Openpolicy

Jan 16, 2024

**Via Electronic Filing**

To: National Institute of Standards and Technology (NIST)

***OpenPolicy comments on***
**NIST SP 800-172r3:Enhanced Security Requirements for Protecting Controlled Unclassified Information**

**Overview**

OpenPolicy appreciates the opportunity to provide feedback on the draft NIST SP 800-172r3. As an organization committed to advancing collaborative policymaking and enabling innovative approaches to cybersecurity governance, we commend NIST's efforts to enhance safeguards for Controlled Unclassified Information (CUI). The enhanced requirements in SP 800-172r3 represent a significant step toward bolstering protections against Advanced Persistent Threats (APTs) and strengthening the overall security posture of nonfederal systems and organizations. We commend NIST for incorporating empirical threat intelligence, prioritizing a threat-centric focus, and introducing additional protection objectives.

As a leader in promoting secure and adaptive practices, OpenPolicy actively engages with federal agencies, industry leaders —such as ***Armis, Censys, Kiteworks, Legit Security, FiniteState, ADAMnetworks, and Wiz***—and academia to develop forward-thinking solutions for managing emerging risks in complex ecosystems. Through partnerships with organizations in AI, data security, cybersecurity, and supply chain automation, we aim to empower stakeholders with tools that ensure transparency, resilience, and security in safeguarding critical infrastructure.

Following NIST's active engagement with government, industry, academia, and the public to understand their needs and develop practical, updated solutions and best practices, we believe that an open and collaborative policymaking dialogue is essential. This approach enhances the implementation of NIST's best practices and ongoing efforts to ensure a secure lifecycle by focusing on the core risks posed by the changing threat landscape, which is critical to fostering an appropriate, updated, and scalable risk management framework. The participation of innovative companies, particularly startups specializing in cutting-edge AI security, IoT, and safety solutions, significantly contributes to this effort.

OpenPolicy and its ecosystem of innovative companies are eager to collaborate with NIST to explore how technology and automation can best support effective security control

enforcement. We look forward to collaborating with NIST to identify and implement technologies that enhance transparency, resilience, and operational security across critical infrastructure.

*Below, we provide specific feedback on the draft guidance and propose redline enhancements to ensure comprehensive and forward-looking security practices.*

**Data-Driven Approaches for Usability and Resilience**

We commend the streamlined structure of NIST SP 800-172r3 and recommend further enhancing its usability by adopting standardized, machine-readable frameworks such as the **Open Security Controls Assessment Language (OSCAL)**. Transitioning from traditional document-based methods to data-driven approaches would allow for automated validation of controls, reduce compliance burdens, and improve interoperability with existing frameworks like SP 800-161 Rev. 1. Given the draft's complexity, which includes 89 enhanced requirements, over 100 organizationally defined parameters (ODPs), and numerous assignment and selection statements, adopting a more user-friendly, automated framework would significantly aid organizations in navigating and implementing its requirements effectively.

While the current structure provides a robust foundation, organizations may face challenges in prioritizing and operationalizing these requirements. Integrating OSCAL as a **core data-driven approach would enhance the draft's utility by enabling automation in mapping enhanced controls to foundational counterparts, streamlining documentation, and supporting real-time risk assessments.** For example, OSCAL could facilitate dynamic evaluations of control mappings, regulatory compliance, and supplier stability, ensuring organizations are well-prepared for both initial submissions and ongoing audits. Its machine- and human-readable architecture would also simplify processes like mapping dependencies, identifying gaps, and maintaining compliance across interconnected systems.

Automation is critical for **ensuring that baseline configurations remain accurate, complete, and up to date.** Mechanisms like those referenced in requirement **03.04.04E (Automation Support for Baseline Configuration)** demonstrate the potential to reduce reliance on resource-intensive manual processes, minimize human error, and maintain compliance while responding to evolving threats. Dynamic compliance tools that validate runtime environments further strengthen the resilience of systems processing CUI. These tools provide continuous monitoring, detect unauthorized changes, and isolate affected components, ensuring rapid mitigation of risks while maintaining compliance.

Additionally, integrating **enhanced visualization tools and cross-reference tables** would

clarify dependencies between SP 800-172r3, SP 800-171, and SP 800-53, making the framework more intuitive and accessible. **Incorporating AI-driven monitoring and data classification capabilities** would enable granular access policies while addressing emerging vulnerabilities in IoT and OT systems. These enhancements would not only support compliance but also improve organizations' ability to adapt to complex, interconnected environments.

