Cybersecurity
Coalition

Cybersecurity Coalition Feedback to the European Commission on the Cyber Resilience Act: Regulation on horizontal cybersecurity requirements for digital products and ancillary services

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the European Commission's Request for Feedback on the *Cyber Resilience Act: Regulation on horizontal cybersecurity requirements for digital products and ancillary services* ("the CRA").[1] The Coalition appreciates the opportunity to provide input and looks forward to working with the European Commission on this initiative.

The Coalition is composed of leading companies specializing in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices throughout the global community.

The Coalition is supportive of efforts to strengthen the resilience and security of products with digital elements used and selected by organizations and consumers alike. The EU has a fundamental role in promoting global cybersecurity practices and while the Cyber Resilience Act's intentions are a step in the right direction, more can be done to ensure increased security across the digital supply chain.

To that end, we have compiled a series of detailed recommendations below for consideration by the Commission as they finalize the CRA. These cover:

- Scope of the proposal
- Incident reporting requirements
- Incident reporting timelines
- Exploited vulnerability reporting
- Security updates
- Conformity
- Open-source exemption
- Distributers
- Enforcement powers
- Liability
- Essential security requirements

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

The Coalition believes that the recommendations outlined below will further strengthen the CRA and ensure that it more effectively meets the Commission's objectives.

We thank the European Commission for providing us with the opportunity to submit feedback on the CRA proposal. Should you have questions or require further clarification on any of the points submitted below, we welcome the opportunity to discuss them with you further.

Respectfully Submitted,
The Cybersecurity Coalition

CC:
Ari Schwartz, Venable LLP
Alexander Botting, Venable LLP
Tanvi Chopra, Venable LLP

Detailed Recommendations

1. Scope

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 covers all products with digital elements, which includes all hardware or software products and individual components. We believe the Cyber Resilience Act is too broad in scope and advocate for a tailored and clarified approach that heightens the overall resilience of the digital ecosystem. Specifically, we question whether it is workable for the CRA to include within its reach enterprise-grade security products, like Data Loss Prevention (DLP) software.

As the Cyber Resilience Act sets out certain conditions that apply to products with digital elements and requires such products to meet cybersecurity requirements throughout the product lifecycle, it fails to take into account differences in the development, functionality, use and security of products with digital elements. For example, a DLP product has a different balance of security requirements around logging, anonymization, retention, and attack surface, in comparison to a firewall. In other words, despite the CRA's ambition to be larger, Annex I's security requirements are more appropriate for finished consumer IoT products. This one-size-fits-all approach requires a massive effort at the standards and delegated acts level where Annex I would need to be calibrated per product group.

Additionally, in tailoring the scope of the proposed regulation, we believe that the inclusion of components adds a level of complexity that is not commensurate with the security benefits. For example, assessing components is a requirement under Annex 3 (either class 1 or class 2). Such components may be used by an OEM manufacturer to produce a device that would be subject to self-assessment. Consequently, in such scenario, the assessment of the components would result in more complexity and delays to the end product in which the components would be integrated. This will have real-world security impacts for consumers and businesses. The goal of the CRA is to increase security, but assessing each component has no real utility because it provides incomplete information regarding the security of products which enter the market. Our recommendation is to remove individual components from the scope of the CRA. The OEM manufacturer has effective control of the security features and overall integration of the various components in the end-product.

In addition, further clarity is needed in terms of what non-embedded software is excluded from the scope of the CRA. Although the Cyber Resilience Act exempts software-as-a-service (SaaS) to prevent overlap with the NIS2 Directive, the exemption does not apply to remote data processing solutions. According to the text, this is "data processing at a distance […] the absence of which would prevent such a product from performing its functions." This essentially describes all SaaS products[2]. Given that SaaS providers and products include remote data processing, the current text creates a lot of ambiguity and uncertainty around compliance. Our preferred approach would be to scope out remote data processing in order to make a clear distinction between on-premise software and cloud services like SaaS and platform-as-a-service (PaaS).

[2] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Given the latter are delivered as services, they are not a good fit for a product regulation, and security measures are better applied at the organizational level, as found in the NIS 2 Directive.

