



2026/0011(COD)

13.10.2026

AMENDMENTS

165 - 464

Draft report
Markéta Gregorová
(PE792.222v01-00)

European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

Proposal for a regulation
(COM(2026)0011 – 2026/0011(COD))

Amendment 165

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Recital 2 a (new)

Text proposed by the Commission

Amendment

(2a) The threat posed by ‘zero-day’ vulnerabilities, which are unknown to developers and for which no corrective measures exist, is intensifying as a result of artificial intelligence. The most advanced AI models are now able to autonomously discover such vulnerabilities in the most prevalent operating systems and browsers, develop the corresponding operating codes and execute most of the tactical operations of a cyberattack with limited human intervention. This development shortens the time between the discovery of a vulnerability and its exploitation and lowers the level of skill required to conduct sophisticated attacks, including for hostile State actors and criminal groups. Cybersecurity practices based on human-led detection, analysis and correction cycles are no longer able to address this specific risk. It is therefore necessary to update these practices, including by equipping public authorities with defensive AI tools capable of operating at the same speed and scale as attackers.

Or. fr

Amendment 166

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Recital 2 a (new)

Text proposed by the Commission

Amendment

(2a) Artificial intelligence, in particular AI agents, may create or amplify cybersecurity risks affecting critical infrastructure and consumers. The manipulation of AI agents, including through prompt injection, may result in unauthorised actions, disclosure of data or disruption of essential services. ENISA should take account of those risks in its analyses of technological cybersecurity trends and its technical guidance.

Or. en

Justification

AI agents can be manipulated through prompt injection to carry out unauthorised actions or disclose data. ENISA should address these risks in its existing work, in line with the Commission's AI Cybersecurity Action Plan.

Amendment 167

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Recital 2 b (new)

Text proposed by the Commission

Amendment

(2b) The use of artificial intelligence by administrations, competent authorities and ENISA in the field of cybersecurity should not create new dependencies on a single provider or on a third country. With AI models released under a free and open-source licence, within the meaning of Regulation (EU) 2024/1689, their functioning can be assessed, their security can be audited, they can be adapted to the specific needs of each authority and they can be deployed on sovereign infrastructure, without transferring sensitive data to third-party services. They thus reduce the risks of technological dependency and exposure to the extraterritorial laws of third countries. Therefore, when selecting, procuring or developing AI tools, administrations,

competent authorities and ENISA should prioritise models released under a free and open-source licence, with equivalent performance and level of security, without prejudice to the freedom of each Member State to determine the tools best suited to the protection of its national security.

Or. fr

Amendment 168

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

**Proposal for a regulation
Recital 3 a (new)**

Text proposed by the Commission

Amendment

(3a) This expansion of the Union cybersecurity acquis has also resulted in additional reporting requirements and a growing administrative burden for businesses. To ensure that cybersecurity rules remain effective and proportionate, the Commission should regularly evaluate the consistency of this Regulation with other relevant Union acts, as well as the consistency between them, with a view to removing overlapping or conflicting obligations, aligning definitions, thresholds and deadlines, and reducing the reporting requirements on companies, in particular small and medium-sized enterprises (SMEs), while maintaining a high level of cybersecurity.

Or. en

Amendment 169

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

**Proposal for a regulation
Recital 8**

(8) In an evolving threat landscape where cybersecurity incidents become increasingly more significant, delivering trust for individuals, public authorities and businesses in their daily use of technologies is even more important than ever. An increase in trust can be facilitated by a reinforced Union-wide certification of the ECCF providing for common cybersecurity requirements and evaluation criteria across national markets and sectors. The new framework should lay down the main horizontal requirements for European cybersecurity certification schemes and allow for European cybersecurity certificates and EU statements of conformity to be recognised and used in all Member States. In doing so, it should establish a procedure and governance framework that allows for the timely and predictable development and maintenance of European cybersecurity certification schemes. The European cybersecurity certification schemes should be applied uniformly in all Member States to ensure a harmonised implementation of cybersecurity requirements, level the playing field and prevent ‘certification shopping’ based on different levels of stringency in different Member States. ENISA should have a key role in providing for the development of the schemes ***through technical specifications*** and ensuring that such schemes remain technically up to date. Furthermore, to meet the market needs effectively, the framework should provide for the possibility for certification of cybersecurity risk management measures addressed to entities and facilitate compliance with other applicable Union legislation in the field of cybersecurity. Alignment with existing Union law, such as Regulation (EU) 2024/2847 and Directive (EU) 2022/2555, is essential for European cybersecurity certification schemes to contribute to reducing compliance burden on businesses, increase their attractiveness

(8) In an evolving threat landscape where cybersecurity incidents become increasingly more significant, delivering trust for individuals, public authorities and businesses in their daily use of technologies is even more important than ever. An increase in trust can be facilitated by a reinforced Union-wide certification of the ECCF providing for common cybersecurity requirements and evaluation criteria across national markets and sectors. The new framework should lay down the main horizontal requirements for European cybersecurity certification schemes and allow for European cybersecurity certificates and EU statements of conformity to be recognised and used in all Member States. In doing so, it should establish a procedure and governance framework that allows for the timely and predictable development and maintenance of European cybersecurity certification schemes. The European cybersecurity certification schemes should be applied uniformly in all Member States to ensure a harmonised implementation of cybersecurity requirements, level the playing field and prevent ‘certification shopping’ based on different levels of stringency in different Member States. ENISA should have a key role in providing for the development of the schemes and ensuring that such schemes remain technically up to date. Furthermore, to meet the market needs effectively, the framework should provide for the possibility for certification of cybersecurity risk management measures addressed to entities and facilitate compliance with other applicable Union legislation in the field of cybersecurity. Alignment with existing Union law, such as Regulation (EU) 2024/2847 and Directive (EU) 2022/2555, is essential for European cybersecurity certification schemes to contribute to reducing compliance burden on businesses, increase their attractiveness and strengthen the cyber resilience of the

and strengthen the cyber resilience of the Union.

Union.

Or. en

Amendment 170

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigríð Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 9

Text proposed by the Commission

(9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around **four** key areas of cybersecurity at Union level. First, ENISA should support Member States in the consistent implementation of Union policy and legislation regarding cybersecurity and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States.

Amendment

(9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around **five** key areas of cybersecurity at Union level. First, ENISA should support Member States in the consistent implementation of Union policy and legislation regarding cybersecurity and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States. ***The fifth should concern artificial intelligence and other emerging technologies with a potential impact on cybersecurity, and their use to strengthen cyber defence, including through testing***

Amendment 171

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

**Proposal for a regulation
Recital 9**

Text proposed by the Commission

(9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around four key areas of cybersecurity at Union level. First, ENISA should support Member States in the consistent implementation *of Union policy and legislation regarding cybersecurity* and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States.

Amendment

(9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around four key areas of cybersecurity at Union level. First, ENISA should support *the Union and* Member States in the consistent *elaboration of Union policies and drafting of legislation, as well as their* implementation and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States.

Amendment 172

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 14

Text proposed by the Commission

(14) The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. Within its mandate, ENISA should support the security and resilience of the public core of the open internet and the stability of its functioning, including, but not limited to, the secure deployment and operation of key protocols (in particular Domain Name System, Border Gateway Protocol, and Internet Protocol version 6) and the operation of the domain name system (such as the operation of all top-level domains), by promoting best practices, guidance, and cooperation, in accordance with established global, multistakeholder Internet governance arrangements and the respective roles and responsibilities of relevant international technical and operational bodies.

Amendment

(14) The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. Within its mandate, ENISA should support the security and resilience of the public core of the open internet and the stability of its functioning, including, but not limited to, the secure deployment and operation of key protocols (in particular Domain Name System, Border Gateway Protocol, and Internet Protocol version 6) and the operation of the domain name system (such as the operation of all top-level domains), by promoting best practices, guidance, and cooperation, in accordance with established global, multistakeholder Internet governance arrangements and the respective roles and responsibilities of relevant international technical and operational bodies. ***The Domain Name System is the basis on which almost every online service depends, which makes its integrity and availability essential to the security of entities in all sectors. Its security is challenged by attacks such as DNS hijacking, cache poisoning, by misconfiguration, and by the limited deployment of security extensions such as DNSSEC. ENISA should therefore support wider deployment and development of Domain Name System Security across the Union, in particular through capacity-building and research. To that end, ENISA should function as a point of contact to advise essential and important entities, issue guidelines and, where necessary, technical specifications.***

Amendment 173

Marc Botenga

on behalf of The Left Group

Proposal for a regulation

Recital 14 a (new)

Text proposed by the Commission

Amendment

(14a) Open-source software and open standards allow public authorities and citizens to inspect, audit and independently maintain the software underpinning critical services, reduce dependence on single suppliers and make vulnerabilities easier to detect and correct. Where software is developed with public funds, its results should in principle be made available to the public under open-source licences ('public money, public code'), strengthening democratic control, and transparency. ENISA should therefore promote open-source, auditable and publicly governed solutions and support public authorities in applying that principle.

Or. en

Amendment 174

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation

Recital 15

Text proposed by the Commission

Amendment

(15) ENISA acts as a reference point for advice and expertise on cybersecurity. Therefore, at the Commission's request, ENISA should assist it by means of expertise, technical advice, information, analyses, including feasibility studies,

(15) ENISA acts as a reference point for advice and expertise on cybersecurity. Therefore, at the Commission's request ***or at its own initiative***, ENISA should assist it by means of expertise, technical advice, information, analyses, including feasibility

opinions and preparatory work regarding any specific matter in the field of cybersecurity with a view to informing the Commission's policymaking and facilitating the Commission's monitoring of the implementation of Union legislation regarding cybersecurity.

studies, opinions and preparatory work regarding any specific matter in the field of cybersecurity with a view to informing the Commission's policymaking and ***legislative proposals and*** facilitating the Commission's monitoring of the implementation of Union legislation regarding cybersecurity.

Or. en

Amendment 175

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Recital 20 a (new)

Text proposed by the Commission

Amendment

(20a) In order to enhance cyber resilience across the Union and to provide technical support to Member States, CSIRTs and industry, ENISA should establish, maintain and operate a Union cybersecurity testing facility ('EU Cybersecurity Testbed'). Rapid technological developments, in particular as regards AI models, connected products and mobile software applications, require advanced evaluation infrastructure. Micro, small and medium-sized enterprises, open-source software stewards and CSIRTs often lack the financial, technical and human resources to carry out comprehensive testing, vulnerability analysis and remediation benchmarking. Access free of charge to the EU Cybersecurity Testbed should enable voluntary testing before and after the placing on the market, support the early detection of systemic vulnerabilities, including through the secure testing of AI with advanced cyber capabilities for cybersecurity use cases, and support the implementation of security by design

*principles, without administrative burden
for the users of the facility.*

Or. en

Amendment 176

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Recital 20 b (new)

Text proposed by the Commission

Amendment

(20b) In order to avoid duplication of investment, the EU Cybersecurity Testbed should operate in close cooperation with the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres established pursuant to Regulation (EU) 2021/887. ENISA should provide the operational testing services, vulnerability evaluation and guidance, while the ECCC should support the financing and technical deployment of testing infrastructure through Union funding programmes, including the Digital Europe Programme and Horizon Europe. Operational findings and recurring vulnerability patterns identified through the EU Cybersecurity Testbed should inform the funding priorities of the ECCC and complement the testing and experimentation facilities referred to in Regulation (EU) 2024/1689.

Or. en

Amendment 177

Francesco Torselli

Proposal for a regulation

Recital 22

Text proposed by the Commission

(22) To support businesses operating in the cybersecurity sector, users of cybersecurity solutions, and to ensure effective **the** implementation of Title **III** of this Regulation, ENISA should develop and maintain a 'market observatory' by **performing** regular analyses and disseminating information on **the main trends in the** cybersecurity market, on both the demand and supply sides.

Furthermore, to support **the** users of the EU Cybersecurity Reserve established **pursuant to** Regulation (EU) 2025/38, ENISA should prepare the mapping of the services needed by **such** users, **and of** availability of **such** services, **pursuant to that Regulation**.

Amendment

(22) To support businesses, **in particular micro and SMEs (MSMEs)**, operating in the cybersecurity sector **and** users of cybersecurity solutions, and to ensure **the** effective implementation of Title **III** of this Regulation, ENISA should develop and maintain a 'market observatory' by **conducting** regular analyses and disseminating information on **key** cybersecurity market **trends**, on both the demand and supply sides, **with a particular focus on shifting responsibilities to smaller operators in relevant supply chains ('liability').** **In addition, for** support users of the EU Cybersecurity Reserve established **under the** Regulation (EU) 2025/38, ENISA should prepare, **in accordance with that Regulation**, the mapping of the services needed by **those** users **and the** availability of **those** services.

Or. en

Justification

Liability dumping jeopardizes the legal and economic sustainability of MSMEs, burdening them

with burdens that go beyond their position in the value chain and therefore beyond their actual

capacity to intervene. Consistent with the principle that responsibilities must follow control, there

is therefore a need for provisions limiting undue transfer of responsibility, especially in relation to

critical digital products. The enforcement measures of the Regulation should take into account

this increasingly widespread phenomenon.

Amendment 178

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

**Proposal for a regulation
Recital 23 a (new)**

Text proposed by the Commission

Amendment

(23a) In view of Russia's war of aggression against Ukraine, ENISA should, within its tasks on international cooperation, offer support to Ukraine in aligning with Union cybersecurity law, including in phasing out, from its electronic communications networks, ICT components provided by high-risk suppliers, and by exchanging best practices on reducing reliance on such suppliers when networks are rebuilt or upgraded. ENISA should also draw on the lessons learned by Ukraine in countering state-sponsored cyberattacks.

Or. en

Amendment 179

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

**Proposal for a regulation
Recital 24**

Text proposed by the Commission

Amendment

(24) To help achieve a high level of cybersecurity in the Union, ENISA should support operational cooperation among Member States, in cooperation with CERT-EU, among Union entities, and between stakeholders. To that end, ENISA's role should be strengthened. ENISA should become a member of the CSIRTs network, contributing to the network information exchange and analysis. ENISA should further promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or

(24) To help achieve a high level of cybersecurity in the Union, ENISA should support operational cooperation among Member States, in cooperation with CERT-EU, among Union entities, and between stakeholders. To that end, ENISA's role should be strengthened. ENISA should become a member of the CSIRTs network, contributing to the network information exchange and analysis. ENISA should further promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or

protected by the CSIRTs. ENISA's active support for the work of the CSIRTs network and the European cyber crisis liaison organisation network (EU-CyCLONe) should enable those networks to continue strengthening their maturity level. ENISA's role in supporting such cooperation includes combating threats to the security and integrity of democratic institutions, elections and other processes, and the critical infrastructure on which they depend, in line with the European Democracy Shield: Empowering Strong and Resilient Democracies²⁶.

