Council of the European Union

Brussels, 20 May 2022
(OR. en)

9317/22

LIMITE

CYBER 182
TELECOM 234
CSC 199
CSCI 68
FIN 564

NOTE

From:	Presidency
To:	Delegations
Subject:	Special report of the European Court of Auditors Nr 05/2022 "Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats" - draft Council conclusions

1. On 30 March 2022, the European Court of Auditors issued its Special Report Nr 05/2022 entitled "*Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats*"[1].

2. At its meeting on 13 April 2022, the Permanent Representatives Committee entrusted the Special Report to the Horizontal Working Party on Cyber Issues[2].

3. On 3 May 2022 the representatives of the Court of Auditors presented the Special Report to the Horizontal Working Party on Cyber Issues.

   Following the discussion of the report at the same meeting of the Working Party, the Presidency prepared draft Council conclusions, the courtesy translation of which as set out in the Annex.

[1] 8040/22.

[2] 8041/22.

4. Once delegations have reached agreement on the text, in accordance with the Council conclusions of 8 May 2000 on improving the examination of special reports drawn up by the Court of Auditors[3], the Permanent Representatives Committee will be invited to suggest that the Council adopt these conclusions at a future meeting.

[3] 7515/00 + COR 1.

Courtesy translation

DRAFT 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[4];

1. TAKES NOTE of the European Court of Auditors' Special Report Nr 05/2022 entitled "Cybersecurity of the EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats".[5]

2. UNDERLINES the importance of strengthening the level of cybersecurity within the EU institutions, bodies and agencies, given the recent intensification of digital transformation within the institutions and the growing number and severity of incidents.

3. RECALLS the European Council conclusions of 20 June 2019[6], 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.

---

[4] 7515/00 + COR 1.

[5] 8040/22.

[6] EUCO 9/19.

4. RECALLS its conclusions of 10 December 2019 on complementary efforts to enhance resilience and counter hybrid threats[7], 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, 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[8].

5. RECALLS its conclusions of 22 March 2021 on the EU's Cybersecurity Strategy for the Digital Decade[9], 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. TAKES NOTE of the systemic risk existing 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.

7. ENCOURAGES therefore the EU institutions, bodies and agencies to continue implementation of cyber risk management measures in order to improve their level of preparedness against cyber threats.

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

9. INVITES the European Union Cybersecurity Agency (ENISA) and the Computer Emergency Response Team of the EU Institutions, Bodies and Agencies (CERT-EU) to intensify their cooperation in supporting the EU institutions, bodies and agencies in their cybersecurity

---

[7] 14972/19.

[8] EUCO 9/19.

[9] 6722/21.

efforts, in particular with regard to capacity building for the EU institutions, bodies and agencies less mature in cybersecurity.

10. TAKES NOTE of the conclusions and recommendations of the Special Report, and RECOGNIZES that the level of cyber security preparedness of the EU institutions, bodies and agencies should be improved. EU institutions, bodies and agencies should have a risk management framework for cybersecurity and systematise the use of cybersecurity awareness and training programmes for staff.

11. EMPHASISES as well that the EU institutions, bodies and agencies should allocate sufficient budget to ensure the implementation of protection measures against cyber threats and TAKES NOTE of the recommendations of the Special Report to designate a body representative of all EU institutions, bodies and agencies, with an appropriate mandate and means, to monitor compliance with the common rules on cybersecurity.

12. RECOGNIZES that CERT-EU should be informed without delay of significant cyber incidents within the EU institutions, bodies and agencies and to this aim, CERT-EU 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 personnel, technical equipment and infrastructure.

13. NOTES that cooperation and exchange of information on cyber security, as well as interoperability of secure communication channels between EU institutions, bodies and agencies should be strengthened and systematised.

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

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