Openpolicy

Feb 5, 2025

Via Electronic Filing

To: Transportation Security Administration (TSA), DHS

OpenPolicy comments on
Enhancing Surface Cyber Risk Management [Docket No. TSA–2022–0001]

I. Overview

OpenPolicy appreciates the opportunity to provide comments on TSA's **NPRM Cybersecurity Rulemaking for Pipeline and Rail Systems**. We commend TSA's **proactive approach** in standardizing cybersecurity practices across **pipeline, freight rail, and passenger rail systems**, ensuring alignment with key industry frameworks such as the **NIST Cybersecurity Framework (CSF) 2.0**, **CISA's Cybersecurity Performance Goals (CPGs)**, and **existing TSA security directives**. The rule's emphasis on **continuous risk management, attack surface monitoring, and cybersecurity incident response** reflects an essential commitment to **enhancing the resilience of critical infrastructure**.

OpenPolicy commends TSA for its leadership in advancing cybersecurity regulations for pipeline and rail systems. However, rather than relying on **static security frameworks**, TSA should mandate **continuous security validation, automated asset discovery, and real-time incident response** to enhance resilience across critical infrastructure operators. To ensure these regulations **remain effective against** evolving cyber threats, TSA should consider prioritizing automation, AI-driven security enforcement, and real-time risk monitoring as foundational elements of cybersecurity compliance.

To fully realize the rule's objectives, TSA should consider requiring AI-driven asset discovery to maintain continuous visibility across IT, OT, and IoT environments. Risk management should be based on **real-time threat exposure assessments** rather than **compliance checklists** that may overlook emerging risks. **Network segmentation policies** should be enforced dynamically using AI-powered micro-segmentation and behavioral analytics. Incident response should be proactive and integrated with real-time threat intelligence, ensuring that organizations can **detect and contain cyber threats before they escalate**.

Compliance mechanisms should also evolve from periodic audits to continuous monitoring, leveraging **automated security dashboards and risk-based policy enforcement** to maintain an **adaptive and scalable cybersecurity posture**. TSA could integrate automation into **compliance artifacts**, ensuring that security validation aligns with **baseline security measures** and **TSA's evolving cybersecurity requirements**.

Automating compliance documentation—such as risk assessments, access control enforcement, and incident tracking—would reduce the administrative burden on operators while enhancing accuracy, transparency, and enforcement of security policies.

Additionally, OpenPolicy would appreciate the opportunity to provide TSA with a **detailed mapping of security controls**, identifying where **Zero Trust principles, NIST CSF 2.0, and CISA's Cybersecurity Performance Goals (CPGs)** should be explicitly addressed within the regulatory framework. Aligning TSA's cybersecurity rule with these best practices will **ensure a forward-looking, risk-adaptive approach to securing critical infrastructure**.

Below, OpenPolicy outlines specific recommendations to **enhance TSA's proposed rule**.

II. Cybersecurity Risk Management Program (CRM): Sections C, D

TSA's Cybersecurity Risk Management (CRM) Program is a critical step in enhancing the security of the nation's transportation infrastructure by requiring comprehensive risk assessments, cybersecurity policies, and incident response plans. However, the proposed regulation must evolve beyond static risk frameworks to address the dynamic and rapidly shifting nature of cyber threats targeting transportation systems. The current requirements for cybersecurity evaluations and vulnerability management rely heavily on periodic assessments and broad risk categorizations, which may fail to capture emerging attack vectors in real time. Instead, TSA should mandate continuous asset visibility across IT, operational technology (OT), Internet of Things (IoT), and cyber-physical systems (CPS) to ensure organizations have an up-to-date understanding of their threat landscape.

Modern cyber threats often exploit **unmanaged or shadow assets** that fall outside traditional security perimeters. TSA can address **growing vulnerabilities** that stem from **overlooked or unmonitored devices** by expanding the definition of **"Critical Cyber Systems"** to explicitly include these assets. Recognizing the **broader and expanding threat landscape**, as emphasized in **NIST CSF 2.0**, requires organizations to **enhance their IoT and OT asset inventories** and **adapt their security strategies to account for network-connected infrastructure**. This shift acknowledges that **IoT and OT devices are increasingly integrated into critical operations** and must be continuously monitored for security risks.