2. Incident Reporting

Article 11 requires manufacturers to report "any incident having impact on the security of the product with digital elements." [3] We would first recommend a clearer definition of the type of incidents to be notified. Without further guidance, 'product security incident' could easily be confused with vulnerability notification, which is the main activity of enterprise *Product Security Incident* Response Teams (PSIRTs). We recommend that incident reporting focus instead on attacks on the manufacturer's *own IT systems* that compromise the *product development, build and distribution environment*. This is a part of the value chain over which the manufacturer has visibility and control and would potentially allow supply chain attacks along the lines of the SolarWinds attack to be captured. Moreover, to the extent that SaaS is included in the scope of the CRA (contrary to our recommendation above), any product incident impacting remote data processing would cross over with the incident notification requirements of NIS2, or even DORA if it concerns EU financial institutions and their third-party ICT providers.

An incident reporting threshold which is too low will lead to high reporting volumes of low-severity incidents, undermining cybersecurity by drawing away resources from response to significant incidents and filling the reporting system with unhelpful data. We urge the Commission to consider focusing on high, severe, and emergency-level incidents, and to consider further specifying what level of incidents are significant enough to qualify for the reporting obligations to prevent overwhelming the relevant authorities with information. The Cybersecurity Coalition suggests the following threshold for reporting cyber incidents:

The incident jeopardizes the integrity, confidentiality, or availability of a product with digital elements, causing substantial impact to the security of the product with digital elements, including:

- *Serious reduction in the safety and resiliency of systems and processes;*
- *Unauthorized access of sensitive information or loss of service due to a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or by a supply chain compromise.*

Finally, we encourage the Commission to harmonize incident reporting requirements between the CRA and NIS 2. In terms of 'who' to report to, under NIS 2, the notice goes to the national CSIRT, whereas, under the CRA, the manufacturer must notify ENISA, which in turn reports to the relevant points of contact. This contradiction would add an unnecessary layer of complexity to the incident reporting and response processes. In a context where affected entities are rushing to contain a serious cybersecurity incident, adding contradictory reporting requirements to different agencies makes strenuous situations even more so. Overall, we believe it is essential to avoid undermining cybersecurity by reporting incidents that are not impactful or significant, or

[3] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

having so many misaligned reporting requirements that we focus resources away from where they are needed most.

3. Incident Reporting Timeline

We encourage the Commission to understand the criticality of ensuring processes that are consistent with industry best practices and international standards. Given that entities can be both designated as important/essential entities under NIS2, have digital products regulated under CRA, and are subject to data breach reporting requirements under GDPR, it is critical that incident reporting requirements are harmonized. For more legal certainty, a 72-hour notification is more suitable than a 24-hour timeframe for incidents. Affected entities' main priority during an incident should first be to deal with containing and mitigating it prior to reporting obligations.

We recommend giving guidance on when a manufacturer is deemed to be aware of an incident, starting the timeline for notification, similar to GDPR[4]. The 'clock' should start once the incident has been triaged by an entity's incident response team. Reporting requirements in a shorter timeframe risks critical and precise information being left out and ultimately, leaving authorities not properly informed about the nature of the incident. We cannot overstate the importance of having enough time to investigate and report in order to be able to provide adequate context for the authorities. Lack of context due to unreasonable timelines may result in inadequate information as part of a notification, which may hinder the authorities' own notification actions or result in additional risk due to misunderstandings about the nature or impact of the incident.

4. Exploited Vulnerability Reporting

The Coalition supports transparency in vulnerability disclosure and believes it can benefit organizations by containing and mitigating emerging threats. However, while we support the concept of transparency, as currently constructed the CRA's language obliging manufacturers to disclose newly discovered exploitation of their products to ENISA prior to mitigation can increase risk. This could ultimately undermine the security posture of products and jeopardize the security of its users. In a similar policy established by China, the Chinese government requires the reporting of vulnerabilities for review prior to the vulnerability being shared with the product or service owner. This type of regulation can enable governments to exploit zero-day vulnerabilities.

Were the EU to follow the Chinese approach, this would further advance the precedent for other countries to follow suit and counter best practices for coordinated vulnerability disclosure. We advise that reporting should be focused on whether *known exploited third-party* vulnerabilities are included in the product. This would provide a predictable yardstick against which to evaluate product risks in the EU and incentivise fixing the highest risk vulnerabilities first.

[4] The WP 250 Article 29 Working Party Guidelines on data breach notification state:
"[…] the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware"."

To facilitate this approach, ENISA should publish an external catalogue along the lines of CISA's Known Exploited Vulnerabilities catalogue, to determine whether a vulnerability is reportable. This would build on top of the European vulnerability database ENISA is charged with creating under NIS 2, by highlighting a subset of known vulnerabilities that are actively exploited in the wild. Reporting against such a catalogue would allow ENISA to build up a picture not only of exploited vulnerabilities but the prevalence of their use in products in the Single Market.

