Process-Level OT Cybersecurity Regulation:

A Global Overview

SIGA

Multi-Level OT Cyber Process Resilience

OT CYBER GUIDELINES

NIST SP 800-82r3

- Provides best practices for ICS, SCADA, and OT security
- Identifies Level 0 (Purdue Model) risks: unauthenticated sensors & actuators
- Recommends segmentation & real-time monitoring to detect spoofed data

Organizations should secure critical processes by implementing risk-based controls at Level 0.

National Institute of Standards and Technology
U.S. Department of Commerce

CSA Singapore

- Mandatory reporting of OT cyber incidents for rapid response
- Intelligence sharing via OT-ISAC to strengthen sector-wide cyber defenses
- Securing Level 0 through monitoring, anomaly detection & control

A holistic approach to OT security must include protecting Level 0 physical processes from cyber threats.

Water Sector Cybersecurity Program 2024 Update

- Technical assistance to help water identify & mitigate cyber risks
- Develops an Incident Response checklist to strengthen OT system resilience
- Encourages protection of Level 0 controls to ensure safe water treatment. distribution

Safeguarding OT systems is critical for managing water processes and ensuring reliable operations.

EPA
OFFICE OF GROUND WATER AND DRINKING WATER

Water Security is National Security

REGULATIONS & STANDARDS

ISA/IEC 62443 Standard 2021 (International)

- Establishes a cybersecurity framework for Industrial Automation & Control Systems
- Security requirements for components including controllers, sensors & field devices
- Emphasizes Level 0 protection to prevent risks that impact safety & system reliability

Protecting physical process components is critical, as vulnerabilities at this level can directly impact industrial safety and reliability.

ISA GLOBAL CYBERSECURITY ALLIANCE

ISO/IEC 27019 Standard 2024 Update (International)

- Security controls for the energy sector, covering generation, transmission & supply
- Establishes best practices for access management, IR & business continuity
- Aligns with NIST Cybersecurity Framework to enhance OT system resilience

While not process-specific, it reinforces cybersecurity measures for OT environments in energy systems

TSA Security Directive Pipeline 2021-02D

- Requires real-time cyber incident reporting to CISA within 24 hours of detection
- Mandates annual vulnerability assessments to identify & mitigate OT security risks
- Enforces access controls & system monitoring to protect pipeline operations

Operators must incorporate incident response, mitigation, and forensic analysis procedures into their OT systems to address threats in real-time.

LEGISLATION

Cyber Incident Reporting for Critical Infrastructure Act 2024 (US)

- Requires reporting of major cyber incidents to CISA within 72 hours of detection
- Mandates ransomware payment reporting within 24 hours to improve threat response
- Encourages process-level OT monitoring to protect critical infrastructure operations

Continuous monitoring of OT environments is essential to ensuring protection against incidents that could disrupt critical services.

EU AI Act 2024 (EU)

- Regulates high-risk AI systems used in Critical Infrastructure operations
- Mandates risk management & transparency to prevent bias & security vulnerabilities
- Ensures AI in OT systems does not disrupt process-level operations, essential services

High-risk AI systems deployed in critical infrastructure must be designed with robust security measures to prevent any disruption to essential services.

EU Artificial Intelligence Act

Network and Information Security Directive Legislation (NISD 2) (EU)

- OT risk identification & security measures for SCADA, PLCs & process sensors
- Mandates real-time monitoring & encryption to protect CI assets
- Process-level security to prevent disruptions in essential industrial operations

NIS2 strongly advocates securing critical OT components to ensure the integrity of physical processes in key sectors.

FINANCIAL DISCLOSURE

Cybersecurity Disclosure Rule 2023 (US)

- Requires disclosure of material cyber incidents within 4 business days
- Mandates board oversight reporting on cybersecurity risk management
- Includes annual reporting on cyber risks affecting OT & critical business operations

Public companies must disclose significant cybersecurity incidents, including those affecting OT, if deemed material to investors.

U.S. Securities and Exchange Commission

Market Abuse Regulation (EU)

- Immediate disclosure of cyber incidents that materially impact financial performance
- Allows delayed disclosure if it protects legitimate business interests
- Imposes strict penalties, including fines & criminal sanctions for non-compliance

Companies listed on EU stock exchanges must disclose cybersecurity incidents if deemed material to investors.

ESMA
European Securities and Markets Authority

Full Report:

www.sigasec.com