²⁶ JOIN(2025) 791 final.

protected by the CSIRTs. ENISA's active support for the work of the CSIRTs network and the European cyber crisis liaison organisation network (EU-CyCLONe) should enable those networks to continue strengthening their maturity level. ***As electoral infrastructure increasingly depends on digital networks and is a recurring target of cyberattacks, as illustrated by the large-scale cyberattacks against the Romanian electoral authorities in autumn 2024,*** ENISA's role in supporting such cooperation includes combating threats to the security and integrity of democratic institutions, elections and other processes, and the critical infrastructure on which they depend, in line with the European Democracy Shield: Empowering Strong and Resilient Democracies²⁶ ***and as highlighted by the European Parliament resolution of 15 September 2026 on the findings and recommendations of the Special Committee on the European Democracy Shield^{26a}.***

²⁶ JOIN(2025) 791 final.

^{26a} ***P10_TA(2026)0286***

Or. en

Amendment 180

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation Recital 24 a (new)

Text proposed by the Commission

Amendment

(24a) In its special report 19/2026, the European Court of Auditors concluded that the added value of the CSIRTs network and EU-CyCLONe is considerably limited by insufficient information sharing between Member States, notably due to national security

legislation and a lack of trust. ENISA should therefore support the Cooperation Group established under Directive (EU) 2022/2555 in analysing measures that could encourage Member States to share more information within those networks on a voluntary basis, while fully respecting Member States' responsibility for national security.

Or. en

Amendment 181

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation Recital 29

Text proposed by the Commission

(29) Access to real-time, verified, reliable cyber threat intelligence (CTI) is crucial for building shared situational awareness in the Union. ENISA, the Commission, CERT-EU and the European Cybercrime Centre (EC3) at Europol have already developed repositories of cyber threat intelligence that are tailored to their specific needs. ENISA and other relevant Union entities should cooperate, voluntarily, to develop repositories of real-time, verified, reliable CTI, and seek synergies to ensure economies of scale and reinforce sound financial management. This work should also include sectoral Union entities such as the EU agency for the Space Programme. They should share only derived analysis, trends, and tactics, techniques and procedures (TTPs), not raw sources, and should respect the independence of entities to manage their own CTI lifecycle in line with their mandates and need-to-know rules.

Amendment

(29) Access to real-time, verified, reliable cyber threat intelligence (CTI) is crucial for building shared situational awareness in the Union. ENISA, the Commission, CERT-EU and the European Cybercrime Centre (EC3) at Europol have already developed repositories of cyber threat intelligence that are tailored to their specific needs. ENISA and other relevant Union entities should cooperate, voluntarily, to develop repositories of real-time, verified, reliable CTI, and seek synergies to ensure economies of scale and reinforce sound financial management. This work should also include sectoral Union entities such as the EU agency for the Space Programme. ***ENISA should also explore ways to assist cooperation with providers of AI models and systems, through the relevant Union networks at horizontal and sectoral level, to enhance the sharing of CTI.*** They should share only derived analysis, trends, and tactics, techniques and procedures (TTPs), not raw sources, and should respect the independence of entities to manage their own CTI lifecycle in line with their

mandates and need-to-know rules.

Or. en

Amendment 182

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrīd Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Recital 32

Text proposed by the Commission

(32) To help increase awareness of cyber threat indicators and recommendations on mitigation measures, ENISA should make an early alert service available to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such generic, voluntary early alerts should benefit in particular SMEs, and should be provided in a machine-readable format made publicly available. In any case, such voluntary service is separate from and not related to any public-private partnerships that ENISA may establish or has already established.

Amendment

(32) To help increase awareness of cyber threat indicators and recommendations on mitigation measures, ENISA should make an early alert service available to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555. ***ENISA may extend that service to other entities of strategic importance, such as semiconductor undertakings. ENISA should establish the procedure to disseminate early alerts to those entities within six months of the entry into force of this Regulation.*** Such generic, voluntary early alerts should benefit in particular SMEs, and should be provided in a machine-readable format made publicly available. In any case, such voluntary service is separate from and not related to any public-private partnerships that ENISA may establish or has already established.

Or. en

Amendment 183

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 34 a (new)

Text proposed by the Commission

Amendment

(34a) Frontier artificial intelligence models can identify cybersecurity vulnerabilities at unprecedented speed and scale. That capability can strengthen cyber defence, but it can also enable malicious actors to discover and exploit vulnerabilities faster and more widely. ENISA should therefore analyse the cyber capabilities of such models and their implications for cybersecurity in the Union, in cooperation with the AI Office where appropriate. ENISA should share its findings with relevant Union entities and Member State authorities, in particular the CSIRTs network, EU-CyCLONe and the European Cybercrime Centre (EC3) at Europol, to support preparedness and response at Union and national level.

Or. en

Amendment 184
Jens Geier

Proposal for a regulation
Recital 35

Text proposed by the Commission

(35) Further, to understand better the challenges in the area of cybersecurity, ENISA needs to analyse current and emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity. In order to ensure easier access of the public to information on cybersecurity risks and possible remedies, ENISA may provide relevant information on its website, in a user-friendly and well-structured manner.

Amendment

(35) Further, to understand better the challenges in the area of cybersecurity, ENISA needs to analyse current and emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity. ***ENISA should build and maintain expertise on cybersecurity risks arising from emerging technologies, in particular artificial intelligence and quantum computing. With regard to artificial intelligence, this should include risks related to agentic and highly autonomous AI systems, open-weight models, AI-enabled automated threat vectors, automated vulnerability discovery and exploitation, and dependencies and***

vulnerabilities across the AI supply chain. ENISA should reflect those developments in its contribution to shared cybersecurity situational awareness and threat analysis. It should also build expertise on the cybersecurity implications of quantum computing and the transition to post-quantum cryptography. In order to ensure easier access of the public to information on cybersecurity risks and possible remedies, ENISA may provide relevant information on its website, in a user-friendly and well-structured manner.

Or. en

Amendment 185

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 37

Text proposed by the Commission

(37) Ransomware attacks are a prominent cybersecurity threat to the Union. To boost the Union's cybersecurity and combat ransomware, ENISA should develop capabilities for situational awareness and ***support for incident response and recovery***. When assisting individual essential and important entities in ***responding to and recovering from*** a ransomware attack, ENISA should closely cooperate with Europol and ***with*** CSIRTs or competent authorities as applicable, thereby drawing from Europol's established experience in fighting ransomware crime. ***Such assistance should complement CSIRTs' activities supporting incident response. To achieve synergies in its work against ransomware, ENISA should establish a helpdesk and, for that purpose, it could pool relevant capabilities and counter-ransomware services and make easily available information, guidance, and tools that can help*** essential

Amendment

(37) Ransomware attacks are a prominent cybersecurity threat to the Union. To boost the Union's cybersecurity and combat ransomware, ENISA should develop capabilities for situational awareness and ***prevention***. When assisting individual essential and important entities in ***preventing*** a ransomware attack ***from taking place***, ENISA should closely cooperate with Europol and ***support*** CSIRTs or competent authorities as applicable, thereby drawing from Europol's established experience in fighting ransomware crime. ***To that end, ENISA should support CSIRTs in establishing, within one year of the entry into force of this Regulation, a ransomware early warning and detection programme. The programme should be established by national CSIRTs with the support of ENISA and may be integrated into other national cybersecurity services offered to*** essential and important entities,

and important entities *respond to and recover from* a ransomware incident.

as long as it aims to prevent ransomware incidents in the pre-encryption phase. National CSIRTs or competent authorities should leverage a wide range of trusted intelligence feeds to deliver alerts to those entities on a regular basis, covering incident notifications, network abuse events, and vulnerabilities or exposed services, enabling earlier identification of ransomware activity. The programme may do so without intrusive network scanning, by relying on shared intelligence from CSIRTs and from trusted public, commercial and closed sources, including cyber threat intelligence procured from the EU Cybersecurity Reserve. CSIRTs may also make use of the European Cybersecurity Alert System established under Regulation (EU) 2025/38. The service may be extended to other entities of strategic importance.

Or. en

Amendment 186

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation Recital 38 a (new)

Text proposed by the Commission

Amendment

(38a) Faster exploitation of cybersecurity vulnerabilities enabled by artificial intelligence increases the risk of several significant or large-scale incidents occurring at the same time in different Member States or sectors. Union-level cybersecurity exercises should therefore also test preparedness to respond to multiple simultaneous incidents. As much of the Union's critical infrastructure is operated by private entities, ENISA should seek to involve the private sector in such exercises.

Or. en

Amendment 187

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews, Michael McNamara

Proposal for a regulation

Recital 39

Text proposed by the Commission

(39) Access to correct and timely information about vulnerabilities and a robust vulnerability management are imperative for ensuring a high level of cybersecurity in the internal market. For that reason, ENISA should maintain a European vulnerability database pursuant to Directive (EU) 2022/2555 and create a common Union vulnerability management service capacity, ensuring a resilient and sustainable service level and reducing the risk of disruptions. To that end, ENISA should explore possibilities to deepen structured cooperation with programmes, registries or databases similar to the European vulnerability database, in order to avoid a duplication of efforts and to seek complementarity on an international level, where appropriate. Furthermore, ENISA should support multi-party coordinated vulnerability disclosure at Union level and provide value added services, such as vulnerability advisories, severity scoring and product lists, as well as providing an enhanced European known exploited vulnerabilities catalogue to help entities in their vulnerability management.

Amendment

(39) Access to correct and timely information about vulnerabilities and a robust vulnerability management are imperative for ensuring a high level of cybersecurity in the internal market. For that reason, ENISA should maintain a European vulnerability database pursuant to Directive (EU) 2022/2555 and create a common Union vulnerability management service capacity, ensuring a resilient and sustainable service level and reducing the risk of disruptions. To that end, ENISA should explore possibilities to deepen structured cooperation with programmes, registries or databases similar to the European vulnerability database, in order to avoid a duplication of efforts and to seek complementarity on an international level, where appropriate. Furthermore, ENISA should support multi-party coordinated vulnerability disclosure at Union level and provide value added services, such as vulnerability advisories, severity scoring and product lists, as well as providing an enhanced European known exploited vulnerabilities catalogue to help entities in their vulnerability management, ***making use of the tools, platforms and laboratories provided under this Regulation and of AI-powered services to help essential and important entities prioritise updates and speed up patching. In view of the reliance of critical infrastructure on open source software, ENISA should, together with the Commission, Member States and open source communities, expedite the mapping of critical open source components and operate a Critical Open***

Source Resilience Campaign for components relevant to essential and important entities. The campaign may rely on a voluntary sponsorship scheme matching open source projects with organisations, such as Member States, Union entities like CERT-EU, operators of critical infrastructure and manufacturers, that are willing to support the maintenance and security of those projects, for instance by providing skilled people or AI models and tools to maintainers.

Or. en

Amendment 188

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Recital 39 a (new)

Text proposed by the Commission

Amendment

(39a) General-purpose AI models with systemic risk and AI systems operating autonomously are increasingly capable of identifying and exploiting vulnerabilities at scale, of operating as coordinated collectives of agents and of circumventing technical measures designed to contain them. Incidents in 2026, in which agentic AI systems under evaluation circumvented isolation controls, used publicly editable websites hosted in the Union as a means of coordination and compromised production infrastructure of third parties, demonstrate that the loss of control over an AI system is a cybersecurity incident in its own right in addition to being under the incidence of laws against unauthorised access to ICT systems. Regulation (EU) 2024/1689 confers on the Commission the power to request documentation, to conduct

evaluations of general-purpose AI models with systemic risk and to request measures from providers. The exercise of those powers requires standing technical capacity, including personnel, tooling, benchmarks and secure facilities and access to high-performance computing capacity, which might not exist yet in an adequate format at Union level: the scientific panel of independent experts established pursuant to Article 68 of that Regulation provides advisory expertise on evaluation methodologies but does not constitute operational capacity to conduct evaluations, and the evaluation capacity announced in the Commission Communication of 7 July 2026 on an Action Plan on Cybersecurity and Artificial Intelligence is to be procured through a call in 2027 without a legal mandate, a deadline or an institutional home. ENISA should therefore establish and operate a European AI Security Evaluation Capability as a standing capacity, acting as the hub of a network of bodies designated by the Member States and as the technical evaluator at the request of the Commission, without prejudice to the competences of the AI Office under Regulation (EU) 2024/1689 and without constituting a conformity assessment body.

Or. en

Amendment 189

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

**Proposal for a regulation
Recital 39 a (new)**

Text proposed by the Commission

Amendment

(39a) The use of frontier artificial intelligence models for vulnerability discovery is increasing the number of disclosed vulnerabilities faster than many

*organisations can remediate them.
ENISA's vulnerability management
services should therefore help
stakeholders to focus their resources,
including through risk-based
prioritisation and information on the
exploitability of vulnerabilities.*

Or. en

Amendment 190

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Recital 39 b (new)

Text proposed by the Commission

Amendment

(39b) Evaluations of advanced AI models are frequently conducted with safety measures reduced or disabled in order to measure capabilities. Such environments present a heightened risk of loss of control, as incidents in 2026 at providers and at a national evaluation body have shown. Bodies conducting such evaluations in the Union, including the European AI Security Evaluation Capability, should apply state of the art containment measures, including continuous human monitoring, control of network egress, per agent identity and logging, and the prevention of shared writable storage between AI agents. AI high risk security incidents should be notified through the single reporting platform established pursuant to Regulation (EU) 2024/2847 to the CSIRTs concerned and to ENISA, which should forward them to the AI Office, irrespective of whether the AI system concerned has been placed on the market, so that operators of Union infrastructure affected by such incidents have a channel to report them and so that the Union does not

depend on the voluntary disclosure of providers.

Or. en

Amendment 191

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Recital 39 c (new)

Text proposed by the Commission

Amendment

(39c) Evaluations should proceed on the basis of graduated access: remote programmatic access as a baseline, access without safety mitigations where provided for under Regulation (EU) 2024/1689 for general-purpose AI models with systemic risk, and full model access on the basis of agreements with providers. Where a provider fails to cooperate with an evaluation lawfully requested under that Regulation, the Commission should assess without delay whether the measures available under Article 93 of that Regulation, including the restriction of the making available of the model on the Union market, are warranted. Access by European organisations to AI models with advanced cyber capabilities should be governed by a Union framework for structured access with binding conditions, including identity verification, misuse monitoring and contingency measures where a provider or a third country authority restricts or withdraws access, rather than by voluntary arrangements that introduce no obligations for providers. The findings of evaluations should inform the Union level coordinated security risk assessments under this Regulation, so that a finding concerning the capabilities of a model, or a dependency of critical entities on a

*model or on AI compute infrastructure,
can trigger the same procedure as a
finding concerning a supplier.*

Or. en

Amendment 192

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Recital 39 d (new)

Text proposed by the Commission

Amendment

(39d) The use of AI has accelerated the discovery of vulnerabilities to a scale that the European vulnerability database, coordinated vulnerability disclosure and the maintainers of open-source software are not designed to absorb. Open-source software components on which essential and important entities depend are often maintained by small communities without the resources to remediate vulnerabilities at that pace. ENISA should therefore map those components at regular intervals, operate a Critical Open Source Resilience Campaign for them, adapt the European vulnerability database and the disclosure methodologies to discovery at scale, and provide AI assisted prioritisation, remediation and patching services, free of charge for open-source software stewards, micro and small enterprises and CSIRTs.

