U.S.NRC
Protecting People and the Environment

Revision of RG 5.71
(Draft Guidance 5061, Rev. 1)

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

U.S.NRC
Protecting People and the Environment

Overview

- Key Messages
- Background
- Updates
- Conclusion
- Q/A

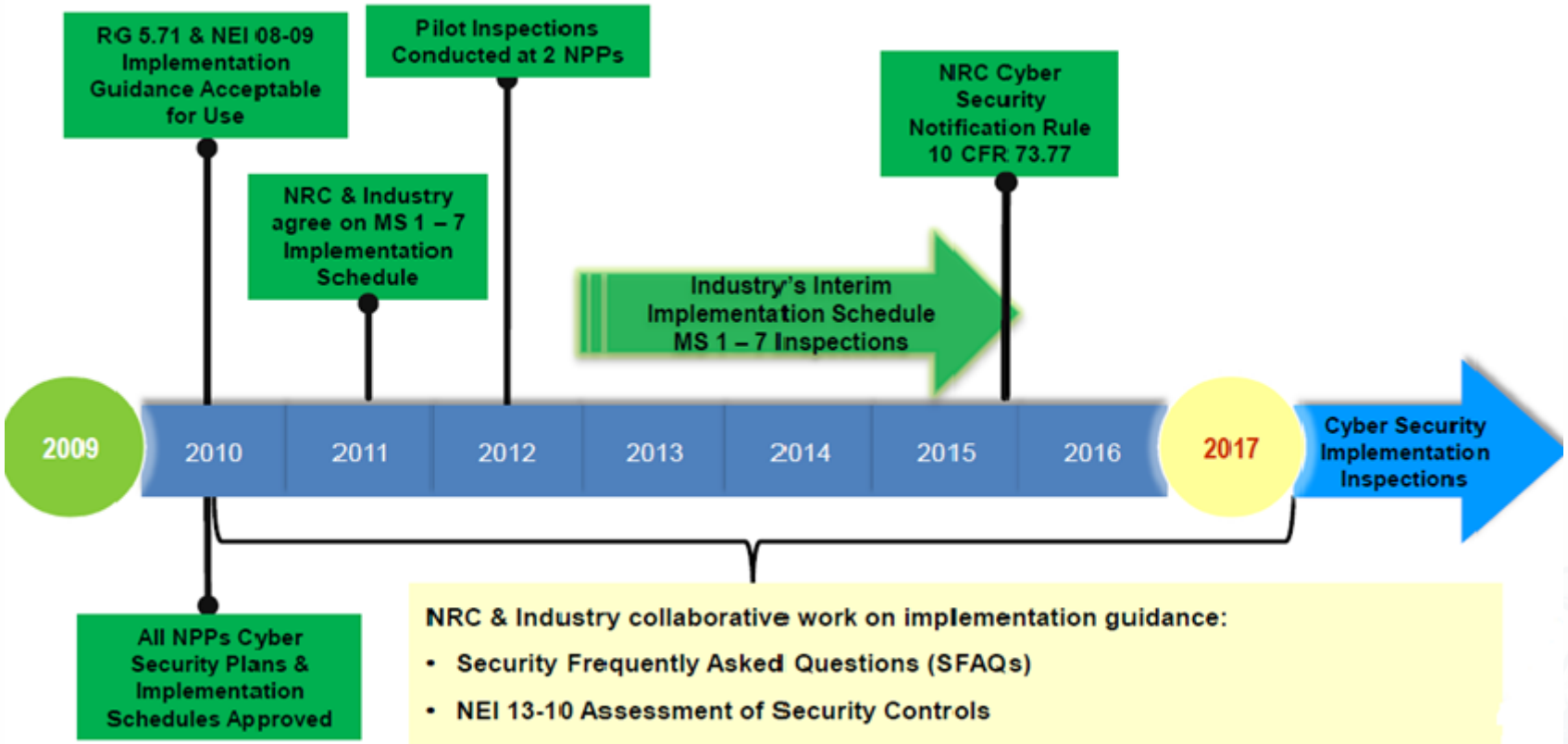
U.S.NRC
Protecting People and the Environment

Key Messages

- Since 2012, licensees have implemented cyber security programs and the NRC has implemented effective oversight of the licensee's cyber security plan (CSP).
- No changes in staff's position in DG-5061, only clarifications and one new NRC regulation 10 CFR 73.77.
- DG-5061 reflects the lessons learned since the issuance of RG 5.71 and prepares for the future.

