Cyber Security Proposed Rulemaking for Fuel Cycle Facilities

Public Meeting

Thursday, March 17, 2016

Fuel Cycle Cyber Security
Rulemaking Working Group

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

Category 3 Meeting

This is a Category 3 Meeting: Public participation is actively sought for this meeting to fully engage stakeholders in discussions regarding the regulatory issues.

Handouts, introductions, webinar, and opening remarks.

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

Agenda Overview

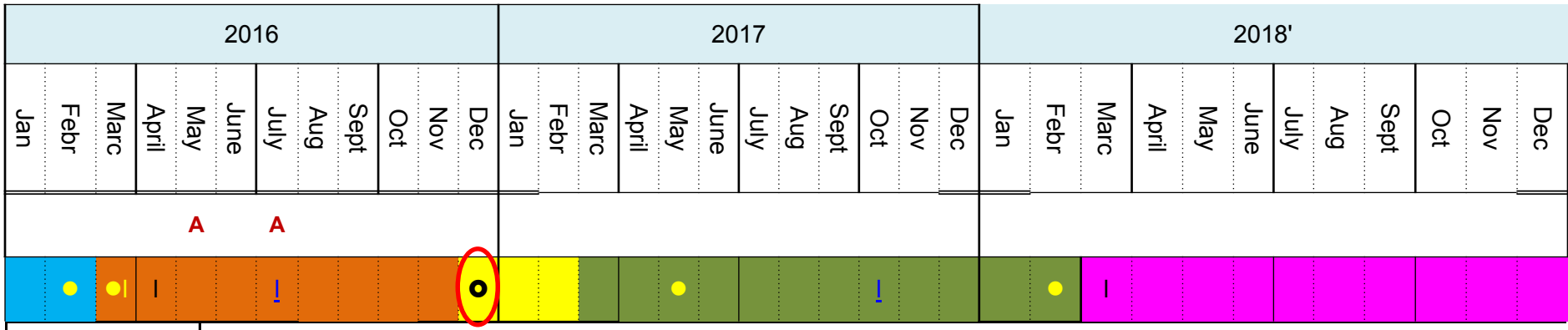
- **Session 1 (8:15am-9:30am)**
  Proposed Rulemaking Considerations
- **Session 2 (9:30am-10:30am)**
  Proposed Rulemaking Insights Gained from the Implementation of 10 CFR 73.54
- **Session 3 (10:45am-12:00pm)**
  Identification of Digital Assets, Determination of Support Systems, and Application of Screening Methodology
- **Session 4 (1:00pm-3:00pm)**
  Cyber Security Controls Overview, Independent Assessment, Role of the Authorizing Official, and Cyber Security Control Monitoring

Agenda – Session 1
Proposed Rulemaking Considerations

- Updated timeline
- Regulatory basis and comment resolution
- Review concepts of the proposed rulemaking
- Additional feedback

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

Introduction and Timeline



Feb/2016	Call with Stakeholders on Draft Rule
Mar/2016	Public meeting at FOC on proposed rule and complete Reg. Basis and notify Commission
Apr/2016	Place proposed rule package into concurrence
May/2016	ACRS sub-committee meeting
Jul/2016	Brief full ACRS committee
Jul/2016	Draft proposed rule language sent to Commission for review
Dec/2016	Public meeting to discuss comments received
May/2017	Public meeting to discuss how comments were addressed
Oct/2017	Draft final rule language sent to Commission for review
Feb/2018	Hold public meeting to discuss final rule and implementation
Mar/2018	SRM-SECY-14-0147 directs an 18 month implementation period

- = Reg. Basis/Draft Guidance
- = Proposed Rule/Draft Guidance
- = Final Rule/Final Guidance
- = Public Interaction
- = Implementation
- = Meeting occurs
- I = Marks a milestone with text
- V = Site Visit
- A = ACRS Meeting

December 2016 - comment period expected to begin on proposed rule

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

Regulatory Basis

1. Completed on March 03, 2016 - ML15355A461

2. Comment resolution, 9 letters summarized to 27 responses - ML15355A469

3. Publish in the *Federal Register* in March 2016

4. NRC transition to proposed rulemaking package

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

Proposed Rulemaking Considerations

1. Applicability
2. Cyber security program objectives
3. Consequences of concern
4. Risk management framework
5. Cyber security plan
6. Periodic review of the program
7. Reauthorization to operate
8. Event reporting
9. Records

