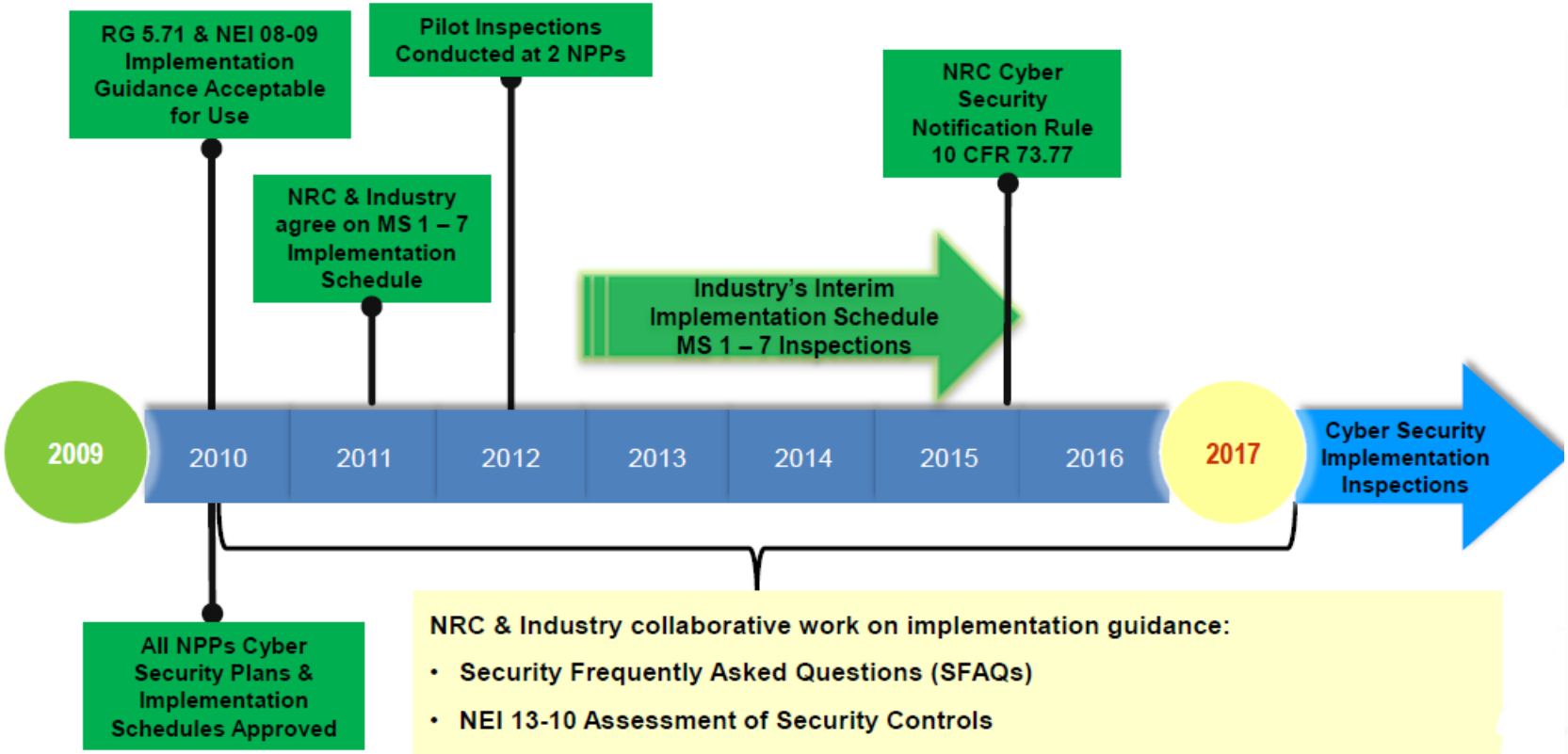
U.S.NRC
Protecting People and the Environment