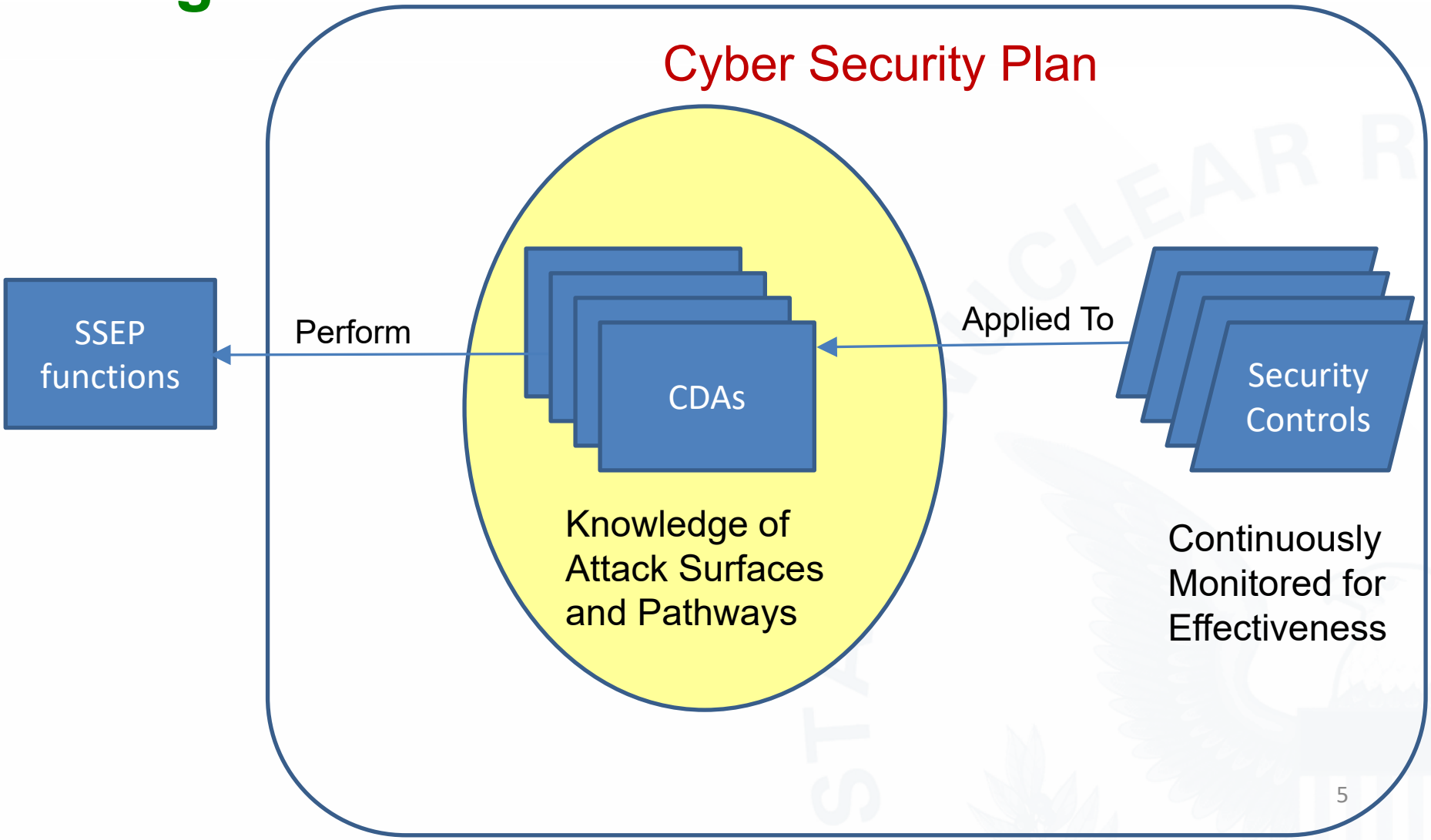
Background

Cyber Security Program Timeline



Background

The Big Picture



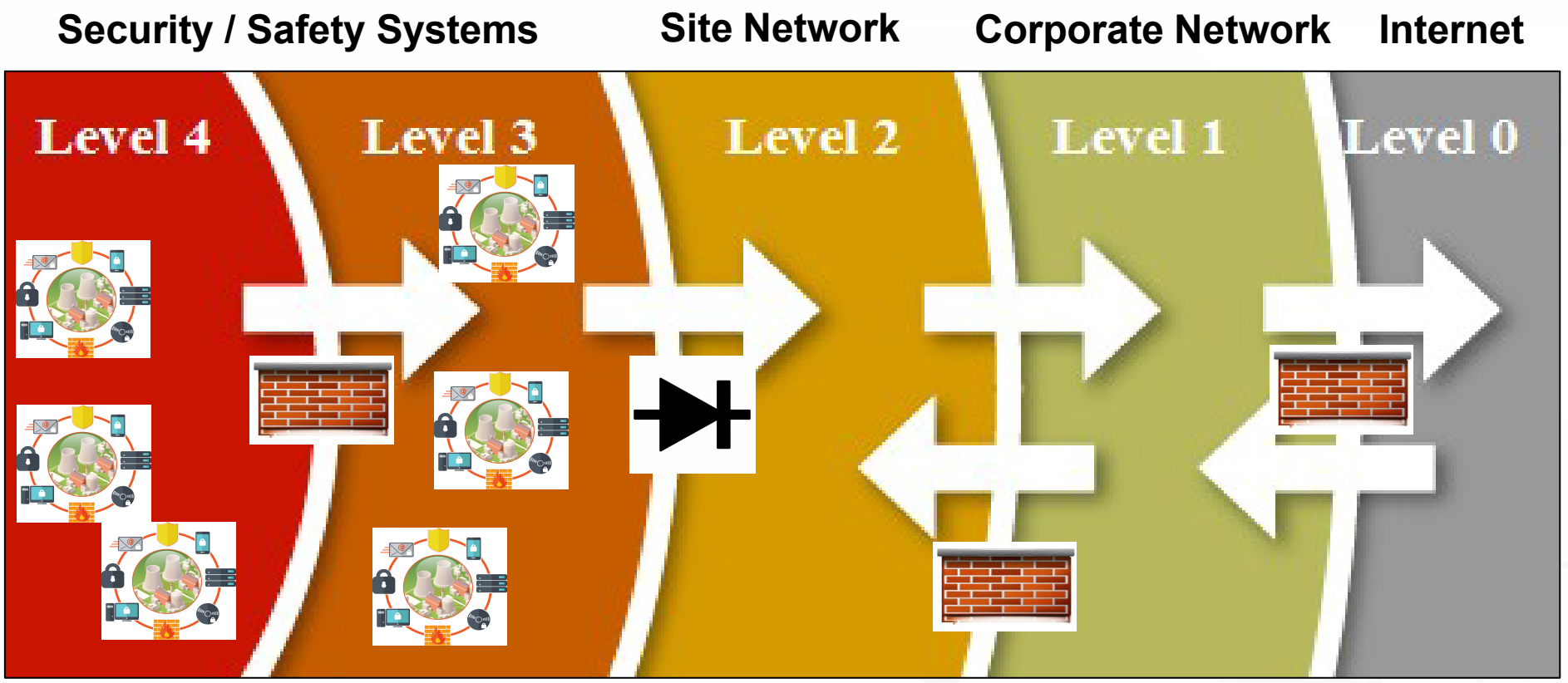
Background

Milestone 1 – 7 Inspections

2013 → 2015

MS 1	MS 2	MS 3	MS 4	MS 5	MS 6	MS 7
Establish the Cyber Security Assessment Team	Identify Critical Digital Assets	Implement One-way Deterministic Device	Access Control for Portable & Mobile Devices	Implement Observation & Identification of Obvious Cyber Tampering	Apply Security Controls to Most Important Critical Digital Assets	Implement Ongoing & Assessment Activities for Controls Applied

