CENTER FOR DATA INNOVATION

Feedback to the European Commission on the Draft Cyber Resilience Act

The Center for Data Innovation (Transparency Register #: 367682319221-26) is pleased to submit this feedback on the European Commission's consultation and call for evidence regarding the Cyber Resilience Act. The Center previously submitted feedback on the roadmap for the Cyber Resilience Act and has been closely following its development.[1]

OVERVIEW OF THE CENTER'S POSITION

The Center would like to commend the European Union (EU) for focusing on the growing threat of cybersecurity incidents, which is predicted to cost $10.5 trillion by 2025.[2] The EU has a critical role in promoting cybersecurity practices that counter global cybersecurity threats and the Cyber Resilience Act is a strong step in the right direction. The Cyber Resilience Act is intended to address gaps in the EU's existing regulatory framework to improve cybersecurity in connected devices. The proposed regulation would apply a broad horizontal regulatory framework to products with digital elements—including connected devices and non-embedded software—to enforce cybersecurity standards across the digital supply chain.[3] Unfortunately, the draft Cyber Resilience Act is too broad in scope and needs clearer definitions. The legislation's fundamental pitfalls will burden businesses with compliance and undermine avenues for innovation like open source software. The following provides an overview of problems in the Cyber Resilience Act and how to address them. With targeted changes, the Cyber Resilience Act can promote better cybersecurity in the internal market without hurting competition and innovation across Europe.

OVERBROAD INTERVENTION LACKS THE FLEXIBILITY TO SUCCEED

The Cyber Resilience Act's overbroad horizontal framework will likely burden businesses with unnecessary implementation and compliance costs, stretching the limited cybersecurity resources of businesses and making it harder for new entrants to compete with incumbents. The EU has already seen the negative impact of overbroad horizontal legislation from the General Data Protection Regulation, and it is likely to see the same if it enacts the Artificial Intelligence Act.[4] Overbroad horizontal legislation inflates compliance costs, makes legislative frameworks inflexible to evolving threats, and ignores unique sectoral cybersecurity needs. Moreover, the Cyber Resilience Act's lack of sectoral specification could make the EU response to evolving cybercrime inflexible by applying the same rules to all industries even if they face different risks.

Overlap of Reporting Obligations

The Cyber Resilience Act creates two major obstacles that will unnecessarily burden businesses

[1] Kir Nuthi, "Feedback to the European Commission on the Cyber Resilience Act initiative" (Center for Data Innovation, May 2022), https://datainnovation.org/2022/05/cyber-resilience-act-roadmap/; Kir Nuthi, "An Overview of the EU's Cyber Resilience Act" (Center for Data Innovation, October 2022), https://www2.datainnovation.org/2022-cyber-resilience-act-overview.pdf.

[2] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025" (Cybercrime Magazine, November 13, 2020) https://cybersecurityventures.com/cybercrime-damagecosts-10-trillion-by-2025/.

[3] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (The Cyber Resilience Act)," September 15, 2022, https://digitalstrategy.ec.europa.eu/en/library/cyber-resilience-act.

[4] Benjamin Mueller, "How Much Will the Artificial Intelligence Act Cost Europe?" (Center for Data Innovation, July 2021), https://www2.datainnovation.org/2021-aia-costs.pdf.

with increased administrative costs and shift more of their resources toward legal compliance rather than tangible improvements in security. The first issue that inflates compliance costs is the overlap of reporting obligations within the Cyber Resilience Act. Between the revised Directive on Security of Network and Information Systems (NIS2), the Radio Equipment Directive, and the Machinery Regulation, some businesses making Internet of Things (IoT) products will face a surplus of reporting obligations and their related requirements. The NIS2 directive requires businesses to report to 27 member states' selected authorities regarding their cybersecurity risk management measures, any incidents that significantly disrupt their service, and any cyber threats resulting from a significant incident.[5] With the addition of the Cyber Resilience Act to the mix—and the fact that Chapter V of the Cyber Resilience Act enables member states to create entirely new market surveillance authorities or reuse NIS2 authorities or designated cybersecurity certification authorities—the overlap in reporting obligations and the varied approaches each member state will have could muddle and balloon the compliance process.[6]

A solution to this problem would be to streamline the reporting obligations in the Cyber Resilience Act by either standardizing the requirements found in similar legislation or presuming conformity of a business if it satisfies a directive like NIS2.