Handout of Proposed Rule Concepts (ML16054A187)

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

Feedback on Proposed Rule Concepts

- NRC considering feedback from February 18, 2016 (meeting summary – ML16048A052)
  - Scope of assets – “digital” and support systems
  - Only applies some of the intermediate consequences listed in 10 CFR 70.61(c)
  - Consider unclassified networks approved by other federal agencies
  - Clarity needed on independent assessment
  - Clarity needed on role of authorizing official
  - Timeframes for review and reauthorization
  - Consider scope of event logging
  - Text edits
- Additional feedback on proposed rulemaking concepts?

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

Conclusion: Session 1

- Comment period in December, 2016, subject to Commission approval
- Developing draft proposed rule language package
- Address stakeholder feedback

Agenda – Session 2
Proposed Rulemaking Insight Gained from the Implementation of 10 CFR 73.54

- Overall approach – proposed rulemaking focuses on risk management framework
- Identifying digital assets
- Applying a risk-informed screening process
- Tailoring controls and recognizing alternate controls
- Establishing a phased implementation schedule with firm deadlines

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

Overall Approach

- Adoption and modification of 10 CFR 73.54 and RG 5.71 was considered
- Alternative approach: similar to NIST Risk Management Framework (NIST SP 800-37, rev. 1)
  - Advantages
    - Less prescriptive
    - Allows licensees to make some risk-based decisions
    - Inspections focused on program rather than control implementation
  - For program effectiveness, licensees must communicate and document risk acceptance ("authorization" step of risk management framework)

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

Identifying Digital Assets

- Risk-inform the selection of digital assets that require protection
- Consequence-based approach vs. adverse impact to functions
- Proposed regulation will provide clear language
- Specific guidance for scoping and screening
- “Active” and “latent” consequence analysis similar to NEI 13-10 “direct” and “indirect”

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

Applying a Risk-Informed Screening Process

- Screening process will allow licensees to leverage existing programs or measures (e.g., items-relied-on-for-safety (IROFS), uncredited controls, physical security, compensatory measures, etc)
- No minimum number of resultant digital assets
- Digital assets can be re-evaluated at any time

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

Tailoring Controls and Recognizing Alternate Controls

- Intent is to provide greater flexibility by applying controls in a graded, risk-informed manner
- Licensees will establish their own baseline control set at the program level, subject to NRC approval
- Licensees may satisfy a control by meeting security objective
- Control implementation may be satisfied by existing measures
- Technical control implementation and effectiveness will be assessed by the independent assessor
- Authorizing Official will have the ability to accept residual risk identified by assessor

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

Establishing a Phased Implementation Schedule with Firm Deadlines

- Intent is to ensure licensee cyber security program meets regulatory requirements prior to focusing on technical implementation
  - Phase 1 (interim milestone) will focus on program implementation and identification of digital assets
  - Phase 2 (full implementation)
- Final implementation date will be contained in the final rule

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

Conclusion: Session 2

- Discussed insights gained
- Different approaches
  - Risk management
  - Screening of digital assets
  - Tailoring of controls
  - Implementation

Agenda – Session 3
Identification of Digital Assets, Determination of Support Systems, and Application of Screening Methodology

- Identification of digital assets is based on the consequences of concern
- Define a clear boundary for support systems
- Apply a risk-informed screening methodology

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

Identification of Digital Assets

Protect digital assets associated with safety, security, and safeguards (3S) functions from cyber attacks that could:

- directly result in a safety consequence of concern (i.e., active); or
- compromise a function needed to prevent, mitigate, or respond to a 3S event associated with a consequence of concern (i.e., latent).

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

Active Consequences of Concern

The cyber attack DIRECTLY CAUSES one of the following:

- A radiological exposure of:
  - 25 rem or greater for any individual; or
  - 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or
- An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.

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

Active Consequences of Concern (continued)

- May use the ISA to identify areas of facility to consider

- Credit barriers that prevent consequence of concern

Examples:

Digital asset compromised to increase exposure

Digital asset manipulated to create a spill

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

Latent Consequences of Concern - Safety

Compromise of a function **NEEDED TO PREVENT, MITIGATE, OR RESPOND** to a event associated with one or more of the following:

- A radiological exposure of:
  - 25 rem or greater for any individual; or
  - 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or

- An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.