Cyber Security Defensive Architecture

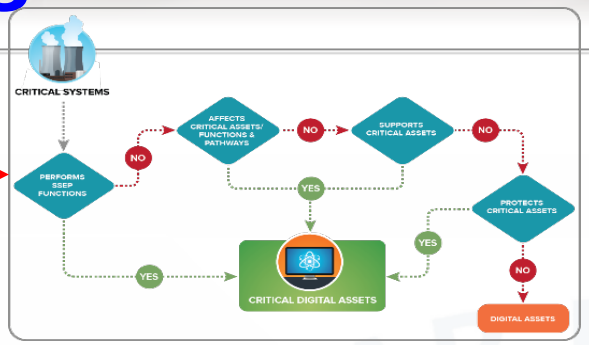


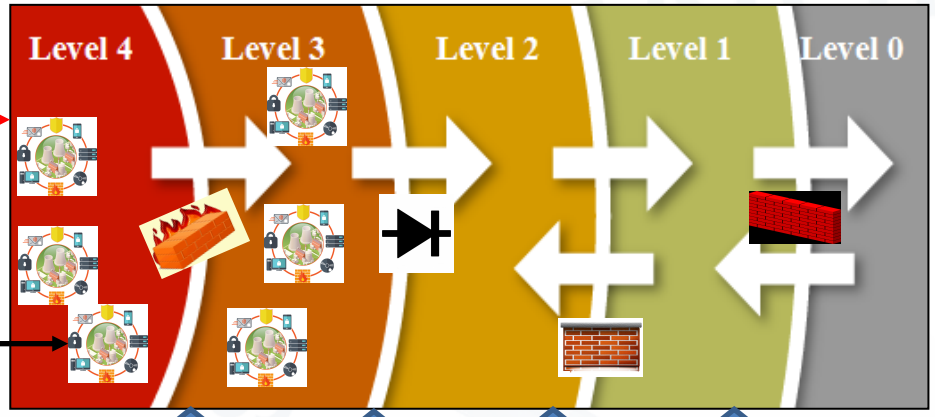
One-way Deterministic Device

U.S.NRC
Protecting People and the Environment

Full Program in RG 5.71

1. Cyber Security Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Apply Security Controls



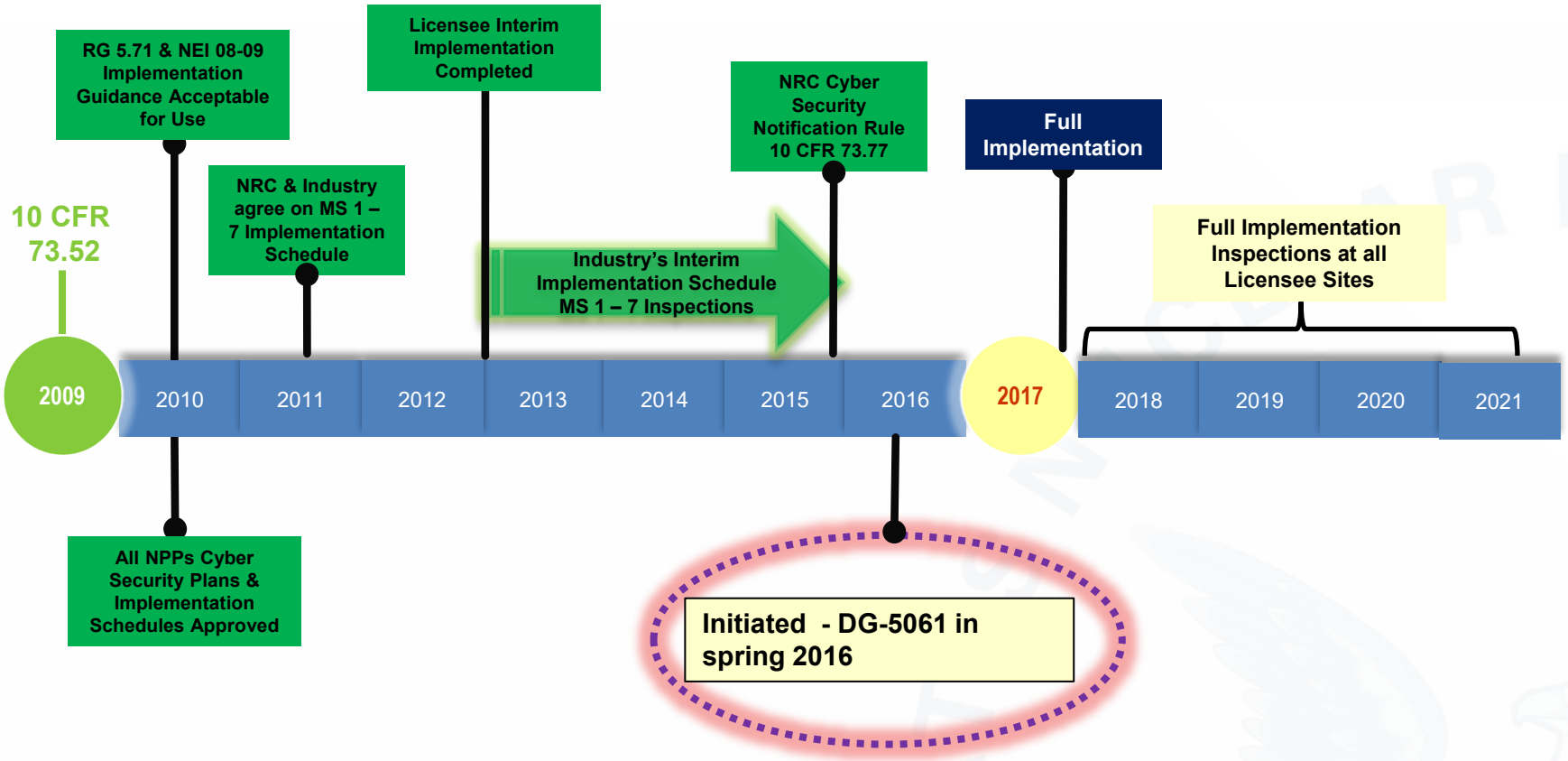


CYBER SECURITY PROGRAM

Defense-in-Depth	Security Controls NEI 13-10	Mitigation Strategies	Training	Manage Cyber Risk
Periodic Review	Modification Evaluation	Incident Response	Procedures	Records Retention

U.S.NRC
Protecting People and the Environment

Timeline with DG-5061 Development



OVERVIEW OF DG-5061 UPDATES

Updates in DG-5061 in 2018

- Clarified existing interpretation of regulations based on lessons learned from Milestones 1 – 7 inspections
- New regulation since 2010
  - Cyber security event notification
- Changes in NIST SP 800-53 r4
- New IAEA security guidance
- Balance of Plant

Updates in DG-5061 in 2020

- Discussed Risk Informed Cyber Security
- Emphasized the need for accurate CDA assessments
- Leveraged new international standards/guidance and updated NIST guidance on cyber security
- Addressed public comments to 2018 DG-5061

Lessons Learned from Full Implementation Inspections

- 57 inspections completed from 2017 - 2021.
- Insights on potential areas for improvement:
  - Quality of licensee critical digital asset and system assessments
  - Vulnerability assessments
  - Periodicity for ongoing monitoring & monitoring of security controls.

