Cybersecurity Coalition

13 November 2025

VIA ELECTRONIC SUBMISSION

Re: Cyber Resilience Act (CRA) Delegated Regulation on specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the European Commission's consultation on the *Commission Delegated Regulation supplementing Regulation (EU) 2024/2847 of the European Parliament and of the Council by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications* ("Delegated Act").

The Coalition is composed of leading companies with a specialty 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. Accordingly, we actively support efforts to identify and promote the adoption of cybersecurity policy best practices that will improve cybersecurity outcomes throughout the global community.

The Coalition and its member companies have consistently engaged with the Directorate-General for Communications Networks, Content and Technology (DG Connect), ENISA, other relevant EU institutions and Member State governments on the Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847) and other related issues. In our February 2023 response to the Commission's consultation on the *Cyber Resilience Act: Regulation on horizontal cybersecurity requirements for digital products and ancillary*, we expressed our support for transparency in vulnerability disclosures and noted our belief that such disclosures can benefit organizations by enabling them to take proactive measures to contain and mitigate emerging threats. However, we also emphasized that broad and premature dissemination of vulnerability information can increase the risk of exploitation by malicious actors. Such an approach requires protecting against public release that could enable exploitation. It also relies upon the existence of clear parameters governing what information is shared, when it is shared, with whom it is shared and how it may be further used or disseminated.

The Coalition is concerned that provisions in the draft Delegated Act could inadvertently require disclosures in circumstances that diminish rather than enhance cybersecurity. The Coalition is also concerned that the draft Delegated Act omits discussion of several core issues, including mechanisms for resolving disputes across different jurisdictions, protecting information shared by manufacturers and limiting how shared information is subsequently used and disseminated. Each is essential to ensuring an effective vulnerability

disclosure regime that serves the core goal of enhancing, rather than undermining, cybersecurity.

Consistent with these outstanding concerns, the Coalition offers the following detailed comments and recommendations on the draft Delegated Act:

1. Concerns related to Article 3: Terms and conditions for applying cybersecurity-related grounds stemming from the nature of the reported information

Article 3 of the draft Delegated Act sets the rules for when a Computer Security Incident Response Team (CSIRT) that has received notification about an actively exploited vulnerability or severe incident impacting the security of a product with digital elements may delay forwarding of that notification to other relevant CSIRTs. Relevant CSIRTs are defined to include those CSIRTS in jurisdictions where the affected product is made available.

A. Concerns related to Article 3(a)

A delay is permitted if "the cybersecurity risks posed by the dissemination [of the notification] outweigh its security benefits"; "those risks cannot be mitigated"; *and* one of the additional conditions provided for in Articles 3(a), 3(b), 3(c) and 3(d) are met. The Coalition is concerned that these conditions do not sufficiently cover the full set of situations in which a CSIRT should seek to delay notification in order to ensure that cybersecurity risks of disclosure do not outweigh the potential benefits.

The Coalition is particularly concerned about the strict timeline in Article 3(a), which authorizes a delay in notification if the relevant pre-conditions are met and the notifying manufacturer also indicates that an effective "risk mitigation measure" (*i.e.*, a security update or user guidance) will be available within 72 hours. If the risk mitigation measure is not made available within that timeframe, the receiving CSIRT must proceed with the notification (unless one of the other criteria in Articles 3(b), 3(c) or 3(d) kick in). There are *no* mechanisms for a company to ask for more time to develop risk mitigation measures described in Article 3(a).

In most cases, a 72-hour period – or up to 144 hours, when combined with the initial 72-hour notification period under Article 14(b) of the CRA – is insufficient for manufacturers to develop, test and release a patch or other mitigation for a vulnerability. In fact, a Rapid7 report, found that in the adjacent market of web applications the average time from discovery to patch of a vulnerability was 38 days, 34 days for high-severity vulnerabilities and 54 days for low-severity ones. Assuming similar timelines applicable to digital products, there is a high risk that the Delegated Act as written would compel CSIRTs to disclose information about vulnerabilities before mitigations are available, thereby increasing the risk of exploitation.

This approach would prevent industry and government stakeholders from adjusting the notification timelines to account for the risks of disclosure. The arbitrary timeline proposed will impose a suboptimal resolution on stakeholders in many circumstances.

In addition, it is unclear what constitutes an "effective risk mitigation measure." While the text uses examples – "such as a security update or user guidance" – it does not provide any additional specificity.

To ensure these protections function effectively, the Coalition urges the Commission and ENISA to:

- Amend Article 3(a) to allow for extensions to the 72-hour timeline for implementing mitigation measures. Such an exception should remain available so long as the manufacturer is actively pursuing mitigation measures and the pre-requisite requirement – that the risks of dissemination outweigh the security benefits – is met.

- Provide additional guidance as to what constitutes an appropriate "risk mitigation measure." In addition, manufacturers should be encouraged to implement organizational risk management measures, pursuant to Implementing Regulation (EU) 2024/2690 which lays down the technical and methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555.