Lack of Clarity in Product Categories

The second issue the Cyber Resilience Act faces that inflates compliance costs is the lack of clarity in product categories. The Cyber Resilience Act segments products into Class I, Class II, and Default. Businesses can use third-party assessments to establish product conformity for Class II products. Businesses can also use these assessments to demonstrate conformity for Class I products, but they are not explicitly required to use a third party like Class II. But these product categories and the required technical specifications have been left to delegated acts—additional supplemental legislation that can happen after the Cyber Resilience Act's entry into force. As a result, businesses currently do not know what assessments they need to prepare for or whether their categorization could change in the future. The Cyber Resilience Act creates a broad overview of what the EU will regulate, but it is unclear which classification—Class I or Class II—specific products in product categories like operating systems that appear in both Classes will end up in. In addition, both Class I and Class II product categories can be expanded or reduced through later amendments by the European Commission to Annex III.[7] This lack of clarity will drive businesses towards often unnecessary third-party assessments, increasing compliance costs for all firms and disproportionately disadvantaging nascent competitors that lack the resources and compliance teams to meet the regulation's requirements.

To solve this problem, the Center recommends clarifying product categories and technical specifications within the Cyber Resilience Act while creating flexible guidelines to implement the regulation on future technologies. The proposal should not leave product categories or technical

[5] Mar Negreiro, "The NIS2 Directive A high common level of cybersecurity in the EU" (EPRS | European Parliamentary Research Service, June 2022), https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf; Ana Hadnes Bruder et al., "NIS2 Directive New Cybersecurity Rules Expected in the EU," Mayer Brown, October 6, 2022, https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/nis2-directive-new-cybersecurity-rules-expected-in-the-eu#:~:text=Amended%20incident%20reporting%20requirements%3A%20NIS2,and%20%E2%80%9Cfinal%E2%80%9D%20reporting%20obligations.

[6] European Commission, The Cyber Resilience Act, Chapter V.

[7] European Commission, The Cyber Resilience Act, Articles 6 and 50.

guidelines to delegated acts as it will still inflate costs by increasing businesses' need to redirect resources towards consistent compliance.

Inflexible to Sectoral Cybersecurity Needs

Many of the best practices currently used by cyber-businesses are codified in Annex I, but these are too broad to regulate unique cybersecurity vulnerabilities different industries face. By being too wide in scope, the Cyber Resilience Act forces businesses to think about cybersecurity issues that do not relate to their practice and will not be the most vulnerable aspects of their products. The categorization of products attempts to avoid burdening industries with compliance. For example, 90 percent of connected products, such as game consoles and photo-editing software, fall into the Default category and can self-assess their vulnerabilities.[8] Still, businesses offering products in every product category need to implement and use strategies that tackle each of the requirements described in the essential security and vulnerability handling requirements of the Cyber Resilience Act. Using expansive definitions in this regard will burden nascent industries or industries whose digital products might not need as stringent measures as more sensitive industrial IoT devices. Similarly, more sensitive IoT devices that affect EU cybersecurity will likely need more stringent measures than are required in Annex I.[9] For example, European digital identity wallets and electronic health records will likely need specific safeguards that industrial modems do not, despite all three working with sensitive and even personally identifiable data.

The EU should ideally focus on sectoral regulatory intervention, ensuring that cybersecurity legislation is flexible, can evolve with technological advancements, and can be narrowed for specific industry needs.