Updates in DG-5061

Risk Informed Cyber Security

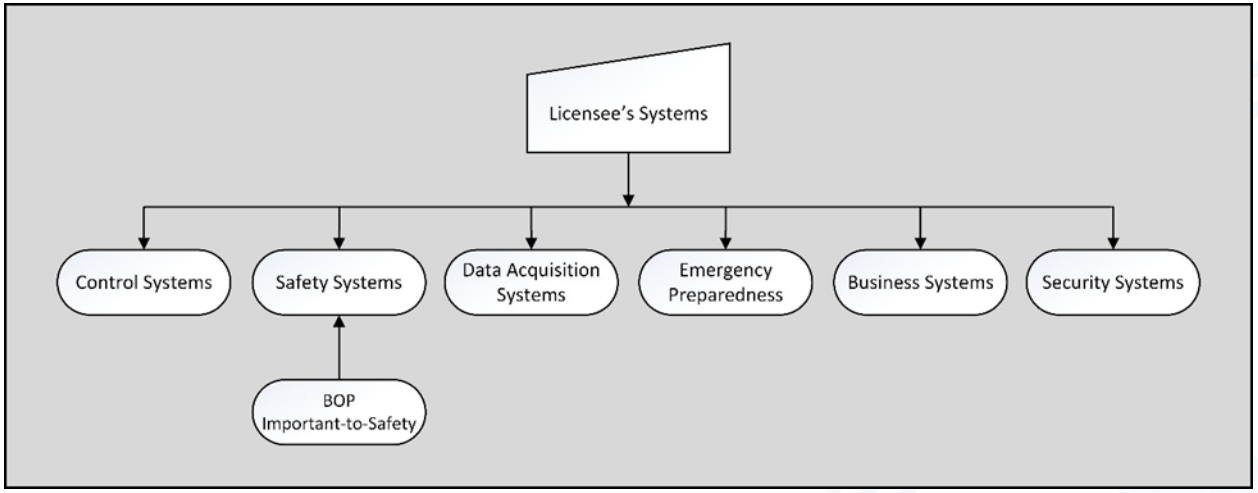
New to section C.3 Establishing and Implementing a Cyber Security Program

- Characterization of facility functions, including the identification of SSEP functions
- Characterization of threats to the facility
- Specification of requirements (including the CSP, the defensive architecture, and defense-in-depth methodology)
- Implementation of the requirements based on consequence analyses
- Validation and verification of the implementation of the cyber security program

