An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Guidelines on reporting obligations under Article 14 of the Cyber Resilience Act (CRA)

This document provides guidance to manufacturers of products with digital elements on their reporting obligations under Article 14 of the CRA (Regulation (EU) 2024/2847).

ncsc.gov.ie

31st August 2026

TLP:CLEAR

Rialtas na hÉireann
Government of Ireland

Disclaimer:
These Guidelines are intended to provide guidance to manufacturers of products with digital elements on their reporting obligations under Article 14 of the CRA.

The Guidelines do not represent legal advice, regulatory direction, operational approval or risk acceptance. No part of these Guidelines should be interpreted as validation, endorsement, or confirmation that a particular approach, control set, or decision meets legal, regulatory, or supervisory requirements howsoever arising including but not limited to EU regulations, directives, national legislation or regulations, guidance, and/or policies. Any examples, opinions, or suggested approaches shared here are illustrative in nature and are not a substitute for your own governance, assurance processes, or independent professional advice. Organisations remain solely responsible for their own decisions (including security decisions), compliance obligations, and risk management outcomes.

These Guidelines may not be relied upon as evidence of compliance, organisational approval, or due diligence, and may not be cited as a defence, justification, or mitigating factor in any regulatory, audit, investigative, or enforcement context.

Save where otherwise indicated or the context so requires, a word or expression that is used in these Guidelines and which is also used in the CRA has the same meaning in these Guidelines as it has in the CRA.

The NCSC reserves the right to amend these Guidelines from time to time, and as required.

The EU Cyber Resilience Act

What is the CRA?

The Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847)[1] is a landmark EU Regulation that entered into force on the 10th December 2024. It establishes mandatory cyber security standards for all connected hardware and software products sold in the EU. The purpose is to ensure that digital products are designed, developed, and produced with security in mind and that manufacturers remain responsible for vulnerability handling throughout the product's full lifecycle.

The core objectives of the CRA are:

- Enforce standards during product design to enhance the cybersecurity of products and encourage secure-by-design.
- Introduce vulnerability management obligations for the handling and patching of vulnerabilities through the lifetime of a product.
- Improve transparency for users regarding security updates and support periods.
- Encourage a harmonised and resilient digital market across the EU.

A staged approach to implementation of the CRA has commenced and spans from December 2024 to December 2027 to allow manufacturers sufficient time to adapt to these new security requirements. The mandatory reporting obligations under Article 14 of the CRA commence from the 11th September 2026, where entities with products in scope must report actively exploited vulnerabilities and severe incidents impacting product security.

[1] 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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) or (CRA).

Scope of the CRA

The CRA applies to a broad range of Products with Digital Elements (PDEs) made available in the EU market. Manufacturers, importers, and distributors of hardware and software products that connect directly or indirectly to a network are in scope, with some exceptions.

Definition of a PDE:

The CRA defines a PDE as *"a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately"*.

This essentially means any software or hardware product that can connect to a device or a network. If a product has a chip, runs code, and uses a data connection (like Wi-Fi, Bluetooth, or a physical network connection) to function, it is likely to be in-scope of the CRA.

- In-scope examples include laptops, smartphones, smart fridges, industrial IoT, operating systems, standalone mobile apps and cloud services that a device cannot perform a function without.
- Out-of-scope examples include non-connected devices like a basic calculator or a "dumb" home appliance, products already covered by specific sectoral legislation including medical devices and motor vehicles.

Within the CRA, products are grouped into three risk categories (Default, Important & Critical). While these risk categories determine how products are assessed for conformity compliance prior to launch, each individual product across all three categories is subject to the same reporting obligations described here.

Important Note: There are specific exemptions for offline products and strictly excluded sectors, however manufacturers must undertake their own appropriate legal and technical assessment to determine if their products fall within the scope of these exemptions.

Mandatory Reporting Obligations

Ahead of the full implementation of the CRA in late 2027, when every relevant product must be fully compliant with all of the CRA technical requirements i.e. CE marking, risk assessments, etc., the critical reporting obligations commence earlier, on the **11th September 2026**. Even though products don't yet need to meet all the secure-by-design rules, manufacturers of products in scope are under a legal obligation pursuant to Article 14 to start reporting serious product security related events.

What Must Be Reported?

1. **Actively Exploited Vulnerabilities**
   If there is reliable evidence that a malicious actor is exploiting a vulnerability in a PDE.

2. **Severe Incidents**
   Any incident which negatively affects or could affect a product's security functions such as protecting data or the integrity of the system.

It should be noted that if an actively exploited vulnerability or a severe incident occurs in an integrated third-party component, the manufacturer of the final product must submit the required notifications if they become aware the specific product is impacted.

Reporting Timelines

Manufacturers must notify the relevant national CSIRT, based on their main establishment within the EU, and the European Union Agency for Cybersecurity (ENISA). These notifications are made simultaneously via the Single Reporting Platform (SRP):

1. **Early Warning**
   - Within **24 hours** of becoming aware of the actively exploited vulnerability or severe incident.
     - In the case of active exploitation, awareness commences when there is reliable evidence that a malicious actor has actively exploited a vulnerability.
   - This is an initial notice outlining a suspicion of malicious intent, and the affected Member States.
     - Complete technical details are **not** required in this notification.
     - The Early Warning must not be delayed while awaiting detailed analysis.