Or. en

Amendment 193

Markéta Gregorová

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 39 e (new)

(39e) Independent security research, including activities conducted by ethical security researchers to detect, analyse, and report system vulnerabilities, contributes significantly to the overall cyber resilience and security of the Internal Market. While unauthorised access to network and information systems must remain fundamentally restricted to safeguard digital integrity, enforcement actions and the application of legal responsibility should distinguish between malicious cyber threats and legitimate research activities aimed at enhancing security. Where security researchers act in accordance with established coordinated vulnerability disclosure frameworks, minimise potential operational disruption, and notify affected entities or competent authorities without undue delay, the legal framework should foster an environment that avoids the unnecessary criminalisation or disproportionate penalisation of actions undertaken in the public interest.

Or. en

Amendment 194

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo

Proposal for a regulation

Recital 40

Text proposed by the Commission

(40) The role of ENISA in the development of the ECCF should be a key aspect of its mandate. ENISA should provide its technical expertise throughout the lifecycle of European cybersecurity certification schemes. In view of a future scheme, ENISA should identify existing standards or technical specifications that

Amendment

(40) The role of ENISA in the development of the ECCF should be a key aspect of its mandate. ENISA should provide its technical expertise throughout the lifecycle of European cybersecurity certification schemes. In view of a future scheme, ENISA should identify existing standards or technical specifications that

can underlie such as a scheme and, where relevant, draft technical specifications itself that can be referenced in a scheme. ENISA should be in charge of preparing candidate scheme following a Commission request. For schemes already in place, ENISA should be responsible for their maintenance. In doing so, ENISA should contribute to building and developing a certification ecosystem where the feedback of Member States and private stakeholders is sought and their certification capacities are reinforced. ***This*** should also ***include operating*** a dedicated certification website where relevant information related to adopted schemes, including certificates and statements of conformity, is freely and publicly accessible.

can underlie such as a scheme and, where relevant, draft technical specifications itself that can be referenced in a scheme. ENISA should be in charge of preparing candidate scheme following a Commission request. For schemes already in place, ENISA should be responsible for their maintenance. In doing so, ENISA should contribute to building and developing a certification ecosystem where the feedback of Member States and private stakeholders is sought and their certification capacities are reinforced. ***To that end, ENISA should consult stakeholders in the preparation of each candidate scheme through the ad hoc working group and a formal, open, transparent and inclusive consultation process, including an open public consultation, and the members of the ECCG may also consult stakeholders. When transmitting a candidate scheme to the Commission, ENISA should describe how it has taken the feedback received into account. ENISA*** should also ***promote the uptake of adopted schemes, including by preparing an uptake roadmap, which should form part of each scheme. ENISA*** should also maintain a dedicated certification website where relevant information related to adopted schemes, including certificates and statements of conformity, is freely and publicly accessible.

Or. en

Amendment 195 Francesco Torselli

Proposal for a regulation Recital 40

Text proposed by the Commission

(40) The role of ENISA in the development of the ***ECCF*** should be a key aspect of its mandate. ENISA should provide ***its*** technical expertise ***throughout***

Amendment

(40) The role of ENISA in the development of the ***European framework of certification the Cybersecurity*** should be a key aspect of its

the lifecycle of European cybersecurity certification schemes. In view of a future **scheme**, ENISA should identify **existing** standards or technical specifications **that can underlie such as a scheme** and, where **relevant, draft** technical specifications **itself that can be referenced in a scheme**. ENISA should be **in charge of preparing candidate** scheme following a Commission request. **For schemes already in place**, ENISA should **be** responsible for their maintenance. **In doing so**, ENISA should contribute to **building and developing** a certification ecosystem where **the** feedback **of** Member States and private stakeholders is **sought** and their certification capacities are **reinforced**. This should also include **operating** a dedicated certification website where relevant information related to **adopted schemes**, including certificates and **statements of conformity, is** freely and publicly accessible.

mandate. ENISA should provide **their own** technical expertise **to** European cybersecurity certification schemes **throughout their lifecycle**. In view of a future **system, through continuous cooperation with business stakeholders (in particular representatives of MSMEs)**, ENISA should identify **possible** standards or technical specifications **on which to base such a system** and, where **appropriate, develop itself the** technical specifications **to be recalled in a system**. ENISA should be **mandated to prepare a proposal for a** scheme following a **request from the** Commission. **Existing systems:** ENISA should **being** responsible for their maintenance. **To that end**, ENISA should contribute to **the creation and development of** a certification ecosystem where feedback **from** Member States and private stakeholders is **required** and their certification capacities are **strengthened**. This should also include **the management of** a dedicated certification website where relevant information related to **the systems in place**, including certificates and **declarations of compliance, are** freely and publicly accessible.

Or. en

Justification

Compliance with the Regulation will depend on the appropriate tools that are made available to

small businesses for regulatory compliance. In this regard, it is considered essential to strengthen

cooperation with MSMEs in the process of establishing harmonised standards. Currently,

participation in technical tables at European standardisation organisations (CEN, CENELEC,

ETSI) is only sustainable for large companies. Without a reimbursement of expenses for MSME

experts, for example, the standards will be tailored exclusively to the needs of large companies,

which have the means to ensure their constant representation at the aforementioned technical tables.

Amendment 196

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation Recital 41

Text proposed by the Commission

(41) To support the implementation of relevant Union legislation, ENISA should shape the state of the art in cybersecurity by delivering technical specifications to support the implementation of relevant Union legislation, including in view of their potential referencing in European cybersecurity certification schemes. ENISA should ***also*** monitor the creation and evolution of standards by relevant standardisation bodies with a view to following standardisation trends at European and global level, and whenever needed, shape such standards by participating to, including through drafting contributions, and leading in the activities of standardisation organisations. In doing so, ENISA should remain impartial. For instance, there might be situations, where ENISA should withdraw from relevant activities in standardisation bodies if ENISA is asked to assess European standards that were requested by the Commission in support of Union legislation. ENISA should not contribute to the drafting of the standards that it is in charge of assessing.

Amendment

(41) To support the implementation of relevant Union legislation, ENISA should shape the state of the art in cybersecurity by delivering technical specifications to support the implementation of relevant Union legislation, including in view of their potential referencing in European cybersecurity certification schemes. ***For example, in the area of vulnerability management, those technical specifications may focus on the prioritization and faster deployment of updates by essential and important entities to ensure risk-based and timely patching in alignment with the Regulation (EU) 2024/2847 and Directive (EU) 2022/2555. While the Union has been successful in adopting technical ICT standards within the Union, European representation, whether governmental or non-governmental, in international ICT standard-setting bodies is lagging behind.*** ENISA should ***therefore*** monitor the creation and evolution of standards by relevant standardisation bodies with a view to following standardisation trends at European and global level, and whenever needed, shape such standards by participating to, including through drafting contributions, and leading in the activities of standardisation organisations. ***To enhance European representation at global level and to counter proposals that harm Union interests, ENISA and the Commission should promote the uptake of***

European standards by participating in international governmental ICT standard-setting bodies and coordinating European input with relevant stakeholders, and by facilitating the coordination and support of European industry and civil society participation in international non-governmental ICT standard-setting bodies. This would also function as a confidence building measure between the ENISA, Commission and relevant stakeholders. In doing so, ENISA should remain impartial. For instance, there might be situations, where ENISA should withdraw from relevant activities in standardisation bodies if ENISA is asked to assess European standards that were requested by the Commission in support of Union legislation. ENISA should not contribute to the drafting of the standards that it is in charge of assessing.

Or. en

Amendment 197

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Recital 41

Text proposed by the Commission

(41) To support the implementation of relevant Union legislation, ENISA should shape the state of the art in cybersecurity by delivering technical specifications to support the implementation of relevant Union legislation, including in view of their potential referencing in European cybersecurity certification schemes. ENISA should also monitor the creation and evolution of standards by relevant standardisation bodies with a view to following standardisation trends at European and global level, and whenever needed, shape such standards by participating to, including through drafting

Amendment

(41) To support the implementation of relevant Union legislation, ENISA should shape the state of the art in cybersecurity by delivering technical specifications to support the implementation of relevant Union legislation, including, ***where the conditions laid down in this Regulation are met***, in view of their potential referencing in European cybersecurity certification schemes. ENISA should also monitor the creation and evolution of standards by relevant standardisation bodies with a view to following standardisation trends at European and global level, and whenever needed, shape

contributions, and leading in the activities of standardisation organisations. In doing so, ENISA should remain impartial. For instance, there might be situations, where ENISA should withdraw from relevant activities in standardisation bodies if ENISA is asked to assess European standards that were requested by the Commission in support of Union legislation. ENISA should not contribute to the drafting of the standards that it is in charge of assessing.

such standards by participating to, including through drafting contributions, and leading in the activities of standardisation organisations. In doing so, ENISA should remain impartial. For instance, there might be situations, where ENISA should withdraw from relevant activities in standardisation bodies if ENISA is asked to assess European standards that were requested by the Commission in support of Union legislation. ENISA should not contribute to the drafting of the standards that it is in charge of assessing.

Or. en

Amendment 198

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 43

Text proposed by the Commission

(43) To support the implementation of conformity assessment activities under European cybersecurity certification schemes and other relevant Union legislation, ENISA may provide relevant technical testing tools to support Member States, businesses and conformity assessment bodies in evaluation activities. Such tools should aim to create synergies at Union level and an efficient operation of conformity assessment procedures to meet the needs of Member States and market needs. Such needs may arise for instance in the area of security by design to support businesses, including small and medium-sized enterprises, in their implementation efforts in the context of Regulation 2024/2847. In this context, ENISA should levy fees to cover relevant costs related to establishing, designing, developing, maintaining and updating needed software and hardware capabilities for such testing

Amendment

(43) To support the implementation of conformity assessment activities under European cybersecurity certification schemes and other relevant Union legislation, ENISA may provide relevant technical testing tools ***and testing laboratories*** to support Member States, businesses and conformity assessment bodies in evaluation activities ***and in demonstrating compliance and conformity with relevant Union legislation through the use of AI tools***. Such tools should aim to create synergies at Union level and an efficient operation of conformity assessment procedures to meet the needs of Member States and market needs. Such needs may arise for instance in the area of ***emerging technologies and to apply*** security by design to support businesses, including small and medium-sized enterprises, in their implementation efforts in the context of Regulation 2024/2847.

tools.

The testing laboratories should serve as a pre-testing environment fostering harmonised, Union-wide testing, setting a common framework and common principles that national laboratories can follow, thereby avoiding market fragmentation and discouraging “testing laboratory shopping”. They may also enable testing of the deployment of advanced AI cyber capabilities in critical infrastructure systems without exposing real infrastructure to risk, building on and expanding existing cyber ranges rather than duplicating them. For those purposes, ENISA may make use of the EU Cybersecurity Reserve to provide services, and should be given access to the computing infrastructure provided by the European high-performance computing infrastructure (EuroHPC). ENISA should also support the Commission and Member States in gaining early access to frontier AI models, and when timely access to frontier AI is needed for general use, explore the potential use of funding instruments available, including joint procurement, for jointly obtaining access to such models or systems. In this context, ENISA should levy fees to cover relevant costs related to establishing, designing, developing, maintaining and updating needed software and hardware capabilities for such testing tools.

Or. en

Amendment 199

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Recital 43 a (new)

Text proposed by the Commission

Amendment

(43a) Testing how artificial intelligence with advanced cyber capabilities performs in realistic conditions, before it is used in

sensitive environments, can strengthen the cyber resilience of critical infrastructure operators and public authorities. ENISA should therefore, together with the Joint Research Centre, provide a secure environment for such testing. Participants should bear their own costs. The testing should concern the suitability of artificial intelligence for specific cybersecurity tasks and should not be aimed at evaluating general-purpose AI models for compliance with Regulation (EU) 2024/1689.

Or. en

Amendment 200
Markus Buchheit

Proposal for a regulation
Recital 44

Text proposed by the Commission

(44) To support Member States in their efforts to address the shortage of cybersecurity professionals and the growing need for a skilled, ***diverse, including with regards to gender balance,*** and agile workforce, and to enable labour mobility and preparedness across Member States, ENISA should build on the principles and work initiated under the Cybersecurity Skills Academy. In particular, ENISA should establish the European Cybersecurity Skills Framework ('ECSF') as a common framework on cybersecurity professional role profiles. ***ENISA should further support Member States in addressing gender disparities in cybersecurity roles.*** This approach is consistent with the vision outlined in the Commission Communication on the Union of Skills and would contribute to its objectives. A quality label for European individual cybersecurity skills attestations should further be explored.

Amendment

(44) To support Member States in their efforts to address the shortage of cybersecurity professionals and the growing need for a skilled and agile workforce, and to enable labour mobility and preparedness across Member States, ENISA should build on the principles and work initiated under the Cybersecurity Skills Academy. In particular, ENISA should establish the European Cybersecurity Skills Framework ('ECSF') as a common framework on cybersecurity professional role profiles. ***Only ability, efficiency and professional competence should be used as a basis for securing and promoting talent.*** This approach is consistent with the vision outlined in the Commission Communication on the Union of Skills and would contribute to its objectives. A quality label for European individual cybersecurity skills attestations should further be explored.

Amendment 201
Marc Botenga
on behalf of The Left Group

Proposal for a regulation
Recital 46 a (new)

Text proposed by the Commission

Amendment

(46a) European individual cybersecurity skills attestations are a voluntary instrument meant to make skills comparable and portable. They should not be used as a way to discriminate when hiring new staff and the employer should provide the opportunity to get attestation after hiring. They should not become a financial burden for workers. Where an attestation is required by an employer, by national law or by collective agreement, the cost should not be borne by the individual. Member States and social partners are encouraged to ensure, in accordance with national law and practice, that the costs of such attestations, including time for preparation and assessment, are borne by employers and counted as working time.

Or. en

Amendment 202
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 52

Text proposed by the Commission

Amendment

(52) The role of the authorised attestation providers is to attest the knowledge and competences of an individual to be able to perform one of the ECSF roles and to give assurance to the

(52) In order to support comparability and transparency of cybersecurity skills across the Union, ENISA should develop and maintain a mapping of internationally recognised professional

employers across the Union. As also employers operating Unions critical infrastructure would look at the assurance of the quality of skills and competences of individuals acquiring European individual cybersecurity skills attestation, the authorised providers attesting the level of skills and competences should be trustworthy from the cybersecurity point of view and should not be subject of the undue influence by a third country that may pose cybersecurity concerns. Therefore, entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation or controlled by such third country, by an entity established in such third country, or by a national of such third country (high-risk suppliers) in accordance with this Regulation should not be eligible to become authorised attestation providers of any European individual cybersecurity skills attestations pursuant to Title II, Section 4.

qualifications and training programmes against the ECSF role profiles, and identify gaps where additional development is needed. This approach should facilitate labour-market mobility and informed recruitment decisions without establishing a new Union credential or creating an authorisation regime for individual attestation providers.

