guidance 5061)

Kim Lawson-Jenkins
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

Reasons for revising RG 5.71

- RG 5.71 released in 2010
- Since 2010…
  - New NRC regulation
  - Implementation of cyber security plans at licensees' plants
  - Milestone 1 – 7 cyber security inspections
  - NEI 13-10
  - Addendums to NEI 08-09
- Work began on DG-5061 in spring 2016

Scope of Updates

- **Clarify existing interpretation of regulations**
- Based on lessons learned from Milestones 1 – 7 inspections
- Changes apply going forward
- New regulation since 2010
  - Cyber security event notification
- Changes in NIST SP 800-53 r4
- New IAEA security guidance

Dependencies

- Resolution of SFAQs
  - Deterministic Devices
  - Data Integrity
  - Moving Data Between Security Levels
  - Treatment of Maintenance & Test Equipment
- Outcome of 2016 Table Top Exercises
  - Detection Response and Elimination
  - Monitoring and Assessment
  - Drills and Exercises
- NEI 08-09 Addendums

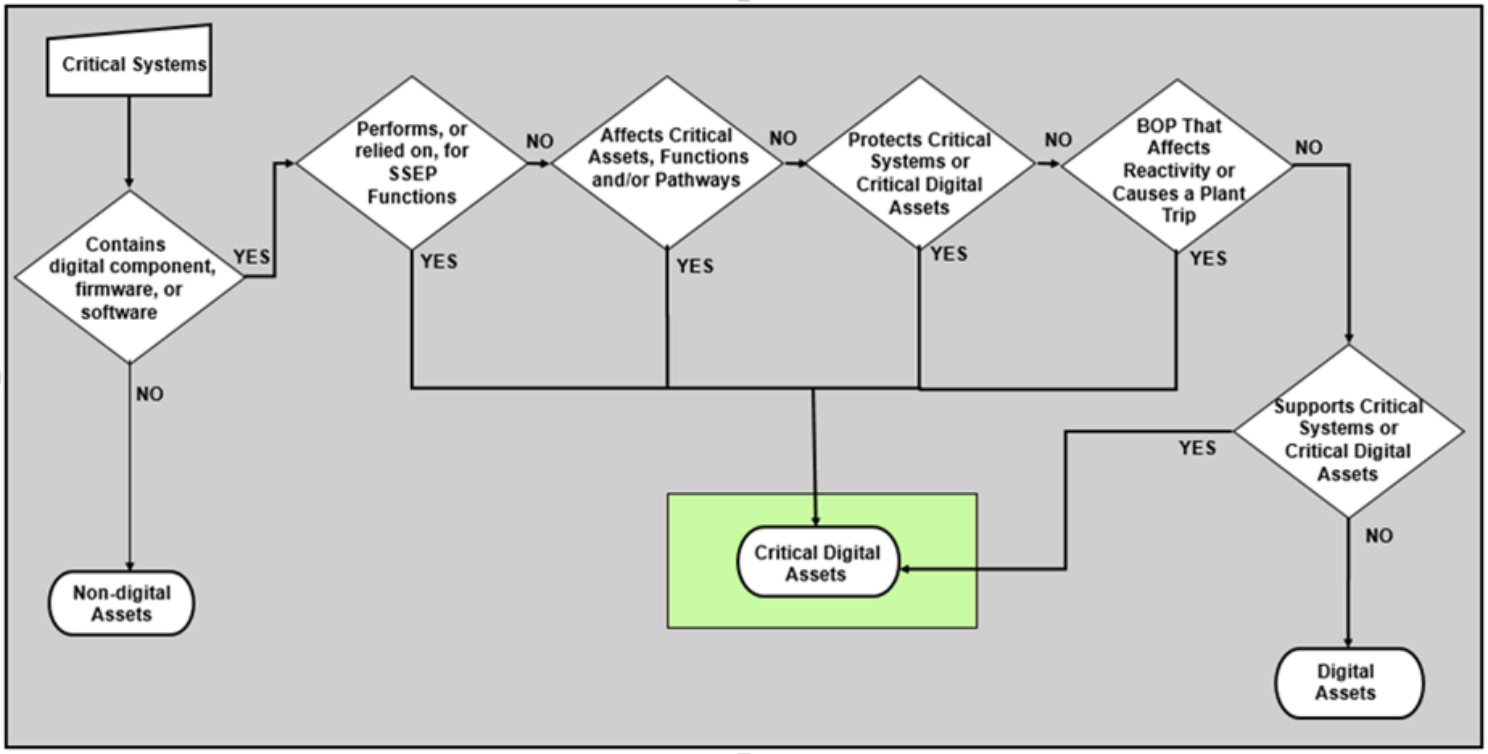
Staff Regulatory Guidance

Asset Identification associated with 10 CFR 73.54

- Balance of Plant Equipment
- The importance of identifying attack surfaces and attack pathways in the analysis of digital systems

