Council of the European Union

Brussels, 21 June 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	21 June 2022
To:	Delegations
No. prev. doc.:	9716/22
Subject:	Council conclusions on the Special Report of the European Court of Auditors No 05/2022 entitled 'Cybersecurity of the EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats' - Council conclusions approved by the Council at its meeting on 21 June 2022

Delegations will find attached the above Council conclusions, as approved by the Council at its meeting on 21 June 2022.

ANNEX

COUNCIL CONCLUSIONS

on Special Report No 05/2022 of the European Court of Auditors
entitled
'Cybersecurity of the EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats'

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING its conclusions on improving the examination of special reports drawn up by the Court of Auditors in the context of the discharge procedure[1];

1. TAKES NOTE of the European Court of Auditors' Special Report No 05/2022 entitled 'Cybersecurity of the EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats'[2].

2. UNDERLINES the importance and urgency of strengthening the level of cybersecurity within the EU institutions, bodies and agencies, given the recent intensification of the digital transformation within the institutions, the sensitive information they process, the ever-increasing number and severity of attacks on EU institutions, bodies and agencies and the level of threat affecting them.

3. RECALLS the European Council conclusions of 20 June 2019[3], in which the European Council invited the EU institutions, together with the Member States, to work on measures to enhance the resilience and improve the security culture of the EU against cyber and hybrid threats from outside the EU, and to better protect the EU's information and communication networks, and its decision-making processes, from malicious acts of all kinds.

---

1 7515/00 + COR 1.
2 8040/22.
3 EUCO 9/19.

4. RECALLS its conclusions of 10 December 2019 on complementary efforts to enhance resilience and counter hybrid threats[4], in which it called on the EU institutions, bodies and agencies, supported by the Member States, to ensure the capacity of the Union to protect its integrity and to enhance the security of EU information and communication networks and decision-making processes from malicious activities of all kinds, on the basis of a comprehensive threat assessment. To this end, the conclusions stated, institutions, bodies and agencies, supported by the Member States, should develop and implement a comprehensive set of measures to ensure their security, in accordance with the mandate of the European Council of June 2019[5].

5. RECALLS its conclusions of 22 March 2021 on the EU's Cybersecurity Strategy for the Digital Decade[6], where it stressed that cybersecurity is vital for the functioning of public administration and institutions, both at national and EU level and for our society and the economy as a whole.

6. RECALLS its conclusions of 23 May 2022 on the development of the European Union's cyber posture[7], in which EU institutions, bodies and agencies were encouraged to participate in the mapping of existing tools for secure communication in the cyber field to be discussed in relevant Council bodies and with relevant cooperation groups, such as the CSIRTs network and the EU CyCLONe.

7. UNDERLINES the need to address the systemic risk that exists in the interconnection between the EU institutions, bodies and agencies, as well as between them and the institutions of the Member States, despite their institutional independence and administrative autonomy.

---

4 14972/19.
5 EUCO 9/19.
6 6722/21.
7 9364/22.

8. TAKES NOTE of the observations of the Special Report, namely that the EU institutions, bodies and agencies have not achieved a level of cyber preparedness commensurate with the threats and have differing levels of cybersecurity maturity. RECOGNISES that the level of cybersecurity preparedness of the EU institutions, bodies and agencies, as well as the synergies among them, should be improved.

9. Strongly ENCOURAGES, therefore, the EU institutions, bodies and agencies to continue the implementation of cyber risk management measures that ensure a commensurate level of cybersecurity, as envisaged by the proposed directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, in order to improve their level of preparedness.

10. INVITES the EU institutions, bodies and agencies to intensify both their efforts to protect themselves against cyber threats and their cooperation on establishing consistent standards and specifications, in particular for public procurement, projects and services related to cybersecurity, and to improve the interoperability of their IT systems, including with a view to ensuring the secure communication of unclassified content.

11. INVITES the European Union Agency for Cybersecurity (ENISA) and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), within the framework of their competences, to intensify their cooperation in supporting the EU institutions, bodies and agencies in their cybersecurity efforts, in particular with regard to capacity building for those EU institutions, bodies and agencies that have a lower level of cybersecurity maturity.

12. TAKES NOTE of the conclusions and recommendations of the Special Report, and RECOGNISES that the level of cybersecurity preparedness of the EU institutions, bodies and agencies, as well as the synergies among them, should be substantially improved. EU institutions, bodies and agencies should have a comprehensive risk management framework for cybersecurity, carry out regular risk assessments and audits, based on a common or well-known methodology and international standards, and systematise cybersecurity awareness and training programmes for staff.

13. EMPHASISES as well that the EU institutions, bodies and agencies should allocate sufficient budget to ensure the implementation of protection measures against cyber threats while respecting the multiannual financial framework, and TAKES NOTE of the Special Report's recommendation that a body representative of all EU institutions, bodies and agencies should be appointed, and given the appropriate mandate and means, to monitor compliance with the common rules on cybersecurity.

14. RECOGNISES that CERT-EU should be informed without delay of significant cyber incidents within the EU institutions, bodies and agencies and, to this end, should be equipped with adequate resources that are predictable and adapted to the current level of threat and to the needs of the EU institutions, bodies and agencies, in particular in terms of staff, technical equipment and infrastructure.

15. NOTES that cooperation and exchange of information on cybersecurity, as well as interoperability of secure communication channels between EU institutions, bodies and agencies, should be strengthened and systematised. CALLs for such cooperation and exchange of information to also include public authorities responsible for cybersecurity in the Member States.

16. TAKES NOTE of the replies from the Commission, CERT-EU and ENISA accompanying the Special Report.

17. INVITES the Commission to take into account the recommendations of the Special Report and be ambitious when designing the cybersecurity policies of the EU institutions, bodies and agencies, and to advocate for more synergies between them.