A **static inventory approach** limits an operator's ability to detect and mitigate threats in real time, whereas an **automated asset discovery framework** enables organizations to **proactively identify risks and enforce security controls before incidents occur**. Continuous monitoring, coupled with **AI-driven risk scoring**, allows security teams to **prioritize vulnerabilities based on exploitability, business impact, and real-world**

threat intelligence, rather than relying solely on **predefined risk tiers or Common Vulnerability Scoring System (CVSS) ratings**. This shift from **compliance-based assessments to an intelligence-driven approach** aligns with **industry best practices**, such as **Continuous Threat Exposure Management (CTEM)**, and would significantly improve **resilience against cyberattacks targeting transportation networks**.

A key challenge in securing transportation systems is ensuring that security controls are not only implemented but also **continuously enforced across all connected assets.** The CRM framework should require organizations to adopt comprehensive asset discovery and risk management solutions that go beyond traditional security measures. Automated, agentless asset discovery technologies can identify all connected devices—including managed, unmanaged, IoT, OT, and IT—without requiring software installation. By integrating **continuous inventory updates**, security teams can maintain full visibility into their environments, ensuring that no device goes undetected or unprotected. This capability is essential for maintaining a current and complete view of an organization's attack surface, particularly in complex, interconnected transportation environments.

In addition to asset discovery, the CRM framework should **emphasize risk assessment and automated vulnerability prioritization** to help organizations allocate resources effectively. Advanced security platforms now provide real-time device risk scoring, vulnerability assessments, and behavioral analysis to determine which vulnerabilities present the greatest risk based on threat intelligence, asset importance, and likelihood of exploitation. Rather than treating all vulnerabilities equally, organizations should adopt a risk-based remediation strategy that prioritizes fixes based on business impact and environmental context. Automated solutions can consolidate security findings, assign context to vulnerabilities, and **ensure high-risk threats are addressed first.** The ability to track, monitor, and demonstrate progress through a centralized dashboard also helps organizations measure the effectiveness of their remediation efforts and **improve overall security posture.**

TSA's proposed rules also address network segmentation and access control as key cybersecurity measures, but these controls must be dynamically enforced rather than statically configured. Security solutions that enable policy-based micro-segmentation and network access control ensure that only authorized devices can communicate with critical systems. Organizations must move beyond perimeter-based security and implement **real-time network segmentation policies that dynamically adapt based on threat activity and asset behavior.** This approach is crucial for preventing lateral movement by attackers who gain initial access to a network. Additionally, advanced threat detection mechanisms—**such as anomaly-based and signature-based behavioral monitoring**—should be mandated as part of TSA's cybersecurity requirements. AI-driven

threat detection capabilities continuously monitor network and device behavior to identify potential attacks before they escalate into major incidents.

A strong incident response and compliance framework is also necessary to ensure timely cybersecurity event detection, containment, and reporting. TSA should require organizations to adopt automated incident response solutions that integrate with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms. Security technologies that provide automated response actions, forensic data collection, and real-time reporting allow organizations to contain threats more efficiently. TSA's focus on compliance monitoring should be expanded to include real-time audit trails, customizable reporting, and integration with broader regulatory frameworks such as NIST CSF 2.0.

To further improve security outcomes, TSA should encourage the use of **open API integrations that allow cybersecurity tools to work seamlessly together.** Cybersecurity in transportation systems cannot be siloed—security solutions must integrate with firewalls, Network Access Control (NAC), and endpoint protection platforms to ensure a unified and coordinated defense. Open API architectures facilitate such integrations, ensuring that security measures extend across the entire enterprise ecosystem.

By embedding **continuous asset intelligence, dynamic risk prioritization, and automated remediation into the CRM framework,** TSA can help ensure that operators are not just meeting regulatory obligations but actively reducing cyber risk in a proactive and scalable manner. The evolving nature of cyber threats requires an adaptive, intelligence-driven approach that aligns with industry best practices. The opportunity to refine these requirements to reflect modern cybersecurity methodologies and emerging threat trends is critical to securing the nation's transportation systems against the next generation of cyber threats.