This list of vulnerabilities manufacturers should prioritize for mitigation would also be a useful standard against which manufacturers should assess products prior to delivery, as referenced in Annex I, Section 1 point (2).

5. Security updates

Art 10 (6) requires that manufactures provide security updates during the 'expected product lifetime or for a period of five years from the placing of the product on the market.' It is unclear how this would apply in the case of software, where new versions are regularly released. It is likely to sow confusion about whether a software release should be considered a new product (starting the support timeline again at zero) or an update to an existing one. If the period of support continues to both apply to the 'old' release and to start afresh with the 'new' one, the result may require a division of effort consuming scarce resources.

Certainly, requiring each version to be supported for five years, long after it has been superseded by multiple new and more secure versions of the software, makes little sense from a security perspective. At some point in the product lifecycle, it is logical to move customers to an updated product and the associated security enhancements, rather than continuing to maintain and patch legacy offerings.

6. Conformity

Security regulation and certification have traditionally focused on high-risk users, data, or types of technology. Under the CRA, however, *all* connected products are in scope. To ensure that security properties and processes can be demonstrated at the scale required – i.e. for any given hardware and software version – we believe several principles can help to guide the approach. Some are currently reflected in the Regulation and can be reinforced, and others should be introduced:

- Focus on the truly high-risk: The list of products in Annex 3 class 1 and class 2 is overly expansive and concerns technologies including many legacy security technologies that would not be considered "high risk". The default position should be self-attestation with perhaps increased penalties for certain categories of products if fraudulent or misleading attestations are discovered. Third party conformity assessment should be limited to truly high-risk scenarios such as SCADA systems in Annex 3.

- Simplicity: Default to the least burdensome means of demonstrating conformity and avoid testing and documentation that brings limited value.
- Similarity: Reduce assessment effort by accepting one product as representative of a family of products for assessment purposes due to them having equitable hardware and/or software.
- Reciprocity: Eliminate duplication by accepting of other entities' assessments or certification in lieu of one's own (e.g. recognition of assessments from qualified bodies outside EU; reuse of certifications).
- Gap analysis: Only focus on additional requirements not covered by other entities' assessments and do not reassess the whole set.
- Attestation: Accept assessments from the manufacturer for certain aspects of the wider third-party assessment.
- Maintenance: Allow certain changes to the product without requiring reassessment.

Harmonized standards

Harmonized standards should be the bedrock of conformity as they leverage the technical expertise of industry while creating broad acceptance and global applicability. Common specifications, on the other hand, undermine the development of quality standards. This is particularly important given that the CRA should promote uniform management of risk across the single market and maximize the likelihood that technology innovations developed within the EU are capable of being readily adopted beyond its borders.

Mutual recognition

Mutual recognition agreements (MRAs) have been adopted in the context of the NLF framework to allow third countries use assessments conducted by notified bodies in the EU and vice versa. These MRAs should be revised to include CRA among the list of covered regulations.

Substantial modification

The CRA introduces the notion of 'substantial modification' to describe scenarios where conformity may need to be reassessed based on existing guidance under the Blue Guide on the NLF. While this is used for existing sector-specific software (medical devices), the concept should be carefully bounded for software under the CRA as it will quickly become a bottleneck due to the velocity of new releases. It will ultimately be unworkable if every new feature would require reassessment.

Components and conformity assessment requirements

To demonstrate compliance with their obligations and place a product on the market, manufacturers are required to conduct a conformity assessment. This could be done via self-assessment or a third-party conformity assessment, depending on the risk classification of the product. For certain products, the rules are stricter, and conformity must be demonstrated by an independent body. However, the requirements of Annex III class 1 and class 2 on conformity assessment result in a cascading effect for all hardware products that have components. For example, while a TV goes through a self-assessment, every component in the TV is subject to Annex 3 class1/2 conformity assessment. This two-track approach creates additional unnecessary cost and delay for a low-risk product. It also delays the introduction of new technologies into the EU for fear of triggering the conformity assessment rules every time a new or different component is introduced.

The security properties of a device are effectively controlled by the final configuration and settings that the OEM manufacturer permits, the firmware and operating system that is running on the device and not by the components that are often operating at a very low level to cause a meaningful security risk. Therefore, components should be excluded from the scope of CRA and only the end-device should be subject to conformity assessment by the OEM manufacturer who should among other aspects provide information on the components and their security features and functionality.