Or. en

Justification

To ensure coherence with Article 20(1), (2) and (2a) as amended (AM26–AM28), the recital should move from an attestation-provider model to a mapping-and-gap-analysis model based on existing qualifications and training. The amendment clarifies that no new Union credential should be created.

Amendment 203

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 56

Text proposed by the Commission

(56) In order for the Management Board to perform its functions effectively, particularly in guiding the overall direction of ENISA's activities and setting its strategic priorities, it is essential for the

Amendment

(56) In order for the Management Board to perform its functions effectively, particularly in guiding the overall direction of ENISA's activities and setting its strategic priorities, it is essential for the

Board to consist of high-level representatives from Member States and the Commission. To that end, each Member State should appoint the head of a national competent authority of that Member State responsible for cybersecurity designated pursuant to Article 8(1) of Directive (EU) 2022/2555 ***as a member of the Management Board.***

Board to consist of high-level representatives from Member States and the Commission. To that end, each Member State should appoint ***as a member of the Management Board a representative with appropriate professional expertise and experience as well as strategic decision-making power, where possible*** the head of a national cybersecurity authority or the head of a competent authority of that Member State responsible for cybersecurity designated pursuant to Article 8(1) of Directive (EU) 2022/2555.

Or. en

Amendment 204
Markus Buchheit

Proposal for a regulation
Recital 57

Text proposed by the Commission

(57) To ensure that alternates in the Management Board can fulfil their roles adequately, Member States should appoint alternates that have appropriate professional expertise and experience. The Commission and the Member States, ***as regards alternates, should make efforts to achieve a balanced representation between men and women on the Management Board*** and should limit their turnover in order to ensure continuity of the Management Board's work.

Amendment

(57) To ensure that alternates in the Management Board can fulfil their roles adequately, Member States should appoint alternates that have appropriate professional expertise and experience. The Commission and the Member States should limit their turnover in order to ensure continuity of the Management Board's work.

Or. de

Amendment 205
Markus Buchheit

Proposal for a regulation
Recital 62

(62) The smooth functioning of ENISA requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant to cybersecurity. The duties of the Executive Director should be carried out with complete independence. The Management Board should appoint the Executive Director from the list of candidates prepared by the Commission, following an open and transparent procedure *that respects the principle of gender* balance.

(62) The smooth functioning of ENISA requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant to cybersecurity. The duties of the Executive Director should be carried out with complete independence. The Management Board should appoint the Executive Director from the list of candidates prepared by the Commission, following an open and transparent procedure *solely on the basis of ability, efficiency and integrity. [...] The Executive Director should ensure that members of ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure an appropriate balance, according to the specific issues in question, between the public administrations of the Member States, Union bodies and the private sector, including industry and in particular SMEs, users and academic experts in network and information security, as well as academic experts in products with digital elements.*

Or. de

Amendment 206

Markéta Gregorová

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 63 a (new)

(63a) As an agency with an operational mandate, ENISA must be able to place its staff where its tasks require, including liaison presence with the Union institutions, support to Member State authorities and CSIRTs, and on site incident related activities, while the seat of

the Agency remains unaffected. Other Union agencies whose staff may be located at the seat, in local offices or at operational locations demonstrate the workability of this approach.

Or. en

Amendment 207

Markéta Gregorová

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 64

Text proposed by the Commission

(64) *The Management Board may decide to create a function of a Deputy Executive Director to assist the Executive Director, where the Management Board considers that such a function is necessary to ensure or maintain the smooth functioning of ENISA. When deciding on whether to create that function, the Management Board may take into account the opinion of the Executive Director.*

Amendment

(64) *ENISA may have a Deputy Executive Director who assists the Executive Director and who is responsible, under the authority of the Executive Director, for the operational tasks of ENISA, such as the operation of the platforms and tools, the vulnerability management services, the early alert service, the ransomware helpdesk, the European AI Security Evaluation Capability and the EU Cybersecurity Testbed. The Deputy Executive Director should be appointed by the Management Board under the same procedure as the Executive Director, including a statement before the competent committee of the European Parliament, and should carry out their tasks from the location at which the operational tasks are performed.*

Or. en

Amendment 208

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 65

(65) ENISA should have an Advisory Group to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The ENISA Advisory Group, established by the Management Board on a proposal from the Executive Director, should focus on issues relevant to stakeholders and should bring them to the attention of ENISA. The ENISA Advisory Group should be consulted in particular with regard to ENISA's draft annual work programme. The composition of the ENISA Advisory Group and the tasks assigned to it should ensure sufficient representation of stakeholders in the work of ENISA. Representatives of national and Union law enforcement, data protection and market surveillance authorities should be eligible to be represented in the ENISA Advisory Group.

(65) ENISA should have an Advisory Group to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The ENISA Advisory Group, established by the Management Board on a proposal from the Executive Director, should focus on issues relevant to stakeholders and should bring them to the attention of ENISA. The ENISA Advisory Group should be consulted in particular with regard to ENISA's draft annual work programme. The composition of the ENISA Advisory Group and the tasks assigned to it should ensure sufficient representation of stakeholders in the work of ENISA. Representatives of national and Union law enforcement, data protection and market surveillance authorities should be eligible to be represented in the ENISA Advisory Group, ***as should experts in countering foreign information manipulation and interference (FIMI)***.

Or. en

Amendment 209

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation Recital 74

(74) Europol has an important role in preventing and combating cybercrime, including cybercrime related to network and information security incidents. To create synergies between the respective tasks of each Agency, ENISA should cooperate with Europol, in particular by sharing information regarding trends in techniques, demands and impacts of ransomware attacks. Such cooperation may also consist in identifying the most

(74) Europol has an important role in preventing and combating cybercrime, including cybercrime related to network and information security incidents. To create synergies between the respective tasks of each Agency, ***as cyber incidents of suspected criminal origin often require both a cybersecurity and a law enforcement response***, ENISA should cooperate with Europol, in particular by sharing information regarding trends in

common ransomware strains targeting entities listed in Annexes I and II to Directive (EU) 2022/2555 to support essential and important entities in incident response and recovery.

techniques, demands and impacts of ransomware attacks. Such cooperation may also consist in identifying the most common ransomware strains targeting entities listed in Annexes I and II to Directive (EU) 2022/2555 to support essential and important entities in incident response and recovery.

Or. en

Amendment 210

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 74 a (new)

Text proposed by the Commission

Amendment

(74a) That cooperation should be close and should involve Europol's European Cybercrime Centre, including through the helpdesk referred to in Article 13(3). It should also support Europol in preventing and responding to cyberattacks of suspected criminal origin and large-scale malicious online activities, including ransomware incidents, within ENISA's mandate and without prejudice to the competences of national law enforcement authorities.

Or. en

Amendment 211

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 76

Text proposed by the Commission

Amendment

(76) To effectively meet the goals outlined in this Regulation, ENISA may

(76) To effectively meet the goals outlined in this Regulation, ENISA may

collaborate in particular with academic institutions that have research initiatives in relevant fields, and develop appropriate channels for input from consumer organisations and other organisations.

collaborate in particular with academic institutions that have research initiatives in relevant fields, ***including countering FIMI***, and develop appropriate channels for input from consumer organisations and other organisations.

Or. en

Amendment 212

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation Recital 77 a (new)

Text proposed by the Commission

Amendment

(77a) European cybersecurity certification should, as a rule, remain voluntary, unless otherwise specified in Union or national law, so that businesses can decide for themselves whether the benefits of certification justify its costs. The evaluation of Regulation (EU) 2019/881 indicated that the voluntary nature of the schemes did not have a notable influence on the efficiency of the ECCF, the shortcomings of which related mainly to procedural, technical and political challenges. Certification should also serve as a simplification tool, notably by enabling businesses, in particular SMEs, to demonstrate compliance with several legal requirements through a single certificate.

Or. en

Amendment 213

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation Recital 83 a (new)

(83a) *The Stakeholder Cybersecurity Certification Group (SCCG) should provide a structured and continuous channel through which industry and other stakeholders can contribute to the ECCF. The SCCG should advise the Commission and ENISA on strategic issues related to European cybersecurity certification, including strategic priorities and requests for new schemes, while ad hoc working groups should continue to provide technical expertise for the preparation of individual schemes. The composition and working methods of the SCCG should ensure a balanced representation of stakeholders, including SMEs, and a genuine opportunity for its members to influence the strategic direction of the ECCF.*

Or. en

Amendment 214
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 87 a (new)

(87a) *European cybersecurity certification schemes should, where relevant to their scope, support secure interoperability between ICT products, ICT services, ICT processes, managed security services and network and information systems, including in heterogeneous and multi-vendor environments. Such interoperability may be facilitated through secure and documented interfaces and, where appropriate, European or international standards or openly specified interfaces enabling machine-readable exchange. Interoperability requirements should preserve the availability, authenticity,*

integrity and confidentiality of data and services and should not require the disclosure of intellectual property, trade secrets or security-sensitive information beyond what is necessary to achieve the relevant security objective.

Or. en

Justification

Secure interoperability can reduce technical barriers between certified products, services and systems and support an open and competitive cybersecurity market. Certification schemes should therefore take interoperability into account where relevant, while ensuring that interoperability requirements do not undermine cybersecurity or require unnecessary disclosure of intellectual property, trade secrets or security-sensitive information.

Amendment 215

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Recital 91

Text proposed by the Commission

(91) European cybersecurity certification schemes should rely on standards or technical specifications, notably for the definition of security requirements and evaluation methodologies. ENISA should be given the possibility to draft technical specifications to support the preparation and maintenance of schemes, *in particular* where deliverables from standardisation organisations are missing or not suitable to fulfil the objectives of the scheme. As part of the drafting process, ENISA should be supported by the ECCG and, where applicable, the ad hoc working group set up for the relevant scheme. ENISA should also seek contributions from stakeholder groups. Additionally, ENISA should consider market acceptance, as well as European and international standards. Taking into account the quality of the technical specifications and the objectives

Amendment

(91) European cybersecurity certification schemes should ***primarily*** rely on ***established*** standards or technical specifications, notably for the definition of security requirements and evaluation methodologies. ENISA should be given the possibility to draft technical specifications to support the preparation and maintenance of schemes, where deliverables from standardisation organisations are missing or not suitable to fulfil the objectives of the scheme, ***and the conditions set out in this Regulation are met***. As part of the drafting process, ENISA should be supported by the ECCG and, where applicable, the ad hoc working group set up for the relevant scheme. ENISA should also seek contributions from stakeholder groups. Additionally, ENISA should consider market acceptance, as well as European and international standards. Taking into account the quality of the technical

of the scheme, it should be possible for the Commission to reference technical specifications drafted by ENISA in a European cybersecurity certification scheme.

specifications and the objectives of the scheme, it should be possible for the Commission to reference technical specifications drafted by ENISA in a European cybersecurity certification scheme.

Or. en

Amendment 216

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation Recital 112

Text proposed by the Commission

(112) The strict separation of the supervisory and certification activities is important to avoid distortions and interferences that may be caused in situations where the entity supervising the market is also competing in the same market. Consequently, activities where the national cybersecurity certification authorities merely carry out their supervisory role, such as by providing prior approval to the issuance of a certificate, should not require further internal separation from other supervisory activities. This includes, for example, a situation where the national cybersecurity certification authority actively gathers information throughout the certification process carried out by private conformity assessment bodies and then gives its opinion on the issuance of the certificate by those bodies ('prior approval model').

Amendment

(112) The strict separation of the supervisory and certification activities is important to avoid distortions and interferences that may be caused in situations where the entity supervising the market is also competing in the same market. Consequently, activities where the national cybersecurity certification authorities merely carry out their supervisory role, such as by providing prior approval to the issuance of a certificate, should not require further internal separation from other supervisory activities. This includes, for example, a situation where the national cybersecurity certification authority actively gathers information throughout the certification process carried out by private conformity assessment bodies and then gives its opinion on the issuance of the certificate by those bodies ('prior approval model'). ***The national cybersecurity certification authority should not repeat the certification activities already carried out by the conformity assessment body under either the prior approval model or the general delegation model.***

Or. en

Amendment 217

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Recital 112 a (new)

Text proposed by the Commission

Amendment

(112a) Private conformity assessment bodies play an important role in the certification market in several Member States. European cybersecurity certification schemes should therefore not reserve the issuance of European cybersecurity certificates to public bodies.

Or. en

Amendment 218

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Recital 114

Text proposed by the Commission

Amendment

(114) Harmonisation plays a crucial role in ensuring robust cybersecurity and enhancing market access for businesses. In contrast, fragmentation and the lack of mutual recognition of certificates pose significant barriers to the seamless flow of data, thereby increasing **operational** costs for Union industry. To mitigate those challenges, it is essential to avoid fragmentation both in the scope of the security controls and in the conformity assessment methods throughout the Union.

(114) Harmonisation plays a crucial role in ensuring robust cybersecurity and enhancing market access for businesses. In contrast, fragmentation and, the lack of mutual recognition of certificates ***and duplicative certification and compliance requirements*** pose significant barriers to the seamless flow of data, thereby increasing ***certification, operational documentation, audit, surveillance, re-certification and other compliance*** costs for Union industry. To mitigate those challenges, it is essential to avoid fragmentation both in the scope of the security controls and in the conformity assessment methods throughout the Union. ***European cybersecurity certification schemes should, to the greatest extent appropriate, build on relevant European***

and international standards and take into account comparable national, European, third-country and international certification schemes and other widely used and market-proven certifications, while preserving the level of assurance required under Union law. Where requirements, evaluation methods or evidence are equivalent, evidence already generated should be taken into account in order to avoid unnecessary duplication.

Or. en

Justification

European cybersecurity certification should reduce rather than duplicate existing compliance burdens. Certification schemes should therefore build on relevant European and international standards and allow equivalent evidence generated under comparable schemes to be reused where appropriate. This can reduce unnecessary certification, audit and re-certification costs while preserving the level of cybersecurity assurance required under Union law.

Amendment 219

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 114

Text proposed by the Commission

(114) Harmonisation plays a crucial role in ensuring robust cybersecurity *and* enhancing market access for businesses. In contrast, fragmentation and the lack of mutual recognition of certificates pose significant barriers to the seamless flow of data, thereby increasing operational costs for Union industry. To mitigate those challenges, it is essential to avoid fragmentation both in the scope of the security controls and in the conformity assessment methods throughout the Union.