Updates in DG-5061

Balance of Plant

Modification to section C.3.1.3 Identification of Critical Digital Assets

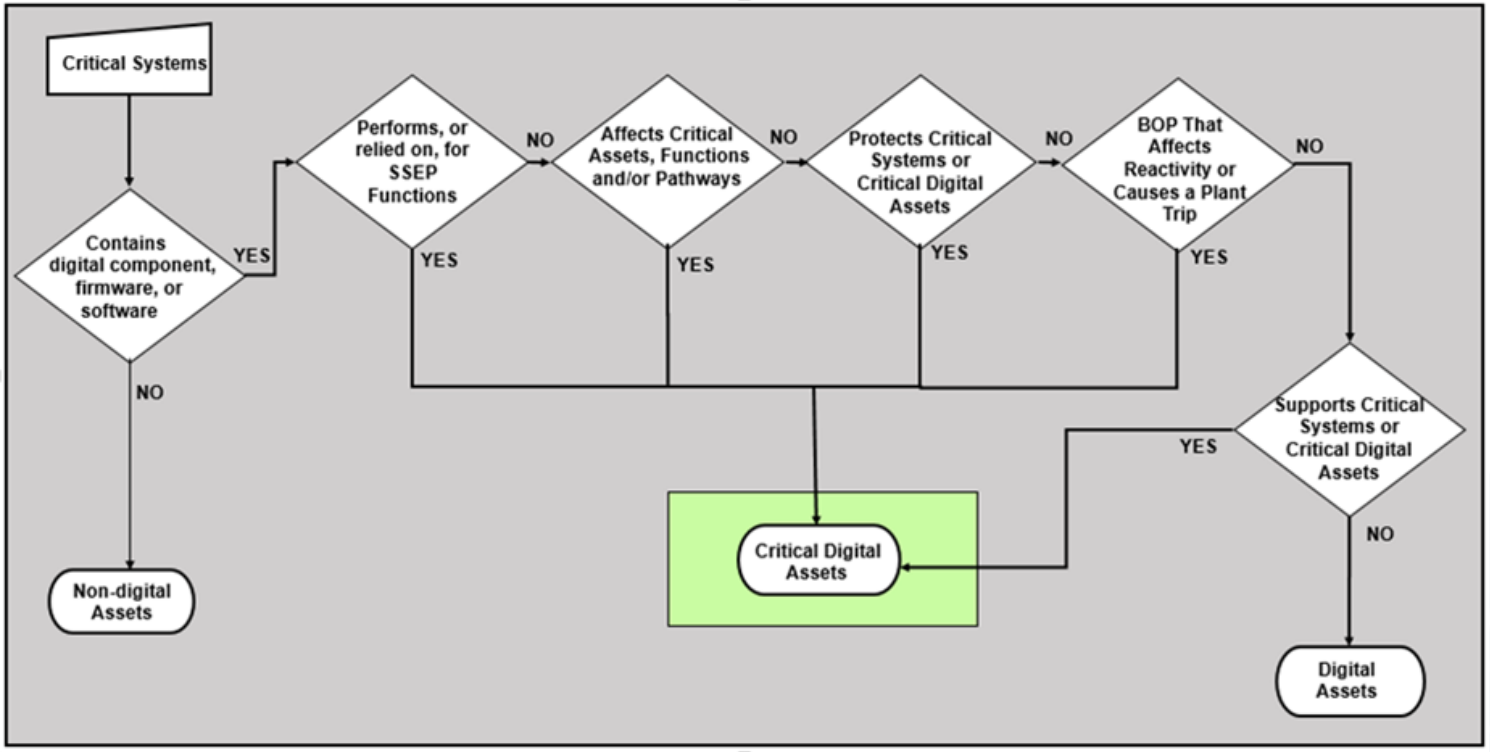


The identification of CSs should include those systems, equipment, and devices that (1) perform or are relied upon for SSEP functions, (2) affect SSEP functions or affect CSs or CDAs that perform SSEP functions, (3) provide a pathway to a CS or CDA that could be used to compromise, attack, or degrade an SSEP function, (4) support a CS or CDA, (5) protect any of the above from cyber attack up to and including the DBT, or (6) are BOP systems, equipment, and devices that affect reactivity and could result in an unplanned reactor shutdown or transient.

Updates in DG-5061

Identification of Critical Digital Assets

Modification to section C.3.1.3



Updates in DG-5061

Defense-in-Depth Protective Strategies

New text in section C.3.2 and section 3.3 Security Controls

Defensive strategy that employs multiple, diverse, and mutually-supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyber attack.

Updates in DG-5061

Defensive Architecture – Protect the SSEP function

New text in section C.3.2.1

- Functions are protected commensurate with their safety and security significance through the determination and use of appropriate security levels.
- Each function is implemented by one or more critical systems. A system's allocation to a security level is determined by its associated function with the highest safety or security significance.

Updates in DG-5061

Defensive Architecture – Communication from lower to higher security levels (vulnerability updates)

New text in section C.3.2.1

Initiation of communications from digital assets at lower security levels to CDAs at higher security levels should be implemented on a "deny-all, permit-by-exception" basis, and the exceptions should be supported by a complete justification and security risk analysis.

Updates in DG-5061

Defensive Architecture – Minimizing attack surfaces and pathways

New text to section C.3.2.1

- Applications, services, and protocols not necessary to support the design-basis function of the contained CDAs are eliminated.
- Implementation of the multiple, diverse technologies used within the plants addresses the attack surfaces and environments associated with the technologies so that the protections of the defensive architecture are not bypassed or circumvented.

Updates in DG-5061

Defensive Architecture – Minimizing attack surfaces and pathways

New text to section C.3.2.1

- For necessary and required firmware, software and/or data update of a digital asset protected behind a data diode, an acceptable way to implement the update that does not circumvent the data diode protection of wired connections in the defensive architecture is by implementing the multiple and diverse security measures that ensure:
  - the update does not contain known malware and
  - the integrity of the update is maintained during transport.

Updates in DG-5061

Security Controls – Use of alternate controls

Updated text to section C.3.3

- The various security objectives are explained in detail with examples.
- If a security control cannot be implemented, use alternative controls or countermeasures that provide at least an equivalent level of protection against the threat or attack vectors and vulnerabilities or weaknesses.

Updates in DG-5061

Security Controls – Consequence based, graded approach

Updated text to section C.3.3

- Analysis done in support of this consequence-based, graded approach should be rigorous and repeatable by ensuring reproducibility and consistency of the applied security controls posture.
- NEI 13-10 is cited as an approach deemed acceptable for use.

Updates in DG-5061

Technical Security Controls

Updated text to section C.3.3.1

- Applicants for design certification may incorporate technical security controls as part of the nuclear power reactor.

Added text to sections C.3.3.1.1 to C.3.3.1.5

- Text was added explaining the purpose of access control, audit and accountability, system and communication protection, identification and authentication, and system hardening.

