U.S.NRC
Protecting People and the Environment

Lessons Learned During Milestones 1 - 7 Cybersecurity Inspections of Nuclear Power Plants

Kim Lawson-Jenkins
Cyber Security Specialist
Cyber Security Directorate
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission

U.S.NRC
Protecting People and the Environment

Background

- **2002-2003:** NRC included the first cyber requirements in Physical Security and Design Basis Threat Orders
- **2005:** NRC supported industry voluntary cyber program (NEI 04-04)
- **2009:** 10 CFR 73.54, Cyber Security Rule
- **2010**: NRC Regulatory Guidance 5.71 was released.
- **2012:** Implementation/Oversight of Interim Cyber Security Milestones.
- **2013-2015:** Milestone 1-7 Inspections
- **2014-2015:** Endorsed NEI 13-10 Cyber Security Control Assessments

U.S.NRC
Protecting People and the Environment

Cyber Security Milestones 1 - 7

1. Establishment of a Cyber Security Assessment Team (CSAT)
2. Identification of Critical Systems (CSs)/Critical Digital Assets (CDAs)
3. Installation of Protective Devices between lower and higher security levels in the Security Defensive Architecture
4. Portable Media and Mobile Device protections
5. Cyber Tampering – Insider Mitigation Rounds
6. Apply Cybersecurity Controls to a Select Group of CDAs
7. Ongoing Monitoring and Assessments of Applied Cybersecurity Controls

Lesson Learned #1

The Need for Better Guidance on Identification of Digital Assets

Identifying the internal functionality and components of CDAs

Licensees should have knowledge of:

- How a device performs a function
- Hardware, software, and firmware that could potentially be used as an attack surface by threat actors by exploiting vulnerabilities in the device

Additional analysis of attack pathways may be needed

- Support functions (e.g. maintenance and test tools)
- Protection mechanisms (e.g., malware on vendor website or boundary protective device)

Lesson Learned #2

The Need for Better Guidance on Selecting Security Controls

- Licensees have identified thousands of CDAs at plants.
- Industry and the NRC have developed additional guidance to streamline the process for selecting controls.
- Industry must perform a consequence analysis to determine:
  - the functionality of the CDA.
  - the impact that a cyber attack could have on the CDA
- CDA examples
  - Rosemount digital transmitters
  - Plant Security Computer

Lesson Learned #3

The Need for Better Guidance on Securing Portable Media and Mobile Devices (PMMD)

Because PMMD bypasses the air gap that protects most CDAs, ensuring these devices are protected is important.

Additional guidance was needed to:

- Provide a better definition of PMMD
- Ensure secure handling of these devices
- Establish procedures for secure data transfer from a vendor to portable media that would be inserted into a CDA

Lesson Learned #4

The Need for Better Guidance for Determining the Effectiveness of Cybersecurity Programs

- Additional guidance was needed regarding effective implementation of security controls

Example of a security assurance statement -

A CDA in a vital area of the plant is effectively protected from malware.