Amendment

(114) Harmonisation plays a crucial role in ensuring robust cybersecurity, enhancing market access for businesses *and helping innovative SMEs and start-ups to grow across the internal market*. In contrast, fragmentation and the lack of mutual recognition of certificates pose significant barriers to the seamless flow of data, thereby increasing operational costs for Union industry *and weakening its competitiveness*. To mitigate those challenges, it is essential to avoid fragmentation both in the scope of the security controls and in the conformity assessment methods throughout the Union.

Or. en

Amendment 220

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 129

Text proposed by the Commission

(129) Beyond technical risks which are addressed by Directive (EU) 2022/55 of the European Parliament and of the Council⁴¹, Regulation (EU) 2024/2847 of the European Parliament and of the Council⁴² and the European cybersecurity certification Framework established by Regulation (EU) 2019/881, ICT supply chains are increasingly exposed to risks of a non-technical nature. Such non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids.

Amendment

(129) Beyond technical risks which are addressed by Directive (EU) 2022/55 of the European Parliament and of the Council⁴¹, Regulation (EU) 2024/2847 of the European Parliament and of the Council⁴² and the European cybersecurity certification Framework established by Regulation (EU) 2019/881, ICT supply chains are increasingly exposed to risks of a non-technical nature. Such non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids. ***Non-technical risk-factors are also taken into consideration in Regulation (EU) 2024/2847 that evaluates the cybersecurity requirements for hardware and software products on the internal market. That evaluation should also take into consideration the non-technical risk-factors of high-risk suppliers identified in this Regulation. This ensures a consistent and risk-based approach across the Union.***

⁴¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333 du 27.12.2022, p. 80-152, ELI: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>).

⁴² Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>).

⁴¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333 du 27.12.2022, p. 80-152, ELI: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>).

⁴² Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>).

Or. en

Amendment 221

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 129

Text proposed by the Commission

(129) Beyond technical risks which are addressed by Directive (EU) **2022/55** of the European Parliament and of the Council⁴¹, Regulation (EU) 2024/2847 of the European Parliament and of the Council⁴² and the European cybersecurity certification Framework established by Regulation (EU) 2019/881, ICT supply chains are increasingly exposed to risks of a non-technical nature. Such non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled

Amendment

(129) Beyond technical risks which are addressed by Directive (EU) **2022/2555** of the European Parliament and of the Council⁴¹, Regulation (EU) 2024/2847 of the European Parliament and of the Council⁴² and the European cybersecurity certification Framework established by Regulation (EU) 2019/881, ICT supply chains are increasingly exposed to risks of a non-technical nature. Such non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled

from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids.

⁴¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333 du 27.12.2022, p. 80-152, ELI: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>).

⁴² Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>).

from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids.

⁴¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333 du 27.12.2022, p. 80-152, ELI: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>).

⁴² Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>).

Or. en

Amendment 222
Jens Geier

Proposal for a regulation
Recital 130 a (new)

Text proposed by the Commission

Amendment

(130a) Open-source software is widely integrated into commercial digital products and critical infrastructure across the Union, and its security and resilience rely on transparent verification, community-driven vulnerability discovery and global developer contributions. The trusted ICT supply chain framework should therefore take account of the specific characteristics of open-source development. An open-source project, repository or non-profit open-source steward should not be subject to restrictive measures under this Title solely because individual contributors are established in or are nationals of a third country designated pursuant to Article 100. Restrictions on Union funding should not prevent support for open-source projects or non-profit open-source stewards where an entity subject to the relevant restriction is not itself the direct beneficiary of that funding.

Or. en

Amendment 223
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 132 a (new)

Text proposed by the Commission

Amendment

(132a) Any obligation, prohibition or mitigating measure imposed on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 under any trusted ICT supply chain framework (as referenced in Recital 132) should concern only those entities' direct source high-risk suppliers and the ICT components (or components that include ICT components) supplied to them by such direct source high-risk suppliers. Those entities should not be required to identify, assess, monitor or act upon suppliers, or ICT components originating from other

suppliers (whether high-risk suppliers or not), situated further upstream in the ICT supply chain and nothing in this proposal should be read to the contrary.

Or. en

Justification

The Act is necessary to better prepare stakeholders to prevent, detect and respond to ICT supply chain security risks. The primary defence that stakeholders have against ICT supply chain security risks is control. A direct contractual relationship with a high-risk supplier is a material source of control. However, requiring covered entities to trace, verify and police the origin of every upstream ICT component would impose a disproportionate and, in many cases, unworkable burden, without a commensurate gain in cybersecurity. As such, consistent with the principle of proportionality, the relevant restrictions and obligations should apply only in relation to high-risk suppliers with whom a covered entity has a direct contractual relationship. Non-technical risks arising further upstream in the ICT supply chain are more appropriately addressed through Union-level mechanisms within the Act (such as coordinated security risk assessments and the identification of high-risk suppliers) rather than by individual entities.

Amendment 224

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 133

Text proposed by the Commission

(133) Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being

Amendment

(133) Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being

detected, with possibly catastrophic consequences.

detected, with possibly catastrophic consequences. ***A Coordinated Risk Assessment has already been finalized for detection equipment, identifying clear and unacceptable supply chain risks that warrant mitigating measures.***

Or. en

Amendment 225

Jens Geier

Proposal for a regulation

Recital 133

Text proposed by the Commission

(133) Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being detected, with possibly catastrophic consequences.

Amendment

(133) Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems, ***including electricity grid technologies and technologies to digitalise the grid***, and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being detected, with possibly catastrophic consequences.

Or. en

Amendment 226

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 133 a (new)

Text proposed by the Commission

Amendment

(133a) Inverters and other network-connected components in solar photovoltaic installations are capable of remote access, data transmission or system control. Hidden communication devices have been discovered in inverters, and the Union market for inverters is dominated by a few suppliers from third countries. Solar photovoltaic generation should therefore be a priority under the trusted ICT supply chain framework, and the Commission should identify the key ICT assets and adopt the necessary mitigation measures in that area within set deadlines.

Or. en

Amendment 227

Jens Geier

Proposal for a regulation

Recital 135 a (new)

Text proposed by the Commission

Amendment

(135a) Given the growing exposure of critical infrastructure to systemic cybersecurity threats and non-technical supply-chain dependencies, Union-level coordinated security risk assessments should be prioritised for sectors where service compromise could lead to cascading cross-border disruptions. : In the electricity subsector, assessments should examine critical control architectures, including inverter-based generation and storage systems, wind turbine and wind power plant controllers, supervisory control and data acquisition (SCADA), transmission and distribution network management systems, substation automation, protection and teleprotection systems, and control systems for HVDC

links and FACTS, firmware-signing and update mechanisms, remote-access interfaces and integrated wireless communications. In the rail transport subsector, assessments should scrutinise safety-critical operational systems, including railway signalling, interlocking, operational communications and the European Rail Traffic Management System (ERTMS). This prioritisation should be without prejudice to assessments in other critical sectors.

Or. en

Amendment 228
Jens Geier

Proposal for a regulation
Recital 135 b (new)

Text proposed by the Commission

Amendment

(135b) The Union-level coordinated security risk assessment for the electricity subsector should also consider the systemic risk that may arise where large numbers of distributed electricity generation or storage assets can be remotely controlled through the same supplier, cloud platform, communications service or update infrastructure. The assessment should examine whether such aggregated supplier-level control creates a systemic dependency, without imposing direct obligations on households or other small private owners.

Or. en

Amendment 229
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 137

(137) Where, as a result of a security risk assessment conducted by the NIS Cooperation Group or the Commission, it appears that a ***specific third country*** poses serious and structural non-technical cybersecurity risks to ICT supply chains, the Commission should verify the ***threat*** posed by that ***country***. ***The Commission may initiate such verification also on the basis of other sources such as a public statement on behalf of the Union or a Member States in response to, instances of irresponsible state behaviour in cyberspace that has led to a cybersecurity incident. In order to assess the level of threat, the Commission should take into account elements such as the existence of laws or practices in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited. Another relevant element is the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct security concerns, including about existing practices, the substantiated information about incidents of threat actors operating out of the territory of that country carrying out malicious cyber activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors. The Commission should also take into account*** information stemming from Union-level coordinated security risk assessments or reports issued by Member States or international organisations ***such as NATO***.

(137) Where, as a result of a security risk assessment conducted by the NIS Cooperation Group or the Commission, ***or on the basis of other specific and substantiated evidence***, it appears that a ***supplier*** poses serious and structural non-technical cybersecurity risks to ICT supply chains, the Commission should verify the ***risk*** posed by that ***supplier***. ***The assessment*** should take into account ***all*** relevant ***circumstances***, including ***specific legal obligations demonstrably applicable to the supplier that give rise to the identified cybersecurity risk, its security practices, documented conduct relevant to the risk identified and relevant*** information stemming from Union-level coordinated security risk assessments or reports issued by Member States or international organisations, ***where such information provides specific and substantiated evidence concerning that supplier. The supplier's country of establishment, the nationality or geographical origin of its owners or controllers, and the general political, institutional or judicial characteristics of a country should not, by themselves, constitute grounds for identifying that supplier as high-risk. Such factors may be taken into account in the assessment only where supported by specific and substantiated evidence relating to the supplier concerned.***

Or. en

Justification

Recital 137 should reflect the individual, evidence-based assessment of high-risk suppliers under Articles 100 and 104. General country-related characteristics, including political and judicial institutions, should not constitute grounds for designation. Information from coordinated security risk assessments and other reports should therefore be relevant only where it provides specific and substantiated evidence concerning the supplier.

Amendment 230

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 137

Text proposed by the Commission

(137) Where, as a result of a security risk assessment conducted by the NIS Cooperation Group or the Commission, it appears that a specific third country poses serious and structural non-technical cybersecurity risks to ICT supply chains, the Commission should verify the threat posed by that country. The Commission may initiate such verification also on the basis of other sources such as a public statement on behalf of the Union or a Member States in response to, instances of irresponsible state behaviour in cyberspace that has led to a cybersecurity incident. In order to assess the level of threat, the Commission should take into account elements such as the existence of laws or practices in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited. Another relevant element is the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct security concerns, including about existing practices, the substantiated information about incidents of threat actors operating out of the territory of that country carrying out malicious cyber

Amendment

(137) Where, as a result of a security risk assessment conducted by the NIS Cooperation Group or the Commission, it appears that a specific third country poses serious and structural non-technical cybersecurity risks to ICT supply chains, the Commission should verify the threat posed by that country. The Commission may initiate such verification also on the basis of other sources such as a public statement on behalf of the Union or a Member States in response to, instances of irresponsible state behaviour in cyberspace that has led to a cybersecurity incident. In order to assess the level of threat, the Commission should take into account elements such as the existence of laws or practices in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited, ***or to share information for intelligence purposes without due process or oversight mechanisms***. Another relevant element is the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct security concerns, including about existing practices, the substantiated information

activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors. The Commission should also take into account information stemming from Union-level coordinated security risk assessments or reports issued by Member States or international organisations such as NATO.

about incidents of threat actors operating out of the territory of that country carrying out malicious cyber activities or campaigns , *or intellectual property theft*, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors. The Commission should also take into account information stemming from Union-level coordinated security risk assessments or reports issued by Member States or international organisations such as NATO.

Or. en

Amendment 231

Marc Botenga

on behalf of The Left Group

Proposal for a regulation

Recital 137 a (new)

Text proposed by the Commission

Amendment

(137a) Designating a third country as a cybersecurity concern for ICT supply chains is a cybersecurity measure and should rest solely on objective, verifiable and publicly reasoned technical and legal evidence and should apply equally to all third countries. Measures taken under this Regulation should respect international law, including the Union's obligations under international trade agreements.

Or. en

Amendment 232

Marc Botenga

on behalf of The Left Group

Proposal for a regulation

Recital 137 b (new)

(137b) Where the laws or practices of a third country grant its authorities access to data held by entities under its jurisdiction, including data located in the Union, without effective safeguards recognised under Union law, the resulting data transfer risks shall be assessed, taking into account the nature and scope of such access, the likelihood of access occurring and the purposes for which the data may be accessed.

Or. en

Amendment 233

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Recital 138

Text proposed by the Commission

Amendment

(138) For the purpose of this Regulation, the notion of control should be understood as the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities ***The control of entities from a third country posing cybersecurity concerns should also be established in situations where such entity is having executive management structures in that country.***

(138) For the purpose of this Regulation, the notion of control should be understood as the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities.

Or. en

Justification

The general definition of control remains relevant, but control should not create a separate automatic route to high-risk supplier status based solely on a link to a particular third country.

Amendment 234

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsik, Barry Andrews

Proposal for a regulation
Recital 139

Text proposed by the Commission

(139) The Union should not fund projects involving high-risk suppliers, which would jeopardise the Union's security and undermine the Union's interests and credibility. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in any Union funding programmes and instruments implemented in direct and indirect management in accordance with the Article 136 of the Regulation (EU/Eurotom) 2024/2509 and Union sector specific rules as well as in any Union funding activities implemented in shared management, including under the next Multiannual Financial Framework ***in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets.*** Union implementing partners, such as European Investment Bank Group and national promotional banks and institutions should refrain from supporting projects that contradict the above, including in operations at own risk.

Amendment

(139) The Union should not fund projects involving high-risk suppliers, which would jeopardise the Union's security and undermine the Union's interests and credibility. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in any Union funding programmes and instruments implemented in direct and indirect management in accordance with the Article 136 of the Regulation (EU/Eurotom) 2024/2509 and Union sector specific rules as well as in any Union funding activities implemented in shared management, including under the next Multiannual Financial Framework. Union implementing partners, such as European Investment Bank Group and national promotional banks and institutions should refrain from supporting projects that contradict the above, including in operations at own risk.

Or. en

Amendment 235

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsik, Barry Andrews

Proposal for a regulation
Recital 140

Text proposed by the Commission

(140) Public procurement can be a strong tool for public authorities to contribute to a more innovative, sustainable and

Amendment

(140) Public procurement can be a strong tool for public authorities to contribute to a more innovative, sustainable and

competitive economy and for spending public money in a strategic manner. Public procurement related to ICT supply chains should not be used to benefit suppliers that threaten the security of the Union's critical infrastructure. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in public procurement *concerning the provision of ICT components or components that include ICT components to be used in identified key ICT assets*.

competitive economy and for spending public money in a strategic manner. Public procurement related to ICT supply chains should not be used to benefit suppliers that threaten the security of the Union's critical infrastructure. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in public procurement.

Or. en

Amendment 236
Jens Geier

Proposal for a regulation
Recital 142

Text proposed by the Commission

(142) Cybersecurity standards play a critical role in the security and trustworthiness of digital infrastructures. It is necessary to take appropriate measures to ensure standardisation in the field of cybersecurity. *The involvement of entities established in or controlled from countries which have been identified as posing cybersecurity concerns to the ICT supply chain in line with this Regulation may lead to influencing cybersecurity standards in a way that undermines their security and trustworthiness.*

Amendment

(142) Cybersecurity standards play a critical role in the security and trustworthiness of digital infrastructures. It is necessary to take appropriate measures to ensure standardisation in the field of cybersecurity.

