Ref. Ares(2026)6787068 - 07/07/2026

Brussels, 10 June 2026

Minutes

5th Meeting of the Expert Group on Cybersecurity of Products with Digital Elements[1]

1. Nature of the meeting

The 5th meeting of the Expert Group on Cybersecurity of Products with Digital Elements (the 'CRA Expert Group') took place in Brussels, with the possibility to join remotely.

Participation was restricted to the members of the Expert Group. ETSI joined the meeting as permanent observer. The Radio Equipment Directive Compliance Association (REDCA) and TIC Council were invited as observer for point 4 of the agenda.

2. Welcome and introductions

The Commission welcomed the experts to the fifth meeting of the CRA Expert Group and thanked them for their active participation and engagement.

The draft agenda was adopted without changes. As part of AOB, one participant suggested to discuss further the CE marking of software and the EUCC-CRA delegated act.

Before turning to the implementation of the CRA, the Commission updated the Expert Group on two broader policy developments of relevance to its work.

The Commission recalled the adoption, in the preceding week, of the sovereignty tech package, comprising the Chips Act 2.0, the Cloud and AI Development Act, the Open Source Strategy and the Strategic Roadmap for Digitalisation and AI in the Energy Sector. The package is intended to support Europe's digital autonomy and reduce structural dependencies on suppliers outside the Union for core digital technologies, at a time of sharply rising demand for computing capacity driven by the uptake of AI. The Commission drew the Expert Group's attention in particular to the Open Source Strategy, which recognises the role of open source for economic growth and technological sovereignty and aims to scale up open-source alternatives in priority areas, including cloud, AI, internet technologies, cybersecurity and semiconductors, while strengthening the long-term maintenance and security of Europe's open-source infrastructure. The Commission noted that several actions bear directly on the implementation of the CRA: the establishment of an Open Source Maintenance Instrument under the next multiannual financial framework was highlighted as an important tool for the security and sustainability of open source, and the voluntary attestation framework foreseen by Article 25 of the CRA was identified as a priority strand of this work. The Commission indicated that it expected to receive shortly the final report prepared by Null Point Studio on the matter, after which the next steps would be taken forward.

The Commission then updated the Expert Group on its response to recent developments concerning frontier AI and cybersecurity. It recalled that, during the plenary session of the European Parliament on 19 May, EVP Virkkunen announced a list of actions on AI and cybersecurity, intended to strengthen the Union's preparedness by bringing together EU

[1] Published in the Register of Commission Expert Groups and Other Similar Entities, code number E03967

expertise in AI and cyber and working in close cooperation with like-minded partners. The Commission explained that the announcement responded to the emergence of frontier AI models with advanced capabilities to detect and exploit software vulnerabilities, a development that has raised significant concerns across the cybersecurity ecosystem and underlined the need to adapt cybersecurity practices and policies to the level and pace at which malicious actors can use AI to detect and exploit vulnerabilities. The action plan would aim to bring together all relevant actors (Member States, EU critical infrastructure, the public sector and businesses, and EU institutions, bodies and agencies) complementing and leveraging the existing EU framework, building notably on the AI Act, the NIS2 Directive, the CRA, the Cyber Solidarity Act and the proposed revision of the Cybersecurity Act.

Turning to the implementation of the CRA, the Commission provided an update on activities that had advanced since the previous meeting.

On delegated and implementing acts, the Commission noted that the delegated act on the terms and conditions for withholding notifications, adopted on 11 December 2025, had not been subject to objection by the Council or the European Parliament and had since been published in the Official Journal.

On guidance and support to industry, the Commission recalled that the public consultation on the draft guidance had run between March and April, thanked participants for the substantial feedback received, and indicated that it would set out the intended way forward under the dedicated agenda point. The Commission added that work had also advanced on the interplay between the CRA and the AI Act, and on the guidance concerning the interplay with DORA. It further noted that ENISA had published a range of supporting material, including technical advisories and a draft secure-by-design playbook, which would be presented during the meeting.

