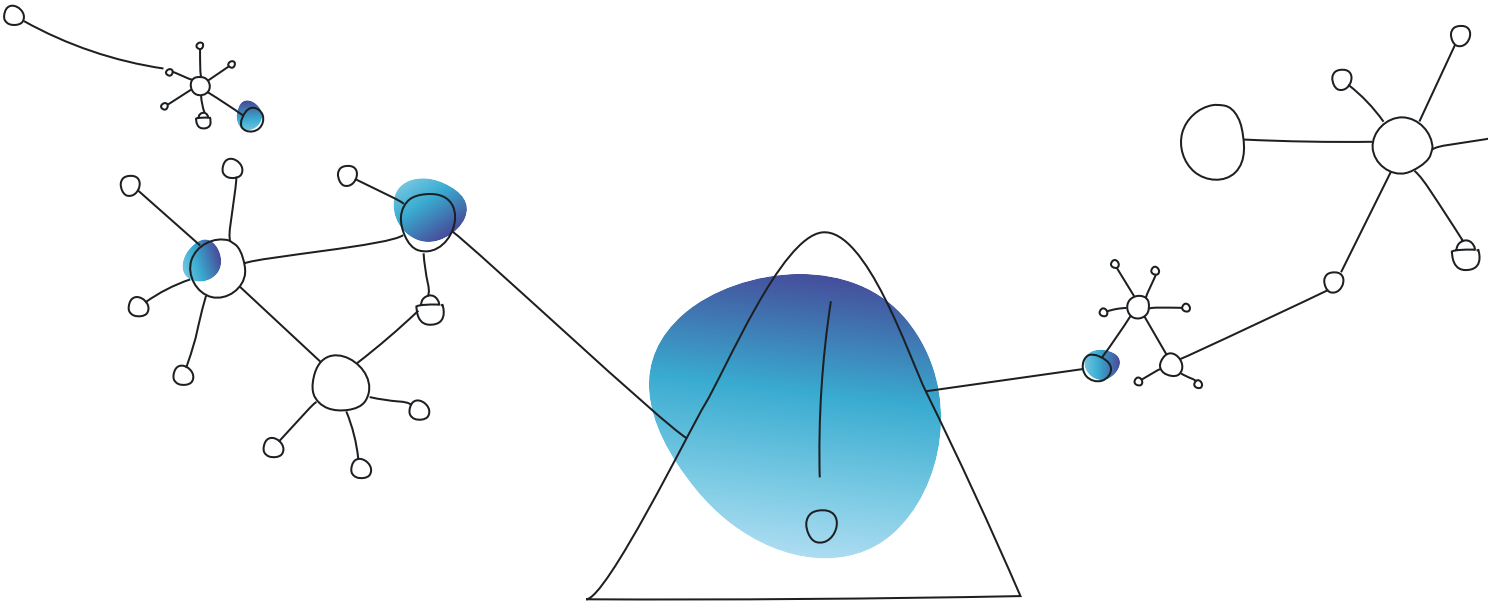
TEAM8™

CISO COMMUNITY RESPONSE

CISA RFI on the Cyber Incident Reporting for Critical Infrastructure Act of 2022



By the Team8 CISO Village

December 2022

WRITTEN BY

Amit Ashkenazi

Former Legal Advisor of the Israel National Cyber Directorate, and before that Head of the Legal Department at Israel's Privacy Protection Authority

Gadi Evron

CISO-in-Residence
Team8

The writers would like to thank members of the community, both in Team8's CISO Village, and outside of it. Due to the sensitivity of the CISO role, most of our 350 members could not openly sign the document, so we kept their contributions anonymous. Over sixty CISOs actively engaged with us in writing this response, with many others reviewing.