2. **Detailed Notification (72-hour notification)**
   - Within 72 hours of becoming aware of the exploit or incident.
   - This is a more detailed notice and will contain the Initial assessment of severity, nature of event, and any mitigation measures.
   - It is important to note that on submission of the 24hrs Early Warning (EW) report to the SRP, the Detailed Notification must be submitted within 48hrs of the EW submission.

3. **Final Report**
   - In the case of an active exploitation, submitted within 14 days after a corrective or mitigating measure is made available.
   - For Severe Incidents, no later than 1 month after submission of the Detailed Notification.
   - This should provide a full technical analysis, root causes, and corrective actions taken.

Please refer to Article 14, here, for full details of the information that manufacturers must report at each of the stages set out above for an actively exploited vulnerability or severe incident.

National CSIRT as the Coordinating CSIRT

When a manufacturer submits a notification, the report is received simultaneously by ENISA and the national CSIRT in the country where the manufacturer is established. This CSIRT becomes the Coordinating CSIRT and performs two key functions:

- Verifies that the person submitting the report is an authorised representative of the manufacturer.
- Disseminates the notification via the platform to other national CSIRTs in EU countries where the manufacturer has indicated that the product has been made available.

In addition, the Coordinating CSIRT has the authority to request intermediate reports from manufacturers following a notification, to get further technical details or status updates as the investigation progresses.

CSIRT Delayed Dissemination

Under the CRA reporting framework[2], the CSIRT has the power to temporarily delay disseminating a submitted vulnerability or incident notification to other regional CSIRTs.

The CSIRT may decide to delay the dissemination of notifications (or parts thereof) in cases where the cybersecurity risks posed by the dissemination outweigh its security benefits, and among other matters, standard sharing protocols are not sufficient to guarantee the information security.

Delays are strictly timebound and limited to specific scenarios, such as:

- An effective mitigation patch is expected within 72 hours.
- There is a high risk of immediate exploit generation if the information is shared.
- An on-going Coordinated Vulnerability Disclosure (CVD) process is in progress.

When a CSIRT delay is invoked, they will immediately inform ENISA of the decision, reasoning and expected dissemination timeline.

ENISA Single Reporting Platform

To streamline and standardise the reporting process, all notifications must be submitted through the centralised Single Reporting Platform (SRP) maintained by ENISA.

- Only notifications submitted via the SRP count as satisfying statutory reporting obligations.
- Once a notification is submitted through the SRP, it will be automatically shared with the relevant national CSIRT and ENISA.
- Through the SRP, the Coordinating CSIRT will disseminate notifications to the other relevant member states.
- The platform is a secure portal that has been designed specifically to handle sensitive vulnerability and incident data.

[2] Commission Delegated Regulation (EU) 2026/881 of 11 December 2025 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

What if the Single Reporting Platform (SRP) is Offline?

- Sending an email to the CSIRT does not constitute a formal notification.
- If ENISA issues a formal alert indicating that the SRP is currently unavailable, a voluntary report via email can be made to the CSIRT for urgent vulnerability or severe incident alerting.
- As soon as the SRP becomes available, any official notifications (the 24-hour Early Warning or 72-hour Notification) must be submitted formally through the platform to satisfy compliance requirements.

It is **not** necessary to pre-register on the platform. Registration is straightforward and need only be completed when submitting the first Early Warning notification. Account validation will be performed in parallel with the reporting process.

Legacy Products

Any PDE's placed on the market before the 11th December 2027 are generally considered exempt from the technical design requirements of the CRA but are **not** exempt from the reporting obligations. If these products are currently available on the EU market, irrespective of when they were first launched or manufactured, they are considered in-scope of the CRA for reporting purposes.

It should be noted that reporting obligations only apply to newly discovered active exploitations. Manufacturers do not need to report active exploits that they are already aware of, prior to the 11th September 2026.

Further Information & Specific FAQs

The European Commission maintains a technical FAQ that addresses many of the complex questions regarding the implementation and intricacies of the Cyber Resilience Act. This FAQ includes technical scenarios and regulatory guidance:

European Commission: FAQs on the Cyber Resilience Act

In addition to the FAQ, the following publication provides practical guidance to help manufacturers, developers, and businesses of all sizes meet their obligations under the Cyber Resilience Act:

Guidance to Support Timely Cyber Resilience Act Implementation

For questions related to the SRP and reporting through the platform, ENISA are maintaining an FAQ page:

CRA Single Reporting Platform FAQ

For inquiries and assistance regarding the technical process of submitting Article 14 notifications please contact the NCSC at cra_helpdesk@ncsc.gov.ie. Please note that any delay in receiving a response from the NCSC does not alter a manufacturer's reporting obligation timelines.

Please note that the NCSC does not provide assistance or guidance in determining product scope or general regulatory applicability.

The mandatory reporting obligation referred to in these Guidelines are one set of legal requirements provided for in Article 14 of the CRA. Manufacturers must undertake their own appropriate legal and technical assessment to satisfy all the requirements of the CRA and related legislation.