Openpolicy

Nov 26, 2024

Via Electronic Filing

To: Federal Energy Regulatory Commission

OpenPolicy comments on
Critical Infrastructure Protection Reliability Standard CIP–015–1—Cyber Security—Internal Network Security Monitoring [Docket No. RM24–7–000]

Overview

OpenPolicy appreciates the opportunity to provide feedback on the Federal Energy Regulatory Commission (Commission) proposition to approve the proposed Reliability Standard CIP-015-1 (Cyber Security—Internal Network Security Monitoring). OpenPolicy is dedicated to democratizing access to policymaking by empowering innovative companies of all sizes to collaborate with regulators and contribute their advanced solutions. We recognize the importance of fostering an open, inclusive, and forward-thinking approach to policy development to achieve robust cybersecurity standards for critical infrastructure sectors, including those addressed under this Notice of Proposed Rulemaking (NOPR). Our ecosystem of IoT, OT, AI, and data security innovators, such as **Armis, FiniteState, Censys, Bastazo, Wiz, and others,** brings unique perspectives on critical infrastructure risk management, threat detection, and remediation recommendations.

These stakeholders have actively contributed to initiatives such as DHS CISA's Secure by Design framework, the FCC IoT Cyber Trust Mark, and CIRCIA, showcasing scalable, adaptive solutions to complex cybersecurity challenges[1]. As a member of the IT Sector Coordinating Council (IT-SCC), OpenPolicy also plays a key role in shaping cybersecurity guidelines for critical infrastructure, bridging industry expertise with regulatory objectives.

By leveraging our network's cutting-edge technologies and fostering information sharing, we are eager to collaborate with the Commission. We believe the Commission can effectively address modern cybersecurity challenges, mitigate risks associated with interconnected systems, and establish a resilient, adaptive framework for critical infrastructure protection.

The Commission's initiative represents a critical opportunity to advance the security of our nation's infrastructure by embracing innovation and collaboration. We would be honored to support its endeavors and provide insights and resources from our ecosystem of innovators.

[1]See more about OpenPolicy filings on these issues at https://www.openpolicy.co/comments-and-submissions.

Expanding INSM Requirements and Trust Zone Coverage

The directive to extend INSM requirements beyond traditional electronic security perimeters is a commendable step forward. To fully realize this potential, it is essential to include all **CIP-networked environments**, ensuring visibility across IT, OT, and IoT systems, and all converged assets. This expanded scope will mitigate risks associated with lateral movement and blind spots, providing comprehensive protection across interconnected infrastructures.

As emphasized in the proposal, monitoring **east-west traffic** within trust zones enhances the detection of unauthorized activity and establishes a defense-in-depth strategy. Monitoring such traffic enables the early detection of unauthorized activity, enhancing both incident response and risk management. Monitoring east-west traffic is a key strategy for detecting threats that bypass traditional perimeter defenses, and extending this monitoring to all trust zones will provide a holistic view of potential vulnerabilities.

However, recent attacks have illustrated the critical need to emphasize at-scale remediation of critical vulnerabilities and the ability to leverage trained AI and ML capabilities to identify anomalies in OT systems. The NOPR's requirement for integrating anomaly responses ensures a proactive stance against potential threats and should be augmented by incorporating a unified, predictive AI-driven security model that combines monitoring, scanning, threat detection, and incident response capabilities—**an expanded attack surface management approach.** By addressing both internal and external attack vectors, the proposed standard can enhance resilience and prevent attackers from exploiting overlooked areas in the attack surface.

To further support this, adopting **scalable and modular INSM architectures** will allow for seamless integration with third-party solutions and the flexibility to adapt to evolving cybersecurity threats. Such frameworks enhance threat detection, simplify compliance processes, and streamline operational oversight, ensuring compatibility with existing infrastructures without the need for costly overhauls. By providing a streamlined and adaptable approach, they effectively address the demands of modern cybersecurity challenges.

