Openpolicy

April. 29, 2024

**Testimony of**
**Dr. Amit Elazari, J.S.D. , CEO and Co-Founder of OpenPolicy**
**Before the 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"**

Wednesday, May 1, 2024, 2:00 PM ET
310 Cannon House Office Building

Chairman Garbarino, Ranking Member Swalwell, and distinguished members of the Subcommittee, on behalf of OpenPolicy and our community of innovative companies, thank you for the opportunity to testify today on the *Cyber Incident Reporting for Critical Infrastructure Act* or (CIRCIA).[1] We appreciate your leadership in supporting the passage of CIRCIA, and commend your critical role in conducting oversight of the Law's implementation process. We very much welcome the opportunity to continue working with this Subcommittee.

At a time when threats to our nation have never been more profound, and the consequences for human lives, critical infrastructure, and the foundational institutions on which we rely, have never been more prominent, the majority of businesses and critical infrastructure providers still stand defenseless against persistent and existential cyber threats. These threats have only expanded with the advancement of AI; the convergence of operational technology (OT), IoT, and IT systems; and the growing sophistication of adversaries.

CIRCIA, perhaps the most comprehensive legislative action on cybersecurity in decades, presents a critical opportunity to increase the government's situational awareness, reduce cyber risk, and move us collectively forward in the endless asymmetric fight against adversaries seeking to undermine U.S. national and economic security.

**But, as I must emphasize - only If implemented properly.**

My name is Amit Elazari, and I am the CEO and Co-Founder of OpenPolicy, a small business and technology company (otherwise known as a "startup"). I'm also the former Head of

[1] 6 U.S.C. 681–681; Public Law 117–103, as amended by Public Law 117–263 (Dec. 23, 2022).

Openpolicy

Cybersecurity Policy at Intel Corporation, served as Chair of the Cyber Committee of the Information Technology Industry Council (ITI), and was a member of the IT-Sector Coordinating Council (SCC) Executive Committee.

In addition to my current role, I teach at the University of California at Berkeley in the Master in Information and Cybersecurity Program and serve as an advisor to the UC Berkeley Center for Long-Term Cybersecurity. I also co-founded Disclose.io, whose body of work related to establishing authorization for third-party "good faith" security research (ethical, or "friendly" hacking) is referred to in the CIRCIA proposed implementing rule ("Rule" or NPRM").

In my capacity as a cyber policy expert, I engaged extensively in the stakeholder process as CIRCIA was drafted, and am now actively engaged in the rulemaking process. Today, I'm honored to share my views, and the view of the OpenPolicy community, on the progress made regarding CIRCIA implementation and the proposed rule.

By way of background, OpenPolicy[2] is the world's first policy intelligence and engagement technology platform, aiming to democratize access to the policy-making process for entities of all sizes by leveraging AI. OpenPolicy is a small business and perhaps the smallest member of the IT Sector Coordinating Council.

OpenPolicy collaborates with and represents leading innovators that develop cutting-edge technologies to enhance cybersecurity and protect critical infrastructure. OpenPolicy members include some of the world's leading AI, IoT, and botnet prevention security companies such as ***Armis, Human Security, FiniteState, HiddenLayer, Kiteworks, Cranium AI,*** and more. Our members' solutions are used extensively by the critical infrastructure community and among federal agencies to protect against malicious attacks.

My testimony identifies concrete policy recommendations that seek to align the Rule and CISA's implementation process with Congressional intent. I also want to highlight the Rule's impact on small businesses. This Committee is right to reflect on the implementation of CIRCIA, given its mandate, and also because of changes in the policy landscape, technology itself, and the threat landscape since both CIRCIA's enactment and the RFI release. OpenPolicy applauds you for facilitating this discussio.[3]

---

[2] www.openpolicygroup.com.

[3] CIRCIA requires covered entities to report to CISA covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made. See 6 U.S.C. 681b(a).

Openpolicy

***Background***

Recent events underscore the urgent need to strengthen national security and defense, and the opportunity CIRCIA has to advance government situational cyber awareness.

