EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

COMMISSION DELEGATED REGULATION (EU) …/...

of XXX

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

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

Regulation (EU) 2024/2847 of the European Parliament and of the Council ('the Cyber Resilience Act') requires manufacturers of products with digital elements to notify, via a single reporting platform, any actively exploited vulnerability or severe incident having an impact on the security of a product with digital elements. Pursuant to Article 16(2) of that Regulation, the computer security incident response team (CSIRT) designated by the Member State as coordinator that initially receives the notification may, in exceptional circumstances and on justified cybersecurity-related grounds, delay the dissemination of the notification to the CSIRTs of other Member States where the product with digital elements has been made available.

This Delegated Act is therefore intended to supplement the Cyber Resilience Act by specifying the terms and conditions for applying the cybersecurity-related grounds to delay the dissemination of notifications. It does so by identifying three types of reason for which the CSIRT initially receiving the notification may decide that it is necessary to delay further dissemination to other CSIRTs. Such a decision to delay may be taken in three circumstances:

- in the light of an evaluation of the nature of the notified information;
- if the CSIRT receiving the notification is unable to ensure the confidentiality of such information;
- if the single reporting platform has been compromised or is temporarily not operational.

Reporting obligations set out in Article 14 of Regulation (EU) 2024/2847 are set to apply from 11 September 2026.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

The CSIRT Network and the European Union Agency for Cybersecurity (ENISA) were consulted on various drafts of this act. A preliminary discussion with guiding questions was held on 26 March 2025, with an opportunity to provide written input by 11 April 2025. A first draft of this act was shared with the CSIRT Network and ENISA on 16 May 2025 and a discussion was held on 6 June 2025, with an opportunity to provide written input by 27 June 2025. A second draft of the act was shared with the CSIRT Network and ENISA on 23 July 2025, with an opportunity to provide written input by 1 September 2025. A third draft of the act was shared with the CSIRT Network and ENISA on 25 September 2025 and a discussion was held on 9 October 2025, with an opportunity to provide written input by 27 October 2025.

The draft act was subject to a public consultation between [insert dates] and was discussed with the Expert Group on Cybersecurity of Products with Digital Elements (E03967) on [22 October 2025].

3. LEGAL ELEMENTS OF THE DELEGATED ACT

The empowerment to adopt delegated acts is provided for under Article 14(9) of the Cyber Resilience Act, which requires the Commission to specify the terms and conditions for

applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications by 11 December 2025.

COMMISSION DELEGATED REGULATION (EU) …/...

of XXX

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

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)[1], and in particular Article 14(9) thereof,

Whereas:

(1) In exceptional circumstances, and, in particular, upon request by the manufacturer and in light of the level of sensitivity of the notified information, and on justified cybersecurity-related grounds, the computer security incident response team (CSIRT) designated as coordinator initially receiving notification of an actively exploited vulnerability or a severe incident having an impact on the security of a product with digital elements (‘the CSIRT initially receiving the notification’) may delay for a period of time that is strictly necessary the dissemination of the notification via the single reporting platform to the CSIRTs designated as coordinators on the territory of which the manufacturer submitting the notification has indicated that the product with digital elements has been made available (‘the relevant CSIRTs’). Therefore it is necessary to set out the terms and conditions for applying such grounds. Under Article 16(2) of Regulation (EU) 2024/2847, where a CSIRT initially receiving the notification decides to invoke such grounds, it should immediately inform the European Union Agency for Cybersecurity (ENISA) of its decision to delay, and its reasons for doing so, and when it intends to further disseminate the notification.

(2) In accordance with Article 16(2), second subparagraph of Regulation (EU) 2024/2847, the terms and conditions for applying the cybersecurity-related grounds set out in this Regulation are not to apply to access by ENISA to the information notified. ENISA’s access to the information notified may only be restricted in particularly exceptional circumstances: when the manufacturer indicates in its notification that one of the three conditions referred to in Article 16(2), third subparagraph, points (a), (b) or (c) of Regulation (EU) 2024/2847 is met, and then only in relation to the 72-hour vulnerability notification referred to in Article 14(2), point (b) of Regulation (EU) 2024/2847. In such cases, the only information to be made available simultaneously to ENISA is information that a notification has been made by a manufacturer; general information about the product with digital elements; information on the general nature of the exploit; and the information that security-related grounds have been invoked.