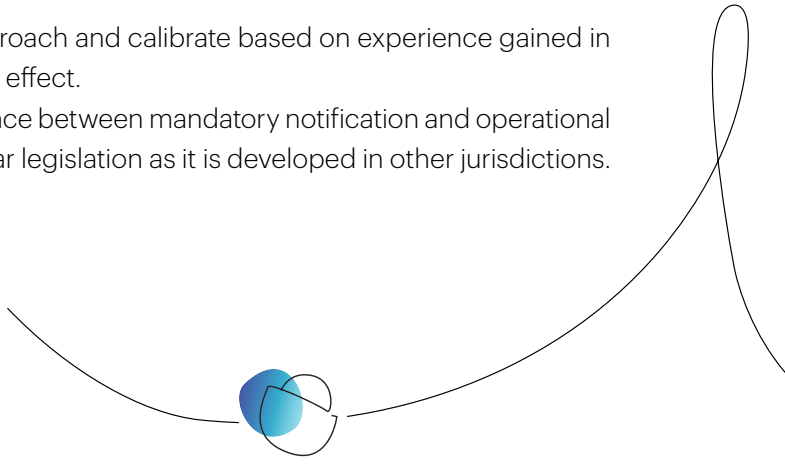
The Team8 CISO Village is an exclusive community of CISOs from the world's leading enterprises.
The primary focus of the Village is to facilitate collaboration among the world's most prominent companies with the goal of sharing information and ideas, conducting intimate discussions on industry and technology trends and needs, and generating value and business opportunities for all parties.
By helping Team8 to identify real pain points and understand the requirements of large organizations, members of the Village are first in line to leverage solutions that are purpose-built by Team8's portfolio companies to support their needs.

To contact the Team8 CISO Village, please email **cisovillage@team8.vc**

The Team8 CISO Village community consisting of roughly 350 Chief Information Security Officers,[1] respectfully submits observations and recommendations regarding the proposed Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rulemaking,[2] to convey the importance of considering CIRCIA's impact on CISOs in general.[3]

Our key points are:

- CISA should specifically consider CIRCIA's potential impact on the role and operations of the CISO:
  - CISO operations in and out of an incident.
  - CISO intra-organizational relations.
  - Unintended consequences and liabilities for the CISO.
- CIRCIA notification rules should be "cybersecurity oriented" and not "regulation-oriented":
  - "Cybersecurity orientation" means rules should focus on promoting information sharing and incident mitigation.
  - "Cybersecurity orientation" also means that rules should reflect industry cybersecurity playbooks, information-sharing taxonomies, standards, and cooperation modalities.
- The application of CIRCIA should be a two-way street:
  - CISA should promote clarity as to what actionable information CISA will share back with the reporting organizations.
  - CISA should clarify the overall process once a notification is submitted, and how CISA and the CISO should interact after a report is issued.
- Focus on clarity as a core principle – where possible:
  - CIRCIA introduces legal rules to a sensitive cybersecurity moment. We recommend that the rulemaking start with a narrow approach.
  - Where issues are not clear, go for a modular approach and calibrate based on experience gained in the field over time, once the regulation goes into effect.
- CISA has the opportunity to establish the right balance between mandatory notification and operational cybersecurity, setting a global benchmark for similar legislation as it is developed in other jurisdictions.



[1] The term "Chief Information Security Officer" is meant to apply to the senior executive with relevant expertise in charge of cybersecurity in an organization, recognizing that the title may change amongst organizations.

[2] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022

[3] The contributors to this process do not represent a specific organization or body, and did so in their personal-professional capacity, which does not necessarily represent the official position of their present employers.

01

CIRCIA's potential impact on the CISO profession and its internal and external interactions – promoting America's cybersecurity workforce

Our first priority is to convey the importance of considering CIRCIA's impact on CISOs in general. Clearly, CIRCIA was enacted to promote important national security and public interest goals. We also support more overall accountability, which the law will incentivize. But, when implemented on the ground, we ask that consideration be given to the host of incentives and disincentives for information sharing and how the law will affect the work of CISOs, and their organizational interactions. The design of rules that consider their impact on these interactions is crucial for the effectiveness of both CIRCIA deployment and the CISO role. We elaborate on this point below.