On market surveillance, the Commission reported that the CRA ADCO was operational and would meet in two weeks in Berlin. It would be chaired by the German BSI, with the Cypriot Digital Security Authority holding the vice-chair. The Commission noted that market surveillance authorities were preparing for the application of the CRA and cooperating closely to ensure efficient enforcement across the Single Market.

On the interaction between the CRA and the EUCC, the Commission indicated that it was refining the concrete conditions under which presumption of conformity via the EUCC would apply. It intended to share a paper outlining the envisaged content of the delegated act in the course of the month, with the draft delegated act to follow at a later stage. Some participants raised questions regarding the interaction between the CRA and the EUCC, including the consequences of an EUCC certificate being withdrawn.

Further updates on conformity assessment, the CRA Single Reporting Platform, SBOMs, and standards are summarised under the relevant agenda point.

3. List of points discussed

Commission guidance on the CRA & on the interplay with AI Act and DORA

The Commission updated the Expert Group on the state of play following the public consultation on the draft guidance package, which had run from 3 March to 13 April 2026. It recalled that, in parallel, four thematic workshops had been held within the Expert Group,

covering free and open-source software; remote data processing solutions and the scope of the CRA; risk assessment and conformity assessment; and substantial modifications, spare parts, the support period, and placement on the market.

The Commission identified a number of key topics that, in light of the feedback received, required further attention, including the link between substantial modification and the support period; the question of risk transfer; and the determination of "who is placing what" on the market.
The Commission set out the approach it intended to follow in reviewing the text. Rather than revising the package in a single step, it would share revised drafts with the Expert Group iteratively, as a means of enabling experts to provide feedback on individual sections as they were finalised. In this context, the Commission had already shared a revised text on substantial modifications and the support period prior to the meeting. It indicated that adoption of the guidance was likely to take place shortly after the summer.

During the discussion, participants raised a range of points on the draft guidance and on areas warranting further clarification. Topics raised included the concept of placement on the market, and whether it should be understood by reference to each individual unit of a product, noting that software appeared to be treated differently in this respect; the interaction between spare parts and substantial modifications and the Data Act; the application of Article 14 to products placed on the market before the CRA becomes applicable, and the treatment of end-of-life products; the provision of as many concrete examples as possible, while supporting case-by-case assessments; the reporting channels available to stewards, and whether they could report to ENISA; and the link with accessibility obligations.

The Commission recalled that Article 26 of the CRA indicates that the Commission should publish guidance on the interplay between the CRA and other related Union legal acts. It noted that guidance on certain aspects of this interplay had already been provided through the Frequently Asked Questions published in December 2025, as well as in the draft guidance package discussed earlier in the meeting. The Commission had since begun work on dedicated guidance addressing, respectively, the interplay between the CRA and the AI Act, and the interplay between the CRA and the Digital Operational Resilience Act (DORA) for financial entities.

On the guidance concerning the CRA and the AI Act, the Commission explained that it was working closely with the AI Office and had adopted a pragmatic approach based on the actual questions and comments submitted by stakeholders, covering matters such as the interplay between security requirements, the conformity assessment approach, and incident reporting. The work had started in November 2025 with a first joint meeting between members of the CRA Expert Group and the EU AI Board. A second joint meeting was held on 20 May 2026 to present the state of play, including draft questions and answers, and participants were invited to submit written feedback until 3 June. The Commission indicated that the feedback received would be used to refine the questions and answers.

On the guidance concerning the CRA and DORA, the Commission explained that it was working closely with DG FISMA, responsible for the financial sector. Work had begun in April and a number of areas for possible coverage had been identified, including scope, documentation requirements, vulnerability management processes, and incident reporting. These elements would be developed in more detail in the coming months. The Commission

indicated that, tentatively, it was working towards adoption of both guidance documents by the end of 2026.
In the exchange, several participants expressed support for the work on interplay guidance. Some participants suggested guidance could also be developed with regard to the interplay between the CRA and the NIS2 Directive. In response to questions, the Commission clarified guidance documents and Frequently Asked Questions in principle have equal authoritative value. The Commission also clarified draft guidance on the interplay between the CRA and DORA will be shared for consultation once it has reached a sufficient level of maturity.