Or. en

Amendment 237
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 142

(142) Cybersecurity standards play a critical role in the security and trustworthiness of digital infrastructures. It is necessary to take appropriate measures to ensure standardisation in the field of cybersecurity. The involvement of ***entities established in or controlled from countries which have been identified as posing cybersecurity concerns to the ICT supply chain in line with this Regulation*** may lead to influencing cybersecurity standards in a way that undermines their security and trustworthiness.

(142) Cybersecurity standards play a critical role in the security and trustworthiness of digital infrastructures. It is necessary to take appropriate measures to ensure standardisation in the field of cybersecurity. The involvement of ***high-risk suppliers identified in accordance with Articles 100 and 104*** may lead to influencing cybersecurity standards in a way that undermines their security and trustworthiness.

Or. en

Justification

The recital should refer to high-risk suppliers identified through the individual assessment procedure rather than to entities based on their establishment or control from a designated country.

Amendment 238

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Recital 144

(144) Where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, the mitigating measures may be applied to entities in relation to their ICT supply chain and in particular to key ICT assets identified. The proposed mitigating measures should be based on the assessment of potential risks and dependencies, including the potential economic and societal impact of such measures on the entities concerned operating in highly critical or other critical sectors and in particular SMEs. The economic impact should look at the costs of the implementation of the mitigation

(144) Where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, the mitigating measures may be applied to entities in relation to their ICT supply chain and in particular to key ICT assets identified. The proposed mitigating measures should be ***proportionate and*** based on the assessment of potential risks and dependencies, including the potential economic and societal impact of such measures on the entities concerned operating in highly critical or other critical sectors and in particular SMEs. The economic impact should look at the costs of the

measures, including the duration of the lifecycle of the relevant components in the key ICT assets in case where the measures include the replacement of suppliers. The availability of alternative suppliers on the market should also be assessed in order to ensure continued provision of the services.

implementation of the mitigation measures, including the duration of the lifecycle of the relevant components in the key ICT assets in case where the measures include the replacement of suppliers. The availability of alternative suppliers on the market should also be assessed in order to ensure continued provision of the services.

Or. en

Amendment 239
Eszter Lakos

Proposal for a regulation
Recital 144 a (new)

Text proposed by the Commission

Amendment

(144a) The replacement of ICT components already installed in key ICT assets is the most intrusive of the measures provided for in this Title. Where the technical mitigating measures referred to in Article 103(2), points (b) and (c), including the disabling of remote access, the segmentation of network systems and third-party audit, are capable of addressing the non-technical risk identified, those measures should be preferred to replacement, in accordance with the principle that the least intrusive effective measure is to be chosen. Entities that have implemented such measures effectively, as verified by an independent third-party audit, should not be required to replace the components concerned, nor should they be disconnected from, or denied access to, the networks and systems they serve on account of the presence of those components.

Or. en

Justification

Establishes the least-intrusive-measure principle for installed equipment. The Commission proposal already lists the relevant technical measures in Article 103(2); this recital clarifies

their relationship to replacement, consistent with recitals 144 and 145 on economic impact and proportionality.

Amendment 240

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 146

Text proposed by the Commission

(146) Use, installation or any other kind of integration of components provided by high-risk suppliers in the operation of key ICT assets may be related to risks of subsequent transfers of data to a third country. In particular, risks may be posed by an insufficient level of protection offered to the data in the third country, such as for the protection of fundamental rights, intellectual property or trade secrets, or unlawful access and exploitation of that data for possible future supply chain disruptions and espionage purposes. To mitigate such risks, restrictions in relation to transfer of specific types of data to third countries may be applied.

Amendment

(146) Use, installation or any other kind of integration of components provided by high-risk suppliers in the operation of key ICT assets may be related to risks of subsequent transfers of data to a third country. In particular, risks may be posed by an insufficient level of protection offered to the data in the third country, such as for the protection of fundamental rights, intellectual property or trade secrets, or unlawful access and exploitation of that data for possible future supply chain disruptions and espionage purposes. To mitigate such risks, restrictions in relation to transfer of specific types of data to third countries *and its entities, and to remote access to and processing of data by such entities*, may be applied *to ensure that the data is not directly, nor indirectly, accessible from a third country and its entities. However, data localization within the Union will not mitigate those risks when a high-risk supplier originates or is controlled from a third country whose laws or practices oblige the entity to share information for intelligence purposes without due process or oversight mechanisms.*

Or. en

Amendment 241

Jens Geier

Proposal for a regulation
Recital 147 a (new)

Text proposed by the Commission

Amendment

(147a) For key ICT assets in the electricity subsector that are already in operation, the sector-specific provisions of this Regulation should prioritise effective technical and operational mitigation of identified risks. They should not in themselves introduce a requirement for the physical replacement or premature phase-out of such assets, especially where mitigation measures are available. The design and implementation of mitigation measures should take due account of grid stability, security of electricity supply and the continued deployment of renewable energy. This approach, however, should not prevent a prohibition of continued use under Article 103 where a serious cybersecurity risk cannot be effectively mitigated.

Or. en

Amendment 242
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 150

Text proposed by the Commission

Amendment

(150) In order to ensure proportionality of measures applied, ***entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation, or controlled by such third country, by an entity established in such third country, or by a national of such third country can apply to be exempted from the prohibition to provide to entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555 ICT components or components that include ICT components for their use, installation***

(150) In order to ensure proportionality of measures applied, ***a high-risk supplier included in a list referred to in Article 104(1) should be able to apply for an exemption from the applicable restrictions*** in accordance with ***Article 105***. For that purpose, the ***supplier*** should demonstrate with clear evidence that effective ***mitigating*** measures ***address*** the non-technical risks ***on which its inclusion in the list is based***. ***Exemptions should remain individual, verifiable and subject to conditions and monitoring appropriate***

*or integration in key ICT assets of that entity and participate in public procurement procedures organised in accordance with legislation transposing Directives 2014/24/EU⁴⁴ and 2014/25/EU of the European Parliament and of the Council⁴⁵ procedures in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets. For that purpose, the *entity* should demonstrate with clear evidence that *it applies* effective measures *addressing* the non-technical risks *and ensuring the absence of any possible undue interference by a third country posing cybersecurity concerns.**

to the risk concerned.

⁴⁴ Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, pp. 65–242, ELI: <https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng>).

⁴⁵ Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94 du 28.3.2014, p. 243-374, ELI: <https://eur-lex.europa.eu/eli/dir/2014/25/oj?locale=fr>).

Or. en

Justification

The exemption recital should be aligned with the individual high-risk supplier model and should focus on whether effective mitigation addresses the specific risks underlying the supplier's designation.

Amendment 243

Markéta Gregorová

on behalf of the Verts/ALE Group

Proposal for a regulation

Recital 150 a (new)

Text proposed by the Commission

Amendment

(150a) In order to preserve the diversity and resilience of ICT supply chains, entities established in third countries which demonstrate, on the basis of strict and cumulative conditions, their independence from undue third country interference should be able to obtain a recognition of their status and may benefit from a trusted supplier status. That status should be awarded based on specific criteria through inclusion in a Union list of trusted suppliers established by delegated act, which is distinct from the designation of high-risk suppliers and allows the European Parliament and the Council to object to every inclusion, and be unavailable to entities included in a list of high-risk suppliers, to entities controlled by such entities and to entities in respect of which an assessment pursuant to this Regulation is pending, for which the procedure laid down in Article [105] remains the sole pathway, in order to prevent circumvention of this Title. Trusted supplier status may also be used as a presumption of compliance with supply chain security obligations

Or. en

Amendment 244

Marc Botenga

on behalf of The Left Group

Proposal for a regulation

Recital 153

Text proposed by the Commission

Amendment

(153) In particular, the cybersecurity of 5G networks is a matter of strategic importance for the Union as those networks form the backbone for a wide range of services of essential importance

(153) In particular, the cybersecurity of 5G networks is a matter of strategic importance for the Union as those networks form the backbone for a wide range of services of essential importance

for the functioning of the internal market ***and are also key in setting up our defence readiness, including in relation to military mobility. 5G networks are capable of providing reliable ultra-fast connectivity, for example for data and information sharing, detection of drones and real-time battlefield coordination.***

for the functioning of the internal market

Or. en

Amendment 245

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation Recital 155

Text proposed by the Commission

(155) In order to address important security challenges in 5G networks, Member States within the NIS Cooperation Group, together with the Commission and ENISA, carried out a Union-level coordinated security risk assessment of 5G networks, examining both technical and non-technical risks. This assessment identified several risks, including potential interference from third countries or third country actors via the supply chain, and categorised assets according to their criticality. This assessment should be taken as a basis for defining the key ICT assets for 5G communications networks.

Amendment

(155) In order to address important security challenges in 5G networks, Member States within the NIS Cooperation Group, together with the Commission and ENISA, carried out a Union-level coordinated security risk assessment of 5G networks, examining both technical and non-technical risks. This assessment identified several risks, including potential interference from third countries or third country actors via the supply chain, and categorised assets according to their criticality. This assessment should be taken as a basis for defining the key ICT assets for 5G communications networks. ***The cybersecurity of fixed electronic communications networks have also been assessed to be of paramount importance. On the one hand IP and optical networks form the foundational infrastructure of 5G networks for data routing, transport, and overall network functionality. If IP and optical networks are compromised or switched off, 5G will stop running. On the other hand, the architecture of fixed networks contains design characteristics that lead to an even higher risk of masked data theft or kill switch installation and***

activation by malicious high-risk suppliers.

Or. en

Amendment 246

Bart Groothuis, Ivars Ijabs, Anna Stürgkh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 156 a (new)

Text proposed by the Commission

Amendment

(156a) In full alignment with the objectives of the EU economic security strategy, which addresses dependencies on single suppliers or high-risk suppliers, as well as concealed vulnerabilities, the potential of software, firmware or hardware backdoors, and systemic ICT supply disruptions, particularly in cases of technological lock-in or supplier dependency, and taking into consideration the public warnings of national cybersecurity agencies about the risk posed by inverter-based resources from high-risk suppliers, as well as the recommendations of the Commission's Smart Energy Expert Group, which represents all relevant stakeholders of the Union electricity sector, the ICT supply chain framework established by this Regulation should be applied as a matter of priority to key ICT assets for inverter-based resources in solar PV, battery and wind technologies. Given the documented cases of both software and hardware backdoors in inverters supplied by vendors from high-risk countries, the standard remote access capabilities of such equipment, including firmware update channels and virtual power plant control systems, and the direct contribution of inverter-based resources to energy generation and storage, grid stability, frequency regulation and voltage control, the increasingly concentrated

supply chain poses a risk to the security and continuity of the Union's electricity supply and therefore warrants mitigating measures.

Or. en

Amendment 247

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigríð Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Recital 157

Text proposed by the Commission

(157) For the purpose of setting up a phasing out period for the key ICT assets of fixed and satellite electronic communications networks, the Commission should carry out an assessment taking due account of the degree of the security risks related to each specific ICT key assets of the fixed and satellite networks, the lifetime of relevant components and the economic impact that the removal of those components would have on the operators concerned. Based on the results of that assessment, the Commission may consider setting up different phasing out periods for the particular key ICT assets and their integral elements.

Amendment

(157) For the purpose of setting up a phasing out period for the key ICT assets of fixed and satellite electronic communications networks, **and of inverter-based resources**, the Commission should carry out an assessment taking due account of the degree of the security risks related to each specific ICT key assets of the fixed and satellite networks, **and of inverter-based resources**, the lifetime of relevant components and the economic impact that the removal of those components would have on the operators concerned. Based on the results of that assessment, the Commission may consider setting up different phasing out periods for the particular key ICT assets and their integral elements.

Or. en

Amendment 248

Eszter Lakos

Proposal for a regulation

Recital 157 a (new)

Text proposed by the Commission

Amendment

(157a) For key ICT assets other than

electronic communications networks, and in particular for assets connected to electricity transmission or distribution systems such as generation and storage installations, the time periods for phasing out ICT components provided by high-risk suppliers should be determined on the basis of the degree of security risk, the remaining technical and economic lifetime of the components concerned and the economic impact of their removal, and should take account of the capacity of alternative suppliers to deliver replacement components on the Union market within those periods. No replacement obligation should be imposed where alternative components are not available in sufficient volume, since such an obligation would compromise the continued provision of essential services, including the generation of renewable energy.

Or. en

Justification

Extends to other critical sectors the approach the Commission itself proposes for fixed and satellite networks in recital 157 (risk, component lifetime and economic impact as the basis for phase-out periods), and reinforces the availability-of-alternatives test that recital 144 already contemplates.

Amendment 249

Adina Vălean

Proposal for a regulation

Recital 157 a (new)

Text proposed by the Commission

Amendment

(157a) The prohibition on deploying, installing or integrating components from high-risk suppliers in key ICT assets of electronic communications networks concerns new deployments, while components already installed are subject to the phasing out obligation. To preserve the security and continuity of electronic

communications services during the phasing out period, providers should be able to maintain, repair and apply security updates to such components, without increasing the capacity, functionality or geographical coverage of key ICT assets relying on high-risk suppliers.

Or. en

Amendment 250

Adina Vălean

Proposal for a regulation

Recital 157 b (new)

Text proposed by the Commission

Amendment

(157b) Where providers of electronic communications networks are required to replace lawfully acquired equipment before the end of its normal investment or replacement cycle, an appropriate compensation mechanism should be available at Member State or Union level, so that the costs of phasing out do not crowd out investment in next-generation networks. Such compensation should take into account the depreciation of the equipment concerned, should not favour providers that delayed mitigation measures and should comply with Union State aid rules. In addition, as national security remains the sole responsibility of each Member State, a Member State should be able to set a longer phasing out period where the period set out in this Regulation would create significant risks to the security, resilience or continuity of its critical national infrastructure, subject to notifying the Commission and taking utmost account of its observations.

Or. en

Amendment 251

Proposal for a regulation
Recital 158

Text proposed by the Commission

(158) For the purposes of effective supervision and enforcement of obligations concerning the providers of mobile, fixed and satellite electronic communication networks, the relevant competent authorities under this Regulation should ensure close cooperation with the competent authorities under *the [DNA proposal]*. Upon request from a competent authority designated under this Regulation, national regulatory authorities or other competent authorities for radio spectrum, where appropriate, should withdraw the rights *referred to in Article 9 and Article 20 [DNA Proposal]* if the provider of public electronic communications networks is not complying with the obligations under this Regulation, including if the provider does not phase out ICT components or components that include ICT components from high-risk suppliers in the operation of key ICT assets within the period specified in accordance with this Regulation.