Organizations' Chief Information Security Officers are the professional pillar of organizational cybersecurity efforts. They are in charge of developing and deploying the cybersecurity framework and are the top managers of the cybersecurity workforce. But being professional is not enough. At the same time, they need the trust, support, and resources of their boards of directors. A notable group of CISOs recently described this relationship based on the NIST framework. [4]

Reporting Cyber Risk to Boards [5]

CISO Edition
Control, Measure, Report, Repeat

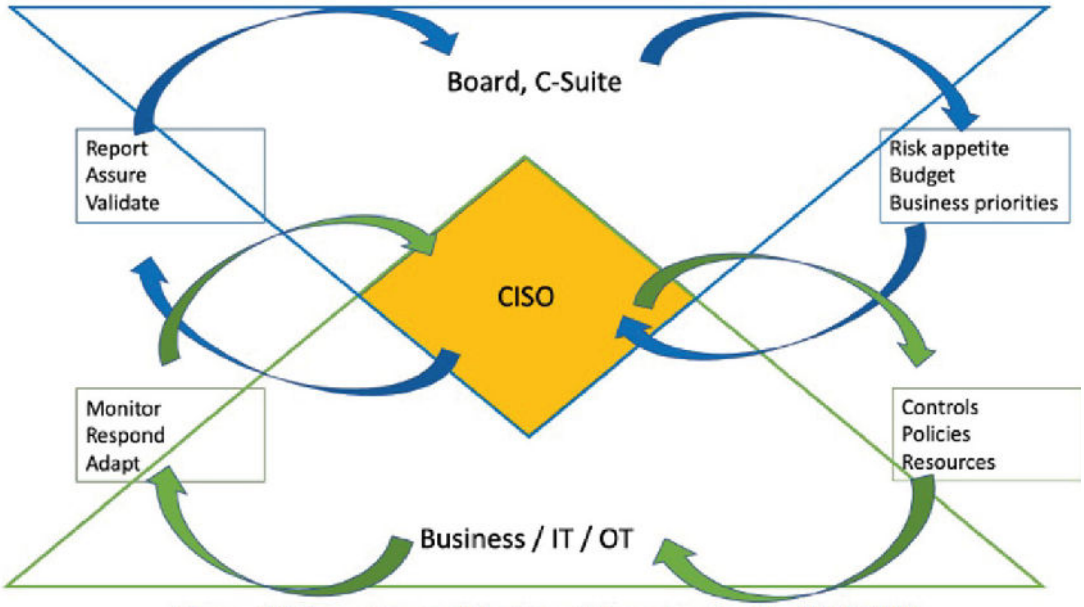


Figure 3 Information and Decision Flows. Inspired by NIST CSF

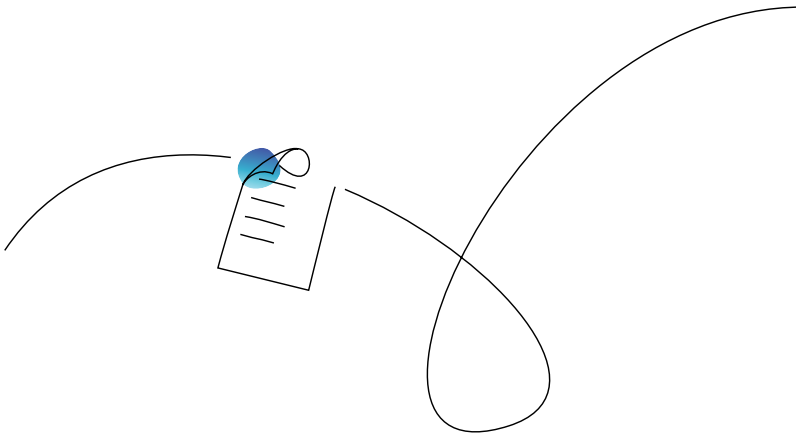
[4] Dezeure F, Webster G., Trost J, Leverett E., Gonvalves J.P., Mana P., Mccord G, Magri J, (Reviewers: Moerel, L., Iftmie A., Deverell C., Bell G., Hutchinson J., Reporting Cyber Risk to Boards, https://cert.be/en/paper/reporting-cyber-risk-boards. Illustartion used with authors' permission

[5] Ibid p. 6.