THE OVERBROAD SCOPE WILL HARM INNOVATION AND DEVELOPMENT

Similar to how the Cyber Resilience Act's overbroad horizontal framework inflates compliance costs, the overbroad scope of the legislation is likely to have unintended consequences for the EU's current IoT economy. The Cyber Resilience Act is likely to stifle digital innovation in entire sectors of the IoT economy, with open source developers, software-as-a-service, and future competitors being harmed the most.

Lack of Clarity Regarding Open Source Software

While the Cyber Resilience Act exempts free and open source software "developed or supplied outside the course of commercial activity," the definitions are unclear and likely to muddle compliance.[10] As described in Recital 10, commercial activity could potentially apply to a variety of monetizable activities, including "charging a price for technical support services, by providing a software platform through which the manufacturer authorize other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software."[11] Article Three further explains that commercial activity can be "in return for payment or free of charge."[12] When combined, these definitions will lead to

[8] European Commission, "Cyber Resilience Act – Factsheet," September 15, 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

[9] European Commission, The Cyber Resilience Act, Annex I.

[10] European Commission, The Cyber Resilience Act, Recital 10.

[11] European Commission, The Cyber Resilience Act, Recital 10.

[12] European Commission, "The Cyber Resilience Act, Article 3.

overbroad interpretations as they fail to distinguish between stages of software development, could cover more open source products than intended, and will likely hamper open source innovation in the EU. There is a lack of clarity over who will be held to account in the open source stack and whether regulators will treat the developer or deployer differently. In the broadest interpretation, developers of open source software would need to monitor and analyze any products built off their code for security vulnerabilities—something that could drive businesses to opt out of sharing their software with other developers in the first place. The lack of clarity in what counts as "commercial activity" could mean that distributors of open source software will have to ensure that manufacturers comply with the Cyber Resilience Act, which will likely stifle access to free and open software through open source repositories like GitHub and GitLab.[13]

A solution to this problem would be to clarify the definition of open source software and clearly exempt it from the of scope of the Cyber Resilience Act. Remaining with the current definition will likely lead to unintended market pressures for open source software and decrease its availability.

Likely to Still Cover Exempted Services

Although the Cyber Resilience Act exempts software-as-a-service (SaaS) in an attempt to prevent overlap with the NIS2 directive, this exemption does not apply to "remote data processing" solutions.[14] Since virtually all SaaS products involve remote data processing, this provision could be seen as a backdoor to covering these products.[15] This ambiguity is likely to also affect other cloud computing products that rely on remote data processing, like platform-as-a-service and infrastructure-as-a-service. Given how essential cloud computing services are for the Internet, such a backdoor could cover a wide variety of digital products and services.

The Commission needs to clarify questions around SaaS and other cloud computing services to ensure that businesses know whether they need to comply. Specifically, the Commission should clarify definitions in Article Three that define its SaaS interactions, such as the definitions of "remote data processing" and "products with digital elements."[16] This clarification will help avoid subjecting SaaS services to multiple regulations already covered by the NIS2 directive.

CONCLUSION

The Cyber Resilience Act has the chance to level out the EU's cybersecurity landscape and ensure IoT businesses have a clear roadmap for success. But without key clarifications, the Commission's proposal could miss the mark and create a compliance nightmare that disincentivizes innovation and entrance into the European IoT economy. The Center welcomes the EU's attention on improving cybersecurity, but it hopes that EU policymakers can work towards a stronger solution instead of accepting the Cyber Resilience Act as is.

[13] Olaf Kolkman, "The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem," *Internet Society*, October 24, 2022, https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/.

[14] European Commission, The Cyber Resilience Act, Article 3.

[15] Pier Giorgio Chiara, "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements" (*International Cyber Security Law Review,* 2022), November 2, 2022, https://link.springer.com/article/10.1365/s43439-022-00067-6.

[16] European Commission, The Cyber Resilience Act, Article 3.