By leveraging OSCAL and other advanced technologies, NIST SP 800-172r3 can become a scalable and adaptive framework, ensuring that the framework meets the demands of an evolving threat landscape, facilitates operational efficiency, and provides organizations with the tools they need to protect CUI in high-risk environments effectively.

**Enhanced Security Requirements and Threat-Centric Focus**

NIST SP 800-172r3 effectively emphasizes a multidimensional defense strategy to counter APTs. We recommend expanding the guidance to integrate real-time, automated mechanisms for threat detection and mitigation. Leveraging advanced tools such as automated allowlisting, runtime monitoring, and threat intelligence aggregation will enhance the efficacy of enhanced security requirements like **03.04.02E (Automated Detection of Unauthorized Components)** and **03.03.04E (Integrated Analysis of Audit Records)**. These technologies enable proactive identification and neutralization of vulnerabilities while supporting continuous monitoring. Additionally, incorporating deception technologies, as outlined in **03.13.08E (Decoys)**, can mislead adversaries, reducing their ability to cause harm. Expanding this requirement to include AI-driven dynamic decoy systems would strengthen the ability to detect and impede APTs.

This draft's alignment with evolving threat intelligence is commendable. We encourage incorporating more explicit guidance on leveraging AI and machine learning to dynamically analyze and respond to threats. Tools that aggregate and contextualize real-time threat intelligence can bolster safeguards like **03.04.03E (Automation Support for System Inventory)** and **03.01.08E (Account Monitoring for Atypical Usage)**. Real-time intelligence is critical for addressing the complexity of interconnected systems, including IoT and OT environments. Expanding the focus to address IoT-specific risks, such as open communication ports and insecure configurations, will further align this standard with modern cybersecurity challenges.

**Supply Chain Risk Management**

NIST SP 800-172r3 rightly emphasizes the protection of CUI in nonfederal systems, yet additional measures are needed to address the increasingly complex and interconnected

supply chain risks. While the framework introduces several key safeguards, such as **notification agreements (03.17.01E)** and **component authenticity (03.17.03E)**, these provisions could be further expanded to encompass **dynamic asset inventory management, IoT/OT-specific security considerations, and advanced remediation capabilities** to close critical gaps in visibility, accountability, and protection, ensuring that exploitable vulnerabilities across diverse ecosystems are identified and addressed proactively.

NIST SP 800-172r3 should also emphasize the use of **anomaly detection and behavioral analytics within supply chain security processes.** These technologies enable organizations to monitor device behaviors, firmware changes, and unauthorized communications in real-time, ensuring that emerging threats are detected and addressed dynamically. Such measures are particularly critical for IoT and OT environments, where traditional security tools are less effective. Coupling anomaly detection with comprehensive asset inventories provides actionable insights that enhance the effectiveness of core security measures, such as multi-factor authentication (MFA) and audit logging, across all connected systems.

The hierarchical organization of suppliers to assess dependencies and risks outlined in **03.17.01E (Notification Agreements)** is a robust starting point. However, the framework should explicitly require **mapping and monitoring all supply chain tiers**, with particular emphasis on **IoT and OT assets**. Unlike traditional IT components, IoT and OT devices often lack built-in security mechanisms, such as agent support, as highlighted in **03.04.02E (Automated Unauthorized or Misconfigured Component Detection)**. These vulnerabilities leave systems susceptible to ransomware, misconfigurations, and exploitation through default credentials. To mitigate these risks, NIST should encourage the adoption of **automated solutions for dynamic supply chain visualization**. This approach would empower organizations to trace the origin, operational lifecycle, and affiliations of devices, thereby addressing vulnerabilities tied to **foreign ownership, control, or influence (FOCI)**, as implied in the focus on **notification agreements and inspection of components (03.17.02E)**.

A **real-time, comprehensive inventory of devices, systems, and components**, including IoT, OT, and cloud assets, as specified in **03.04.03E (Automation Support for System Component Inventory)** and **03.04.04E (Automation Support for Baseline Configuration)**, provides the foundation for maintaining supply chain integrity. Incorporating **dynamic tracking of software dependencies and device configurations** ensures proactive remediation of risks such as open-source vulnerabilities, default passwords, and outdated firmware. These measures align with **Secure by Design principles**, embedding risk prioritization and mitigation directly into operational workflows

and reducing exposure to Advanced Persistent Threats (APTs). This aligns with the multidimensional protection strategy outlined in **Section 2.2** of the document.