The CISO's leadership and organizational status are essential for the rest of the cybersecurity workforce. Recent events have drawn attention to CISO's possible legal exposure and the challenges of the CISO-management-board interactions.[6]

In a cyber incident, the CISO needs to manage cyber defense, deal with recovery, and communicate findings and implications to a host of stakeholders. The trust of the board is essential. While the CISO needs to manage triage and incident response, legal and regulatory officers must assess and manage exposure. Management needs to oversee and manage the event, compliance, and recovery. The additional legal obligations that CIRCIA adds could create additional challenges in an already complex and tense environment. It also may have unintended consequences and potential liabilities for the CISO, which may cause a "chilling effect" on sharing information. Noting CIRCIA's important limitations on the "legal" use of reports,[7] questions still arise as to whether reports can be later used against a CISO.

Thus, CIRCIA has broader implications for CISO operations, intra-organizational relations, and obligations. From this point of view, CIRCIA should align with the policy imperative of strengthening America's cybersecurity workforce.[8] Our recommendations below explore how CIRCIA rules can be developed to promote the coherence and clarity of the cybersecurity discipline and support cybersecurity professionals within their organizational settings.



[6] For a discussion of some of the issues that are worrying CISOs, see: Team 8, A CISO's Guide to Legal Risks and Liabilities, October 2022, https://team8.vc/rethink/cyber/cisos-guide-to-legal-risks-and-liabilities/

[7] See the limitations and protection on information shared according to Section 2245(5) of CIRCIA.

[8] See Executive Order 13870 of May 2, 2019, "America's Cybersecurity Workforce," 84 FR 20523, https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce, section 1: **"America's cybersecurity workforce is a diverse group of practitioners who govern, design, defend, analyze, administer, operate, and mainatain the data, systems, and networks on which our economy and way of life depend. Whether they are employed in the public or private sectors, they are the guardians of our national economic security."**

On "Cybersecurity Burnout" see for example: ThreatConnect Inc, Cybersecurity Burnout: The Critical Risk for Organizations to address in 2022, https://www.prnewswire.com/news-releases/cybersecurity-burnout-the-critical-risk-for-organizations-to-address-in-2022-threatconnect-research-301466507.html

"Key Findings Include:

- Senior decision-makers across the US report an average security staff turnover rate of 20%.
- 64% of senior decision-makers have seen a rise in turnover over the past year.
- 43% of US respondents attribute a lack of skills as the biggest barrier for recruitment.
- 1 in 5 US respondents are considering quitting their jobs in the next six months.
- 57% of US respondents have experienced an increase in stress over the past six months."

02

CIRCIA notification rules should be "cybersecurity-oriented" and not "regulation-oriented."

2a. Promoting information sharing and incident mitigation.

CIRCIA is based on the long-recognized rationales **for public-private and private-public information sharing**, as described aptly by the CISA Director.[9] Thus, to our understanding, its main focus is on filling critical information gaps in knowledge of the actual level of risk and supporting government activity to reduce the impact on national security, public safety, and essential interests.

Unlike typical breach notification regimes, it seems that CIRCIA is not focused on compliance, enforcement, or investor protection. Rather, it pragmatically focuses on **national "situational awareness"** that enables real-time action. Indeed, real-time responses are essential for cyber defense.

In the discussions within the CISO community in preparing this submission, we have heard different interpretations regarding the intent and scope of the additional legal duties in CIRCIA, the effects on thresholds of reporting, and the implications of reporting.