Information and technical documentation

Transparency benefits in providing documentation to the user and regulator should be weighed against the assumed knowledge of the manufacturer and disadvantages in terms of security and administrative burden. In many instances, for example, the manufacturer will have limited knowledge about intended use of foreseeable use versus the user. Use cases for consumer and enterprise uses of the same or similar technologies may also vary widely. In addition, providing complete information and the design and development of a product presents a significant security risk in itself.

Practical difficulties and impact of conformity assessment on competitiveness

Whereas the requirements for conformity assessment have a role to play for certain categories of products and risk, one needs to reflect on the implications of having such a wide-ranging conformity assessment requirements as the proposal currently stipulates. The broad conformity assessment requirements unless they are more streamlined to focus on areas of substantial risk are difficult to implement in practice because:

- There are not enough conformity assessment bodies to conduct the assessment.
- There is not enough expertise available to service the assessment bodies.
- The broad ranging conformity assessment requirements will result in substantial delay and price increase for the products to enter the EU market unless companies are able to self-assess.

The conformity assessment requirements of Annex 3 class 1 concern mostly legacy cybersecurity products that are not of high risk and are already available in the market. In addition, the features of Annex I are by design in those security products included in Annex 3 class 1, without which they would not have been adopted in the enterprise security market. Imposing a conformity assessment requirement with standards that do not exist delays the availability of the latest security technologies and its updates in the European security market without addressing any of the concerns around vulnerability management. It should be stressed that the requirements of Annex 1, which the conformity assessment would identify for Annex 3 class 1 security products, are more suitable for consumers, as they provide an indication of the features but not of the actual security state or security configuration or risk environment of the Annex 3 class 1 product.

Moreover, the broad requirements in conjunction with the vague conditions for re-assessment especially in the case of software or components create incentives for companies to delay the introduction of the latest and most innovative technologies in Europe for fear of having to go through an extended period of conformity assessment.

Extensive delays in conformity assessment create the additional risk of having two different supply chains of technology for European companies present internationally. The one would be "home" intra-EU where only technologies that are conformity assessed can be made available and the other one would be "abroad" where there is more and faster available choice. The maintenance of such a dual infrastructure is likely to impact competitiveness and create complexity.

7. Open-Source Exemption

According to Recital 10, "in order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable."[5] We support this proposal as the industry is reliant on upstream open source, however, we believe the text could be improved to avoid legal uncertainty. The first recommendation is to move the definition of 'Technical Support Services" in Recital 10 into the definition of what the CRA terms as upstream open source and thus benefit from exemption.

The second recommendation is to amend Article 2 to reflect software produced under open-source license and distributed on not-for-profit basis out of scope for the certification requirements in the regulation. In particular, platforms that distribute open-source software should be excluded from the regulation because code warehouses such as GitLab, GitHub, Bitbucket, and Sourceforge all make open-source software available, making them potential "distributors" and thus liable under Article 10 obligations.

Lastly, according to Article 4(3), "Member States shall not prevent the making available of unfinished software which does not comply with this Regulation provided that the software is only made available for a limited period required for testing purposes and that a visible sign clearly indicates that it does not comply with this Regulation and will not be available on the

[5] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

market for purposes other than testing."[6] To bring the articles of the regulation in-line with intentions of the articles, we recommend a small amendment: "provided that software is open source or is only made available for a limited period required for testing purposes."

8. Distributors

Given our understanding of the definition of "distributors" in the CRA, we believe that App Stores should be included. The CRA imposes new requirements on distributors to serve as security gatekeepers for all apps distributed through the store. This includes verifying compliance of apps with the requirements and reporting evidence of non-compliance to regulators. These requirements conflict with the goals of other EU regulations which seek to place limits on the "gatekeeper" powers of App Stores.

9. Overly Broad Enforcement Powers

We value the role that ENISA currently plays and how it benefits from voluntary cooperation with industry. We are concerned, however, that the CRA grants ENISA powers around comprehensive market monitoring, investigative and regulatory powers. In regard to ENISA receiving sensitive information, such as incident notifications, we are worried that it would harm ENISA's mission. Along with these extensive reporting obligations, the CRA proposes that ENISA evaluate the security of products to determine if a product recall, a withdrawal, or a penalty is required. Given that ENISA has no expertise in this field, and as industry benefits with ENISA as a key partner, we recommend removing the regulatory role from their remit.

