Cyber Security Program Performance Review (CSPPR)

David Neff Principal Licensing Engineer
Exelon Generation

February 2020

NUCLEAR ENERGY INSTITUTE

CSPPR Presentation Overview

- Initiative objectives
- Current licensee assessments and NRC baseline inspection
- Ongoing monitoring and assessment
- Road to performance based program assessment
- Performance metrics
- Maintaining defense-in-depth protective strategies
- Next steps / implementation

CSPPR Initiative Objectives

- Continuous Improvement of licensee performance
- Create performance metrics to identify gaps and drive for program improvement
- Provide for authentic verification process for Boundary and Detection device capabilities
- Increase focus on Safety and Security

Current Licensee Assessments and NRC Baseline Inspection

- Milestone 8 Inspection readiness assessment
- Review of station Comprehensive Assessment Program (CAP) data
- Industry inspection lessons learned
- 24-Month Program Effectiveness Review CSP 4.4.3
- Cyber Security Program review – 10CFR73.55(m) and CSP 4.12
- NRC Inspection Procedure IP 71130.10P

Ongoing Monitoring and Assessment (OM&A)

- OM&A (CSP Section 4.4)
- Configuration Management of CDAs (4.4.1)
- Cyber Security Impact Analysis (4.4.2)
- Ongoing Assessments of Cyber Security Controls (4.4.3)
  - Effectiveness Analysis (4.4.3.1)
  - Vulnerability Assessments (4.4.3.2 and App E.12)
- Verification Rogue Assets Not Connected (App D.1.18)
- Cyber Security Program Review (10CFR73.55(m), 4.12)

Ongoing Monitoring and Assessment

- Cyber Security Controls Effectiveness Analysis (CSP 4.4.3.1)
- Configuration Management and Change Control (CSP 4.4.1, E.10)
- Impact Analysis of Changes and Environment and Risk/Vulnerability Assessments (CSP 4.4.2, 4.4.3.2, 4.9, E.4, E10.5)
- Attack Mitigation / Incident Response (CSP 4.6, CSIRT Event Results)
- Contingency Plan Maintenance (CSP 4.7)
- Training (CSP 4.8)
- Records Retention (CSP 4.13)
- System/Services Acquisition and Supply Chain (CSP E.11)

Programmatic Changes / Event Reporting

- Changes to CSP, procedures, new or deleted controls (10CFR50.54(p))
- Operating experience (CSP 4.3.9)
- Problem Identification and Resolution (CSP 4.9.4, CAP)
- Cyber Security Program Review (CSP 4.12, 10CFR73.55(m))

Road to Performance Based Program Assessment

Building a Program Performance Assessment Process

- Maintain CSP requirements
- Utilize existing self assessment program
- Assure programmatic compliance
- Create performance metrics to drive results
- Perform defense-in-depth protective strategies

Road to Performance Based Program Assessment

Building a Program Performance Assessment Process

- Maintain CSP requirements
- Utilize existing self assessment program
- Assure programmatic compliance
- Create performance metrics to drive results
- Perform defense-in-depth protective strategies

Performance Metrics – The Why

- Identify weaknesses
- Determine trends to better utilize security resources
- Determine the success or failure of implemented security solutions
- Evaluate compliance with regulations
- Improve the performance of implemented security controls
- Answer high-level business questions regarding security

Reference: CYBER SECURITY METRICS AND MEASURES
Paul E. Black, Karen Scarfone and Murugiah Souppaya
National Institute of Standards and Technology,

Performance Metrics - The How

- Objectives / intended results
- Critical success factors / performance standards
- Key performance indicators
- Performance metrics
- Measures

REFERENCE: 5 Steps to Actionable Key Performance Indicators, Unilytics, Peder Enhorning

Performance Metrics – The Specifics

Objective: Maintaining Detection, Response, Elimination and Restoration Capability (CSP 4.6, 2.2.13, 2.2.14)

Performance Standard: Personnel are trained, practiced and available to perform the attack mitigation, incident response and recovery actions

Measure:
1. Qualified Cyber Security Incident Response Team (CSIRT) is comprised of sufficient numbers of qualified members including performance in a drill or actual investigation
2. Cyber Security Specialists are available, experienced and current with industry issues

Metric:
1. Minimum numbers of qualified CSIRT members exist
2. Minimum numbers of Specialists that meet the criteria