Updates in DG-5061

Incident Response

Updated text to section C.3.3.2.6

- Cites 10 CFR 73.77 Cyber security event notifications
- Updated references to incident response documents generated by NIST and DHS Cybersecurity and Infrastructure Security Agency

Updates in DG-5061

System and Service Acquisitions

Updated text to section C.3.3.3.1

- Update cites Section 2.1 through Section 2.5 of RG 1.152, Rev. 3

Updates in DG-5061

Continuous Monitoring and Assessment

Updated text to section C.4.1

- Added more examples of continuous monitoring
  - continuous monitoring of inbound and outbound network traffic and analysis of event logs
  - periodic vulnerability scans and assessments
  - ongoing verification using established baseline configurations that CDAs are being protected commensurate with their safety and security significance
- Expanded text to discuss the importance of anomaly detection

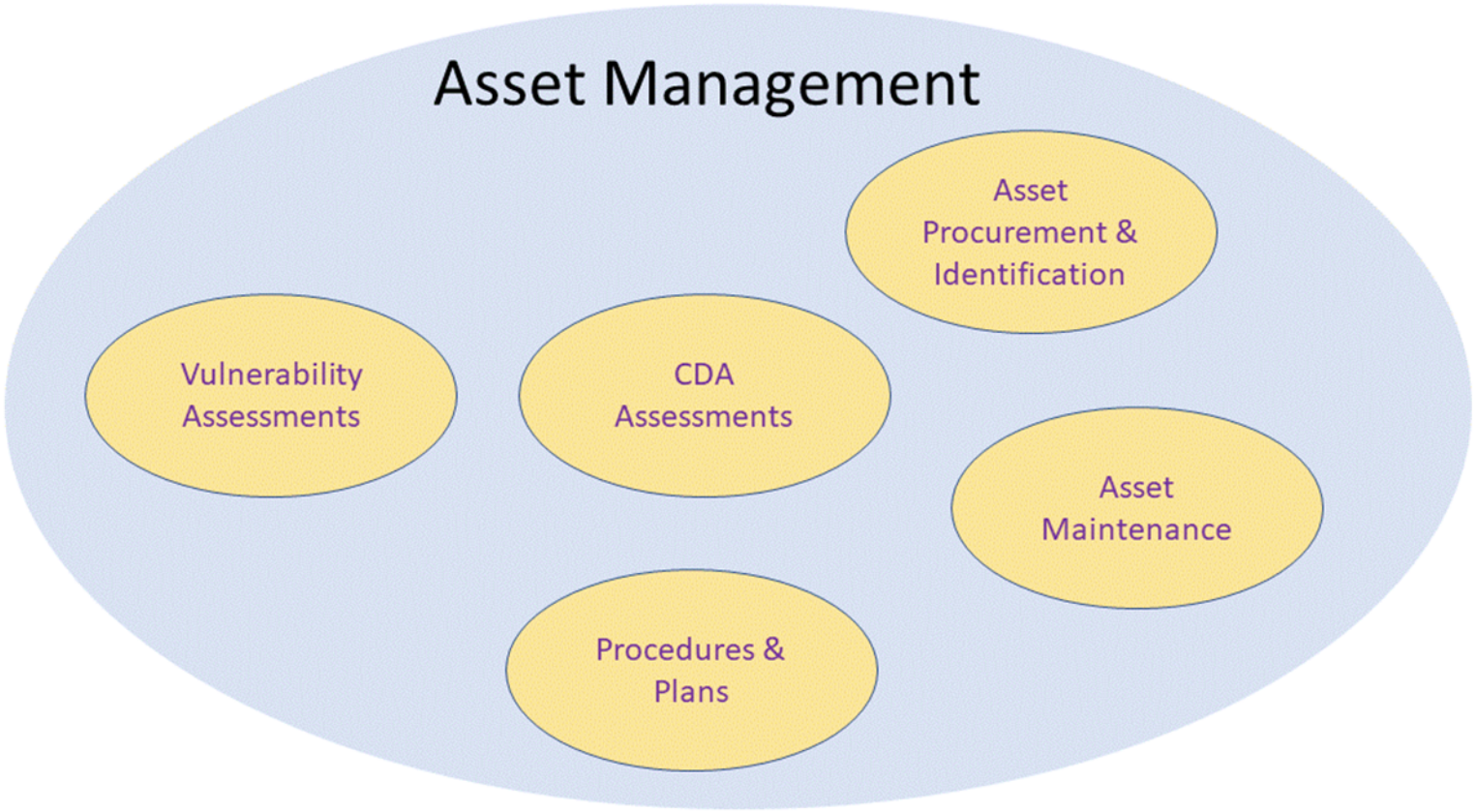
Updates in DG-5061

Effectiveness Analysis of Security Controls

Updated text to section C.4.1.2

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

Assessments and Plant Assets



Updates in DG-5061

Updates to Security Controls in Appendices B and C

- Control intent added to every security control
- Text added regarding reducing or eliminating attack surfaces and attack pathways
- Aligned with text in NIST 800-53 revision 5

U.S.NRC
Protecting People and the Environment

Appendices B & C (security controls)