III. Cybersecurity Operational Implementation Plan (COIP) (1580.307, 1582.207, 1586.207)

TSA's COIP establishes a structured framework for risk management, system security, and incident response across the transportation sector. However, to ensure that COIP requirements remain adaptable to emerging cyber threats, TSA should integrate **Zero Trust principles, automation in compliance enforcement, real-time asset intelligence, and advanced supply chain security measures**. A risk-based, intelligence-driven approach will allow organizations to proactively mitigate cybersecurity risks rather than relying on static compliance frameworks.

TSA's requirements for **network segmentation and access controls** provide a strong foundation for protecting Critical Cyber Systems (CCS), but the framework should explicitly incorporate **Zero Trust Architecture (ZTA)**. Traditional perimeter-based security is no longer sufficient, particularly as IT, OT, and IoT environments become increasingly interconnected. By shifting from static access controls to a continuous verification model, TSA can ensure that segmentation and identity management strategies remain adaptive and responsive to evolving threats. Organizations should implement **Zero Trust Network Access (ZTNA)** solutions to ensure that only verified users and devices can access Critical Cyber Systems, preventing lateral movement in case of a breach. AI-driven access policy enforcement should be encouraged to dynamically adjust security measures based on user behavior and anomalous network activity. These enhancements will significantly reduce the risk of unauthorized access, supply chain compromise, and ransomware attacks targeting transportation infrastructure.

COIP requires organizations to document cybersecurity measures, maintain security logs, and implement patch management strategies. While these requirements are essential, relying on **manual compliance tracking** creates operational inefficiencies and increases the risk of oversight. TSA should require organizations to adopt **automated compliance tracking and risk assessment tools** to ensure continuous validation of security configurations. By leveraging machine-readable formats such as **Open Security Controls Assessment Language (OSCAL)**, organizations can streamline regulatory reporting, dynamically update asset inventories, and improve security governance. Real-time configuration monitoring should be mandated to detect and remediate misconfigurations before they become security vulnerabilities. Automating compliance enforcement will reduce administrative burdens, improve accuracy, and allow organizations to focus resources on proactive security measures rather than static documentation.

TSA's definition of **Critical Cyber Systems (1580.313, 1582.213, 1586.213)** should explicitly include unmanaged **IoT, shadow IT, and cloud infrastructure**, as these assets often serve as primary attack vectors. Static asset inventories are insufficient in a rapidly evolving threat landscape. Instead, organizations should be required to **map interdependencies between Critical Cyber Systems dynamically**, ensuring that risk is assessed in real time rather than through static classifications. AI-powered asset intelligence and attack surface mapping should be mandated to continuously track system exposures, unauthorized connections, and high-risk configurations. This approach would ensure that organizations prioritize the most critical security gaps based on real-time risk exposure rather than relying on predetermined classifications that may overlook emerging vulnerabilities.

The proposal requires **supply chain cybersecurity oversight and vendor incident reporting**, but these requirements should be expanded to include **real-time monitoring**

and automated threat intelligence sharing. The increasing sophistication of supply chain attacks necessitates a more proactive approach to vendor security and third-party risk management. Organizations should be required to adopt **Software Bills of Materials (SBOMs)** to track vulnerabilities in third-party software and hardware components. TSA should also encourage the use of automated threat intelligence sharing mechanisms to improve industry-wide visibility of emerging supply chain risks. Vendor authentication policies should be strengthened to ensure that suppliers meet strict cybersecurity requirements before being granted access to operational environments. A **risk-informed, continuous supply chain security framework** will help prevent cyber incidents linked to software supply chain attacks, unsecured remote access points, and third-party data breaches.