This is a core issue, as CISOs and the organizations they work for, need clarity as to the implications of reporting. If sensitive details are exposed, or an incident report to CISA immediately triggers a duty to report to the Securities and Exchange Commission, then reporting may create additional direct regulatory, reputational and financial risk. These implications should rightly concern the board and legal counsel, and may put additional legal pressure on the CISO.

We are concerned that if CIRCIA becomes mainly a regulatory compliance regime, the "cyber" line of communications will be further driven by legal considerations. This would cause legal "friction" or process blockers to communications that need to be timely and often unfiltered to contain attacks.

The law needs to recognize that the primary goal of the CISO during a breach is to restore business operations and continuity, as well as the investigation. Moving the focus from defense to compliance limits the CISO's capacity to protect. In the discussions within the CISO community, questions have arisen regarding the potential personal liability of the CISO in these scenarios. Exploring these issues may also create more overhead during the critical incident response time, take attention from mitigating the event, and create a disincentive for reporting.

[9] See statement by CISA Director Jen Easterly: "The Cyber Incident Reporting for Critical Infrastructure Act of 2022 is a game changer for the whole cybersecurity community and everyone invested in protecting our nation's critical infrastructure. It will allow us to better understand the threats we are facing, to spot adversary campaigns earlier, and to take more coordinated action with our public and private sector partners in response...We can't defend what we don't know about and the information we receive will help us fill critical information gaps that will inform the guidance we share with the entire community, ultimately better defending the nation against cyber threats. We look forward to continuing to learn from the critical infrastructure community – through our request for information and our coast-to-coast listening sessions – to understand how we can implement the new cyber incident reporting legislation in the most effective way possible to protect the nation's critical infrastructure." (emphasis not in original). https://www.cisa.gov/news/2022/09/09/cisa-welcomes-input-new-cyber-incident-reporting-requirements

Our recommendations are as follows:

- Set very clear thresholds for reporting that require as little interpretation as possible and can be applied by legal counsel based on clear triggers. Given the novelty of CIRCIA, in case of doubt, set thresholds high.
- Clarify with explicit guidance CIRCIA limitations on use of the report, in line with the CIRCIA statutory language.[10] There should also be clarity as to who will see the report in the government, and that the government will respect the secrecy of the company such that the report will be considered "TLP red,"[11] unless otherwise agreed by the reporting company or redacted. Thus, information should be restricted to law enforcement/national security for the purpose of mitigating the attack or its impact only.
- Aim to uncouple the threshold reporting from the actual content of the report. For example, appropriate company officers and legal counsel should decide if the reporting threshold has been passed, while the actual content of reporting should be carried out through technical channels by the CISO.
- Clarify that the reporting duty is the organization's and not the CISO's.
- Consider having a "CISO" hotline where CISOs can informally consult.

2b. The rules should reflect industry standard practices

Cybersecurity as a discipline has matured and encompasses industry standards, playbooks, and information-sharing taxonomies and modalities. CIRCIA should interface with these practices as smoothly as possible to reduce regulatory burden and encourage voluntary sharing.

Our recommendations are as follows:

- The content of the incident report should be based on existing industry standards for cyber-related information.
- Content should focus on cyber-related information about the attack vector and relevant (and known) indicators of compromise. Focus on aspects such as the affected dataset, the nature of telemetry, and its accuracy. Be advised that fast reporting will affect accuracy and allow for room to correct or clarify.
- Explore the role of existing information-sharing communities that enable organizations to quickly share information on their incidents with CISA and simultaneously with the sector or organizations that fall in the same category (possibly anonymized, either manually or automatically).
- Clarify how CIRCIA mandatory reporting fits in the larger context of information-sharing modalities.
- We propose that CISA conduct a focused professional discussion to define what content will be appropriate for the report, building upon existing formats.