Support for manufacturers and SMEs
ENISA presented an update on its work to support manufacturers and SMEs, covering its SME survey, its technical advisories on secure use of package managers and on secure updates (draft for public consultation open until 10 July 2026), and the draft Secure by Design Playbook.

The survey, conducted between February and March 2026 with a final report to be published shortly, examined several aspects of SME readiness for the CRA. ENISA noted that the size of the SME was the most consistent factor influencing maturity and that incident response and lifecycle management was the weakest area overall. It also observed that SMEs do not rely on a single source of information on the CRA.

ENISA explained that it seeks to provide practical tools to help SMEs meet the objectives of the CRA. Two technical advisories had been published, with further topics of common interest, such as vulnerability reporting, to be addressed through similar advisories. The secure-by-design playbook is available in draft for consultation. ENISA is also establishing an Ad-Hoc Working Group on Security Architecture Engineering and Vulnerability Management, which will support this work, including with a roadmap for new advisories.

During the discussion, participants raised the need to avoid duplication with EU-funded projects (DEP), and greater clarity on the nature of the tooling those projects would make available (support with their CRA implementation journey, cybersecurity tools, etc.); the importance of placing SMEs at the centre and providing practical tooling and templates, rather than general guidelines; the need to reach SMEs at large and to communicate these initiatives more widely. ENISA explained that its intention is to continue working together closely with interested stakeholders (such as companies, associations, and stewards) to provide such tools. ENISA intends to promote these initiatives also via the CRA EG.

Proposal for an FAQ document on conformity assessment
The Commission presented the state of play on conformity assessment, recalling two milestones: Chapter IV of the CRA applies as of 11 June 2026, and Member States are to have a sufficient number of notified bodies in place by the end of 2026. It noted that all Member States intend to rely on accreditation, and that discussions were advancing in parallel with European Accreditation.

The Commission recalled that some 300 representatives of conformity assessment bodies (CABs) had taken part in an event in April, and that a meeting with notifying authorities was scheduled for 18 June, alongside bilateral exchanges. While the notification of CABs is a national competence, the Commission was facilitating the process, including by outlining pragmatic options for accreditation based on alternatives where standards are not yet available

The Commission noted that ENISA had published, that week, a document on the technical competence requirements for CABs, while a gap analysis assessing the differences, for CRA purposes, between CABs notified under the EUCC and the RED delegated act would be circulated shortly. The Commission added that a high-level FAQ document addressing basic questions and key principles (such as where a CAB may apply for accreditation) would be shared with the Expert Group and notifying authorities shortly.

During the discussion, participants raised a number of points, including on the concrete application on Module H; on the differences in the testing requirements for notified bodies as compared with the RED delegated act, and the treatment of subcontracting, including whether test reports from laboratories outside the EU could be accepted; that Module B is where most requests are expected and that competition for notified bodies could intensify, including in light of the fact that manufacturers of default products may wish to undergo third-party assessment; and whether a body comparable to RED CA would be established for the CRA to support consistent interpretation across the Single Market. The Commission confirmed that such a body would be established in due course, once notified bodies are in operation.

Global Cybersecurity Labelling Initiative

The Commission presented the Global Cybersecurity Labelling Initiative (GCLI), an international platform that gathers 11 states, notably from Europe and the Indo-Pacific region, whose objective is to have a common understanding on cybersecurity requirements in order to ensure policy interoperability and reduce barriers to trade.

The Commission noted that, at its most recent conference in April 2026, the governmental members of the GCLI had decided to establish a discussion forum with the private sector, in order to better understand the implications for industry of legal cybersecurity requirements on products and of labelling schemes. Each member would appoint one industrial player from its jurisdiction. The Commission indicated that it would open a call for European industrial members to volunteer for this workstream, with a deadline at the end of August.