While COIP establishes **incident reporting requirements and mandates centralized log retention**, organizations must be equipped to **detect and respond to cybersecurity incidents in real-time**. TSA should require the implementation of **AI-powered log analysis and anomaly detection** to identify security threats faster and reduce the burden on security teams. Integrating **security orchestration, automation, and response platforms** will enable organizations to automate incident response workflows, reducing manual intervention and accelerating remediation efforts. Threat intelligence-driven security analytics should be adopted to detect and mitigate sophisticated cyberattacks before they escalate. Compliance-driven incident reporting alone will not prevent widespread disruptions to critical infrastructure without real-time detection and response capabilities.

By integrating **Zero Trust principles, compliance automation, AI-driven asset intelligence, and enhanced supply chain security measures**, TSA can create a **dynamic, risk-based cybersecurity framework** that evolves with emerging threats. A **proactive, intelligence-driven approach** will allow organizations to improve cyber resilience, enhance compliance enforcement, and reduce the risk of operational disruptions caused by cyberattacks.

IV. Network Segmentation and Incident Detection (1580.317, 1582.217, 1586.217)

Effectively securing critical infrastructure requires a shift from traditional, static cybersecurity approaches to **adaptive, real-time security enforcement mechanisms**. TSA's proposed requirements for **network segmentation and access controls** are necessary to reduce the attack surface and prevent lateral movement within IT and OT environments. However, relying on manually enforced segmentation policies creates challenges, as these policies are often resource-intensive, difficult to manage at scale, and prone to misconfiguration. To strengthen this requirement, TSA should mandate **AI-driven micro-segmentation**, which dynamically enforces network access controls based on

real-time risk scoring and behavioral analytics. By leveraging AI to continuously monitor network traffic and adjust segmentation policies accordingly, organizations can ensure that only **authorized systems communicate with Critical Cyber Systems**, significantly reducing the risk of **ransomware propagation, supply chain intrusions, and insider threats**.

Beyond network segmentation, TSA's **incident detection and response requirements (1580.321, 1582.221, 1586.221)** must evolve to match the speed and sophistication of modern cyber threats. Traditional **signature-based detection and periodic log reviews** are no longer sufficient, as advanced attackers employ **stealth techniques that bypass static security controls**. Instead, organizations should be required to implement **real-time behavioral threat modeling, automated forensic data collection, and AI-driven anomaly detection**. These capabilities enable early detection of deviations from normal system behavior, allowing organizations to rapidly identify and mitigate cyber threats before they escalate **into full-scale incidents.**

A more effective approach to network segmentation and incident detection must incorporate **Zero Trust principles**, ensuring that **ac**cess to critical systems is continuously verified based on live threat assessments rather than static access permissions. By integrating real-time policy enforcement mechanisms, organizations can automatically **adapt access controls based on emerging risk factors**, such as unusual device behavior, privilege escalation attempts, or unauthorized lateral movement. This approach not only enhances **network security but also improves operational efficiency**, reducing the need for **manual policy updates and time-consuming access reviews**.

TSA's segmentation policies should also require continuous compliance monitoring, ensuring that network configurations align with **baseline security policies at all times**. Automating this process will prevent **misconfigurations that can create security gaps**, ensuring that network defenses remain aligned with evolving threats. Additionally, **AI-driven monitoring should extend beyond traditional IT assets** to include **unmanaged IoT and OT devices**, which often serve as entry points for cyberattacks due to limited built-in security controls. By incorporating real-time asset visibility and automated anomaly **detection**, organizations can immediately **identify unauthorized devices and isolate high-risk assets**, preventing threats from spreading across operational networks.

Further, TSA should refine its incident reporting and threat containment requirements by mandating real-time security observability and forensic data collection. Rather than relying on post-incident reporting, organizations should implement automated security intelligence platforms that continuously capture and analyze security data. This would allow for **immediate threat detection, faster containment, and enhanced post-incident analysis**,

ensuring that security teams can **act on real-time intelligence rather than after-the-fact forensic investigations**.

V. Enforcement, Compliance, and Documentation (1580.329, 1582.229, 1586.229)

The **Cybersecurity Evaluation (1580.305, 1582.205, 1586.205)** requirement mandates the development of an enterprise-wide cybersecurity profile, updated annually, to assess security risks. However, an **annual review cycle is insufficient** to address the **dynamic nature of cyber threats**. TSA should require **real-time cybersecurity evaluations** that continuously assess **asset vulnerabilities, security control effectiveness, and active threats**. Automated exposure management platforms should be leveraged to ensure **continuous monitoring and adaptive risk assessment**, reducing reliance on **static, point-in-time compliance checks**.