Supply chain monitoring should also integrate **automated solutions for mapping supplier networks** and **assessing FOCI risks**, as discussed in **03.17.01E (Notification Agreements)** and **03.17.03E (Component Authenticity)**. Advanced tools capable of tracing the origin, affiliations, and lifecycle of IoT and OT components will enable organizations to reduce vulnerabilities tied to geographic or foreign influence. This approach aligns with the emphasis on supply chain risk management in NIST SP 800-161 Rev. 1 and strengthens the overarching goal of holistic supply chain security.

In addition to inventory and visualization, the inventory system should support **data encryption and secure storage** as foundational components for protecting sensitive information. This complements compliance frameworks such as NIST SP 800-171, GDPR, and ISO 27001, which prioritize encryption to safeguard sensitive data at every stage of its lifecycle. Encryption reduces the attack surface while enabling secure collaboration. Furthermore, adopting a **content-defined zero-trust model**, consistent with access control principles in **03.01.09E (Attribute-Based Access Control)**, ensures that access to data and systems is restricted to authorized entities, enforcing consistent security measures across organizational processes.

**Cloud Security in Supply Chain Risk Management**

Modern cloud environments, characterized by virtual machines, containers, serverless functions, and data volumes, introduce unique challenges that require **continuous visibility and adaptive risk management**, as suggested in the emphasis on automation and proactive strategies across multiple sections (e.g., **03.04.03E, 03.04.04E**). NIST SP 800-172r3 should advocate for governance frameworks that enable **real-time monitoring of cloud assets**, including mechanisms to detect and remediate misconfigurations, long-lived access tokens, and other exploitable cloud-specific vulnerabilities. The integration of **security observability** ensures comprehensive logging and runtime monitoring, capturing evidence of intrusions and insider threats while bolstering operational resilience. These provisions align with NIST's emphasis on cyber resiliency as a core strategy in **Section 2.2**. By integrating dynamic supply chain risk management with **IoT/OT security**, **real-time inventory**, **data encryption**, and **cloud observability**, organizations can enhance their ability to mitigate threats across interconnected ecosystems while achieving compliance with NIST and related frameworks.

**Post-Quantum Cryptography and Cryptographic Attestation**

The **adoption of post-quantum cryptography** represents a crucial enhancement to the security requirements outlined in **NIST SP 800-172r3**, particularly in the context of cryptographic protection and attestation mechanisms. As quantum computing advances, the vulnerabilities of traditional cryptographic algorithms to quantum attacks necessitate a proactive transition to quantum-resistant solutions. This aligns with the principles in **03.05.01E (Cryptographic Bidirectional Authentication)**, which emphasizes the use of cryptographically based bidirectional authentication to safeguard system connections. Extending this to include quantum-resistant algorithms would bolster the resilience of client-server and device authentication processes against future threats.

Furthermore, the requirement for **03.05.03E (Device Attestation)** underscores the importance of validating devices based on their configuration and operating state. By incorporating **post-quantum cryptographic attestation mechanisms**, the framework can ensure that only devices employing quantum-resistant cryptographic libraries and algorithms are deemed compliant. This approach strengthens the comply-to-connect policy and mitigates risks associated with supply chain vulnerabilities, as these mechanisms validate the integrity of cryptographic components embedded within critical systems.

The provisions in **03.14.01E (Software, Firmware, and Information Integrity)** and **03.14.09E (Cryptographic Protection)** further reinforce the value of integrating post-quantum cryptography. These sections call for cryptographic mechanisms to detect unauthorized changes and ensure the integrity of software, firmware, and information. Incorporating hybrid cryptographic approaches that combine classical and post-quantum algorithms can serve as a transitional solution, maintaining operational trust while facilitating the shift to fully quantum-resistant frameworks. This is particularly vital for safeguarding data at rest, in transit, and in use, as outlined in these sections.

Together, these measures not only address gaps in current cryptographic protections but also future-proof the security posture of supply chain components. By including **post-quantum cryptographic standards and hybrid approaches**, **NIST SP 800-172r3** can ensure resilience against emerging cryptographic vulnerabilities while meeting stringent security benchmarks for critical systems.