B. Limitations of Article 3(b)

It is possible that Article 3(b) could safeguard against this concern in certain cases. Article 3(b) permits receiving CSIRTs to delay notification if the information included in the notification "is deemed sufficient, in light of the nature of the notified active vulnerability, to create an exploitation technique, particularly when the vulnerability can be easily identified and exploited by actors with limited skills and expertise." In such cases, the CSIRT would disseminate the information only after the mitigation measure becomes available.

But this provision appears most likely to be triggered when the vulnerability is easy to identify and exploit. There are also significant, and perhaps even more existential risks, posed by sophisticated actors that might be able to exploit a notified vulnerability not readily understood by less sophisticated actors. Additional factors should be considered, including the risk that the exploited vulnerability could provide sophisticated actors access to a range of interconnected systems and devices, beyond the specific product identified by the reporting manufacturer.

To ensure these protections function effectively, the Coalition urges the Commission and ENISA to:

- Adopt a broad and inclusive interpretation of what it means for information to be "deemed sufficient… to create an exploitation technique."

- This should not be limited to those circumstances when the vulnerability could be easily identified and used by limited-skill actors. It should also account for the risks posed by more skilled and sophisticated actors – including the risks that such actors

could exploit such a vulnerability to gain access to a wide array of interconnected systems.

C. Dispute mechanisms

It is inevitable that there will be disputes about whether the conditions that justify a delay in notification under Article 3 are met. However, neither the draft Delegated Act nor the CRA describe a formal process for how such disputes will be resolved. This lack of procedural clarity could result in inconsistent application of the notification rules, undermining the uniformity and predictability that the CRA seeks to achieve.

The Coalition urges the Commission and ENISA to:

- Establish a clear, transparent adjudication process to resolve disagreements regarding CSIRT delay decisions.

- This process should establish criteria for ENISA's review authority, timelines for resolution and communication procedures to ensure consistent implementation of Article 3 across all Member States.

2. Concerns related to Article 4: Terms and conditions for applying cybersecurity-related grounds in relation to a specific CSIRT

Article 4 of the Delegated Act defines criteria under which a national CSIRT receiving a notification about a vulnerability or incident associated with a covered product is permitted to delay forwarding notification to other CSIRTs. Specifically, the receiving CSIRT may delay dissemination if: (i) a relevant CSIRT has been "affected by a cybersecurity incident casting doubt on its ability to ensure the confidentiality of the notified information" (Article 4(a)), or (ii) it has "sufficient reason to believe that the capabilities of the relevant CSIRT are inadequate to ensure the confidentiality of the notified information" (Article 4(b)).

The Coalition is concerned that these provisions create standards that are hard to apply, create perverse incentives,and fail to account for the full set of instances in which the security costs of disclosure outweigh the benefits of information sharing.

A. Cybersecurity incidents at relevant CSIRTs

Article (4)(a) authorizes a delay in notification to a relevant CSIRT that has been "affected by a cybersecurity incident casting doubt on its ability to ensure the confidentiality of the notified information."

In order to function properly, Article 4(a) requires the receiving CSIRT to know that a relevant CSIRT has been compromised by a cybersecurity incident. In practice, however, there are several reasons why a receiving CSIRT may not have access to this information, including:

- *Lack of a defined notification process:* Neither the CRA nor the draft Delegated Act establishes a formal mechanism requiring CSIRTs to inform ENISA and other members of the EU CSIRT Network when they experience a cybersecurity incident. In the absence of such a process, each CSIRT carries the burden to effectively monitor the status of all 26 others. This is an unrealistic expectation given constraints on time, resources, language capabilities and cross-border relationships between CSIRTs.

- *Disincentives to disclosure:* A CSIRT affected by an incident may be reluctant to disclose the compromise, as doing so could risk reputational damage or limit its continued access to shared information.

- *Delayed awareness:* A CSIRT may not immediately realize that it has been compromised, meaning other CSIRTs could continue to share sensitive information with a potentially affected entity without knowing the risk.

The Coalition urges the Commission and ENISA to:

- Add a requirement that CSIRTs affected by a potential cybersecurity incident immediately notify ENISA of that possibility and keep ENISA updated of that status;

- Add a requirement that ENISA make information about a potential compromise available to a CSIRT that is posed to disseminate a notification *prior* to such information sharing; and

- Establish mechanisms to limit information sharing to CSIRTs that violate information sharing requirements that are essential to effective application of this process. This would be consistent with the requirement that ENISA provide timely notification of any security incident to the single reporting platform under Article 16(4) of the CRA.

B. Capabilities of relevant CSIRTs

Article 4(b) of the Delegated Act permits a receiving CSIRT to delay notification if it has "sufficient reason to believe that the capabilities of the relevant CSIRT are inadequate."