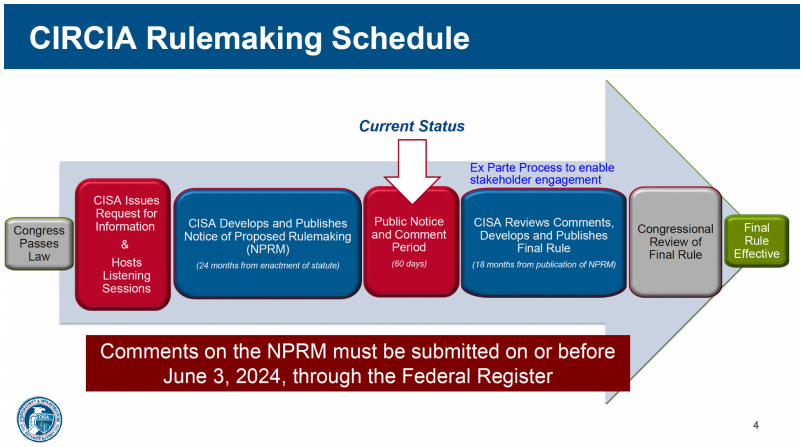
The promise CIRICIA holds relies on the ability of CISA to quickly intake reports, allocate resources, and provide support to entities affected by cyber incidents. CISA seeks to identify trends and swiftly disseminate this information to network defenders. Such proactive sharing will help alert other potential targets about emerging and existing threats and ideally prevent them from succumbing to similar attacks.

This use of information from the time an incident is reported, in support of immediate remediation but also to further longer-term prevention - is what CIRCIA aims to achieve and is meant to enhance our collective security. **Congress intended for CIRCIA to not only improve government awareness of cyber incidents but also to enhance security resilience throughout the entire ecosystem and ultimately advance risk reduction.**

The effectiveness of CIRCIA and its underlying regulations should be measured not only by how efficiently information from reported cyber incidents is examined, enriched, and transferred, but also by how that information is leveraged to improve the security of the entire ecosystem, i.e., in a manner proportional to the cost (estimated in $U.S. billions). Achieving this goal will entail a unified federal policy for leveraging the reported information to increase cyber resilience. This will require actions that extend beyond CIRCIA and the Rule. But the Rule, implemented correctly, presents a critical opportunity to advance this goal.

***On the matter of Rulemaking process:***

***The landscape will continue to change - The Rulemaking process on CIRCIA should enable "ex parte" filings and engagements in the 15 months that follow the comment period***




*[ex parte comment process added, source: CISA]*

CISA's 450-page NPRM on CIRCIA was released on April 4, 2024. Indeed, CISA's comprehensive and diligent work has resulted in an extensive Rule that will have a significant impact on our nation, its security posture, and definitions that will have a profound impact on small businesses and the startup/innovation community. The majority of impacted entities may not be able to bring their unique point of view forward during this timeframe, and most lack the resources and access to government affairs professionals.

CISA has engaged extensively with stakeholders via the RFI, and various listening sessions, yet the critical phase of the regulatory development process ***begins now*** - with the release of the Proposed Rule, the Comments Consideration and adjudication process, and preparation for Final Rule release. **Thus, we encourage CISA not only to extend the comment period and continue with the stakeholder engagement process but to also create a process that will allow for additional "ex parte" meetings and filings on the Rule. This should be accompanied by a transparent process for ex parte filings publication, similar to the proposed rules processes conducted and operated by the Federal Communications Commission or the Copyright Office.**[4]

Such a process would ensure that perspectives could be provided in a transparent and inclusive manner to CISA as the policy, technology, and threat landscape evolves in the 15-month period that follows the NPRM release and after the comment period has ended.

---

[4] See, for the FCC, 47 CFR §§ 1.1200–1.1216, and Federal Communication Commission, "Ex Parte Resources", https://www.fcc.gov/proceedings-actions/ex-parte/general/ex-parte-resources. See, for the Copyright Office, 37 CFR §§ 201, 205, U.S. Copyright Office, Ex Parte Communications, https://www.copyright.gov/rulemaking/ex-parte-communications/.

This would enable additional engagement and better alignment on the Rule, following the formal comment period.[5]

***On matters of policy:***

***The cumulative cost of compliance burden, due to the proposed scope and expansion of liability, should be balanced and reciprocated with increased cyber resilience and risk reduction value***

The record on stakeholder engagement reflects consensus on underlying concerns associated with definitions and issues proposed to be addressed in the Rule:

- **Complexity and Regulatory Duplicity** (among federal agencies and regulators, states and federal laws, and other applicable global regimes, such as E.U. NIS 2.0 directive) that will result in duplicative reporting, information and data overload, "noise", and extensive compliance burden on entities, including on small businesses, during the critical, "fire-fighting" period of incident response, when resources are limited. There is an urgent need for "harmonization" and streamlining of requirements.
- Concerns related to the definition of "covered cyber incident" capturing "**too much**" and in a manner that does not advance CISA's situational awareness, but rather overwhelms CISA.
- Concerns related to the **chilling effect of expanded liability,** which may hinder the public-private partnership model that undergirds information-sharing and threat mitigation practices today with the U.S. government and CISA, in particular.
- Concerns related to the **scope of covered entities** and impact on smaller businesses.
- Concerns related to the adverse impact to privacy and security due to increased information sharing, in certain cases, and the case of sharing sensitive "vulnerability" information in particular.

