Cyber Regulations

In the realm of Industrial Control Systems (ICS) and Operational Technology (OT) for critical infrastructure, there are several regulations and standards that mandate network monitoring as part of their cybersecurity requirements. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards are one of the most prominent in this area, especially for the energy sector.

1. NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)

- Applicability: Primarily for the electrical utility industry in North America.
- Requirements: Includes requirements for security management controls, system security, incident reporting and response planning, recovery plans for Critical Cyber Assets, and more. NERC CIP standards such as CIP-005 (Electronic Security Perimeter(s)) and CIP-007 (Systems Security Management) implicitly require network monitoring to identify and protect against potential cybersecurity threats.

2. IEC 62443 (International Electrotechnical Commission)

- Applicability: Global standard for industrial automation and control systems.
- Requirements: Focuses on securing and managing network infrastructure within industrial sectors. It covers aspects like identifying risks, system requirements for secure communications, and guidelines for network monitoring and incident handling.

3. ISA/IEC 62443 Series (International Society of Automation)

- Applicability: Similar to IEC 62443, aimed at industrial control systems.
- Requirements: Provides detailed guidance on how to implement robust security controls, including network monitoring, within ICS environments.

4. CFATS (Chemical Facility Anti-Terrorism Standards)

- Applicability: U.S. chemical facilities.
- Requirements: Includes risk-based performance standards for security. While not explicitly focused on network monitoring, the need for cybersecurity measures is implicit in its broader security requirements.

5. GDPR (General Data Protection Regulation)

- Applicability: Not specific to ICS/OT but applicable to any organization processing the data of EU citizens.
- Requirements: Includes obligations to secure processing of personal data, which can extend to network monitoring in industrial settings handling such data.

6. FISMA (Federal Information Security Management Act)

- Applicability: U.S. federal agencies.
- Requirements: Mandates continuous monitoring of information systems, which includes network monitoring.

7. HIPAA (Health Insurance Portability and Accountability Act)

- Applicability: U.S. healthcare industry.
- Requirements: Requires safeguarding of medical information, which may involve network monitoring in ICS environments within healthcare facilities.

8. Sarbanes-Oxley Act

- Applicability: U.S. public company boards, management, and public accounting firms.
- Requirements: While primarily financial, it requires the integrity of the systems that manage financial data, potentially involving network monitoring.

These regulations, while varying in their specific focus and industry applicability, all underscore the importance of network monitoring as a key component in protecting ICS/OT environments from cyber threats. Compliance with these regulations often necessitates a robust approach to cybersecurity, including continuous network monitoring, incident detection, and response mechanisms.