Additionally, extending INSM requirements to include Electronic Access Control and Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) addresses potential attack vectors that originate from connected cyber assets outside traditional trust zones. This expansion aligns with the NOPR's acknowledgment of vulnerabilities arising from these connected systems. **By encompassing IT, OT, and IoT environments,** INSM can

enhance visibility and reduce risks associated with lateral movement and hidden vulnerabilities within interconnected systems. EACMS and PACS are critical for operational control and monitoring and must be protected against unauthorized access and communication. By requiring **baselines for network activity and monitoring device communications,** the proposed standard would ensure that IoT environments remain secure and resilient against emerging threats.

Incorporating OT systems into INSM frameworks is a vital aspect recognized in this NOPR, reflected in referencing guidance from NIST SP 800-82 Rev. 3, which acknowledges the need for **segmenting and monitoring OT traffic.** These measures are critical for preventing lateral movement in industrial automation and control environments, where even minor disruptions can have significant operational impacts. **Agentless monitoring** solutions, which integrate seamlessly with existing infrastructures, should be considered to avoid disrupting sensitive operations in both IoT and OT systems. These solutions enhance **continuous monitoring, attack surface management, and remediation capabilities in real-time without disrupting sensitive operations.** By providing a comprehensive view of the security landscape, they enable robust protection while maintaining the integrity of critical processes. Leveraging AI-driven methodologies for network activity baselining and anomaly detection further strengthens the defense posture, swiftly identifying **deviations and enabling timely, effective responses to emerging threats.**

Further, the NOPR's focus on logging and analyzing network traffic with high fidelity is fundamental for anomaly detection and response. Leveraging dynamic anomaly thresholds, integrated with adaptive threat intelligence systems, minimizes false positives and enhances operational efficiency. These systems can adjust in real-time to evolving threats, enabling responsible entities to prioritize high-impact vulnerabilities and ensure timely mitigation. Also, the integration of proactive data governance policies would ensure streamlined operational efficiency and support rapid, effective incident response, which not only aligns with the NOPR's objectives but also sets the stage for a resilient, adaptive cybersecurity framework that meets the challenges of increasingly complex and interconnected infrastructures.

Incorporating Real-Time Simulation and Training Programs

A critical component of bolstering INSM effectiveness is workforce preparedness. Scenario-based training and simulation programs should be integrated into the regulatory framework to enhance entities' ability to detect and respond to threats. Advanced simulation environments that emulate real-world OT, IT, and IoT scenarios can strengthen preparedness for evolving cyber threats. Such training programs enable entities to test and refine their defenses against lateral movements and anomalies within complex network

environments. Additionally, these programs should align with the NOPR's emphasis on baselining network activity and anomaly detection. Emulating east-west traffic patterns and adversary tactics in controlled training environments enhances detection capabilities and provides actionable insights for improving operational resilience. This approach aligns with the NOPR's goal of equipping entities with the tools and skills to address vulnerabilities effectively in real-time scenarios.

Strengthening Data Retention Policies and Incident Response

The proposed emphasis on data retention and protection is another critical aspect of post-incident analysis and system integrity. Robust encryption standards should be mandated to secure logs against tampering or unauthorized access. Strong encryption protocols, automated anomaly detection (including real-time incident alerts), and secure logging mechanisms will maintain data fidelity, ensure accountability during incident investigations, and provide tangible insights when needed. By aligning these measures with the NOPR's focus on anomaly detection and response processes, **responsible entities can maintain high-confidence data fidelity while reducing the manual burden on security teams-** ensuring operational readiness, accountability in incident investigations, and resilience.

Further, integrating advanced incident response tools into INSM frameworks can enhance real-time threat mitigation and remediation recommendations. AI-driven systems for prioritizing vulnerabilities and implementing automated remediation workflows will support entities in responding efficiently to emerging threats. Such capabilities not only address the NOPR's logging and data protection requirements but also improve response times, reduce operational disruption, and enhance overall security posture, including addressing all risks found within the external attack surface.

As this NOPR implementation progresses, we encourage the Commission to leverage the expertise and solutions of our network, which stands ready to assist in building a stronger, more secure future for critical infrastructure.

We appreciate the opportunity to contribute to this critical initiative and look forward to continued engagement in refining these standards.

/s/ Michelle Sahar
Michelle Sahar
Cybersecurity Policy Director, OpenPolicy

Openpolicy

/s/ Dr. Amit Elazari
Dr. Amit Elazari
CEO & Co-Founder, OpenPolicy

Document Content(s)