REPLIES OF THE EUROPEAN COMMISSION

TO THE EUROPEAN COURT OF AUDITORS' SPECIAL REPORT

on Detecting and responding to cybersecurity incidents

Contents

This document presents the replies of the European Commission to observations of a special report of the European Court of Auditors, in line with Article 265 of the Financial Regulation and to be published together with the special report.

I. THE COMMISSION'S REPLIES IN BRIEF

The Commission welcomes the continued interest of the European Court of Auditors (ECA) in cybersecurity and, specifically in this special report, in the detection of and response to cybersecurity incidents, as well as in its programme management practices.

The Commission recalls that the EU framework for significant and large-scale incidents is relatively new and has been based on largely voluntary cooperation and information sharing between EU entities and Member States, reflecting the balance between EU and national competences with regard to security. It was only with the adoption of Directive (EU) 2022/2555[1] that the concept of large-scale incidents was defined in EU law, and that the EU-CyCLONe Network was set up to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information between Member States and EU institutions, bodies, offices and agencies. Nevertheless, this framework, as the report notes[2], has become increasingly important given the rapid digitalisation of critical infrastructure and geopolitical volatility notably with an escalating cyber threat picture. The Council Recommendation on an EU blueprint for cyber crisis management adopted in June 2025 ('the Cybersecurity Blueprint')[3] describes the framework and the distinct roles and responsibilities of the various stakeholders. The Cybersecurity Blueprint recommends actions to improve the practical operation of this framework, such as agreeing on a common aligned taxonomy of incident severity levels and urging the computer security incident response teams (CSIRTs) network and EU-CyCLONe to agree without delay, as required under Directive (EU) 2022/2555, on procedural arrangements in the event of a potential or ongoing large-scale cybersecurity incident. The Commission is now working with other relevant EU entities and Member States on implementing the Council Recommendation.

Member States were obliged to transpose Directive (EU) 2022/2555 by October 2024, and the Commission continues to pursue infringement decisions with respect to Member States which have not communicated measures taken to transpose the Directive into national law. The Cyber Solidarity Act was adopted in 2025 and the tools that it creates, such as the Cybersecurity Reserve and Cyber Hubs, will take time to be fully operational. The Commission recognises the need for an enhanced role for the European Agency for Cybersecurity (ENISA) in contributing to EU-level preparedness and response in the event of large-scale incidents, including through issuing early alerts and providing support in incident response and review. This is accordingly an important component of the Commission's proposal for revision of the Cybersecurity Act[4]. It is therefore of utmost urgency that Member States fully implement the existing rules, and that the package of new measures be adopted by Parliament and the Council as soon as possible.

The Commission agrees with the ECA's finding[5], based on reporting from ENISA on the threat landscape, that significant incidents, in particular those of a cross-border nature, remain under-reported, and that the potential value of the cooperation mechanisms which exist in the EU framework has yet to be realised. At the same time, the Commission recalls that cooperation in

[1] OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

[2] Special report, paragraphs 01-05.

[3] OJ C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

[4] COM(2026) 11 final.

[5] Special report, paragraph 35.

cybersecurity depends on confidence and trust and there is no obligation under applicable EU rules for information sharing between EU entities and Member States. The CSIRTs Network, created by the first Directive on security of network and information systems (NIS)[6], and EU-CyCLONe should be encouraged to foster a culture of information sharing within and between the two networks. However, national security remains the exclusive responsibility of each Member State, which cannot be obliged to supply information the disclosure of which would be contrary to its essential interests of national security, public security or defence.

While the Commission agrees with the Recommendation 2 to 'Rationalise EU cybersecurity situational awareness capabilities and optimise the dissemination of information,' it recognises the necessity for some element of context: as set out in the Cybersecurity Blueprint, various stakeholders at EU level have distinct roles to play in the management of significant and large-scale incidents. The Commission, as an institution with political and operational responsibilities for crisis preparedness and response, including in the event of potential and ongoing large-scale cybersecurity incidents, has accordingly invested in developing a Cyber Situation Centre within one of its departments, with the support of bespoke services from an external service provider contracted for a limited period. It acknowledges the need for exploring further synergies and increasing efficiency with ENISA, while emphasising that the responsibilities of responsible Commission services, along with the external services contract for the Cyber Situation Centre, are separate matters. There is no duplication between the role of the Commission and that of ENISA, because they are carrying out activities in line with their respective mandates[7]. Moreover, structures are in place to ensure the flow of information between Commission departments and between relevant EU entities, including ENISA, in the event of a significant or large-scale incident.

