Cyber Security Rulemaking

Monday July 13, 2015
2:00pm-4:30pm

Matt Bartlett
Brian Smith

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

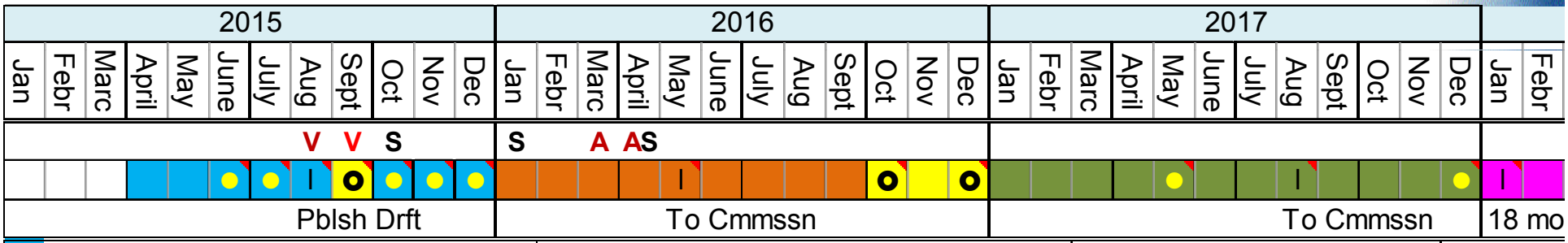
Agenda

- Status of Rulemaking
- Cyber Security Rulemaking Objective
- Draft Regulatory Framework
- Draft Guidance Development
- Site visits

Status of Rulemaking

Rulemaking to comply with SRM-SECY-14-0147 (ML15083A175)

Schedule



= Reg. Basis/Draft Guidance	↓ = Change occurred below arrow
= Proposed Rule/Draft Guidance	V = Site Audit
= Final Rule/Final Guidance	A = ACRS Meeting
= Public Interaction	S = Steering Committee
= Implementation	
= Meeting occurs	
I = Marks a milestone with text	

http://fusion.nrc.gov/nmss/team/fcss/CyberSec/GntChrts/Gantt%20Chart%20for%20Cyber%20Rulemaking.xlsx

Publish Draft Regulatory Basis end of August

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cyber Security Rulemaking Objective

What are we trying to prevent?

A cyber attack resulting in

- A safety/security consequence of concern or
- The compromise of a function needed to prevent, mitigate, or respond to a safety/security event with a potential consequence of concern

Draft consequences of concern

- Releases of radioactive materials or chemicals resulting in significant exposure to workers and members of the public
- Nuclear criticalities
- Loss/theft/diversion of special nuclear material
- Loss/theft of classified information
- Inability to maintain communications during normal and emergency operations

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Framework

How do we propose to prevent these consequences?

Risk-informed, performance based, and graded approach in applying the requirements informed by:

- Power reactor cyber security rule (10 CFR 73.54) and the lessons learned
- Uniqueness of fuel cycle facilities
- Insights learned from site visits
- Industry standards

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Framework

Digital assets currently anticipated to be within scope:

Those digital assets associated with:

- Safety
- Security (physical and information)
- Emergency Preparedness
- Material Control and Accounting (SSEPMCA)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Framework

How is the draft approach risk-informed and consequence based?

The NRC staff currently envisions that the scope of the framework will be limited to digital assets associated with risk significant functions, as identified by the ISA, security plans, emergency plan, and MC&A plan as commitments to satisfy risk-informed regulations (Parts 40, 70, 73, and 74).

- IROFS are required to prevent or mitigate significant exposure events
- IROFS are required to prevent nuclear criticalities
- Physical security and MC&A programs are required to prevent the loss/theft/diversion of significant quantities of SNM
- Information security programs are required to prevent the loss/theft of classified information
- Emergency preparedness programs are required to facilitate the communications between licensees and the NRC and local responders

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Framework

Considerations to avoid unintended consequences to safety and security programs

- The cyber program would utilize the ISA and existing security and MC&A plans to inform the cyber program but not require their revision
- Cyber controls would make digital IROFS and digital assets used in implementation of the security and MC&A plans more available and reliable

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Framework

Screening - determine the applicable digital assets

Consider all digital assets on site

↓

Identify SSEPMCA digital assets
- Certain IROFS
- Digital assets used to implement security, emergency preparedness, material control and accounting plans
- Associated systems

↓

Apply screening method to digital assets

↓

Final set of digital assets that need controls

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Regulatory Framework

Application of cyber controls

Use consensus standard approach (NRC provided risk assessment based on facility type and SSEPMCA)

Things to consider when evaluating cyber controls

- Utilize existing controls and program elements (e.g., training, configuration management program, physical security controls)
- Justify not applying certain controls
- Apply certain controls to the entire network rather than individual digital assets on a network
- Use templates for similar digital assets

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Draft Guidance Development

Create a new Regulatory Guide – available with the proposed rule

Use industry recognized and consensus standards, e.g.,

- NIST SP 800-53 rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-82 rev. 2, *Guide to Industrial Control Systems (ICS) Security*
- NIST SP 800-37, rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*

We would welcome any input on other standards to consider

A screening method for digital assets would be included in the guidance

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Site Visits

- Conduct visits at a range of facilities
- Timeframe: August and September 2015
- Provide audit plan and calls in advance

Goals:

- Gather information on voluntary efforts
- Understand existing programs
- Obtain lessons learned
- Feedback on useful standards

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Conclusions

- Draft regulatory basis for comment during September
- Framework: risk-informed, graded, performance based, facility-type approach addressing SSEPMCA
- Regulatory guide based on standards and provide a screening method
- Additional interactions with stakeholders