This provision will be difficult to implement in practice for the same reasons flagged with respect to Article 4(a) of the Delegated Act. In most cases, CSIRTs will not have direct visibility into the capabilities, resources or maturity levels of the 26 other members of the CSIRT Network. Moreover, CSIRTs may be disincentivized from disclosing potential weaknesses to their peers if doing so could limit their continued access to shared information. CSIRTS may also not know of their own capability gaps in advance of disclosure.

The Coalition urges the Commission and ENISA to:

- Establish a formal, transparent process through which the capabilities of CSIRTs can be periodically and objectively assessed and the results communicated confidentially to network members.

C. Failure to account for other significant security concerns

In addition to those created by cybersecurity incidents or capability gaps, there are several other legitimate cybersecurity-related reasons why one CSIRT may be reluctant to disclose a particular vulnerability to another. For example, a receiving CSIRT may be concerned that a relevant CSIRT would broadly publicize or not sufficiently safeguard the information, including from foreign adversaries, even if the CSIRT had the technical means and capabilities to do so.

These risks are amplified by the fact that EU Member States currently lack harmonized laws or formal policies dictating how governments may handle and use vulnerability information (e.g., U.S. Vulnerabilities Equities Process (VEP)).

The Coalition urges the Commission and ENISA to:

- Develop clear rules about how CSIRTs can use, disseminate and retain shared vulnerability information, applicable to all of the CSIRTS.

- Amend the draft Delegated Act to enable the receiving CSIRT to delay notification of a vulnerability based on onward dissemination concerns.

D. Disputes among CSIRTs

Invocation of the provisions under Article 4 requires the receiving CSIRT to make a potentially sensitive assessment of the competence and integrity of another country's CSIRT, and by extension, the credibility of the Member State it represents. These will almost inevitably be disagreements about such determinations–and potential backlash as a result that could escalate into significant diplomatic disputes and erode trust within the CSIRT Network.

The Coalition urges the Commission and ENISA to establish a clear, transparent adjudication process to assess key security and capabilities questions and proactively resolve disagreements. This framework should address the following key questions:

- Who determines when the conditions in Article 4 are met? Can one Member State unilaterally raise concerns about another's CSIRT, or must such findings be self-reported?

- Would a CSIRT be informed if another CSIRT or ENISA determined it was compromised or lacked capability? Would ENISA be responsible for conveying such assessments, and in what circumstances?

- Would a CSIRT have the opportunity to challenge a decision that restricts its access to vulnerability information? How would such disputes be communicated and resolved?

- Who would manage potential fallout or disagreements between CSIRTs or Member State governments if these determinations become contentious?

3. Concerns related to reporting by manufacturers

Article 5 of the Delegated Act states that a national CSIRT is permitted to delay the dissemination of notifications to other relevant CSIRTs via ENISA's single reporting platform if the platform has been "affected by a cybersecurity incident casting doubt on its ability to ensure the confidentiality of notified information."

The Coalition supports this provision, but notes it is insufficient, given that it only covers CSIRT reporting. Article 14 of the CRA requires manufacturers to notify *both* ENISA and the relevant CSIRTs about actively exploited vulnerabilities through "electronic notification end-points" connected to the single reporting platform. However, manufacturers are not provided with any mechanism to delay reporting if the single reporting platform has been compromised.

Furthermore, while Article 16(4) of the CRA requires ENISA to inform the CSIRT Network and the Commission of any such incident, there is no corresponding obligation to notify manufacturers. As a result, manufacturers could unknowingly submit sensitive, unmitigated vulnerability information to a compromised platform — potentially increasing the risk of further exploitation or attack.

Similarly, while Article 4 of the draft Delegated Act protects CSIRTs from notifying a compromised CSIRT about a vulnerability, there is no equivalent safeguard to prevent a manufacturer from reporting directly to a compromised CSIRT. To the contrary, Article 14(1) of the CRA requires the manufacturer to submit its notification to the CSIRT "designated as coordinator," without exception.

The Coalition urges the Commission and ENISA to:

- Amend the draft Delegated Act and adopt measures to ensure the security and integrity of reporting by manufacturers.

- These measures should ensure manufacturers are informed of security compromises affecting either the single reporting platform or an individual member of the EU CSIRT Network. They should also enable manufacturers to delay reporting to the single reporting platform or a national CSIRT in the event of a compromise that would put the information at risk.

* * *

The Coalition thanks the European Commission for providing us with the opportunity to submit feedback on the *Commission Delegated Regulation supplementing Regulation (EU) 2024/2847 of the European Parliament and of the Council by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications.* Should you have questions or require further clarification on any of the points submitted below, we welcome the opportunity to discuss them further.

Respectfully Submitted,
The Cybersecurity Coalition

CC: Ari Schwartz, Venable LLP
CC: Alexander Botting, Venable LLP
CC: Jennifer Daskal, Venable LLP
CC: Luke O'Grady, Venable LLP