Staff Regulatory Guidance

Protection of digital assets



Staff Regulatory Guidance

Protection of digital assets

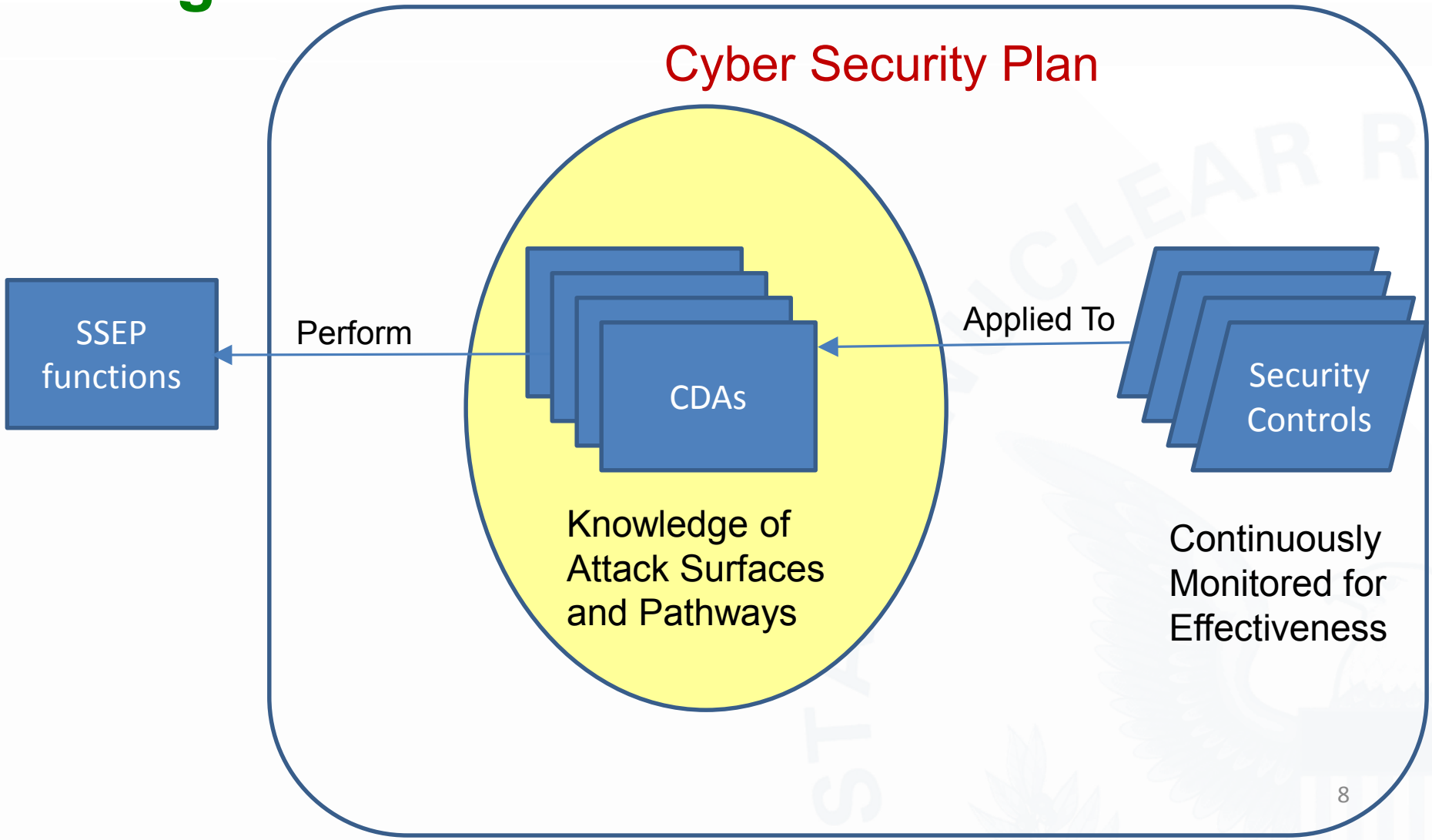
- Purpose of security controls
  - Control intent added to Appendices B and C
- Reducing or eliminating attack surfaces and attack pathways

Effectiveness of security measures

- Cyber security metrics
  - What is being measured?
  - Why is it being measured?
  - What do the metrics mean?

Staff Regulatory Guidance

The Big Picture



Other Changes

- Defensive Architecture
- Glossary
- References
- Appendix A (CSP template) – only editorial changes

U.S.NRC
Protecting People and the Environment

Appendices B & C (security controls)

	DG-5061	NEI 08-09	Rationale for change/difference
B.1.9 Previous Logon Notification	Removed control		Intent covered in covered in logging/audit controls
B.1.11 Supervision and Review – Access Control	Removed control		Intent covered in covered in logging/audit controls
B.1.14 Automated Labeling	Removed control	Removed control	Intent is covered in C.1.3 Media Labeling/Marking
B.3.5 Resource Priority	Removed control	Removed control	Any safety requirements for resource priority would have precedence. This control is usually applicable in the design phase of a digital device.
B.3.19 Thin Nodes	Removed control	Removed control	This control would be covered in the B.5.1 Removal of Unnecessary Services and Programs.
B.3.20 Heterogeneity/Diversity		Removed control	Different depending on safety or security context.
B.3.21 Fail in a known state		Removed control	Important for security

Tentative Schedule

- Public Comment Period – 60 days
- Comments Resolution – late 2018
- Publication of RG 5.71 rev 1- early 2019

Questions