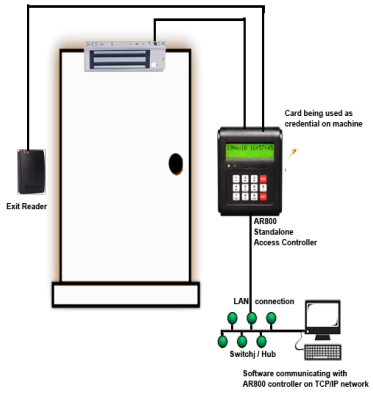
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Latent Consequences of Concern – Safety (continued)

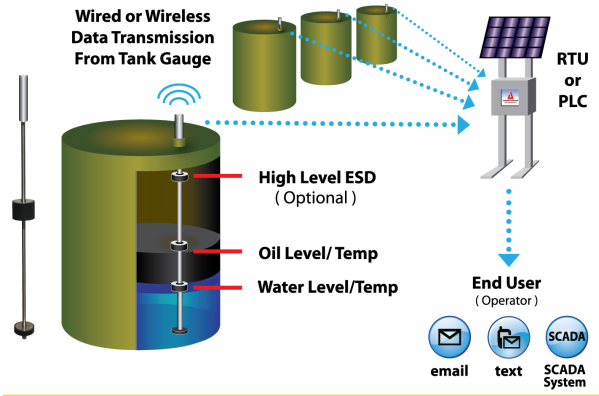
- May use the ISA to assist identification of digital assets
- Analyze "digital asset" – not necessarily a "digital IROFS"
- Evaluate digital assets within the IROFS boundary

Examples:

Disable interlock to high radiation area



Compromise digital gauge on a chemical tank



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

Latent Consequences of Concern - Security and Safeguards

Compromise of a function **NEEDED TO PREVENT, MITIGATE, OR RESPOND** to one or more of the following:

- Unauthorized removal of special nuclear material of moderate strategic significance as specified in 10 CFR 73.67(d);
- Loss of control and accounting of special nuclear material of moderate strategic significance as specified in 10 CFR 74.41(a)(1)-(4); or
- Loss or unauthorized disclosure of classified information.

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

Latent Consequences of Concern - Security and Safeguards (continued)

- Use security and MC&A plans to inform analysis
- Security considerations: intrusion detection, barriers, surveillance, detection, communications, access control, physical protection of classified information
- Safeguards consideration: track the types, quantities and locations of material, maintain inventory, detect loss

Examples:

Disable monitoring of access	Compromise controlled access barriers	Incorrect tracking of material

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

Latent Consequences of Concern - Design Basis Threat

Applies to licensee authorized to possess or use a formula quantity of strategic special nuclear material (SSNM), as defined in 10 CFR 73.2.

- Compromise a function **NEEDED TO PREVENT, MITIGATE, OR RESPOND** to:
  - Radiological sabotage,
  - Theft or diversion of SSNM, or
  - Loss of control and accounting of formula quantities of SSNM.

Latent Consequences of Concern - Design Basis Threat (continued)

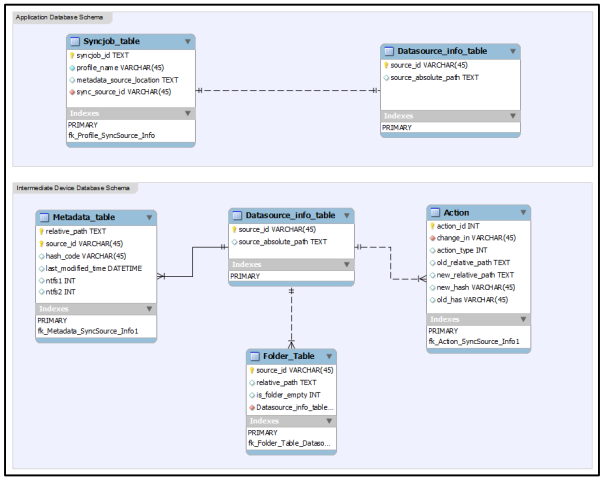
Digital assets used to:

- protect against radiological sabotage
- prevent theft or diversion of special nuclear material
- maintain a material control and accounting system

Examples:

Compromise central alarm station

Modify the tracking database



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

Support Systems

- Look at input from other assets to determine a boundary
- Effects on digital asset from loss of power, HVAC, calibration equipment, diagnostic equipment, etc

Active – What elements could trigger the digital asset to cause the consequence of concern?