Amendment

(158) For the purposes of effective supervision and enforcement of obligations concerning the providers of mobile, fixed and satellite electronic communication networks, the relevant competent authorities under this Regulation should ensure close cooperation with the competent authorities under **Directive (EU) 2018/1972**. Upon request from a competent authority designated under this Regulation, national regulatory authorities or other competent authorities for radio spectrum, where appropriate, should withdraw the **relevant rights to provide electronic communications networks or to use radio spectrum, in accordance with applicable Union and national law**, if the provider of public electronic communications networks is not complying with the obligations under this Regulation, including if the provider does not phase out ICT components or components that include ICT components from high-risk suppliers in the operation of key ICT assets within the period specified in accordance with this Regulation.

Or. en

Amendment 252
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 160

Text proposed by the Commission

(160) The competent authorities should provide support to entities of the type referred to in Annexes I and II *o* Directive (EU) 2022/2555 for the compliance with their obligations under this Regulation. For

Amendment

(160) The competent authorities should provide support to entities of the type referred to in Annexes I and II **of** Directive (EU) 2022/2555 for the compliance with their obligations under this Regulation. For

that purpose, the Commission should assess *whether* suppliers *that may be* affected by specific prohibitions *are established in third country posing cybersecurity concerns or controlled by such third country or by an entity established in such third country or by a national of such third country*. Competent authorities should cooperate closely with the Commission and other competent authorities within the Network established under this Regulation. Based on the assessment by the Commission, the competent authorities should share relevant information concerning high-risk suppliers with relevant entities of the type referred to in Annexes I and II *to* Directive (EU) 2022/2555. Entities are not expected to verify whether a supplier *is under foreign control* but may rely fully on information received from competent authorities. The competent authorities should ensure that no unnecessary administrative burden is imposed on those entities.

that purpose, the Commission should assess suppliers *potentially* affected by specific prohibitions *on an individual basis, in accordance with the relevant provisions of this Regulation and on the basis of specific and substantiated evidence concerning those suppliers*. Competent authorities should cooperate closely with the Commission and other competent authorities within the Network established under this Regulation. Based on the assessment by the Commission, the competent authorities should share relevant information concerning high-risk suppliers with relevant entities of the type referred to in Annexes I and II *of* Directive (EU) 2022/2555. Entities are not expected to verify whether a supplier *should be identified as high-risk* but may rely fully on information received from competent authorities. The competent authorities should ensure that no unnecessary administrative burden is imposed on those entities.

Or. en

Justification

The recital should reflect the individual, evidence-based identification of high-risk suppliers established under Articles 100 and 104, rather than the original country-based assessment of establishment, ownership and control. The amendment also clarifies that affected entities may rely on information provided by competent authorities without conducting independent supplier risk assessments.

Amendment 253

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Recital 166

Text proposed by the Commission

(166) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of the adoption of implementing acts

Amendment

(166) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of the adoption of implementing acts

laying down detailed rules relating to fees levied by ENISA, implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, implementing acts laying down common principles and reference provisions intended to provide for elements across European cybersecurity certification schemes, implementing acts specifying procedures for prior approval or general delegation models, implementing acts on recognising a third country or international organisation cybersecurity certificates as equivalent to European cybersecurity certificates, implementing acts establishing a plan for peer review, implementing acts to establish the procedures, including on cross-border cooperation, for authorisation of the conformity assessment bodies, implementing acts to establish the circumstances, formats and procedures for notifications of conformity assessment bodies, implementing acts *designating a third country as a country posing cybersecurity concerns to ICT supply chains, implementing acts* identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to Annexes I and II to Directive (EU) 2022/2555, implementing acts establishing that entities operating in sectors of high criticality and other critical sectors are subject to specific mitigating measures and specifying the time periods for the phasing out of ICT components or components that include ICT components provided by high-risk suppliers, implementing acts further specifying conditions regarding *the exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns*, as well as the adoption of implementing acts laying down detailed rules relating to fees levied by the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council, and the

laying down detailed rules relating to fees levied by ENISA, implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, implementing acts laying down common principles and reference provisions intended to provide for elements across European cybersecurity certification schemes, implementing acts specifying procedures for prior approval or general delegation models, implementing acts on recognising a third country or international organisation cybersecurity certificates as equivalent to European cybersecurity certificates, implementing acts establishing a plan for peer review, implementing acts to establish the procedures, including on cross-border cooperation, for authorisation of the conformity assessment bodies, implementing acts to establish the circumstances, formats and procedures for notifications of conformity assessment bodies, implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to Annexes I and II to Directive (EU) 2022/2555, implementing acts establishing that entities operating in sectors of high criticality and other critical sectors are subject to specific mitigating measures and specifying the time periods for the phasing out of ICT components or components that include ICT components provided by high-risk suppliers, implementing acts further specifying conditions regarding *exemptions for high-risk suppliers*, as well as the adoption of implementing acts laying down detailed rules relating to fees levied by the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council, and the examination procedure should be used. In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should also be conferred on the Commission in respect of

examination procedure should be used. In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should also be conferred on the Commission in respect of establishing a list of high-risk suppliers relevant for certain measures provided for in this Regulation.

establishing a list of high-risk suppliers relevant for certain measures provided for in this Regulation.

Or. en

Justification

The recital on implementing powers should be aligned with the individual high-risk supplier regime by removing the obsolete power to designate third countries and by referring to exemptions for high-risk suppliers.

Amendment 254

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík

Proposal for a regulation

Recital 167

Text proposed by the Commission

(167) It is necessary that European cybersecurity certification schemes reflect the latest technological developments, new related threats, and the adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. For these reasons, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to add or modify the security objectives that European cybersecurity certification schemes pursue. Similarly, in the interests of a trusted ICT supply chain framework, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend Annex II to this Regulation in order to adapt *it* to technological developments. It is of particular importance that the Commission

Amendment

(167) It is necessary that European cybersecurity certification schemes reflect the latest technological developments, new related threats, and the adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. For these reasons, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to add or modify the security objectives that European cybersecurity certification schemes pursue. Similarly, in the interests of a trusted ICT supply chain framework, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend Annex II *and Annex IIa* to this Regulation in order to adapt *them* to technological developments. It is of particular importance that the

carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

Or. en

Amendment 255
Jens Geier

Proposal for a regulation
Recital 167

Text proposed by the Commission

(167) It is necessary that European cybersecurity certification schemes reflect the latest technological developments, new related threats, and the adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. For these reasons, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to add or modify the security objectives that European cybersecurity certification schemes pursue. Similarly, in the interests of a trusted ICT supply chain framework, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend *Annex II* to this Regulation in order to adapt it to technological developments. It is of

Amendment

(167) It is necessary that European cybersecurity certification schemes reflect the latest technological developments, new related threats, and the adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. For these reasons, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to add or modify the security objectives that European cybersecurity certification schemes pursue. Similarly, in the interests of a trusted ICT supply chain framework, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend *Annexes II and IIa* to this Regulation in order to adapt it to technological developments. It is of

particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

Or. en

Amendment 256

Auke Zijlstra, Ewa Zajączkowska-Hernik, Barbara Bonte

Proposal for a regulation

Recital 172

Text proposed by the Commission

(172) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives,

Amendment

deleted

Or. en

Amendment 257

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 172 a (new)

Text proposed by the Commission

Amendment

(172a) The identification of high-risk suppliers and the adoption of measures addressing risks in ICT supply chains require a consistent approach throughout the Union. The identification of a high-risk supplier should be based on an individual assessment carried out in accordance with Article 104 and on specific and substantiated evidence concerning that supplier. The supplier's country of establishment, the nationality or geographical origin of its owners or controllers, and the general political, institutional or judicial characteristics of a country should not, by themselves, constitute grounds for identifying that supplier as high-risk. Such factors may be taken into account in the assessment only where supported by specific and substantiated evidence relating to the supplier concerned. Member States should be appropriately consulted in the preparation of acts adopted under this Title, in accordance with the procedures laid down in this Regulation, while preserving the capacity of the Commission to act rapidly and uniformly where necessary to address serious cybersecurity risks.

Or. en

Justification

High-risk supplier identification should be based on specific and substantiated evidence concerning the individual supplier. General country-related characteristics, including political and judicial institutions, should not serve as grounds for designation. This clarification ensures consistency with the supplier-specific assessment under Articles 100 and 104 while preserving Member State involvement in the decision-making process.

Amendment 258

Auke Zijlstra, Barbara Bonte, Ewa Zajączkowska-Hernik

Proposal for a regulation
Recital 172 a (new)

Text proposed by the Commission

Amendment

(172a) National security is the sole responsibility of each Member State, as Article 4(2) of the Treaty on European Union lays down. Whether a supplier is a high-risk supplier, and whether and when its components are to be phased out of electronic communications networks, depends on each Member State's own assessment of the threats it faces. Such decisions are an expression of national sovereignty and cannot be taken over by the Union. The Union may support Member States through coordination, in particular through Union-level coordinated security risk assessments and in line with the approach of the EU 5G Toolbox, but this support shall never replace the decisions of the Member States. Member States that have already adopted measures shall not be required to duplicate or revise them.

Or. en

Amendment 259
Aura Salla

Proposal for a regulation
Recital 172 a (new)

Text proposed by the Commission

Amendment

(172a) Fixed networks are highly critical in their own right, as they constitute an additional vector for the potential deployment of malicious functionalities, but beyond they are also indispensable to the functioning of the entire mobile ecosystem. The obligations to phase out components of high-risk suppliers from fixed and satellite electronic communications networks should follow

the sequence applied to mobile networks, in which a Union-level coordinated security risk assessment preceded coordinated mitigation and binding obligations. Time periods for such phase outs should be laid down in this Regulation in order to provide legal certainty to operators and suppliers alike.

Or. en

Amendment 260
Diego Solier, Mariateresa Vivaldini

Proposal for a regulation
Recital 172 b (new)

Text proposed by the Commission

Amendment

(172b) The assessment of non-technical risks presented by a supplier should be based on specific and substantiated evidence. In determining how an identified non-technical risk could materialise and how it can be mitigated, account should be taken, as relevant, of technical characteristics or access capabilities that could enable unauthorised access or interference; weaknesses in the supplier's own security posture, governance or supply-chain integrity; specific legal obligations demonstrably applicable to the supplier that could compel it to act contrary to the security interests of the Union or its Member States; or documented conduct demonstrating deliberate compromise, serious security breaches or cooperation with malicious or hostile actors. Measures adopted under this Regulation should be tailored to the risk identified. Technical and supply-chain integrity concerns should, where possible, be addressed through appropriate technical, operational and contractual safeguards. Risks arising from legal compulsion should be addressed through measures capable of providing effective legal and

operational separation. Where documented conduct demonstrates that the supplier itself deliberately poses a security risk, measures dependent on the supplier's voluntary compliance should not be considered sufficient. The supplier's country of establishment, the nationality or geographical origin of its owners or controllers, and the general political, institutional or judicial characteristics of a country should not, by themselves, constitute grounds for identifying that supplier as high-risk. Such factors may be taken into account in the assessment only where supported by specific and substantiated evidence relating to the supplier concerned.

Or. en

Justification

The assessment of non-technical cybersecurity risks should rely on specific and substantiated evidence concerning the individual supplier, rather than general country-related characteristics. The amendment clarifies that political, institutional or judicial characteristics cannot serve as grounds for high-risk supplier identification, while preserving the assessment of demonstrable supplier-specific risks and the recognition of effective mitigating measures.

Amendment 261

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Recital 172 c (new)

Text proposed by the Commission

Amendment

(172c) ICT supply chain risks may arise from ICT components integrated into or embedded in physical equipment or installations, as well as from stand-alone ICT products. The framework laid down in Title IV should therefore apply in a technology-neutral manner to ICT components and components that include ICT components used in ICT assets of entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555, irrespective of whether such components

are supplied directly, incorporated into other equipment or provided through another entity in the supply chain. The identification of key ICT assets and the adoption of measures in relation to such components should remain subject to the risk assessment, necessity and proportionality requirements laid down in this Regulation.

Or. en

Justification

ICT components embedded in physical equipment can create the same supply chain risks as stand-alone ICT products. The Regulation should therefore apply consistently to embedded components across the sectors already covered by its horizontal supply chain framework, while ensuring that any restrictions remain subject to the applicable risk assessment and proportionality requirements.

Amendment 262

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Recital 172 d (new)

Text proposed by the Commission

Amendment

(172d) Customer premises equipment and other ICT components deployed at the edge of networks may constitute a significant attack surface where they are widely deployed, remotely accessible or perform functions relevant to the security or operation of network and information systems. Such equipment should therefore be capable of being identified as a key ICT asset in accordance with Article 102 where the criteria laid down in that Article are fulfilled. The assessment should take into account the function performed by the equipment, its connectivity and access capabilities, the scale of its deployment and the potential consequences of its compromise, irrespective of whether the relevant ICT component is supplied as a stand-alone product or embedded in other equipment.

Justification

Customer premises equipment and other edge devices can create significant cybersecurity risks where they are widely deployed or provide remote access to networks and systems. The Regulation should therefore allow such equipment to be addressed through the horizontal supply-chain framework where the Article 102 criteria are met, while preserving the requirement for an individual risk assessment rather than automatically subjecting entire categories of equipment to restrictions.

Amendment 263**Diego Solier, Mariateresa Vivaldini****Proposal for a regulation****Recital 172 e (new)***Text proposed by the Commission**Amendment*

(172e) Measures addressing risks in ICT supply chains should comply with the principle of proportionality and should target the risk identified at the least restrictive level capable of adequately addressing it. Before imposing a prohibition on the use, installation or integration of ICT components from a high-risk supplier, the Commission should therefore assess whether the identified risk can be adequately mitigated through technical, operational or contractual measures, including restrictions on remote access or data processing, independent security audits, network segmentation, operator-controlled maintenance or other safeguards appropriate to the risk concerned. A prohibition should be imposed only where such measures are insufficient to address the identified risk, cannot reasonably be implemented or where the supplier fails to comply with the measures required. Where restrictions affect ICT components already deployed, appropriate transition and phase-out periods should take account of the lifecycle of the relevant assets, the availability of alternative suppliers and

the need to ensure continuity of essential services.

Or. en

Justification

Supply-chain restrictions should be proportionate to the risk identified. Where targeted safeguards can adequately address that risk, they should be preferred to a full prohibition. Prohibitions should therefore remain a measure of last resort, while appropriate transition periods should limit unnecessary disruption and take account of existing investment and the availability of alternatives.

Amendment 264

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Recital 172 f (new)

Text proposed by the Commission

Amendment

(172f) Where risks identified in relation to a high-risk supplier can be adequately addressed through effective and verifiable mitigation measures, a conditional exemption from the applicable restriction should be prioritised as the proportionate response. Such exemptions should be granted individually, be limited in time and be subject to clearly defined technical, operational, contractual or organisational commitments capable of addressing the identified risk. Their duration should reflect the nature of the risk and the measures required to mitigate it. Exemptions should remain subject to monitoring and may be revoked where the applicable conditions are no longer fulfilled or the agreed measures are not implemented. They may be renewed where the conditions for granting the exemption continue to be satisfied and the relevant mitigation measures remain effective.

