SOLUTION BRIEF

How Dragos Supports US Nuclear Regulatory Commission NRC Cyber Protection

The Dragos Platform and solutions provide nuclear generation operators and asset owners with the ability to build effective OT threat defense and assist with ongoing assessments related to NRC Title 10 Section 73.54 Regulations.

Cyber events impacting nuclear power plants can have a major effect on public safety and the environment. In recognition of this, the United States (US) Nuclear Regulatory Commission (NRC) has issued NRC Title 10 regulations governing all persons and organizations who receive an NRC license to use nuclear materials or operate nuclear facilities. A component of Title 10 is NRC 73.54, which focuses on the protection of digital computer and communication systems and networks.

Dragos specializes in cybersecurity for operational technology (OT), including nuclear facilities. We offer a unique combination of technology to monitor OT networks, threat intelligence that specializes in industrial adversaries and techniques, and professional consulting services that support building an effective OT cyber defense.

Audit, Governance & Training for OT

Dragos Services provides OT cybersecurity assessments, penetration testing, incident response, training, and other services delivered by skilled OT cybersecurity consultants to help evaluate and recommend necessary steps to build industrial cybersecurity maturity.

About Dragos, Inc.

Dragos, Inc. was established in 2016 by cybersecurity experts who pioneered the ICS cyber mission for US Government agencies.

Recognizing the rise of OT cyber attacks and the lack of solutions, they assembled a top-tier team of ICS/OT security practitioners to develop the Dragos Platform and offer services aimed at safeguarding critical infrastructure from escalating OT cyber threats.

Identify OT Assets, Detect & Hunt Threats

The Dragos Platform automates OT asset inventory, with risk-based vulnerability management and threat detection for OT systems. Continuous monitoring prioritizes notifications, while detailed logging enables fast investigation and threat hunting. Optional expert OT threat hunting services are available with OT Watch.

Response & Recovery from Cyber Events

Incident responders experienced in OT cyber event investigation and recovery are available through a Rapid Response Retainer. Retainer hours can be used for assessments, penetration tests, tabletop exercises, plus more to help optimize response plans and protection posture for OT.

Mapping Dragos Capabilities to NRC Title 10 Section 73.54 Requirements

NRC Title 10 Section 73.54 provides detailed requirements for protecting digital computer and communication systems and networks at nuclear facilities. We identify how Dragos technology and services can help support operational technology (OT) compliance for each category requirement shown in the table below.

CATEGORY	NRC INSPECTION MANUAL DESCRIPTION	DRAGOS OT-FOCUSED SERVICE
03.01a - Review Ongoing Monitoring Activities	Ongoing monitoring and assessment activities are performed to verify that the cyber security controls implemented for CDAs remain in place. Representative sample of controls.	• OT Cybersecurity Assessment (OTCA) which includes a program review, collection management framework, crown jewel analysis, topology review, standards & regulations review, threat discovery, asset inventory, and asset vulnerability assessment.
03.01b - Review Effectiveness Analysis	NEI 08-09 Section 4.4.3.1 periodic audits of the physical security program, security plans, implementing procedures, cyber security programs; safety/security interface activities, and the testing, maintenance, and calibration program as it relates to cyber security.	• Network Vulnerability Assessment • Penetration Test
03.01c - Review Vulnerability Assessment Activities	The vulnerability assessment program establishes programs/procedures for screening, evaluating, and dispositioning threat notifications, and vulnerabilities against CDAs received from a credible source. The licensee will use their corrective action program to document the potential vulnerability and to initiate corrective actions. CAP evaluations should consider the threat vectors associated with the vulnerability.	• Vulnerability Assessments – with scope • specialized to evaluate Corrective Action Program (CAP) items

