



PERIODICITY SERVICES IN-DEPTH

OVERVIEW

NRC Title 10, Part 73 "Physical Protection of Plants and Materials," Section 54 (10 CFR 73.54) requires that nuclear Licensees establish, implement, and maintain a cybersecurity program for the protection of digital computer and communication systems and networks associated with safety-related, important-to-safety, Security and Emergency Preparedness (SSEP) functions. Regulatory Guide (RG) 5.71 and NEI 08-09 provides guidance for licensees to establish an Ongoing Monitoring and Assessment Program to maintain cybersecurity controls used to support CDAs, defense in-depth protective strategies, policies, procedures and near real-time monitoring and management for the life cycle of their critical digital assets (CDAs).

RG 5.71 and NEI 08-09 defines many events that must trigger monitoring and assessment tasks at prescribed intervals. Many actions occur at intervals defined by the licensee in accordance with installed equipment, outage schedules, incident detection and the overall cybersecurity policies of the site.

Timely execution of these activities, consistent and accurate documentation are essential to a robust program and required by the NRC. Many of the ongoing tasks are proactive in nature and can be scheduled and highly regimented while others such as cybersecurity alerts are reactive in nature. The cybersecurity team is responsible for evaluating the overall cybersecurity impact of all changes that occur to CDAs over the life cycle of the CDA. In addition, specialized skill sets are required to perform many cybersecurity related tasks associated with changes to CDAs.

This table provides a summary of the periodic activities required to maintain the cyber security program.

Topic	NEI 08-09 Reference	RG 5.71 Reference	Period*
Ongoing Assessment of Cyber Security Controls	A.4.4.3	A.4.1.1	24 months
Effectiveness Analysis	A.4.4.3.1	A.4.1.2	24 months
Vulnerability Assessments and Scans, Threat and Vulnerability Management, Alerts & Advisories, and Patch Management	A.4.4.2, A.4.4.3.2, A.4.9.1, D.5.5, E.3.2, E.3.5, E.12	A.4.1.3, A.4.2.2, B.5.5, C.3.2, C.3.5, C.13.1	92 days
Cyber Security Program Review	A.4.12	A.4.3	24 months
Access Control Policy and Procedures Account Management	D.1.1	B.1.1	12 months
Account Management	D.1.2	B.1.2	31 days
Wireless Access Restrictions	D.1.17	B.1.17	31 days
Insecure and Rogue Communications	D.1.18	B.1.18	31 days
Auditable Events	D.2.2	B.2.2	12 months
Audit Review, Analysis, and Reporting	D.2.6	B.2.6	31 days
Identification and Authentication Policies and Procedures	D.4.1	B.4.1	31 days
Password Requirements	D.4.3	B.4.3	92 days
Identifier Management	D.4.6	B.4.6	31 days
Authenticator Management	D.4.7	B.4.7	12 months
Media Sanitation and Disposal	E.1.6	C.1.6	92 days
Malicious Code Protection	E.3.3	C.3.3	Varies
Monitoring Tools and Techniques	E.3.4	C.3.4	7 days
Security Functionality Verification	E.3.6	C.3.6	Varies
Software and Information Integrity	E.3.7	C.3.7	92 days
Defense-in-Depth	E.6	C.7	92 days
Incident Response Testing and Drills	E.7.3	C.8.3	12 months
Contingency Training	E.8.3	C.9.4	12 months
CDA Backups	E.8.5	C.9.6	Varies
Technical Training	E.9.3	C.10.3	12 months
Baseline Configuration	E.10.3	C.11.3	92 days
Access Restriction for Change	E.10.6	C.11.6	92 days
Least Functionality	E.10.8	C.11.8	31 days

*Period is defined by the plant specific Cyber Security Plan. Periods listed are from the NEI 08-09 security plan template.

SOLUTION

Your cybersecurity program is in place and running. Continuous work of maintaining and improving the cybersecurity program is required to keep up with:

- The evolving threat landscape.
- Revisions to regulatory guidance.
- Changes to the plant Instrumentation & Control (I&C) systems to address obsolescence and plant life extension.