During the discussion, participants raised a number of points, including which part of industry the single representative would be drawn from, given its diversity; whether the initiative carried any ambition towards mutual recognition; the interaction between labelling schemes and mandatory requirements that govern market access.

In response, the Commission explained that the initiative aimed to align approaches to cybersecurity requirements on a voluntary basis. The Commission recalled that the CRA provides for maximum harmonisation: no additional market access requirements may be imposed, though Member States may require higher levels of security through voluntary labelling for specific uses, such as public procurement. It also clarified that mutual recognition agreements are explored bilaterally through relevant process and not in a multilateral fora.

SBOM

ENISA presented the results of its SBOM survey. It reported that the principal outcome of the survey was a request for guidance, and set out its planned next actions: an SBOM reference architecture blueprint; an SBOM reference implementation; support for informed decisions on SBOM tool selection; the exploration of VEX capabilities.
ENISA also issued a call for interest for an SBOM workstream under the Expert Group.

During the discussion, participants raised several points, including the suggestion that the reference architecture be approached as a long-term, public-private effort; and questions on a potential implementing act under Article 13(24) of the CRA.

In response, the Commission clarified that, for CRA purposes, SBOMs are used only for vulnerability handling. It explained that ENISA's actions were complementary to the policy dialogue on SBOMs, which falls within the Commission's remit.

State-of-play on standardisation

The Commission provided an update on the standardisation work, noting that it was progressing well, with deliverables now reaching a second or even third assessment.
On the horizontal deliverables, the Commission was finalising its third assessment of PT1 (principles, product risk management and lifecycle activities), placing it in its final stretch. It reported fruitful discussions on PT3 (vulnerability handling requirements) and hoped the resolution of comments could be concluded swiftly, underlining the strategic importance of this standard.

On the vertical standards, four standards relating to MPU/MCU and smartcards were reaching a final stage, while many further vertical standards were about to enter public enquiry, with ETSI standards expected for a second assessment from mid-June onwards.

The Commission welcomed recent progress on cross-vertical work, with agreement reached on cryptography, RDPS and secure update, as well as the ETSI initiative to create a "skeleton" to improve consistency across verticals.

The Commission clarified some aspects relating to the CRA standard for PKI products. The Commission noted that existing standards developed to support the implementation of eIDAS, in particular EN 319 411, are not sufficient for CRA compliance. There is no intention to harmonise these standards under the CRA. The Commission thus explained that the work on the CRA standard for PKI products should not exclude eIDAS applications.

Lastly, the Commission reported that it was working on a second standardisation request under the CRA. As set out in the 2026 Annual Union work programme for European standardisation, the request would complement the first by addressing gaps for products with digital elements outside the categories listed in Annexes III and IV, broadening the range of products able to benefit from presumption of conformity. The Expert Group would be consulted on the text.

During the discussion, participants raised a number of points, including whether the Commission could consider an open-ended standardisation request.

Single Reporting Platform

ENISA delivered an update on the CRA Single Reporting Platform (CRA SRP) that it is establishing pursuant to Article 16 of the CRA. The platform is on track for go-live on 11 September 2026, with a user acceptance testing (UAT) currently being performed by the CSIRT Network. Extensive security testing is also being carried out by an external contractor, by the Computer Security Incident Response Teams (CSIRTs) of the Member States and by

the Cybersecurity service for the Union institutions, bodies, offices and agencies (CERT-EU). Representatives of the CRA Expert Group have also been invited to perform UAT in July.

ENISA also updated the FAQ on the CRA SRP on their website, including a range of additional information.

ENISA delivered a live demo of the CRA SRP, showing the manufacturer (or steward) workflow, from registration to submission of the notification.