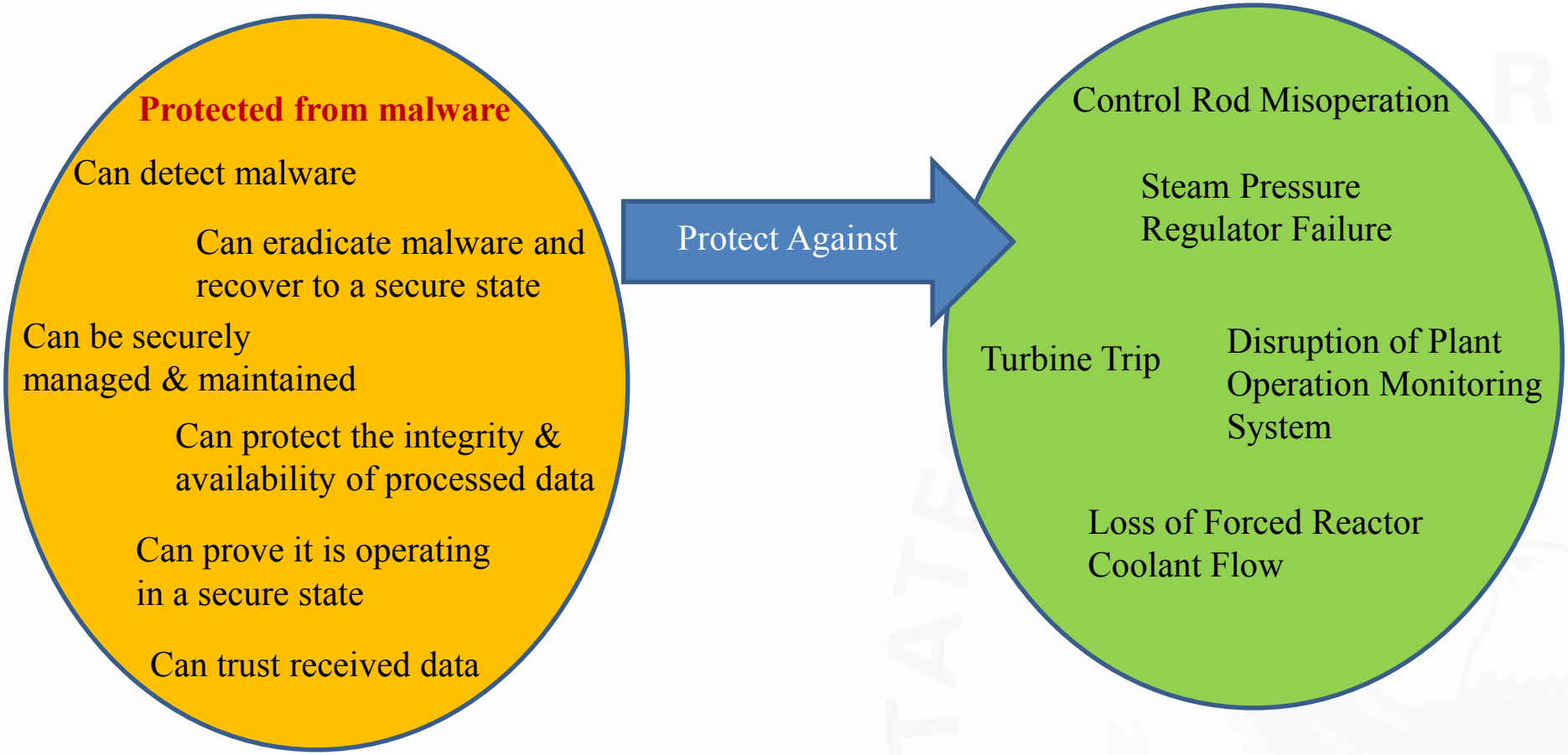
Evidence provided by implementing the following security controls:

- Host intrusion detection system
- Flaw remediation
- Malicious code protection
- Security functionality verification
- Security alerts and advisories
- Software and information integrity

What is the Effect on SSEP Functions?

Defense-in-depth protection of critical digital assets

Assure safety, important to safety, security, & emergency preparedness functions are protected against cyber attacks



Critical digital assets are located in critical systems that perform SSEP functions

Work with Stakeholders

- NRC is working with stakeholders to improve industry guidance.
- NRC is currently reviewing and revising regulatory guidance based on lessons learned.
- NRC is working to streamline the process for gathering information prior to inspections.

Full Implementation Cybersecurity Inspections

- Additional focus areas include:
  - Detection, Response, Elimination
  - Defense-in-Depth
  - Supply Chain
  - Data Integrity
  - Program Monitoring, Assessment, Configuration, and Change Management
  - Attack Mitigation, Incident Response, and Contingency Planning

Full Implementation Cybersecurity Inspections

- Staff is working on processes to streamline resolution of policy questions and support consistency during the inspections.
- Inspections scheduled to begin in mid 2017.
- The inspection program will take 2-3 years to complete.

Revision of RG 5.71

RG 5.71 Revision Work

- Original version released in 2010
- Work began in April 2016
- Policy & regulatory changes since 2010
  - Balance of Plant
  - Cyber event notification
- Milestones 1-7 inspections lessons learned
- New versions of NIST SP 800-53 and NIST 800-82

Scope of Updates

- **Clarify interpretation of existing regulations**
- Changes apply going forward
- Not imposing any new requirements on licensees with operating plants or plants currently under construction
- Each control is being reviewed using updated guidance and consideration of the current threat environment to ensure all controls are necessary and effective in the implementation of 10 CFR 73.54.

High Value Updates in RG 5.71

1. Protection of boundary protection devices and maintenance & test equipment.
2. The concept of self-protection
   - audits, incident response, security functionality verification, tamper resistance & detection, unauthorized access indications, indications of compromise
3. Determining the effectiveness of a Cyber Security Plan
4. Glossary
5. Additional text to explain the protections afforded by implementing individual controls

So what are we NOT changing?

- No updates are planned for Appendix A – Generic Cyber Security Template
- No new technical controls will be added to Appendix B.
- No new Operational & Management controls will be added to Appendix C.

Schedule

- RG 5.71 revision 1 will be available for public comment during summer 2017

Questions