Maintaining your cyber program can be time consuming with a large overhead. FoxGuard Solutions can assist with the program and, in turn, lower your overall cost associated with this program. Under this program FoxGuard will provide industry guidance, expertise, and continuing services in support of on-going maintenance and cybersecurity related changes for licensees. FoxGuard will use team members who have a proven track record supporting specialized cybersecurity analysis, assessments, documentation, implementation, and service-related projects. FoxGuard offers a broad cybersecurity skill set from overall project management to support roles while performing managed tasks and staff augmentation .

The advantages to using FoxGuard Solutions to perform periodic cybersecurity tasks over self-performance by plant staff are:

- FoxGuard Solutions provides lower costs due to economies of scale and efficiencies.
- FoxGuard Solutions has experience across several US and international nuclear plants making us better qualified to apply risk informed and optimized techniques to meet regulatory requirements.
- FoxGuard Solutions has cybersecurity experience in other critical infrastructure industries and that broader experience can lead to innovations in completing periodic cybersecurity tasks.

FOXGUARD DOES THE WORK

FoxGuard Solutions will staff your program with regulatory compliance and security experts to help address each requirement defined. This team will consist of both continuous staff members and supporting staff members. All team members will work at site and/or remotely and coordinate through a team lead. This will give you the needed team to focus and address all your security compliance needs on a day-by-day basis and cost-effectively address longer task cycles.

To maintain our capabilities and awareness of cybersecurity regulations and best practices, FoxGuard Solutions is actively involved with several cybersecurity related industry groups and standards organizations such as ISA, IEC, NEI, EPRI, and NERC.



LOWER OPERATION AND MAINTENANCE (O&M) COSTS

BETTER PREPAREDNESS FOR NRC INSPECTIONS

DYNAMIC TEAM OF CYBERSECURITY SPECIALISTS

RELATED SERVICES

Vulnerability Reporting

Validation Services

On-Site Security Control Implementation Services

Asset ID & Baseline Consultative Services

SERVICES OFFERED UNDER THIS PROGRAM INCLUDE:

REQUIREMENT/CONTROL	NEI 08-09	FOXGUARD PRODUCTS AND SERVICES
Ongoing Assessment of Cybersecurity Controls	A.4.4.3	Ongoing assessments are performed to verify that the cyber security controls implemented for CDAs remain in place throughout the life cycle. FoxGuard can review all cyber related Corrective Action Program (CAP) items to validate or invalidate the proper functioning of applied cyber technical, management and operational controls. A sample of CDAs can be reviewed to verify that the controls are correct per the plant's specific Security Control Implementation Strategy (SCIS), cybersecurity procedures, and CDA Assessment reports.
Effectiveness Analysis	A.4.4.3.1	FoxGuard can conduct an independent effectiveness analysis using the methodology developed by the U.S. Department of Energy known as the Cybersecurity Capability Maturity Model (C2M2) to conduct an evaluation of the plant's maturity and sophistication of the cybersecurity risk management approach at a strategic and holistic level. This is a programmatic review not a CDA specific review. A C2M2 Evaluation Report will be developed to provide the plant with a visual analysis on the maturity of its cybersecurity program.
Vulnerability Assessments and Scans, Threat and Vulnerability Management, Alerts & Advisories, and Patch Management	A.4.4.2 A.4.4.3.2, A.4.9.1, D.5.5, E.3.2, E.3.5, E.12	The plant's defensive architecture, particularly the data diode, is often credited for avoiding the necessity to apply patches. However, plants must screen for applicability of vulnerability notices, have a documented patch management program, and implement any required mitigation measures. FoxGuard offers a mature Patch and Update Management Program (PUMP) for critical infrastructure Industrial Control Systems (ICS). Services include: Patch Availability Reporting (PAR), Vulnerability Notification Report (VNR), and Patch Binary Acquisition (PBA).
Cybersecurity Program Review	A.4.12	Threats, regulatory guidance, and plant digital systems are constantly changing. FoxGuard can assist in cybersecurity procedure revisions to implement changes to regulatory guidance (i.e., future revisions to RG 5.71, NEI 08-09, 13-10, 10-04, NRC SFAQs). FoxGuard can assist design engineering and/or the I&C vendor during conceptual design and detailed design to assure new designs comply with the plant specific cybersecurity plan, processes, and procedures.
Access Control Policy and Procedures, Account Management	D.1.1, D.1.2	FoxGuard can assist in implementing account management procedures by periodically auditing access control rights. FoxGuard can implement a Centralized Account Management system to prevent unauthorized access to master user/password lists.
Wireless Access Restrictions, Insecure and Rogue Communications	D.1.17, D.1.18	FoxGuard can conduct scans for unauthorized wireless access points and install automated systems to detect and alarm on unauthorized network changes.
Auditable Events, Audit Review, Analysis, and Reporting	D.2.2, D.2.6	Most plants have implemented a Security Information and Event Management (SIEM) system. FoxGuard can assist plants in reviewing, tuning, and testing asset configurations and SIEM rules to enhance detection of unauthorized changes and security events. FoxGuard can implement automated detection methods such as Endpoint Detection and Response (EDR), Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS), and Application Whitelisting.
Identification and Authentication, Password Requirements, Identifier Management, Authenticator Management	D.4.1, D.4.3, D.4.6, D.4.7	FoxGuard can assist in ensuring that the user identifiers are issued to the intended party, and copies of master passwords are stored in a secure location with limited access. FoxGuard can implement Windows Domain Controllers and a centralized group policy where applicable to centrally manage CDA authenticators.
Media Sanitation and Disposal	E.1.6	FoxGuard can provide media sanitation services to ensure portable media and mobile devices are sanitized prior to disposal or release for reuse.
Malicious Code Protection	E.3.3	FoxGuard can implement automated malware scanning systems for Portable Media and Mobile Devices (PMMD) and Maintenance and Test Equipment (M&TE) laptops.
Monitoring Tools and Techniques, Security Functionality Verification, Software and Information Integrity	E.3.4, E.3.6, E.3.7	FoxGuard can assist with SIEM configuration and tuning, NIDS and HIDS signature updates, and periodic testing. We can assist with employing hardware access controls (e.g., hardwired switches), to prevent unauthorized software changes. We can assist with deploying centrally managed integrity verification tools. We can assist in the use of physical tamper evident packaging or seals for system components.

