Openpolicy

July 23, 2024

OpenPolicy comments on the

Streamlining Federal Cybersecurity Regulations Act

OpenPolicy is grateful for the opportunity to contribute comments on the proposed bill, as part of our ongoing commitment to improving national cybersecurity policies and regulatory frameworks. We appreciate this opportunity to contribute to the development of more coherent and harmonized cybersecurity regulations.

OpenPolicy is a technology company seeking to democratize the ability of innovative companies of all sizes to engage with policymakers and provide feedback on relevant policy deliverables, which underscores the transformative potential of aligning standards, controls, and guidelines across various agencies and international frameworks. This alignment is not just a necessity for enhancing national cybersecurity resilience, but also a catalyst for a diverse ecosystem of innovative companies.

The necessity for coherence between existing cyber requirements and newly introduced cybersecurity mandates is paramount and could not be emphasized enough. Aligning with established guidelines and controls promotes open channels for sharing information on AI risks, leading to broader compliance and national resilience at lower costs. This regulatory endeavor underscores our broader ecosystem's dedication to fostering an environment that supports innovation, mitigates risks, and promotes a more coherent approach to cybersecurity across various governmental, sectorial, and international domains. By addressing the challenges of overlapping and conflicting regulations, we can significantly reduce operational burdens and simplify compliance with new AI cybersecurity mandates.

Establishing regulatory harmonization is a fundamental first step; however, deploying a scalable strategy is crucial to ensure the effective implementation of standards, controls, and future regulations. In the face of AI's rapidly evolving threat landscape, adopting a risk-based approach that leverages ***technological solutions*** **to measure cybersecurity outcomes, and support reciprocity,** is indispensable. Simply establishing unified security and risk measurement controls is not enough; there must also be a scalable strategy to ensure these controls are effectively implemented and aligned with the evolving threat landscape - as they seek to adopt controls. Put simply, it is not sufficient to lay down and unify controls for cybersecurity and risk measurement if we do not have a scaled approach to ensure such controls are adopted harmonically. Such solutions must be capable of ensuring broad compliance with continuously evolving regulatory frameworks. As

highlighted in Mr. David B. Hinchman's testimony, numerous legislative efforts, including the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and various initiatives by the Government Accountability Office (GAO), have been directed towards enhancing these harmonization efforts. These initiatives are designed to streamline and synchronize requirements across different strategic areas. However, many of these vital recommendations have only been partially implemented, underscoring an urgent need for a scalable regulatory strategy ***that leverages automation and measurable compliance to advance risk governance.***

Enhancing our focus on leveraging automation and measurable compliance is essential, as it significantly advances risk governance and supports a unified government approach in regulatory alignment. This strategic enhancement increases the capability of agencies and the broader industry to scale and standardize measurements efficiently. Collaboration between agencies, auditors, and developers with solution providers is crucial to automate control measurements and ensure consistency across compliance efforts. Such an approach can benefit from tools like the OSCAL tool developed by NIST, which transitions traditional document-based methods to a data-centric approach using standardized formats to represent control catalogs, baselines, and security plans, ensuring interoperability and facilitating seamless communication among stakeholders. Further, these measures could also foster more accurate and scaled techniques for implementation validation, human rights impact assessments, and controls for public application presentation, which are crucial aspects and practices of risk management strategies and secure development and deployment of new and current cybersecurity strategies. For example, OSCAL's extensible architecture supports both machine—and human-readable formats, allowing tool developers to implement APIs and create compliance tools based on standardized data, further enhancing integration across various systems as well as speeds up documentation and streamlines reporting, enhancing risk management through readable reports generated automatically from continuous monitoring systems. This application can further support harmonization processes, with OSCAL expansion requiring more stakeholder contribution and appropriate funding.

Incorporating mechanisms such as OSCAL and similar processes, in the Streamlining Federal Cybersecurity Regulations Act is significant as it supports control mappings and strongly supports the ongoing implementation of the Cyber Executive Order and other government initiatives. A technology alignment that fosters more accurate and scaled techniques for implementation validation, human rights impact assessments, and controls for public application presentation, crucial aspects of risk management strategies. These measures prepare organizations for initial submissions and auditing to achieve compliance,

securing the development and deployment of new and current cybersecurity strategies and ensuring that the harmonization broader goal is achieved and implemented effectively.

Further, Nicholas Leiserson's testimony remarks underscore a pivotal area of concern—the need to harmonize federal cybersecurity regulations to reduce unnecessary expenditures and enhance overall security outcomes. The presence of duplicative or contradictory regulations not only imposes unwarranted costs on regulated entities but also diverts critical investments away from substantive cybersecurity improvements. By implementing a strategic, unified regulatory approach, we can achieve superior cybersecurity outcomes that are more cost-effective for businesses and their customers. Moreover, the cumulative cost of compliance, driven by the several proposed expansions of liability and scope, as in the revised CIRCIA ruling, necessitates a balanced approach that aligns with enhanced cyber resilience and value-driven risk reduction. Stakeholder engagement has consistently highlighted, further emphasized in the ONCD report, the issues stemming from regulatory complexity and duplicity, particularly the challenges it poses for small businesses during critical incident response phases when resources are scarce. There is a pressing need to simplify these requirements to alleviate the extensive compliance burden.