Airborne contamination

Controller within scope

Update to software within scope

Latent – What is needed to perform the function?

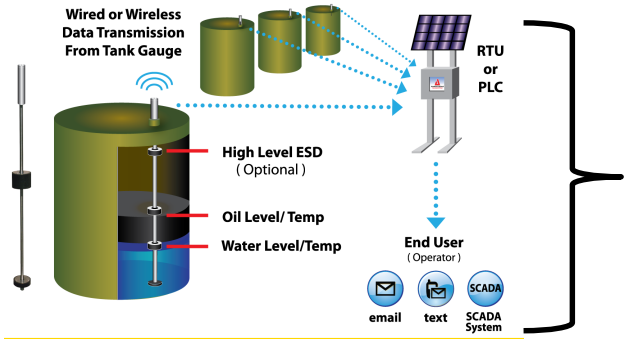
Central alarm station

- Loss of back-up power
- HVAC digital controller
- System updates

Screening Methodology

- Screen digital assets associated with latent consequences of concern
- Maintain function by alternate means

Overflow has no impact



Failed camera compensated by guard

- Compromise addressed in a timely manner
- Consider cumulative impacts

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

Conclusion: Session 3

- Protect against active and latent consequence of concern
- Ensure support systems are part of screening
- Apply screening methodology

Agenda – Session 4
Cyber Security Controls Overview, Independent Assessment, Role of the Authorizing Official, and Cyber Security Control Monitoring

- Applying a baseline set of cyber security controls to digital assets
- Engaging in an independent assessment
  - Characteristics
  - Risk communication
- Designating an Authorizing Official – roles and responsibilities
- Tracking and managing status and changes

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

Cyber Security Control

Definition

"A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements." (NIST SP 800-53 rev. 4)

- Each cyber security control is designed to address a specific security concern
- The objective of a cyber security control may be accomplished in more than one way

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

Cyber Security Control (continued)

Controls can generally be described in one of 3 ways:

- A “thing” you can add
  - Having login restrictions based on user type, establishing automated audit logs, using firewalls to control traffic
- An “action” you can take
  - Having a tested incident response procedure, training staff on security awareness, testing updates to equipment before using
- A “decision” you can make
  - Requiring vendors to provide products that are tamper resistant, setting rules of behavior for employees, choosing what devices can be connected to the network

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

Cyber Security Control Families

TABLE 1-1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

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

Baseline Cyber Security Control Set

- Developed by licensee
  - NRC guidance will contain recommended baseline cyber security control sets based on facility type
  - Allows licensee flexibility and can account for other standards already in use
- Documented in licensee's Cyber Security Plan
  - Cyber Security Plan approved thru NRC license amendment
  - NRC review ensures baseline cyber security control set provides sufficient depth and breadth of coverage and meets security objectives
- Implemented through licensee's Control Implementation Plans

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

Implementing Cyber Security Controls

Control Implementation Plan (CIP)

- Similar to information system security plan from NIST SP 800-53, rev. 4
- Developed for in-scope systems by system owner or responsible party
  - System function (e.g., safety, security)
  - System purpose
  - Environment and location
  - Responsible individuals
  - Support systems
  - Interconnections
  - Inventory (hardware, software)
  - Monitoring strategy
  - Control status table
  - Controls template
- Intended to provide readers with sufficient information to assess the security posture of the system

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

Implementing Cyber Security Controls (continued)

- CIP may document the control is addressed "as written" in NRC approved Cyber Security Plan
  - Employ the measures contained in the control description
- CIP may document the intent of the control is satisfied by alternative means
  - Can be technical or operational measures
  - Must provide equivalent protection
  - Demonstrate and document programs, processes, and mechanisms are in place that address the control intent
- CIP may designate the control as "not applicable"
  - Licensee must demonstrate the related security concern does not exist and provide justification

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

Implementing Cyber Security Controls (continued)