SERVICES OFFERED UNDER THIS PROGRAM INCLUDE:

REQUIREMENT/CONTROL	NEI 08-09	FOXGUARD PRODUCTS AND SERVICES
Defense-in-Depth	E.6	To maintain the defensive architecture, FoxGuard can periodically perform a review of hardware and software firewall configurations. FoxGuard can review network segmentation designs and implement additional controls. FoxGuard can implement new boundary devices where necessary for plant design changes to digital I&C systems.
Incident Response Testing and Drills	E.7.3	FoxGuard can develop and conduct training and drills for the plants Cybersecurity Incident Response Team (CSIRT).
Contingency Training	E.8.3	FoxGuard can develop and conduct training for personnel involved in performing contingency planning.
CDA Backups	E.8.5	FoxGuard can perform, manage, and validate CDA backups. FoxGuard can provide protected offsite storage of backup media.
Technical Training	E.9.3	FoxGuard can provide cyber security-related technical training to cybersecurity specialists, system owners, network administrators, and design engineering.
Baseline Configuration	E.10.3	FoxGuard can develop, document, and maintain a current baseline configuration of CDAs and employ an automated mechanism to maintain an up-to-date, complete, accurate, and readily-available baseline configuration of CDAs.
Access Restriction for Change	E.10.6	FoxGuard can assist in the definition, documentation, and audit of physical and logical access restrictions associated with changes to CDAs. FoxGuard can implement automated mechanisms to detect unauthorized changes.
Least Functionality	E.10.8	FoxGuard can assist in the configuration and documentation of CDA configuration settings to prohibit, protect and restrict the use of insecure functions, ports, protocols, and services. A hardening process can be implemented to eliminate unnecessary functions, ports, protocols, and services. FoxGuard can implement automated mechanisms to prevent unauthorized program execution.

one source. many solutions.



www.foxguardsolutions.com



requestinfo@foxguardsolutions.com



877.446.4732

framatome

FoxGuard Solutions® is a wholly owned subsidiary of Framatome, an international leader in nuclear energy.

