Council of the European Union

Brussels, 20 April 2023
(OR. en)

8512/23
ADD 1

Interinstitutional File:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	19 April 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 209 final - Annex
Subject:	ANNEXES to the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

Delegations will find attached document COM(2023) 209 final - Annex.

Encl.: COM(2023) 209 final - Annex

EUROPEAN
COMMISSION

Strasbourg, 18.4.2023
COM(2023) 209 final

ANNEX

ANNEXES

to the

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

ANNEX

Regulation (EU) 2021/694 is amended as follows:

(1)In Annex I, the section/ chapter 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:

'Specific Objective 3 – Cybersecurity and Trust

The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union's digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.

Initial and, where appropriate, subsequent actions under this objective shall include:

1. Co-investment with Member States in advanced cybersecurity equipment, infrastructures and knowhow that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace ***including National SOCs and Cross-border SOCs forming the European Cyber Shield***, as well as other tools to be made available to public and private sector across Europe.

2. Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.

3. Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.

4. Support closing the cybersecurity skills gap by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training.

5. ***Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents through deployment of cybersecurity services across***

borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted cybersecurity providers at Union level.';

(2) In Annex II the section/chapter 'Specific Objective 3 – Cybersecurity and Trust' is replaced by the following:

'Specific Objective 3 – Cybersecurity and Trust

3.1. The number of cybersecurity infrastructure, or tools, or both jointly procured[1]

3.2. The number of users and user communities getting access to European cybersecurity facilities

3.3 The number of actions supporting preparedness and response to cybersecurity incidents under the Cyber Emergency Mechanism'

ANNEX […]