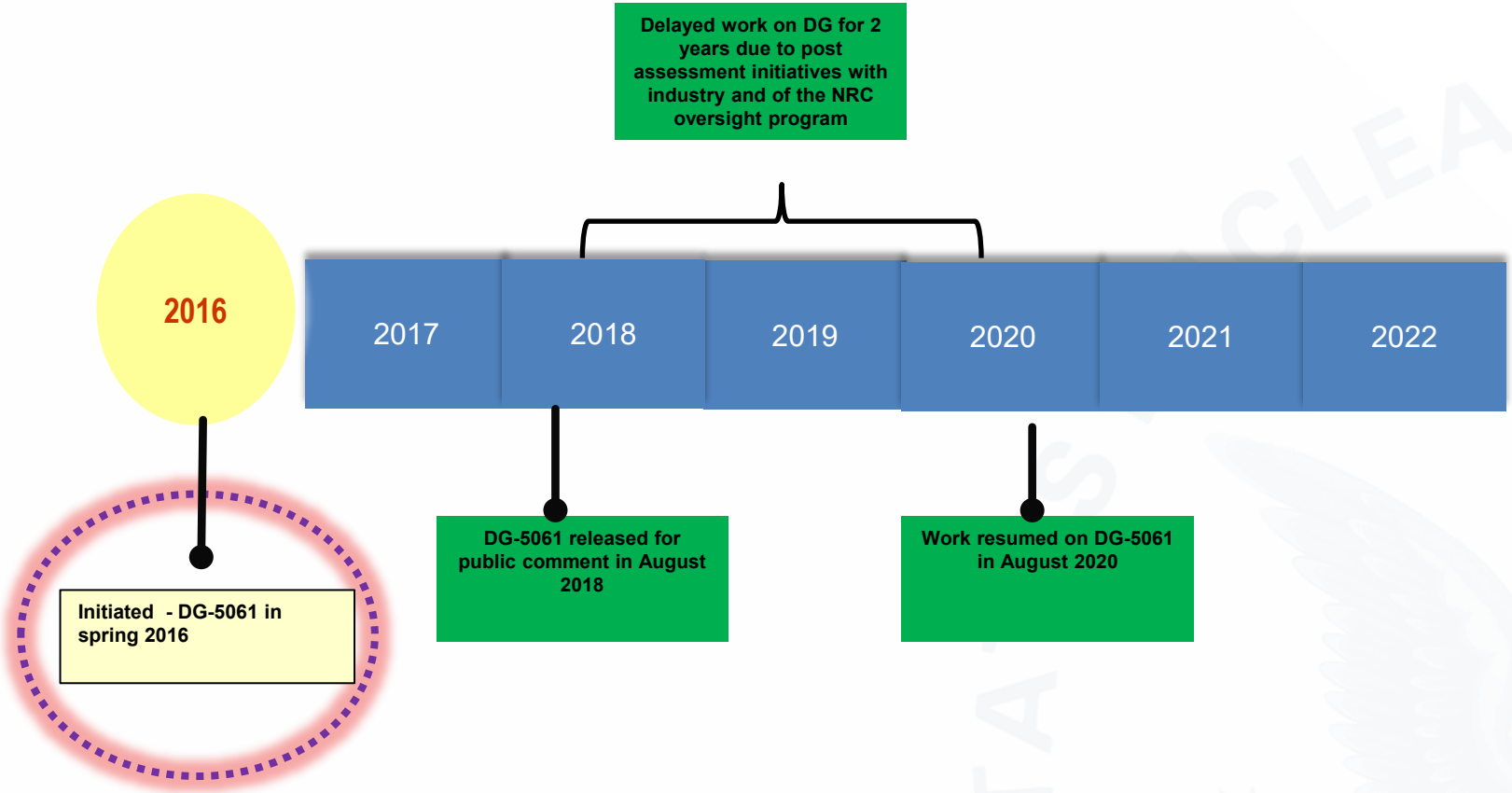
	DG-5061	NEI 08-09	Rationale for change/difference
B.1.9 Previous Logon Notification	Removed control		Intent covered in covered in logging/audit controls
B.1.11 Supervision and Review – Access Control	Removed control		Intent covered in covered in logging/audit controls
B.1.14 Automated Labeling	Removed 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

Other Changes

- Supply chain
  - Removed prescriptive guidance from Appendix C.12.5 Developer Security Testing and Evaluation and C.12.6 Licensee/Applicant Testing
  - Added text to evaluate attack surfaces and attack pathways
- Glossary
- References
- Numerous editorial changes

DG-5061 STATUS AND NEXT STEPS

DG-5061 Timeline



Timeline

Task	Date
RGGIB issues DG for Public	March 2022
Public Comment Period	2 months
Update and finalize the RG	9 months
Publish RG	1st quarter 2023

Conclusion

- Since 2012, licensees have implemented cyber security programs and the NRC has implemented effective oversight of the licensee's CSPs.
- No changes in staff's position in DG-5061, only clarifications and one new NRC regulation 73.77.
- The world has changed since RG 5.71 revision 0 was issued in 2010. DG-5061 reflects the lessons learned and prepares for the future.

Questions