CATEGORY	NRC INSPECTION MANUAL DESCRIPTION	DRAGOS OT-FOCUSED SERVICE
03.02a - Defense-in-Depth Protective Strategies	Defense-in-Depth strategies have been implemented, documented, and are maintained to ensure the capability to detect, delay, respond to, and recover from cyber-attacks on CDAs. Licensees may have implemented near real-time automatic detection mechanisms to capture logs and to generate alarms, manual means of detection, or through the demonstration that a compromise can be detected along an attack pathway (e.g. supply chain testing).	• Collection Management Framework • Network Penetration Test • OT Cybersecurity Architecture Review • Compromise Assessment
03.02b - Defensive Security Architecture	Multi-level security defense architecture that established the required level of cyber security. May have separated their levels by security boundary devices, such as firewalls, air gaps, or deterministic devices, through which digital communications are monitored and restricted in accordance with CSP requirements.	• OT Cybersecurity Architecture Review • Topology Review
03.02c - Maintain Security Controls	Verify that the licensee maintained the implemented security controls to provide high assurance that the CDAs are continuously protected against cyber- attacks. Verify that the licensee is verifying and validating that the implemented security controls are implemented correctly, operating as intended, and continuing to provide high assurance that the CDAs are protected against cyber-attacks up to and including the Design Basis Threat (DBT).	• Network Penetration Test • Compromise Assessment • OT Cybersecurity Assessment • Threat Hunt
03.02d - User Identification and Authentication	NEI 08-09 Appendix D Section 1, Access Control and Section 4, Identification and Authentication. The licensee also has policies and procedures for the periodic review of the access authorization list.	• OT Cybersecurity Assessment - Focused Program Review
03.02e - Portable Media and Mobile Devices	Licensees utilize portable media and mobile devices to update software and manage changes to CDAs. Verify that licensees have established policies and procedures that describe control, update and use of portable media, mobile devices. Mobile devices should be hardened in accordance with the CSP.	• OT Cybersecurity Assessment - Focused Program Review

CATEGORY	NRC INSPECTION MANUAL DESCRIPTION	DRAGOS OT-FOCUSED SERVICE
03.03a - Design Changes or Replacement Equipment	Verify that the licensee evaluates modifications to CDAs prior to implementation to assure that digital computer and communications systems and networks are adequately protected against cyber attacks.	• OT Cybersecurity Assessment - Focused Program Review
03.03b - Security Impact Analysis of Changes and Environments	A cyber security impact analysis is performed prior to making a design or configuration change to a CDA, or when changes to the environment occur. The licensee evaluates risks introduced by the changes.	• OT Cybersecurity Assessment - Focused Program Review
03.03c - Supply Chain and Service Acquisition	Since many replacements for CDAs will be purchased off-the-shelf, a review of supply chain and acquisition controls should be performed, and the replacement CDAs should be hardened.	• OT Cybersecurity Assessment - Focused Program Review
03.04a - CSP Changes and Implementing Procedures	Ensure that testing of the incident response capability for CDAs has occurred at least every 12 months. If a cyber security incident occurred, ensure that the licensee took effective actions to ensure that the function of CDAs are not adversely impacted and that the licensee implemented appropriate corrective actions. Observe a licensee- conducted Cyber Security Incident Response drill to ensure that site-defined tests or drills are used, that staff are aware of their roles and responsibilities, and that results of the drill are evaluated and documented.	• Incident Response Plan Review • Tabletop Exercises (TTX)
03.04b - Review Incident Response and Contingency Plans	Ensure that testing of the incident response capability for CDAs has occurred at least every 12 months. If a cyber security incident occurred, ensure that the licensee took effective actions to ensure that the function of CDAs are not adversely impacted and that the licensee implemented appropriate corrective actions. Observe a licensee- conducted Cyber Security Incident Response drill to ensure that site-defined tests or drills are used, that staff are aware of their roles and responsibilities, and that results of the drill are evaluated and documented.	• Incident Response Plan Review • Tabletop Exercises (TTX)

CATEGORY	NRC INSPECTION MANUAL DESCRIPTION	DRAGOS OT-FOCUSED SERVICE
03.04c - Review Training	Verify that appropriate facility personnel, including contractors, are aware of cyber security requirements, and receive the training necessary to perform their assigned duties, and responsibilities.	• OT Cybersecurity Assessment - Focused Program Review
03.05 - Evaluation of Corrective Actions	The CSP specifies that the licensee will use the site CAP to: 1. track, trend, correct, and prevent recurrence of cyber security failures and deficiencies, and 2. evaluate and manage cyber risks	• OT Cybersecurity Assessment - Focused Program Review

For more detailed information about the Dragos Platform technology and Services offerings, visit dragos.com or connect with us at sales@dragos.com.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo Contact Us