Furthermore, Member State regulators and the Commission have expansive powers to recall or force changes to products even if the product is compliant with CRA. The Commission is seeking to grant itself wide delegated/implementing powers including, (1) to determine which products should be classified as "highly critical," and thus subject to the most onerous certification regime; (2) to define and thus delimit the scope of class I and class II products, and; (3) to set common specifications for the "essential requirements" in Annex I. The Commission's delegated/implementing powers should be limited by setting conditions for the exercise of these powers, namely consultation with relevant industry stakeholders to avoid the scope of the legislation or obligations being expanded unreasonably through secondary legislation following adoption.

Whichever body ultimately takes on these powers, they must be amply resourced to properly carry out the new extensive obligations. Failure to do so could result in serious security risks, if, for instance, they cannot protect the list of actively exploited vulnerabilities in all products in Europe.

[6] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

10. Liability

The Act, building on the New Legislative Framework, sets out specific horizontal cybersecurity requirements for all products with digital elements being placed or made available on the internal market. It seeks to cover the entire digital supply chain and envisions including, among other digital products, non-embedded software ("any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately").

Notably, the CRA proposes a duty of care for the placement of products with digital elements on the market, including:

> *[Annex II] As a minimum, the product with digital elements shall be accompanied by:*
> *... 4. the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;*
> *5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks; ...*

There are two facets of these promises ("intended use", "any known or foreseeable circumstances", "reasonably foreseeable misuse") that are problematic. Foremost, none of them were developed (nor have been applied) in the area of product security. Moreover, they are drawn entirely from the field of tangible products (e.g., consumer products such as a toaster or in the enterprise field, construction contracts). Applying these concepts to product security in the intangible, digital environment raises enormous risks of confusion and unintended consequences.

There are important differences that exist between tangible goods and intangible digital products in law and practice, especially in the area of security. By its very nature, software and software components are fungible; i.e., they can be repurposed by an end user (this is especially true of open source software). By contrast, tangible products are largely static; certainly, less dynamic. Second, current known evaluation schemes of software and software components are inherently dependent on the risk environment in which it is used, and practically depends on how the user controls and which may not be transparent or apparent to the software publisher.

It is often unclear and very difficult to determine what exactly be the cause of a malfunction or security incident in a litigation where a digital product is involved (especially when it is used in the context of tangible products). A basic example to illustrate this distinction in the consumer context is a refrigerator with a software operating system. If a refrigerator stops operating, is that a result of the software? Is it a failure of a mechanical component? Some hardware defects or flawed circuitry might render a digital product inoperable or create unforeseen risks in a digital element. In this particular example, the tangible part of the good may in fact be causing an intangible malfunction.

In an enterprise context, the complex interoperability involved in integrating systems may incorporate a multitude of applications, interfaces, middleware and operational environments. As such, it belies any formulaic way to know and foresee any and all circumstances where the digital component or product will interact and operate. Today, those issues are the subject of complex negotiations between sophisticated operators in the market and it is typical to limit liability and disclaim explicit and implied warranties and manage the costs of digitization.

We therefore recommend that the Commission revise or remove this component of the CRA.

11. Essential Security Requirements

Given the penalties associated with non-compliance, and the novelty of notified bodies addressing cybersecurity, in some circumstances it will make sense to either amend the essential security requirements, so they are applicable in all settings, or to provide additional guidance on their applicability. The nature of the problem is that certain essential security requirements are open to interpretation that needs to balance conflicting security objectives. Interoperability vs Attack surface is one example. Another can be anonymity/privacy vs logging/identification and retention. The balance would be shifting depending on the use case or the product family. For instance, a network router would have very different attributes than a data leakage prevention (DLP) software. Therefore, guidance would be needed for the conformity assessment bodies to uniformly interpret these attributes per product family in the form of a standard. This highlights again the need to rationalize the number of conformity assessments otherwise there is a major bottleneck around standard creation.

One example is the secure by default configuration requirement. While this may make sense in a consumer environment, in an enterprise setting, which configuration is the most secure is highly dependent on contextual factors – such as the configuration and versions of interconnected devices and networks – it does not make sense to refer to a single ‘secure by default’ configuration. Another example is the potential trade-off between different essential requirements. Minimizing the attack surface may come at the cost of making software updateable – such as by making firmware read-only.