Performance Metrics – The Specifics

Maintaining Detection, Response, Elimination and Restoration Capability

Qualified CSIRT Team NEI 08-09 Appendix A4.11, E7, E8	GREEN (3)	Exceeds the minimum requirements of CSIRT Members
	WHITE (2)	Meets the minimum requirements of CSIRT Members
	YELLOW (1)	One department does **not** meet the minimum requirements.
	RED (0)	More than one department does **not** meet the minimum requirements.
Cyber Security Specialist Proficiency NEI 08-09 Appendix A, Section 4.11	GREEN (3)	2 or more people fully qualified with over a year of experience in the program and attend either one industry meeting (NEI, NITSL, EPRI CTAC), or a non-XXXXX Inspection, a non-XXXXX pre-inspection assessment, or a non-XXXXX benchmarking within the last 2 years.
	WHITE (2)	1 person fully qualified with over a year of experience in the program and attend either one industry meeting (NEI, NITSL, EPRI CTAC), or a non-XXXXX Inspection, a non-XXXXX pre-inspection assessment, or a non-XXXXX benchmarking within the last 2 years with a backup specialist fully qualified with less than one year of experience.
	YELLOW (1)	1 Person fully qualified with less than one year of experience, and no backup persons.
	RED (0)	No one qualified in the Primary or Backup role.

Performance Metrics – The Specifics

Objective: Threat and Vulnerability Management Process Effectiveness (CSP 4.4.3.2, 2.2.14, E12)

Performance Standard: Threats and vulnerabilities are evaluated and mitigation actions tracked in CAP and implemented timely

Measure: 1. Number of completed, open and overdue remediation actions

Metric: **1.** Remediation actions completed per the action plan due dates

Performance Metrics – The Specifics

Threat and Vulnerability Management Process Effectiveness

Threat & Vulnerability Management, OE Remediation, NER NEI 08-09 E.12, A4.9.1	GREEN (3)	**No** open remediation actions OR 1 open remediation action **and** corrective action plan has been developed with implementation on schedule **and no** due date extensions.
	WHITE (2)	Has > 1 open remediation actions **and** corrective action plan has been developed with implementation on schedule **and no** due date extensions.
	YELLOW (1)	Has > 1 open remediation actions **and** corrective action plan has been developed, but due date has been extended.
	RED (0)	Has > 1 open remediation actions **and no** corrective action plan has been developed.

Performance Metrics – Other Areas

- Cyber security controls are maintained throughout the life cycle of CDAs. (CSP 4.4.1, 4.5, 2.2.1, 2.2.2, 2.2.3, 2.2.6, E10)
- Maintaining Defense-In-Depth architecture and preventing potential bypasses. (CSP 4.3, 2.2.7, 2.2.8, E6)
- Maintaining Detection, Response, Elimination and Restoration capability (CSP 4.6, 2.2.13, 2.2.14)
- PI&R Effectiveness (CSP 2.2.11, 4.9.4)

Performance Metrics – Other Areas

- Threat and Vulnerability Management Process effectiveness (CSP 4.4.3.2, 2.2.14, E12)
- Records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work. Records are retained and retrievable. (CSP 4.13, D2.6, D2.7, D10.3)
- Sustainability of future program improvement (CSP 4.8, 2.2.10, E7.2, E9)

Maintaining Defense-In-Depth Protective Strategies

- Assurance of defensive model (levels)
- Physical/logical isolation of safety and security CDAs
- Network boundary & monitoring device effectiveness
- Options for providing assurance of effectiveness

Maintaining Defense-In-Depth Protective Strategies

- Options for Providing Assurance of Effectiveness
  - Previously conducted licensee testing
  - Analysis of monitoring audit logs
  - Configuration setting review
  - Vendor testing
  - Laboratory testing
  - Post-Mod Testing protocols
  - Portable multi-media device (PMMD) Kiosk Health
  - Vulnerability assessments and remediations
  - Configuration control of devices
  - CSIRT drill that tests detection and response capability

CSPPR and Performance Metrics Next Steps

- NEI Cyber Security Task Force Tiger Team initiative developing written guidance for the CSPPR process.
  - Objectives, Performance Standards, Measures and Metrics

CSPPR Implementation

- Industry Guidance Issuance 2Q2020
- NRC Informed of Guidance 2Q2020
- Industry / NRC Workshops 3Q/4Q2020
- Industry Pilots 4Q2020
- Licensee implementation TBD

Questions ?

Contact Information
David Neff – David.Neff@exeloncorp.com