***Below are our detailed comments and proposed redlines:***

**03.04.02E: Automated Unauthorized or Misconfigured Component Detection**

The requirement for automated detection of unauthorized or misconfigured components is vital for maintaining the integrity of critical systems. However, its effectiveness could be

enhanced by incorporating **real-time, runtime monitoring and automated allowlisting** to detect anomalies in system configurations more dynamically. The inclusion of **AI-driven detection mechanisms** would further bolster the framework by enabling adaptive threat analysis, particularly for IoT and OT devices, which are prone to misconfigurations and exploitation due to their limited built-in security measures. Addressing IoT-specific vulnerabilities such as default credentials and open communication ports would align this section with the broader goal of countering advanced persistent threats (APTs).

**03.04.03E: Automation Support for System Component Inventory**

While this section effectively highlights the need for automated tools to manage system component inventories, it would benefit from an explicit focus on **dynamic asset inventory management**. This would involve tracking IoT, OT, and cloud-based components in real time, providing visibility into software dependencies, firmware versions, and lifecycle statuses. By incorporating **automated SBOM analysis**, the inventory process can detect and mitigate vulnerabilities tied to counterfeit or outdated components. This aligns with the goals of NIST SP 800-161 Rev. 1 and supports Secure by Design principles by embedding risk mitigation directly into asset management workflows.

**03.04.04E: Automation Support for Baseline Configuration**

Automation is a cornerstone of scalable compliance and operational efficiency. By leveraging automated mechanisms to maintain **accurate, complete, and up-to-date baseline configurations**, organizations can reduce reliance on manual processes prone to human error. These automated tools should continuously validate and update configurations, aligning them with current security standards. This capability is especially critical in dynamic environments where system configurations must frequently adjust to respond to emerging threats or operational changes.

Automation also supports **runtime environment validation**, enhancing system resilience by detecting deviations from approved configurations in real time. For example, unauthorized changes to system components can be promptly identified, isolated, and addressed through automated alerts to appropriate personnel. This continuous monitoring and validation create a feedback loop that strengthens compliance while enabling rapid responses to potential threats. This requirement could be expanded to integrate **real-time compliance monitoring** tools that automatically validate configurations against predefined baselines. These tools should also incorporate anomaly detection to identify unauthorized changes, particularly in IoT and OT environments, where such deviations are common due to their susceptibility to exploitation.

**03.05.01E: Cryptographic Bidirectional Authentication**

This section provides an essential safeguard for verifying identities in communication exchanges. However, additional emphasis on **secure certificate management** and automated renewal processes would reduce the risks posed by expired or compromised certificates. Extending the use of cryptographic bidirectional authentication to IoT and OT systems would further secure these vulnerable environments.

**03.05.03E: Device Attestation**

Device attestation is critical for ensuring the trustworthiness of components. To strengthen this requirement, organizations should leverage **automated attestation tools** capable of continuously validating the integrity of devices during their operational lifecycle. This is particularly relevant for IoT devices, which often lack robust security features and require consistent monitoring to detect tampering or unauthorized modifications.

**03.06.02E: Integrated Incident Response Team**

The creation of integrated incident response teams is critical for addressing complex threats like APTs. To enhance this requirement, NIST should advocate for the inclusion of **threat intelligence sharing platforms** that enable teams to access real-time data on evolving adversary tactics. Additionally, mandating regular incident response drills and the use of AI-driven tools to simulate APT scenarios would improve preparedness and response times.

**03.06.04E: Automation Support for Incident Reporting**

While this section focuses on incident reporting, it could be improved by advocating for **security observability** mechanisms. These mechanisms would ensure comprehensive logging, capturing not only intrusions but also insider threats, misconfigurations, and other vulnerabilities across the system lifecycle. Leveraging AI and machine learning to analyze these logs in real time would enable organizations to prioritize critical incidents and respond more effectively.

**03.12.04E: Internal System Connections**

This requirement could be strengthened by adding a clause to enforce **strict encryption and authentication for internal file transfers**. Specifically, segmenting data repositories ensures that only approved systems or services can interact with high-value files, reducing the risk of unauthorized access or data exfiltration. By isolating sensitive files and encrypting internal transfers, organizations can better align with zero-trust principles and mitigate potential attack vectors that exploit weak internal connections.

### 03.14.01E: Software, Firmware, and Information Integrity

The focus on protecting the integrity of software, firmware, and information is essential. However, this section could be expanded to include **integrity monitoring for IoT and OT environments**, where firmware updates are particularly vulnerable to tampering. Requiring the use of trusted update mechanisms and secure boot processes would ensure that only authenticated updates are applied.