[1] OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

(3) Access to the notified information enables CSIRTs to have an overview of the security environment in their territory and to put in place mitigating measures, raising the overall level of cybersecurity in the Union. Therefore, further restrictions on the dissemination of notifications in light of the nature of the information being notified should be possible only in cases where, in light of the sensitivity of the information notified, the cybersecurity risks stemming from further dissemination outweigh the security benefits to the Union, and those risks cannot be adequately mitigated by placing restrictions on the handling and further sharing of the notification through appropriate protocols in use within the CSIRT Network, such as the Traffic Light Protocol (TLP) or the Permissible Actions Protocol (PAP). This may be the case, for example, where a manufacturer has informed the CSIRT initially receiving the notification that it expects to provide a mitigating measure (such as a patch) shortly. It may also be the case, when the CSIRT initially receiving the notification decides to share only parts of a notification, and these parts are nonetheless sufficient for the relevant CSIRTs to ensure that they are able to put in place adequate risk mitigation measures. Furthermore, and in order to encourage cooperation on vulnerability identification and disclosure between manufacturers, CSIRTs and security researchers, this may also be the case when the CSIRT is acting as a trusted intermediary for an ongoing coordinated vulnerability disclosure (CVD) procedure as referred to in Article 12(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council[2]. In ~~such case, when the CSIRT~~ decides to delay the dissemination of ~~a notification,~~ and in accordance with Article 16(6) of Regulation (EU) 2024/2847, that CSIRT is to delay it for a period that is no longer than strictly necessary and until consent for disclosure by the parties involved in the CVD is given.

(4) The information included in the notification will help CSIRTs fulfil their tasks in the context of risk mitigation and incident handling. ~~In rare~~ cases, however, such information could be sufficient to enable the creation of an exploitation technique without additional research, even by ~~actors~~ with limited skills and resources. If that information were accessed by malicious actors, the cybersecurity of the Union would be heavily impacted, given the ease of the exploitation. This could be the case, for instance, where the vulnerable version of a piece of software differs only marginally from previous, non-vulnerable versions. In such cases, if the CSIRT initially receiving the notification believes that the cybersecurity risks stemming from further dissemination cannot be adequately mitigated by placing restrictions on handling and further sharing, it may decide to delay the dissemination until an effective risk mitigation measure, such as a security update or user guidance, is available.

(5) If a relevant CSIRT is not able to protect adequately the notified information, sensitive information could be accessed by malicious actors and exploits be put in place throughout the Single Market. Therefore, where there are serious concerns about a relevant CSIRT's ability to ensure the confidentiality of the notified information, the CSIRT initially receiving the notification may decide to delay the dissemination of a notification until such concerns have been addressed. This may be the case in situations where a relevant CSIRT has been hit by a cybersecurity incident affecting its ability to operate securely, or where there is evidence or information that significant

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80–152).

shortcomings in the capabilities of the CSIRT have been detected, such as serious resource constraints compromising its ability to carry out its functions, or reliance on outdated or vulnerable software.

(6) In order to prevent malicious actors from accessing sensitive information, where the single reporting platform established under Article 16 of Regulation (EU) 2024/2847 has been compromised by a cybersecurity incident, the CSIRT initially receiving the notification should delay the dissemination via the single reporting platform until the platform's ability to ensure the confidentiality of notified information has been restored.

(7) In accordance with the first subparagraph of Article 16(2) of Regulation (EU) 2024/2847, the CSIRT initially receiving the notification need not disseminate a notification to any other relevant CSIRT if the manufacturer indicates that the product with digital elements is only made available on the market of the Member State of the CSIRT initially receiving the notification.

(8) The Commission has consulted and sought the views of relevant stakeholders in preparing the draft delegated act, and has consulted the Expert Group on Cybersecurity of Products with Digital Elements.

(9) In accordance with Article 14(9) of Regulation (EU) 2024/2847, the Commission has cooperated closely with the CSIRTs Network established pursuant to Article 15 of Directive (EU) 2022/2555 and with ENISA, in preparing the draft delegated act,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation specifies the terms and conditions for applying the cybersecurity-related grounds referred to in Article 16(2) of Regulation (EU) 2024/2847 that enable the CSIRT designated as coordinator initially receiving a notification in accordance with Article 14(1) and (3) and Article 15(1) and (2) of that Regulation to delay the dissemination of the notification to the CSIRTs designated as coordinators on the territory of which the manufacturer has indicated that the product with digital elements has been made available.