[5] OpenPolicy conducted meetings and filed "ex parte" comments on a recent Cybersecurity policy related Rule and Order released by the FCC, which were ultimately cited in the final Order. We find this process to be very useful and essential in a case where the evolving landscape merits continued, transparent engagement during the long period of comments adjudication, and particularly beneficial for small businesses who may not be able to engage on NPRM by the end of the comment period. We acknowledge the robust engagement processes already done by CISA, and further encourage CISA to continue and expand its engagement processes with innovative companies and small businesses, especially for sectors where they serve a large proportion of the impacted community, such as the DIB.

The Rule proposes a broad scope on many of these issues, notably the definitions of covered entities, incidents, and required fields. It notes however CISA's goal is to "achieve the proper balance among the number of reports being submitted, the benefits resulting from their submission….". Our overarching recommendation is to ensure that the ***cumulative impact and increased costs*** associated with such expansion, will in fact, result in ***additional value*** to risk reduction and enahnced cyber resilience.

To that end, OpenPolicy proposes the following policy recommendations:

To ensure enhanced situational awareness of cyber threats across critical infrastructure sectors "translates" into enhanced cyber resilience and risk reduction, CISA should consider:

- Additional reports, support functions, and public-private partnership structures focused on impacted under-resourced entities for information sharing and cyber resilience resources.
- Robust consideration to ensure that state-of-the-art secure and diverse sets of technology solutions, including AI capabilities, are used to intake incident reports,[6] review them, respond, and enable real-time mitigation in a way that supports entities' ability to transition from "remediation" to "prevention".[7]
- Alignment of other CISA, and other government-supported, resources (including programs such as CDM) to the nexus of threats, indicators, and compromises "spotted" via the reporting.
- Increased funding and resources to support the intake of remediation solutions and overall resilience of critical infrastructure, including federal infrastructure, to attacks - embodying the zero trust and secure by design culture.

---

[6] One method of technology adoption could be adopting standardized reporting forms supported by advanced programmatic and technological capabilities, whereby CISA can quickly operationalize, anonymize and share data with the industry in a way that is not attributed to specific entities. This approach ensures that incident information, rather than being relegated to solely routine threat reports, is transformed into actionable intelligence that can be immediately utilized to protect entities and enhance industry awareness and preparedness. The primary purpose of this reporting requirement should be to deliver critical and practical information in real time, enabling frontline cyber defenders to thwart attacks. Clarifying this goal will significantly aid in addressing the tactical details of the final rule. It would not only ensure that it meets its intended objectives effectively but also foster the overall resilience and awareness of the entire cyber ecosystem.

[7] CISA notes, the concern from "noise" increased scope (as illustrated by a broader set of "entities", "incidents", and "reporting fields"), "can be mitigated through technological and procedural strategies." [Rule, at 23652-3]. More attention and resources should be provided in support of such ***technological and procedural strategies***, to achieve the desired "translation" effect. CISA also recognizes further the breadth of duplicity and also that agencies may have different motivations in requesting such information.

Openpolicy

Our continued focus should be ***preventing attacks, not only remediating them***. The volume of reports should be calibrated in service of this cause. Achieving this goal will entail a broader technical and programmatic collaboration between all federal agencies involved, as well as the adoption of technology solutions.

To summarize, CISA was tasked with regulatory development and proposed definitions seeking to balance these inquiries with the underlying congressional intent of CIRCIA. The NPRM reflects a ***cumulative extended scope*** of proposed definitions with respect to covered entities, the scope of incidents to be reported, the application on small businesses, and the potential (and actual risk) for duplicative burden for reporting.