To further strengthen compliance, TSA should require organizations to maintain a **centralized risk dashboard** that provides **real-time visibility into cyber risks, security incidents, and remediation efforts**. This dashboard should integrate with automated cyber exposure management tools, enabling security teams to **dynamically track threat intelligence, vulnerability prioritization, and incident response progress**. A **continuous threat exposure management approach**, as outlined by industry best practices, would enhance security resilience by ensuring that risk assessments remain **actionable, proactive, and aligned with evolving threat landscapes**.

TSA's proposed **Governance (1580.309, 1582.209, 1586.209)** structure establishes clear **cybersecurity accountability measures** within organizations. However, **effective governance depends on comprehensive visibility into all cyber assets, including IT, OT, IoT, and cloud environments**. TSA should require organizations to implement real-time asset intelligence solutions that enable security teams to track all managed and unmanaged devices, assess their security posture, and enforce compliance dynamically. Governance models should also integrate **AI-driven automation to monitor risk exposure continuously**, ensuring security policies remain **adaptive and responsive to evolving cyber threats**.

Further, the **Cybersecurity Coordinator (1580.311, 1582.211, 1586.211)** role is critical for incident response, regulatory compliance, and security oversight. TSA could clarify that **Cybersecurity Coordinators must have access to automated risk intelligence platforms** to enhance **situational awareness, threat monitoring, and security coordination**. TSA could also require that these coordinators utilize real-time risk assessment tools to proactively detect threats, manage vulnerabilities, and enforce compliance. Ensuring that security decision-making is data-driven and integrated with

continuous monitoring capabilities will improve regulatory compliance and organizational resilience.

The **Identification of Critical Cyber Systems (1580.313, 1582.213, 1586.213)** requirement should emphasize not only the classification of critical assets but also the **continuous validation of their security posture**. Many organizations lack **real-time visibility into system health and security**, relying instead on compliance-driven asset documentation that does not reflect **live risk conditions**. To address this, TSA should require organizations to automate risk assessment and security validation, ensuring that **identified Critical Cyber Systems are continuously monitored for security gaps, misconfigurations, and unauthorized access**. Additionally, integrating automated anomaly detection and predictive risk modeling would allow organizations to identify and mitigate vulnerabilities before they can be exploited, enhancing the resilience of critical infrastructure against dynamic threats.

The **Supply Chain Risk Management (1580.315, 1582.215, 1586.215)** provisions reflect TSA's recognition of the need to mitigate third-party security risks, aligning with CISA's Cybersecurity Performance Goals (CPGs). However, to enhance transparency and risk mitigation across complex supply chains, TSA should explicitly require organizations to implement **SBOM tracking** and **third-party risk intelligence platforms**. These measures would enable organizations to proactively identify and address vulnerabilities in supply chain dependencies. Furthermore, TSA should enforce **real-time monitoring of vendor security postures, software components, and supply chain cyber risks** to prevent cascading failures and systemic threats stemming from compromised third-party assets.

The **Protection of Critical Cyber Systems (1580.317, 1582.217, 1586.217)** provision includes measures such as network segmentation, access controls, and software patching. However, traditional perimeter-based security models are no longer sufficient to address the sophistication of modern cyber threats. TSA should consider requiring organizations to implement AI-driven **network segmentation and anomaly detection technologies** that can **automatically enforce least-privilege access, identify suspicious activity, and respond to cyber threats in real time**. Integrating these advanced capabilities into TSA's compliance enforcement framework would enable organizations to maintain a proactive defense posture, detect cyber intrusions more effectively, and prevent lateral movement of threats within critical infrastructure networks.

As this draft implementation evolves, we look forward to discussing these proposals with TSA and are available for any questions. We remain excited to collaborate with TSA to increase engagement with innovative companies.

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

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