With regard to the Cybersecurity Reserve[8], the Commission recalls that the underlying objective is to have a 24/7 tool available, in the event of significant or large-scale cybersecurity incidents, to all Member States, EU institutions, bodies, offices and agencies as well as certain Digital Europe Programme associated third countries. It should, however, be underlined that it is practically impossible to predict how many cybersecurity incidents of that scale will occur.

With regard to the European Cybersecurity Competence Centre (ECCC)[9], it is acknowledged that it has taken some time for the Cybersecurity Competence Community and the Strategic Advisory Group to be set up. It should, however, be borne in mind that since then the Network of National Coordination Centres has been operating as an intermediary and direct link with stakeholder communities in Member States for the purpose of gathering information and preparing work programmes.

The Commission takes due note of all the findings of the report and will carefully consider them going forward.

[6] OJ L 194, 19.7.2016, p. 1, ELI: http://data.europa.eu/eli/dir/2016/1148/oj.

[7] Special report, title page 19, paragraphs 11 and 48.

[8] Special report, paragraphs 52-61.

[9] See report, Sections 17 and 77-81.

II. REPLIES TO THE RECOMMENDATIONS

Recommendation 1 – Strengthen information sharing between Member States

To improve the detection of and response to cybersecurity incidents, the Commission, with the support of the European Union Agency for Cybersecurity (ENISA), should:

(a) propose, to the Network and Information Security Cooperation Group, that it carry out a detailed analysis of national security restrictions that limit information sharing and affect the EU's cyber resilience, and that it identify legal and technical solutions to increase information sharing while respecting the boundaries of national security;

(b) without prejudice to the decisions of the co-legislators, ensure, in collaboration with member states, that the single-entry point for incident reporting proposed by the Digital Omnibus can detect potential cross-border incidents;

(c) work on solutions to enable real-time incident reporting to ENISA.

(Target implementation date: (a) and (b) 2027, (c) 2028)

The Commission **accepts** Recommendation 1(a, b & c).

Recommendation 2 – Rationalise EU cybersecurity situational awareness capabilities and optimise the dissemination of information

To increase efficiency, the Commission should, in collaboration with ENISA, assess the feasibility of joint acquisition and analysis of information for situational awareness. It should also make this information and the related cyber threat reports available across relevant departments and agencies of the EU.

(Target implementation date: 2027)

The Commission **accepts** Recommendation 2.

The Commission supports this recommendation. It is in line with the Council Recommendation on an EU blueprint for cyber crisis management and with the Commission's proposal for a Regulation for a EU Cybersecurity Act, which envisages relevant EU entities, including the Commission and ENISA, working together to develop repositories for cyber threat intelligence data, and acknowledges the need for further streamlining, while also maximising sound financial management.

The Commission accepts this recommendation without prejudice to the provisions and scope of Regulation (EU, Euratom) 2023/2841[10] and the independent status of CERT-EU, which, for operational matters, remains under the authority of the Interinstitutional Cybersecurity Board.

[10] OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj.

Recommendation 3 – Integrate the European Cybersecurity Alert System into the EU cybersecurity landscape

The Commission should, together with ENISA and Member States, ensure that cooperation arrangements and interoperability standards are in place to facilitate information sharing among cross-border hubs that are part of the European Cybersecurity Alert System, the CSIRTs network, and EU-CyCLONe.

(Target implementation date: 2028)

The Commission **accepts** Recommendation 3.

Recommendation 4 – Ensure a robust ownership and control assessment of entities receiving EU funding under the Digital Europe Programme

The European Cybersecurity Competence Centre should:

(a) ***obtain reasonable assurance that beneficiaries responsible for providing financial support to third parties have the administrative and technical capacity necessary to perform adequate ownership and control assessments, based on the existing methodology available to beneficiaries implementing financial support to third parties; and***

(b) ***check, on a sample basis, whether only eligible entities have received EU funding.***

(Target implementation date: (a) 2026, (b) 2027)

The Commission notes that the recommendation is addressed to the ECCC.

Recommendation 5 – Strengthen the performance monitoring framework of the cybersecurity component of the Digital Europe Programme

To enable adequate progress and performance monitoring, the European Cybersecurity Competence Centre should:

a) ensure, prior to grant signature, that all projects have defined milestones, deliverables, and performance indicators that comply with the instructions provided in the application form;

b) design and implement a robust system for the collection, traceability, verification, and aggregation of the data for the performance indicators of the cybersecurity component of the Digital Europe Programme, to ensure the indicators accurately reflect the results achieved.

(Target implementation date: 2027)

The Commission notes that the recommendation is addressed to the ECCC.