### 03.14.09E: Cryptographic Protection

Cryptographic protection is essential for safeguarding sensitive information at rest, in transit, and during use. However, this section could be improved by incorporating **post-quantum cryptography (PQC)** guidance to prepare for the future risks of quantum computing. Hybrid cryptographic approaches that combine classical and quantum-resistant algorithms should be explicitly encouraged to ensure a smooth transition to PQC. Additionally, integrating **cryptographic attestation mechanisms** would enhance trust by verifying the authenticity of components before they are deployed in secure environments.

### 03.14.18E: Automated Organization-Generated Alerts

To enhance incident response capabilities, organizations should **enable file versioning and quarantines**. When a file is identified as suspicious or corrupted, it should be immediately isolated, examined, and either repaired or removed. Automated quarantining and versioning mechanisms ensure that potentially harmful files are neutralized quickly, reducing the risk of system-wide compromise. This capability also supports forensic investigations and aligns with the need for robust incident management processes.

### 03.15.02E: Defense In Depth

The **defense-in-depth approach** detailed in this requirement should incorporate **advanced content-based risk policies, encryption, and multi-factor authentication (MFA) at the file level**. By designing security architectures that protect documents, endpoints, and networks holistically, organizations can achieve comprehensive coverage against dynamic threats. This recommendation aligns with the **CISA Secure By Design Initiative**, emphasizing the proactive integration of layered security measures across systems. Such an approach ensures that every layer of the infrastructure contributes to the overall security posture, protecting CUI with robust and interoperable defenses.

### 03.17.01E: Notification Agreements

This section rightly emphasizes establishing agreements for timely supplier notifications. To enhance its scope, organizations should adopt **dynamic monitoring tools** that provide real-time updates on supply chain risks, such as counterfeit components or geopolitical vulnerabilities tied to foreign ownership, control, or influence (FOCI). These agreements could also mandate the use of automated reporting platforms to streamline communication and improve transparency.

**03.17.03E: Component Authenticity**

This section's emphasis on verifying component authenticity is commendable. Expanding this requirement to mandate **automated SBOM analysis** would strengthen the ability to detect counterfeit components and validate the integrity of software and hardware across supply chains. Such tools can also be used to cross-check against resources like the Known Exploited Vulnerabilities (KEV) Catalog, ensuring timely mitigation of risks. Integrating these capabilities with **03.17.01E (Notification Agreements)** would facilitate real-time supplier notifications and enable rapid resolution of component authenticity issues.

**Supply Chain Risk Management (General)**

The framework addresses key supply chain risks but lacks explicit guidance on **cloud-specific considerations**. Cloud environments introduce unique challenges, such as the risks posed by long-lived access tokens, misconfigurations, and container vulnerabilities. Proactively integrating **cloud risk management tools** that enable real-time visibility, runtime monitoring, and automated remediation processes would ensure comprehensive protection. **Security observability** tools should also be emphasized to provide actionable insights into potential threats across virtual machines, serverless functions, and data volumes.

**Definition of Internet of Things**

The current draft defines the "Internet of Things" as [t]he network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information; and "Industrial Internet of Things" as "[t]he sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications.

The recent attack surface expansion has elevated the establishment of baseline security controls and evolved the concept of zero trust to the Internet of Things. Accordingly, recent policies released, including the IoT Cybersecurity Improvement Act, OMB memo 24-04

(section 2)[1], and most notably, NISTIR 8259 series and the IoT Cyber Trust Mark Rule and applicable baseline (NISTIR 8425), have expanded the definition of IoT to include operational technologies. NIST 8259, referred to in federal and OMB memo 24-04 refers to the IoT as: "having at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface". NISTIR 8425 expanded the definition of IoT products. Consistent with this approach and to align this NIST guidelines with the emerging attack landscape, we proposed the following changes to these definitions:

"Internet of Things" - ~~[t]he network of~~ [D]evices or products that contain the hardware, software, firmware, sensors or actuators, and their network. ~~which allow the~~These devices, networks or products to connect, interact, and freely exchange data and information. IoT devices or products typically have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface" (see NISTIR 8529). IoT devices can include the Industrial Internet of Things and operational technologies.

We further propose to amend the "Industrial Internet of Things" to: "[t]he sensors, instruments, machines, components, products, other devices and the networks that support them, that typically use internet connectivity to enhance industrial and manufacturing business processes and applications or support operational technologies.

***As this draft implementation evolves, we look forward to discussing these proposals with NIST and are available for any questions. We remain excited to collaborate with NIST 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

[1]See M-24-04 Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements (December 4, 2023). 5-8. https://shorturl.at/aDJLw