By advancing a strategy emphasizing automation and measurable compliance, the cybersecurity ecosystem can improve risk governance and adopt a whole-of-government approach in regulatory alignment. This strategy would facilitate the scaling of measurements and foster collaboration among agencies, auditors, and developers with solution providers to automate control measurements, ensuring consistency in compliance efforts. The benefits of a harmonized and reciprocal cybersecurity oversight approach would reduce the administrative burden associated with varied or redundant regulatory requirements, allowing entities to allocate more resources to enhance their cybersecurity frameworks. This leads to the establishment of a national common cybersecurity baseline with standardized tools and services, increasing compliance while decreasing cybersecurity costs.

1. **Scalability and Future-Proofing Cybersecurity Measures:** Consistent with the principles laid out in OpenPolicy's CIRCIA testimony,[1] We recommend implementing streamlined reporting mechanisms across federal agencies. This would reduce the administrative overhead on small businesses and startups, which are disproportionately

[1] See United States House Committee on Homeland Security Subcommittee On Cybersecurity and Infrastructure Protection hearing entitled, "Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking", OpenPolicy testimony, available at https://www.congress.gov/118/meeting/house/117105/witnesses/HHRG-118-HM08-Wstate-ElazariJSDA-20240501.pdf (May 1, 2024).

affected by the complexity and duplicity of current regulations. With AI threats as a constantly evolving challenge, we suggest scalable cybersecurity strategies that utilize advanced technological solutions to ensure that risk assessments and regulatory measures are dynamically adjusted to align with the evolving threat landscape, enhancing compliance and national security.

2. **Leveraging Technology and Automation:** OpenPolicy encourages identifying further opportunities to utilize technology and automation tools to guarantee that agencies and industry adoption practices align with a similar proactive, secure, and safe approach to cybersecurity management and resilience. Automation can further support the complex goal of aligning the implementation of the AI EO, with the Cyber Executive Order with the ongoing implementation and upcoming revisions of FedRamp FISMA 2024 priorities related to IoT and OT protections (where AI can be leveraged), and NIST documents such as CSF 2.0 and NIST RMF/SSDF revisions. A further focus on leveraging automation and measurable compliance (e.g., schemes like OSCAL) can advance risk governance in this respect and increase the ability of NIST, CISA, OMB, and other agencies to scale agency measurements, as agencies and auditors can collaborate with solutions providers to automate control measurements. Such technologies will enable agencies and the industry to collaboratively enhance the accuracy of control measurements and ensure consistent compliance efforts across the board.

3. **Focus on 'Secure by Design' Principles:** Integrating Secure by Design principles across developing and revising directives for software, products, and IoT security is crucial. This integration supports a scalable technology framework that enhances the effective and efficient management of cybersecurity risks. Essential revisions to existing directives—including CISA's Secure-by-Design, NIST CSF 2.0, and SP 800-53—are necessary to broaden the product security scope and encompass comprehensive IoT and software development requirements. Utilizing advanced technology, precise control measurements and compliance automation tools is fundamental to achieving a secure posture alignment. These tools support a scaled approach to securely designing software and IoT systems and managing AI risks, bolstering compliance, and enhancing governance across all levels of cybersecurity infrastructure. This approach fortifies security measures and ensures that cybersecurity practices keep pace with technological evolution, thereby safeguarding our digital infrastructure more effectively.

4. **Addressing Global Cybersecurity Standards:** In the ongoing efforts to fortify national cybersecurity infrastructure, it is imperative to adopt and integrate comprehensive guidelines and best practices that cover a wide range of technologies, including IoT, IT, software, cloud services, and AI. These practices should not only safeguard against

adversarial threats but also ensure the protection and integrity of data, privacy, and security across these platforms. As part of our commitment to international collaboration, particularly in light of the NIST-EU dialogues, aligning some of the scopes and used languages ongoing federal and state cybersecurity efforts, such as the CCPA, with global regulations, such as the GDPR, EU Cyber Act, and AI Act, is crucial. This alignment will enhance the adaptability, development, and deployment of cross-national technologies, ensuring that our cybersecurity measures meet common ground with international standards development and deployment requirements. Such harmonization promotes broader mutual recognition and facilitates scaled information sharing and security compliance measurements. By aligning our standards, languages, and use cases with other international endeavors, we can better support the seamless integration of security protocols across borders, thereby enhancing the resilience and efficacy of global cybersecurity infrastructure and positioning the US as the leading entity of cybersecurity standardization.

/s/ Dr. Amit Elazari
Dr. Amit Elazari
CEO and Co-Founder of OpenPolicy

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