Full Implementation Cyber Security Inspections

James Beardsley, Chief
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

Cyber Security Inspections Timeline

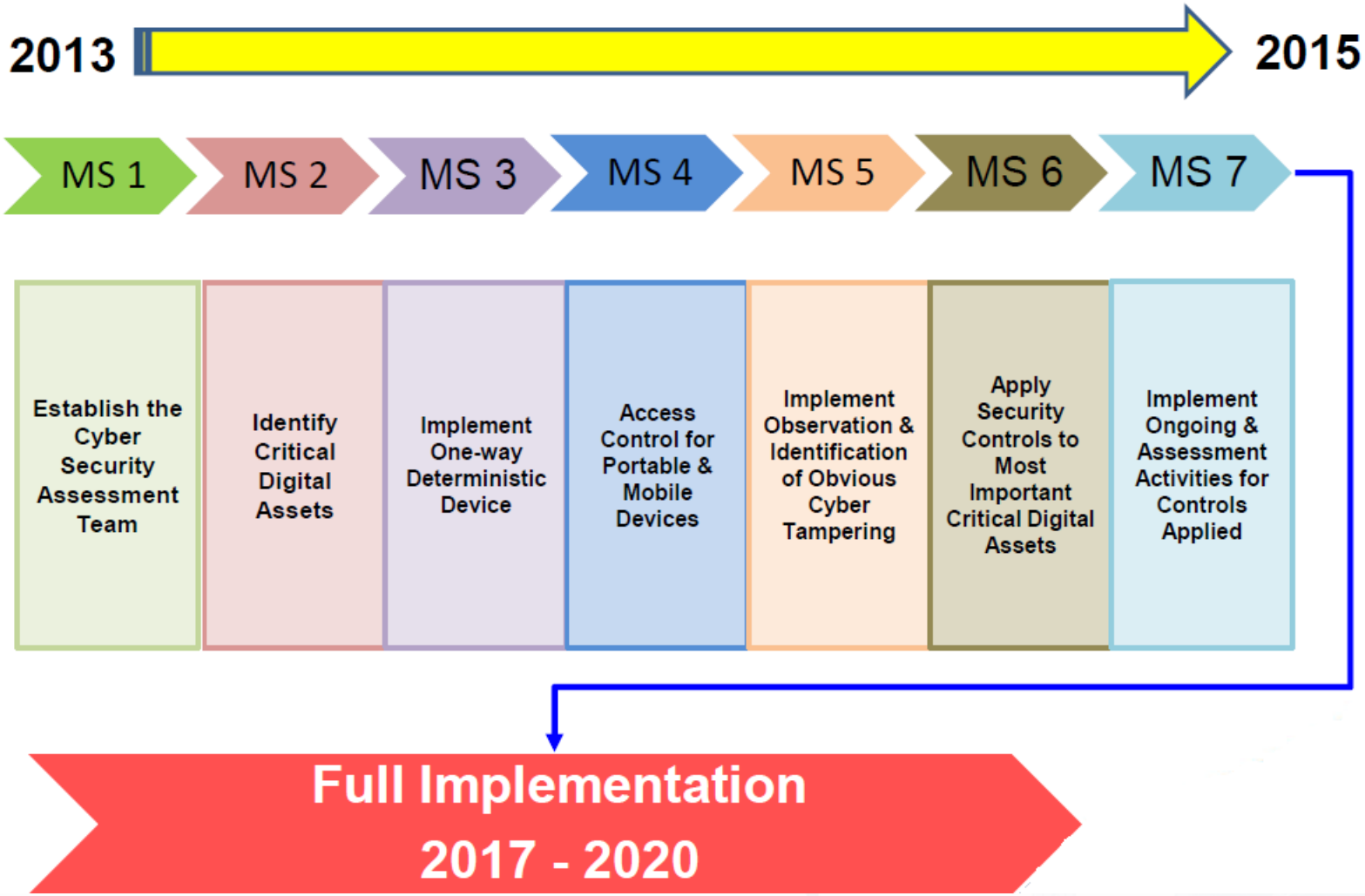


NRC & Industry collaborative work on implementation guidance:

- Security Frequently Asked Questions (SFAQs)
- NEI 13-10 Assessment of Security Controls
- NRC Participates in Industry Workshops (MS 1 – 7 Inspections Lessons Learned)
- Tabletops to assess inspection procedure
- Development of Additional Guidance for Implementation Schedules
- Meetings with the Industry

U.S.NRC
Protecting People and the Environment

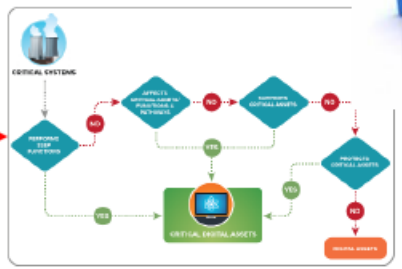
Early Interim Inspections

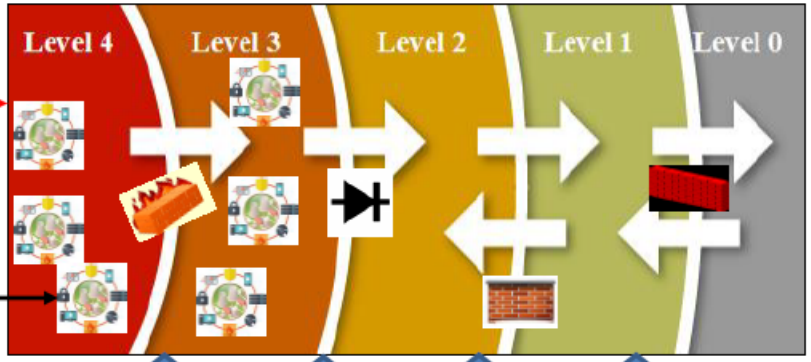


U.S.NRC
Protecting People and the Environment

Full Implementation Inspections

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

Schedule of Full Implementation Inspections

YEAR	NUMBER OF INSPECTIONS
2017	2
2018	18
2019	24*
2020	13*

* Some inspections may shift from 2019 to 2020

U.S.NRC
Protecting People and the Environment

Some Inspection Areas of Focus

- **CDA Assessments**
  - Evidence of knowledge of attack surfaces, attack pathways
  - Adequate protection
    - Use of alternate controls
    - Protection of devices that protect multiple CDAs
  - Clearly documenting the assessments and the analysis associated with the implementation of alternate controls
- **Management of Cyber Risks**
  - Ongoing threat analysis
  - Ongoing vulnerability analysis
  - Continuous monitoring of the cyber security posture of the plant

U.S.NRC
Protecting People and the Environment

Some Inspection Areas of Focus

- **Enforcement of Defensive Architecture**
  - Verification of information flow enforcement
  - Verification of protection of pathways within and between security levels
  - Protection of boundary protection devices
  - Verification of mechanisms in place to detect and respond to attempts to circumvent the defensive architecture protections
    - Management of Portable Media and Mobile Devices
    - Procedures regarding Supply Chain

U.S.NRC
Protecting People and the Environment

Some Inspection Areas of Focus

- **Defense in Depth**
  - The ability to detect, respond to, and recover from a cyber attack
  - The application of multiple layers of defensive security controls throughout the system with the intent of providing overlapping defenses

Current Status of Inspections

- **As of August 20 2018, thirteen inspections have been completed.**
- **Areas for improvement:**
  - Additional guidance on portable media & mobile device program
  - Guidance on periodicity for ongoing monitoring & assessment modifications.
  - Additional guidance on critical digital asset assessments (direct vs indirect).

Future Plans

- **In 2019 NSIR plans to conduct an overall assessment of the power reactor cyber security program to include:**
  - Effectiveness of the 10 CFR 73.54 rule
  - Effectiveness of the guidance and licensee implementation of the rule
  - Effectiveness of the full implementation inspection program
  - External factors and lessons learned over the course of program implementation
- **The assessment will result in a paper to the Commission.**

Questions