***Overall this approach reflects a higher "cost" and "burden" that needs to be accompanied by a balanced "value", and progress in situational awareness and risk reduction - thereby enabling a significant "giving back" component.***

***Further action is needed to reduce the potential cost associated with regulatory duplicity and the potential for liability***

CISA has acknowledged both the concerns of stakeholders associated with a complex reporting landscape and the need for further action on this matter.[8]

We recommend the following:

- CIRCIA Agreements, geared to enable information-sharing mechanisms and the underlying technology architecture to support such sharing in a secure manner, should be ***prioritized, resourced and achieved***. The Rule clarifies that good-faith efforts to reach such agreements would be made. However and as demonstrated by policy actions in the last two years, achieving this goal requires a more holistic and deliberate effort from all agencies involved and Congress. As the Congressional Research Report on CIRCIA puts it:

  > "It seems unlikely that federal regulators will relinquish their specific reporting requirements in deference to CISA because existing regulations and the proposed CIRCIA rule *serve different purposes*."[9]
  > (emphasis added).

[8] "In an attempt to minimize the burden on covered entities potentially subject to both CIRCIA and other Federal cyber incident reporting requirements, CISA is committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable and seeks comment from the public on how it can further achieve this goal." Id. at 23653.

[9] Congressional Research Service, CIRCIA: Notice of Proposed Rule Making: In Brief, April 11, 2024.

- One of the focal points of the CIRCIA agreements should be addressing the potential overlap with reporting requirements applicable to the Defense Industrial Base (DIB), under DFARS clause 252.204-7012. This path will reduce the considerable burden on a sector that is largely composed of small businesses (see below). This approach could be enabled by two related policy actions that recently matured. First, The DoD DFAR is soon to be revised,[10] thereby enabling further harmonization, despite the difference in scope of the "incident" definition.[11] Second, the DoD recently announced supporting infrastructure that can potentially enable a CIRCIA Agreement.[12]
- Congress should conduct oversight and perhaps even act in service of achieving additional CIRCIA agreements and reducing duplicity, when practical and desired, to achieve agency alignment.
- The need for harmonization and reducing duplicity is clear.[13] **The path towards reducing regulatory duplication, including with globally applicable regimes, should move away from aspirational and exploratory, toward actionable and practical - and such efforts will likely require a common technology architecture, where additional resources may be needed.**
- **On legal liability, we recommend enhanced "due process" mechanisms for covered entities.** We are concerned about liability protection erosion in the case of good-faith disagreements between CISA and the covered entity. As drafted, liability protection measures are "abandoned" once a subpoena is issued but without intervening process. While CIRCIA provides CISA the ability to use its subpoena power, the current NPRM does not include further consideration, or a "curing" process, an arbitration process, or other procedures to deliberate with CISA, in

[10] The Defense Acquisition Regulations Council Director has recently tasked a team with rule development, exploring a revision for DFARS clause 252.204-7012, DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (See DFARS Case 2023-D 024, has described, on the DFARS Open Cases Report, https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf.

[11] Compared to the CIRCIA proposed rule definition, covered entities in the Defense Industrial Base (DIB) Sector are already obligated to report cybersecurity incidents in a substantially similar timeframe (72 hours) pursuant to DFARS clause 252.204-7012, see *Safeguarding Covered Defense Information and Cyber Incident Reporting*. In contrast, the current scope of the DIB sector reportable incidents is narrower, and focuses on compromises of Controlled Unclassified Information while the CIRCIA proposed rule outlines a broader scope for "covered incident".

[12] On March 12th, 2024, DoD published the Defense Industrial Base Cybersecurity Activities (DIB CS) final rule, which expands eligibility to DoD's voluntary incident reporting and cyber threat intelligence sharing program to all DIB entities (rather than just cleared defense contractors).These revisions will allow all defense contractors who own or operate an unclassified information system that processes, stores, or transmits covered defense information to benefit from bilateral information sharing.

[13] See also the National Cybersecurity Strategy, at p. 11, "The Federal Government must coordinate the authorities and capabilities of the departments and agencies that are collectively responsible for supporting the defense of critical infrastructure".

good-faith, the amount of information requested prior to CISA leveraging its subpoena power, while enabling the entity to maintain liability protection (see § 226.14(d)(1), and ps. 23735). We recommend further consideration and Congressional oversight to ensure a measured approach in the Final Rule implementation on this topic.

