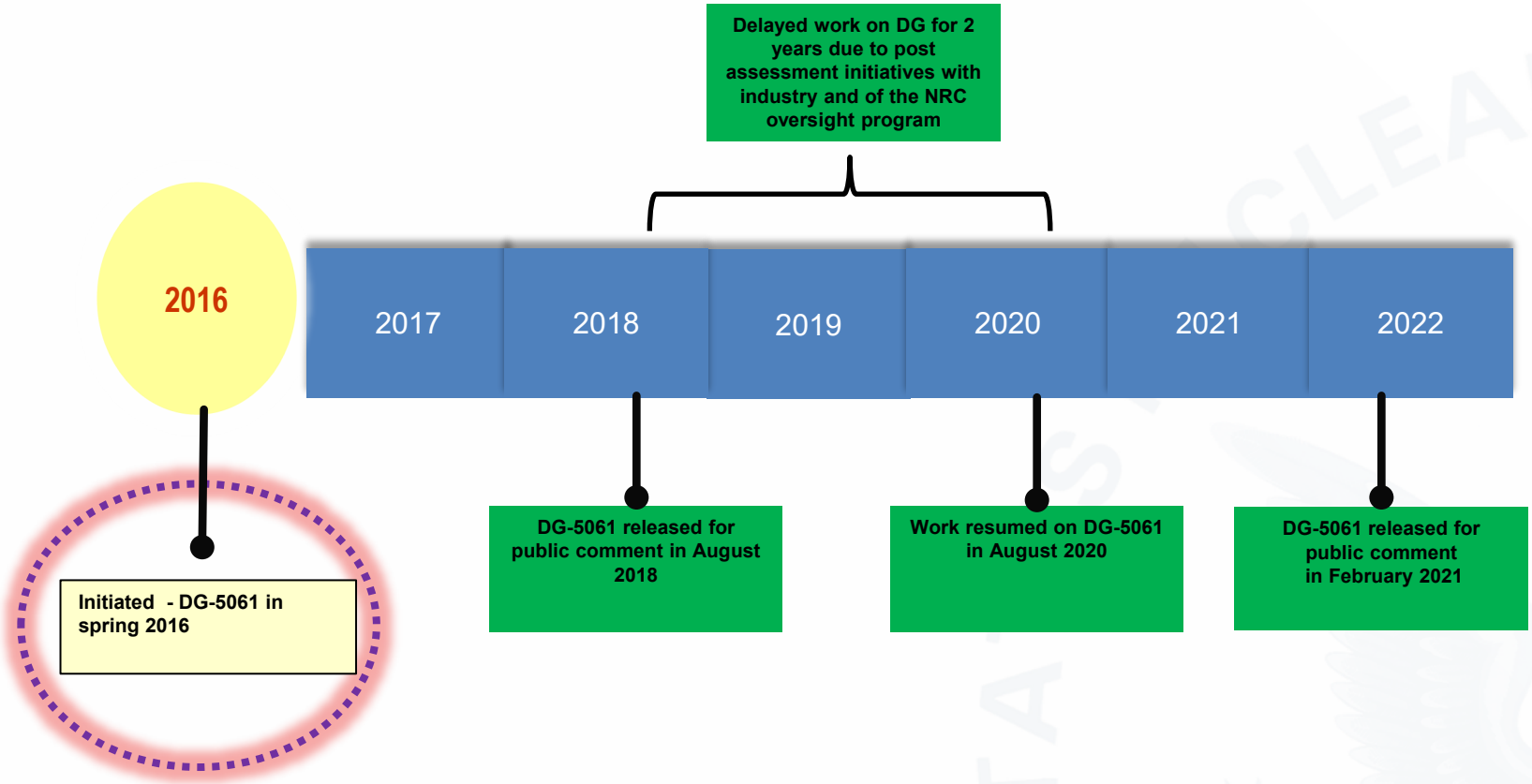
U.S.NRC
Protecting People and the Environment

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(Draft Guidance 5061)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

U.S.NRC
Protecting People and the Environment

DG-5061 Timeline



U.S.NRC
Protecting People and the Environment

Estimated Timeline

Task	Date
FRN announces DG is issued for Public Comment; The FRN Docket Number is Docket ID NRC–2021–0143. ML21095A329 is the ADAMS No. for the DG.	March 3, 2022
Public Comment Period for DG Begins	March 3, 2022
Information Public Meeting with a Q & A session	Early April 2022
Public Comment Period for DG Ends	May 2, 2022
Publish RG	March 2023

DG-5061 Updates in 2018

- Clarify existing interpretation of regulations based on lessons learned from Milestones 1 –7 inspections
- New regulation since 2010
  - "Cyber security event notification" 10 CFR 73.77
- Changes in NIST SP 800-53 r4 "Recommended Security Controls for Federal Information Systems"
- New IAEA security guidance
- Commission direction regarding Balance of Plant equipment

U.S.NRC
Protecting People and the Environment

DG-5061 Updates in 2020 & 2021

- Discussed Risk Informed Cyber Security
- Emphasized the need for accurate Critical Digital Assets (CDAs) assessments
- Leveraged new international standards/guidance and updated NIST guidance on cyber security
- Addressed public comments to 2018 DG-5061
- Generated updates in response to Advisory Committee on Reactor Safeguards comments (ML22014A419 and ML21175A332)

U.S.NRC
Protecting People and the Environment

Updates in DG-5061

Section	Reason for Change
C.3	Added text for Risk Informed Cyber Security
C.3.1.3	Added Balance of Plant asset identification
C 3.1.3	Added new decision points and text for identifying CDAs
C 3.2.1 & C 3.3	Updated text for Defense in Depth protective strategies
C 3.2.1	Updated text for Defensive Architecture for protecting functions, addressing vulnerabilities, and minimizing attack surfaces and pathways
C.3.3	Updated text regarding the use of alternate controls
C.3.3	Updated text to clarify the use of a consequence based, graded approach in applying security controls
Background C.3.3.1	Added text stating technical controls can be incorporated during design certification
C.3.3.1.1 to C.3.3.1.5	Text was added explaining the purpose of various technical security control groups
Background C.3.3.2.6	Text was updated to cite new cyber event notification rule and guidance

U.S.NRC
Protecting People and the Environment

Updates in DG-5061

Section	Reason for Change
Background, C.3.3.3.1	Updated reference to sections of RG 1.152, Rev. 3
C.4.1	Expanded examples of Continuous Monitoring; discussion of anomaly detection
C.4.1.2	Added new text on using metrics for effectiveness analysis
C 3.1.3, C.3.3.1.5,C.4.1, C.4.1.3,C.4.2.1,C.4.2.2, multiple sections in Appendix A, various controls in Appendices B & C	Added text regarding quality CDA assessments
Appendices B & C	Clarification of all security controls
Glossary	Added new terms and definitions; clarified terms in Rev. 0
References	Updated references
Throughout document	Editorial changes based on OGC comments, public comments, peer reviews

Conclusion

- Licensees have implemented cyber security programs and the NRC has implemented effective oversight of licensees' cyber security programs.
- 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 and positions the guidance for future licensees.