Article 2

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) 'CSIRT initially receiving the notification' means the CSIRT designated as coordinator initially receiving the notification in accordance with Article 14(1) and (3) and Article 15(1) and (2) of Regulation (EU) 2024/2847;

(2) 'relevant CSIRT' means the CSIRT designated as coordinator on the territory of which the manufacturer has indicated that the product with digital elements has been made available.

Article 3

Terms and conditions for applying cybersecurity-related grounds stemming from the nature of the reported information

The CSIRT initially receiving the notification may decide to delay for a period of time limited to that strictly necessary the dissemination of notifications or parts thereof to relevant CSIRTs in cases where, in light of the sensitivity of the notified information, the cybersecurity risks posed by the dissemination outweigh its security benefits and those risks cannot be mitigated by placing restrictions on the handling or further sharing of the notification through appropriate protocols, such as the Traffic Light Protocol (TLP) or the Permissible Actions Protocol (PAP), and where at least one of the following conditions is met:

(a) the manufacturer has informed the CSIRT initially receiving the notification that an effective risk mitigation measure, such as a security update or user guidance, is expected to be made available within 72 hours; if an effective risk mitigation measure is not made available within this timeframe, the CSIRT initially receiving the notification shall disseminate the notification to the relevant CSIRTs;

(b) the information included in the notification is deemed sufficient, in light of the nature of the notified actively exploited vulnerability, to create an exploitation technique, particularly when the vulnerability can be easily identified and exploited by actors with limited skills and resources; once an effective risk mitigation measure, such as a security update or user guidance, is available, the CSIRT initially receiving the notification shall disseminate the notification to the relevant CSIRTs;

(c) the CSIRT initially receiving the notification is able to share with the relevant CSIRTs sufficient information to ensure that the relevant CSIRTs can put in place adequate risk mitigation measures; once an effective risk mitigation measure, such as a security update or user guidance, is available, the CSIRT initially receiving the notification shall disseminate the full notification to the relevant CSIRTs;

(d) the CSIRT initially receiving the notification of the actively exploited vulnerability has been made aware of it as part of a coordinated vulnerability disclosure (CVD) for which that CSIRT is acting as a trusted intermediary in accordance with Article 12(1) of Directive (EU) 2022/2555; in such case, and in accordance with Article 16(6) of Regulation (EU) 2024/2847, the CSIRT initially receiving the notification shall disseminate the notification to the relevant CSIRTs when a delay is no longer strictly necessary and consent for disclosure by the parties involved in the CVD is given.

Article 4

Terms and conditions for applying cybersecurity-related grounds in relation to a specific CSIRT

The CSIRT initially receiving the notification may decide to delay for a period of time that is strictly necessary the dissemination of notifications or parts thereof to a specific relevant CSIRT in cases where:

(a) the relevant CSIRT has been affected by a cybersecurity incident casting doubt on its ability to ensure the confidentiality of the notified information;

(b) it has sufficient reason to believe that the capabilities of the relevant CSIRT are inadequate to ensure the confidentiality of the notified information.

In cases referred to in point (a) of the first subparagraph, the CSIRT initially receiving the notification may delay the dissemination until the relevant CSIRT has informed the CSIRTs Network referred to in Article 15 of Directive 2022/2555 that its ability to ensure the confidentiality of notifications has been restored.

In cases referred to in point (b) of the first subparagraph, the CSIRT initially receiving the notification may delay the dissemination to the relevant CSIRT until that CSIRT has provided evidence that it has addressed the shortcomings identified.

Article 5

Terms and conditions for applying cybersecurity-related grounds in relation to the single reporting platform

The CSIRT initially receiving the notification may decide to delay the dissemination of notifications via the single reporting platform established by Article 16 of Regulation (EU) 2024/2847 where ENISA has informed the CSIRTs Network, in accordance with Article 16(4) of that Regulation, that the single reporting platform has been affected by a cybersecurity incident casting doubt on its ability to ensure the confidentiality of notified information. In such cases, the CSIRT initially receiving the notification may delay the dissemination via the single reporting platform until ENISA has informed the CSIRTs Network that the platform's ability to ensure the confidentiality of notifications has been restored.

Article 6

This Regulation shall enter into force on [the twentieth day following that of its publication in the *Official Journal of the European Union*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President
Ursula Von der Leyen