***Small Businesses First "Mindset"***

Although the CIRCIA proposed rule affects many small entities across all critical infrastructure sectors, its impact on the ***DIB Sector*** small business community is profound. Defense security compliance ***Industry Expert Jacob Horne*** provided some striking analysis:[14]

- Nearly a quarter of all affected entities are in the Defense Industrial Base Sector
  - Of the 316,244 affected entities, CISA estimates 72,000 of them are in the DIB
- 17% of entities affected by the CIRCIA proposed rule are DIB SMBs
  - DoD has stated that roughly 75% of the DIB is made from small and medium-sized businesses

  That amounts to 54,000 of the 72,000 DIB entities in Table 1 Affected Population, by Criteria (see NPRM, at 23742).
- 98% of affected entities are SMBs, 17% of affected SMBs are in the DIB

  o Of the 316,244 covered entities, CISA estimates that 310,855 would be considered small entities (See, *Id*. at 23763).

| | DIB Sector | Wire/Radio Comms | Critical Manufacturing | Financial Services |
|---|---|---|---|---|
| % Total Affected Entities | 23% | 20% | 12% | 12% |
| % Total Costs | 16% | 14% | 9% | 9% |

**See Table 1 and Table 10 of the NPRM, *Id.***

***We, therefore, recommend prioritizing "scoping" activities (such as achieving CIRCIA agreements) impacting small businesses that are profoundly impacted by the Rule, such as the DIB small business community.***

[14]See also Jacob Horne, Sum IT Up Podcast: CIRCIA Rulemaking and Double Incident Reporting for the DIB, available at: https://www.summit7.us/blog/circia-rulemaking?hs_amp=true.

,

Openpolicy

***Summary***

The Congressional intent for CIRCIA is “preserv[ing] national security, economic security, and public health and safety”, and assisting the federal government with increasing situational awareness and visibility to cyber threats in support of a broader mission to achieve systemic risk reduction for the United States and its underlying critical infrastructure. This ultimate value, of increasing cyber resilience merits additional proportionality between the cost, and value of and processes CISA and the federal government will exercise to “give back” to impacted communities who bear the implementation cost. This balance may require more resources and additional infrastructure to “rapidly deploy resources” and better diverse, state-of-the-art solutions to stay ahead of malicious actors and deploy alerting systems. It will further require those who need to alert the government - to have solutions, and “alert systems”, to spot issues, and to intake alerts and process them into action. To achieve cyber resilience we must approach CIRCIA implementation in the context of the broader common fabric of cybersecurity policy efforts, implemented in the U.S and globally.

Creating the architecture, technically, procedurally, and programmatically, and the culture, that truly achieves the underlying risk reduction goal of CIRCIA will require action from CISA, and other agencies, that may extend beyond the Rule, but proper implementation of CIRCIA can result in considerable progress. Much progress has been made - we will continue to rely on Congress's relentless attention to this matter, as we move forward with CIRCIA’s implementation.

*Thank you for the opportunity to testify today and look forward for your questions.*

Dr. Amit Elazari
CEO and Co-Founder
OpenPolicy

Openpolicy

***About OpenPolicy***

OpenPolicy[15] is the world's first policy intelligence and engagement technology platform, aiming to democratize access to the policy-making process for entities of all sizes by leveraging AI. OpenPolicy collaborates with and represents leading innovators who develop cutting-edge technologies to enhance cybersecurity and protect critical infrastructure. OpenPolicy members include some of the world's leading AI, IoT, and botnet prevention security companies such as *Armis, Human Security, FiniteState, HiddenLayer, Kiteworks* and more. Our members' solutions are used extensively by the critical infrastructure community and among federal agencies to protect against malicious attacks. OpenPolicy aims to represent the voice of smaller entities and innovators, which are at the forefront of developing solutions to address emerging threats. We strive to focus on actionable policy recommendations to advance our collective goal to secure and protect the nation. OpenPolicy has engaged on policies related to IoT security, AI security, software security, OT security and cloud security. OpenPolicy previously submitted written testimony for the record for this esteemed Subcommittee on Security Threats to Water Systems.[16] And while we have been operating less than a year, OpenPolicy is honored to be quoted and recognized by the White House, the Federal Communication Commission, the Department of Justice, and other government agencies for our substantive contributions to the policymaking process. We believe there is tremendous potential for increasing the voice of innovative companies, including cybersecurity solutions providers, in the policy-making process.

[15] www.openpolicygroup.com.

[16] Subcommittee Hearing, on Cybersecurity and Infrastructure Protection hearing entitled, "Securing Operational Technology: A Deep Dive into the Water Sector", Feb. 6, 2024.