During the discussion, participants raised a number of practical questions, many of which were answered during the meeting. Some topics will need to be further discussed during next steps, including lesson learned from the test phase for manufacturers and stewards. These include the authentication and registration process, including the role of EU Login; the number of users permitted per manufacturer; the possibility of an API to interface the platform with companies' existing systems; the withdrawal of a notification; a series of points on the notification form, including the available language, export options, the use of links, the reasons for non-dissemination; whether stewards should use the platform;

In response, ENISA explained that an API for national platforms is under evaluation, and that an API for manufacturers could be considered after we have learnt whether the business case can be built based on the usage of the platform. Additional releases are already scheduled after September 2026 to add additional features, based on set priorities and risk management principles. Several points on the notification form will be addressed as part of the UAT process. ENISA noted that its FAQ, together with the Commission's FAQ, addressed a range of questions raised by participants.

4. Next meeting

The next meeting was tentatively scheduled for Wednesday 18 November 2026. However, the Commission informed Members that it intends to reschedule the meeting, with a view to bring it forward. It was agreed that a point to be added to the agenda would include discussions on tools being developed to support CRA compliance.

5. List of participants

Type A

- Sarah Fluchs
- Lukasz Kister
- Bart Preneel
- Roger Riera

Type C

- APPLiA (Home Appliance Europe)
- BSH Hausgeräte GmbH (BSH)
- BUSINESSEUROPE
- Cisco Systems Inc. (Cisco)
- Dekra
- DIGITALEUROPE
- Eclipse Foundation AISBL (Eclipse Foundation)

- Ericsson
- European DIGITAL SME Alliance (DIGITAL SME)
- European Electronic Component Manufacturers' Association (EECA), and particularly the European Semiconductor Industry Association (ESIA)
- Eurosmart
- IN Smart Identity France (INSI)
- Legrand
- Microsoft Corporation
- Nokia
- Open Source Security Foundation (OpenSSF)
- Orgalim – Europe's Technology Industries (Orgalim)
- Red Alert Labs (RAL)
- Siemens AG (SAG)
- Stackable
- The Apache Software Foundation (ASF)
- The European Consumer Voice in Standardisation (ANEC)
- UNIFE (UNIFE)

Type D

The public authorities of the following Member States:

- Austria (AT)
- Belgium (BE)
- Bulgaria (BG)
- Croatia (HR)
- Cyprus (CY)
- Czechia (CZ)
- Denmark (DK)
- Estonia (EE)
- Finland (FI)
- France (FR)
- Germany (DE)
- Greece (EL)
- Ireland (IE)
- Italy (IT)
- Latvia (LV)
- Lithuania (LT)
- Luxembourg (LU)
- Malta (MT)
- Netherlands (NL)
- Poland (PL)
- Portugal (PT)
- Romania (RO)
- Slovakia (SK)
- Slovenia (SI)
- Spain (ES)
- Sweden (SE)

Type E

- European Union Agency for Cybersecurity (ENISA)
- Norwegian Communications Authority (Nkom)

Observers

- European Telecommunications Standards Institute (ETSI)
- The Radio Equipment Directive Compliance Association (REDCA)
- TIC Council

Annex I: Final agenda

	AGENDA ITEM	NOTES
	Welcome coffee and communications check	
1.	**Welcome and administrative issues**	
1.1	Adoption of the draft agenda	
1.2	Update by the Commission on the implementation of the CRA	
2.	**State-of-play on guidance**	
2.1	Update by the Commission on CRA guidance	
2.2	Update by the Commission on AIA-CRA guidance and DORA-CRA guidance	
3.	**Support for manufacturers and SMEs**	
3.1	Update by ENISA	
	Coffee break	
4.	**Proposal for an FAQ document on conformity assessment**	
4.1	Update by the Commission	
	Lunch break	
5.	**Global Cybersecurity Labelling Initiative**	
5.1	Update by the Commission	
6.	**SBOMs**	
6.1	Update by the Commission and ENISA	
	Coffee break	
7.	**State-of-play on standardisation**	
7.1	Update by the Commission	
8.	**Single Reporting Platform**	
8.1	Update by ENISA	
9.	**Conclusions**	
9.1	Next steps	
9.2	AOB	