Common controls

- Controls that apply to multiple digital assets (systems and networks), possibly facility-wide
- Documented by reference in multiple CIPs
- Common controls are implemented once, credited on ("inherited by") each digital asset that it governs
- Policies and procedures
- Enterprise-wide technical measures (firewall, intrusion detection)
- Common infrastructure or protections (UPS, fire protection, physical access control)

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

Implementing Cyber Security Controls (continued)

Plan of Action & Milestones (POAM)

- Developed for in-scope digital assets
- Companion or appendix to CIP
- Maintained by system owner or responsible party
- Documents controls that are not fully addressed
- Documents alternative controls that do not provide equivalent protection
- For each control not in place, describes:
  - Control description
  - Description of security impact and consequences
  - Risk rating (e.g., high, moderate, low)
  - Timing, resources, and cost for acceptable remediation

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

Implementing Cyber Security Controls (continued)

POAM (continued)

- Describes residual risk to digital asset based on controls not fully addressed
- As POAM items are resolved, POAM and CIP are updated
- Maintained by system owner or responsible party
- Is used to aid in:
  - Ongoing risk management
  - Aid in planning, resourcing, and other corrective action activities

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

Independent Assessment Characteristics

- Assessors must possess the necessary skills and technical expertise to perform the assessment
- Assessors must have independence
  - Separation of roles: an assessor cannot be a stakeholder, operator, implementer, or maintainer of digital assets they assess
  - Free from undue influence or conflict of interest
- Assessors formally evaluated and approved by Cyber Security Team management
- Controls assessment – are the controls:
  - Implemented correctly?
  - Operating as intended?
  - Producing the required outcome with regards to the intent of the control?

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

Independent Assessment Output

- Assessors provide Security Assessment Report that includes:
  - Assessment methodology
  - Findings
  - Residual risk determination
- Cyber Security Team updates:
  - CIPs to accurately reflect control status and implementation details
  - POAMs to accurately reflect observed control deficiencies

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

Communication of Risk

Residual risk

- Residual risk is a measure of the difference between ideal control implementation and actual control effectiveness
- Assign a residual risk rating (e.g., high, moderate, or low)

Example

- Digital asset audits user logins, but most administrative activities are performed using a shared account
- Residual risk – some administrative actions may be performed without sufficient attribution for the purposes of supporting after-the-fact investigation of incidents

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

Authorizing Official

- Senior licensee official
- Role is risk management of in-scope digital assets
  - Final system documentation package (CIP, Security Assessment Report, and POAM) submitted to Authorizing Official for review
  - System authorization
    - Authorizing Official reviews residual risks
    - Authority to Operate is granted or denied
      - Digital assets denied authority to operate may re-apply after addressing issues
      - Authority to Operate expires after a specific number of years
      - Authority to Operate memo is issued, signals acceptance of residual risk by Authorizing Official
    - Review and subsequent actions are documented
  - Ongoing risk management
    - Authorizing Official reviews POAMs periodically

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

Monitoring Cyber Security Controls

- Manage changes to digital assets and support systems, for example:
  - Minor system changes
    - Follow configuration management processes
    - Update CIPs as necessary
  - Major system changes
    - Significant system changes trigger full re-authorization
    - Operating system version upgrade, major firmware release, significant component replacement
    - Licensee defines “major change” in configuration management plan
- Ongoing assessments
  - Periodic risk and vulnerability assessments
  - Security controls typically tested annually (considering alternate timeframe)

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

Monitoring Cyber Security Controls (continued)

- Ongoing remediation
  - Flaw remediation based on findings from periodic risk and vulnerability assessments
  - POAM management
    - POAM items entered into licensee Corrective Action Program
    - Where no Corrective Action Program exists, licensee must review and update POAMs periodically
    - CIP updated when POAM items addressed
- Key updates
  - CIPs, POAMs, other documentation updated based on system changes, policy updates, etc.

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

Monitoring Cyber Security Controls (continued)

- Security status reporting
  - POAM status updates
  - Results of periodic risk and vulnerability assessments
  - Results of flaw remediation efforts
- Ongoing risk determination and acceptance
  - Authorizing Official reviews security status reporting
  - Organizational risk profile updated accordingly
  - Ongoing risk decisions

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

Conclusion: Session 4

- Application of controls
  - CIPs
  - POAMs
- Independent assessment
- Authorization official
- Monitoring