[10] See the limitations and protection on information shared according to Section 2245(5) of CIRCIA.
[11] See: CISA, Traffic Light Protocol (TLP) definitions and use, https://www.cisa.gov/tlp

03

The application of CIRCIA should be a two-way street – CISA should promote clarity as to what information CISA will share back, its notification feedback loop, and interactions with CISA after a report.

Clarity about the feedback loop, CISA response, and the possible sharing of information relevant to the incident provide an important incentive for effective information sharing.

We think CISA should have a published process for its feedback loop that lets the reporting organization know what is being done with the data, if any relevant government action will be taken, and whether the reporting organization can expect additional support from CISA. Feedback should come back to the reporting organization within a defined timeframe that is relevant to the mitigation process.

In addition, it would be useful for CISA to promote rules about the way it shares and distributes information, under CIRCIA section 2245(B), in tandem with the rules that apply to organizations.

Our recommendations:

- CISA should clarify how notification fits in the operational process that is relevant to the reporting organization.
- CISA should inform organizations what they can expect in terms of information from CISA.
- CISA should have clear communication guidelines with a unique point of contact.

04

Focus on clarity and a narrow approach - given the novelty of this law

CIRCIA is a new legal obligation that applies to one of the most sensitive events in organizational cybersecurity. It sets legal rules of behavior in a constantly developing field. Thus, it risks burdening cybersecurity operations or flooding CISA with notifications. We suggest narrowly tailoring terms under the law to allow all to gain experience with its application. Where issues are unclear or may cause interpretation issues, we recommend erring on the side of clarity at the price of comprehensiveness. As all parties gain more experience in the actual application, CISA can update and recalibrate the rules.

This also applies to the **content** of the incident notification. The mandatory requirements should acknowledge the difficulty in assessing the situation in the first 72 hours. Therefore, it should include minimal details, such as the attack vector and the estimated timeframe for producing a clearer picture.

05

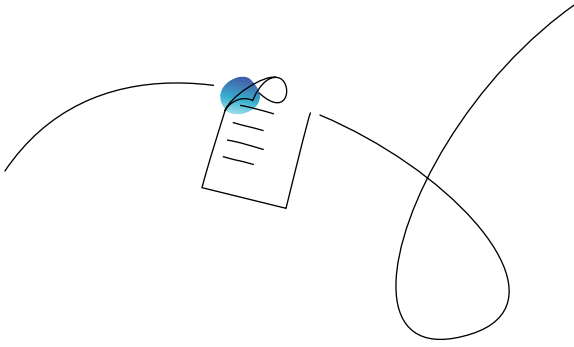
CISA has the opportunity to establish the right balance between mandatory notification and operational cybersecurity, setting a global benchmark for similar legislation as it is developed in other jurisdictions.

Many jurisdictions are developing mandatory notification rules. If CIRCIA rules effectively promote public-private information sharing, they can affect the global policy discussion in this area, promoting coherence and serving as a benchmark. The existing situation that applies to data protection breach notification has already been described as a "global patchwork."[12] Therefore, such an outcome should be avoided.

CONCLUSION

CISOs are a key part of the organizational cybersecurity process; therefore, legal rules that apply to cyber incidents affect them. When designing legal rules, these effects should be taken into account. CIRCIA rules should be developed with the aim of promoting the coherence and clarity of the cybersecurity discipline and of supporting cybersecurity professionals within their organizational settings.

We appreciate the opportunity to contribute to this important process and remain at your disposal for any clarifications.



[12] On the challenges of the different data protection breach notification regimes see: U.S. Chamber of Commerce and Hunton, Andrews, Kurth, Seeking Solutions: Aligning Data Breach Notification Rules Across Borders, 2019, https://www.huntonprivacyblog.com/2019/04/04/hunton-partners-with-the-u-s-chamber-of-commerce-on-seeking-solutions-aligning-data-breach-notification-rules-across-borders/