Or. en

Justification

Where an identified supply-chain risk can be effectively mitigated, a conditional exemption can achieve the required level of security without imposing a disproportionate restriction. Exemptions should therefore provide a practical route for addressing manageable risks, while remaining time-limited, verifiable, subject to monitoring and revocable in cases of non-compliance.

Amendment 265

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 1 – paragraph 1 – point a

Text proposed by the Commission

(a) the mission, objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA);

Amendment

(a) the mission, objectives, tasks, ***including the operation of testing and evaluation infrastructure***, and organisational matters relating to the European Union Agency for Cybersecurity (ENISA);

Or. en

Amendment 266

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article premier – paragraph 1 – point b

Text proposed by the Commission

(b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, managed security services ***or the cybersecurity posture of entities in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity***

Amendment

(b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes ***and*** managed security services in the Union;

certification schemes in the Union; *and*

Or. fr

Amendment 267

Jens Geier

Proposal for a regulation

Article 1 – paragraph 1 – point b

Text proposed by the Commission

(b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring ***an adequate*** level of cybersecurity for ICT products, ICT services, ICT processes, managed security services or the cybersecurity posture of entities in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union; and

Amendment

(b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring ***a high*** level of cybersecurity for ICT products, ICT services, ICT processes, managed security services or the cybersecurity posture of entities in the Union, as well as for the purpose of ***ensuring the proper functioning and*** avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union; and

Or. en

Amendment 268

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, András Gyürk, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article premier – paragraph 2

Text proposed by the Commission

2. The framework referred to in paragraph 1, point (b) applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.

Amendment

2. The framework referred to in paragraph 1, point (b) applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification, ***as well as to national measures needed for the protection of Member States' essential security interests.***

Or. fr

Amendment 269
Markus Buchheit

Proposal for a regulation
Article 1 – paragraph 4

Text proposed by the Commission

4. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

Amendment

4. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State. ***This Regulation is without prejudice to the right of Member States to decide autonomously on the use or exclusion of specific providers, ICT products or ICT services in their critical infrastructures, for reasons of national security. This is without prejudice to national measures of this kind adopted or agreed before the entry into force of this Regulation.***

Or. de

Amendment 270
Auke Zijlstra, Ewa Zajączkowska-Hernik, Barbara Bonte

Proposal for a regulation
Article 1 – paragraph 4

Text proposed by the Commission

4. This Regulation is without prejudice to the Member States' essential State functions, ***including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular,*** national security remains ***the*** sole responsibility ***of each Member State.***

Amendment

4. This Regulation is without prejudice to the Member States' essential State functions ***as*** national security remains ***its*** sole responsibility, ***as laid down in Article 4(2) of the Treaty on European Union. Nothing in this Regulation shall be construed as affecting that responsibility or as conferring any competence on the Union in this field. Union action under Title IV shall be***

confined to cooperation within the NIS Cooperation Group. The Union-level coordinated security risk assessments referred to in Article 99 may be taken into account by Member States, without prejudice to their own national assessments

Or. en

Justification

National security is and remains a national competence. Article 4(2) TEU is explicit on this, and the draft report's wording turns that principle upside down. Under the draft, a Member State that invokes national security would still be bound by the Regulation, so the exception effectively becomes the exception to the exception. That is unacceptable. Member States, not Brussels, decide how they protect their vital infrastructure, intelligence services and citizens. This amendment restores the balance. National security stays with the Member States, and Union action is limited to coordination. Risk assessments at Union level may serve as input, but they must never replace the national judgment of the Member States themselves

Amendment 271

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article premier – paragraph 4

Text proposed by the Commission

4. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

Amendment

4. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State. ***No provision of this Regulation may be interpreted or applied in a way that would undermine this exclusive responsibility, restrict the competences of the Member States in matters of national security or supersede decisions they take in that respect.***

Or. fr

Amendment 272

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article premier – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. In the event of a conflict between a measure adopted by the Commission under Title IV and a decision of a Member State relating to its national security, territorial integrity or public order, the decision of the Member State shall prevail. The Member State concerned shall inform the Commission thereof and that information shall not be subject to prior authorisation.

Or. fr

Amendment 273

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 1 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. This Regulation is without prejudice to Article 346 TFEU and shall not prevent Member States from taking measures falling within the scope of that Article where necessary for the protection of their essential security interests.

Or. en

Justification

The Regulation should expressly preserve Member States' rights under Article 346 TFEU in matters concerning their essential security interests. This clarification provides legal certainty that the cybersecurity framework does not prejudice the Treaty safeguards applicable in the field of defence and security.

Amendment 274

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article premier – paragraph 4 b (new)

Text proposed by the Commission

Amendment

4b. Member States may maintain or adopt more stringent requirements, including requirements relating to data localisation, critical infrastructure sovereignty and protection against the extraterritorial application of the law of a third country.

Or. fr

Amendment 275

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Article 2 – paragraph 1 – point 18

Text proposed by the Commission

Amendment

(18) ‘ICT process’ means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

(18) ‘ICT process’ means a set of activities performed to design, develop, deliver, **update** or maintain an ICT product or ICT service;

Or. en

Amendment 276

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Article 2 – paragraph 1 – point 35

Text proposed by the Commission

Amendment

(35) ‘key ICT assets’ means ICT assets

(35) ‘key ICT assets’ means ICT assets

identified in accordance with Article 102;

identified in accordance with Article 102
*or listed as key ICT assets in an Annex to
this Regulation;*

Or. en

Amendment 277

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 2 – paragraph 1 – point 38 a (new)

Text proposed by the Commission

Amendment

(38a) ‘supplier’ means any natural or legal person who, in the course of a commercial activity and in the context of a contractual relationship, supplies an ICT component or a component that includes ICT components for distribution or use on the Union market, whether in return for payment or free of charge. Communities and projects that openly develop, maintain and distribute free and open-source software shall not be considered suppliers where no contractual relationship exists beyond adherence to a standardised free and open-source software licence, or where the contractual relationship concerning such software is with an open-source software steward within the meaning of Regulation (EU) 2024/2847;

Or. en

Justification

The concept of supplier should reflect the commercial and contractual relationships addressed by the ICT supply-chain framework. Open-source communities and projects should not be treated as commercial suppliers merely because software is made available under a standardised open-source licence. The clarification preserves the application of the Regulation to commercial actors supplying or integrating open-source software while avoiding disproportionate obligations for non-commercial open-source development.

Amendment 278

Jens Geier

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – introductory part

Text proposed by the Commission

Amendment

(39) ‘high-risk supplier’ means ***either of the following***:

(39) ‘high-risk supplier’ means ***an entity identified in a list established pursuant to Article 104(1) or an entity subject to a prohibition adopted pursuant to Article 103(7), and any entity controlled by such an entity***;

Or. en

Justification

This amendment separates country-related eligibility restrictions from supplier-specific restrictions on ICT components. Point (39) links high-risk supplier status to formal identification under Article 104 or action under Article 103(7). Point (39a) preserves a distinct category for entities linked to a designated third country. This improves legal certainty and ensures that the two categories are applied consistently.

Amendment 279

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – introductory part

Text proposed by the Commission

Amendment

(39) ‘high-risk supplier’ means ***either of the following***:

(39) ‘high-risk supplier’ means ***a supplier included in a list established pursuant to Article 104(1) following an individual assessment in accordance with Articles 100 and 104***;

Or. en

Justification

The definition of a high-risk supplier should reflect the individual, evidence-based identification procedure. Establishment, ownership, control or corporate affiliation should not automatically make an entity a high-risk supplier.

Amendment 280

Adina Vălean

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – introductory part

Text proposed by the Commission

Amendment

(39) ‘high-risk supplier’ means ***either of the following:***

(39) ‘high-risk supplier’ means ***an entity designated in accordance with Article 104 and entities controlled by that entity;***

Or. en

Justification

The procedure for identifying high-risk suppliers should be set out solely in Article 104, through a supplier-specific assessment, without requiring a prior designation of a third country under Article 100. The risk of influence by a third country remains a key criterion in that assessment.

Amendment 281

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – point a

Text proposed by the Commission

Amendment

(a) ***an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country;***

deleted

Or. en

Amendment 282

Jens Geier

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – point a

Text proposed by the Commission

Amendment

(a) an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country; *deleted*

Or. en

Amendment 283
Adina Vălean

Proposal for a regulation
Article 2 – paragraph 1 – point 39 – point a

Text proposed by the Commission

Amendment

(a) an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country; *deleted*

Or. en

Justification

Not necessary after the definition of the ‘high-risk supplier’.

Amendment 284
Francesco Torselli

Proposal for a regulation
Article 2 – paragraph 1 – point 39 – point a

Text proposed by the Commission

Amendment

(a) an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country;

(a) **(a)** an entity established in a third country posing **concrete** cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third

country;

Or. en

Justification

While Cybersecurity concerns should be treated with the outmost attention, especially in a complex geopolitical context, it is important that the qualification of a company as high-risk supplier is based on an in-depth assessment and grounded on concrete evidence. Indeed, a proper assessment would reduce the risks of: i) retaliatory measures from third countries; i") supply-chain disruptions..._

Amendment 285

Jens Geier

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – point b

Text proposed by the Commission

Amendment

(b) an entity designated in accordance with Article 103(7) and entities controlled by that entity; **deleted**

Or. en

Amendment 286

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – point b

Text proposed by the Commission

Amendment

(b) an entity designated in accordance with Article 103(7) and entities controlled by that entity; **deleted**

Or. en

Amendment 287

Adina Vălean

Proposal for a regulation

Article 2 – paragraph 1 – point 39 – point b

Text proposed by the Commission

Amendment

(b) an entity designated in accordance with Article 103(7) and entities controlled by that entity; *deleted*

Or. en

Justification

Not necessary after the definition of the ‘high-risk supplier’.

Amendment 288

Jens Geier

Proposal for a regulation

Article 2 – paragraph 1 – point 39 a (new)

Text proposed by the Commission

Amendment

(39a) ‘entity established in or controlled from a third country posing cybersecurity concerns’ means an entity that is established in a third country designated pursuant to Article 100 (2) or is controlled by that third country, by an entity established in that third country, or by a national of that third country;

Or. en

Justification

This amendment separates country-related eligibility restrictions from supplier-specific restrictions on ICT components. Point (39) links high-risk supplier status to formal identification under Article 104 or action under Article 103(7). Point (39a) preserves a distinct category for entities linked to a designated third country. This improves legal certainty and ensures that the two categories are applied consistently.

Amendment 289

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 2 – paragraph 1 – point 39 a (new)

Text proposed by the Commission

Amendment

(39a) 'direct source high-risk supplier' means a high-risk supplier that has a direct contractual arrangement in place with an entity pursuant to which such high-risk supplier supplies such entity with ICT components or components that include ICT components;

Or. en

Justification

This amendment is necessary to achieve, and consistent with, the justification set out in respect of Amendment 001. It defines the key concept through which the proposed amendments are intended to operate (i.e. to limit the ICT supply chain obligations and restrictions on covered entities solely to those high-risk suppliers over which such entities maintain direct control.

Amendment 290

Markéta Gregorová

on behalf of the Verts/ALE Group

Proposal for a regulation

Article 2 – paragraph 1 – point 39 a (new)

Text proposed by the Commission

Amendment

(39a) 'trusted supplier' means an entity included in the Union list of trusted suppliers established in accordance with Article [105a];

Or. en

Amendment 291

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 2 – paragraph 1 – point 40

Text proposed by the Commission

Amendment

(40) 'ICT supply chain' means a sum of ICT services, ICT products and ICT processes that encompass activities and

(40) 'ICT supply chain' means a sum of ICT services, ICT products and ICT processes that encompass activities **of all**

actors involved at all stages upstream of a product being made available or a service being delivered on the market;

direct source high-risk suppliers and and actors involved ***in*** at all stages upstream of a product being made available or a service being delivered on the market;

Or. en

Justification

This amendment is necessary to achieve, and consistent with, the justification set out in respect of Amendment 001. In a world of global business with multiple supply chain tiers, it is neither possible nor proportionate for stakeholders to exercise due diligence on and control their entire upstream supply chain.

Amendment 292

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 2 – paragraph 1 – point 42

Text proposed by the Commission

(42) ‘non-technical risk’ means the likelihood ***of the supplier being subject to influence by a third country with the potential to*** cause loss or disruption of the service provided or ***to*** compromise the product manufactured by an entity or ***to*** lead to exfiltration of data, including for the purposes of espionage or revenue generation;

Amendment

(42) ‘non-technical risk’ means the likelihood ***that circumstances specific to an individual supplier, including its governance and security practices, documented conduct or legal obligations demonstrably applicable to it, could*** cause loss or disruption of the service provided or compromise the product manufactured by an entity or lead to exfiltration of data, including for the purposes of espionage or revenue generation. ***Such risk shall be established on the basis of specific and substantiated evidence concerning the supplier. The supplier's country of establishment, the nationality or geographical origin of its owners or controllers, and the general political, institutional or judicial characteristics of a country shall not, by themselves, constitute grounds for identifying that supplier as high-risk. Such factors may be taken into account in the assessment only where supported by specific and substantiated evidence relating to the supplier concerned.***

Justification

The definition of non-technical risk should reflect specific circumstances affecting an individual supplier rather than assumptions based on third-country influence. Requiring specific and substantiated evidence prevents the use of geographical, political, institutional or judicial characteristics as automatic proxies for cybersecurity risk, while preserving the assessment of concrete risks arising from the supplier's conduct, governance, security practices or demonstrably applicable legal obligations.

Amendment 293

Aura Salla

Proposal for a regulation

Article 2 – paragraph 1 – point 44

Text proposed by the Commission

(44) ‘core network functions of mobile electronic communications networks’ means the central architectural element of the mobile electronic communications networks connecting major network nodes to the Internet and managing essential system functions that includes user equipment authentication, lawful interception (LI) functions, security gateways (SeGW) at the network edge, signalling security functions, roaming and session management, user and control plane data transport, access policy management, registration and authorisation of network services, storage of end-user **and** network data, critical network services including domain name system (DNS), interconnection with third-party mobile networks, exposure of core network functions to external applications, and the selection and management of network slices;

Amendment

(44) ‘core network functions of mobile electronic communications networks’ means the central architectural element of the mobile electronic communications networks connecting major network nodes to the Internet and managing essential system functions that includes user equipment authentication, lawful interception (LI) functions, security gateways (SeGW) at the network edge, signalling security functions, roaming and session management, user and control plane data transport, access policy management, registration and authorisation of network services, **online charging and other systems which require the processing and/or** storage of end-user **and/or** network data, critical network services including domain name system (DNS), interconnection with third-party mobile networks, exposure of core network functions to external applications, and the selection and management of network slices;

Amendment 294
Francesco Torselli

Proposal for a regulation
Article 2 – paragraph 1 – point 45 a (new)

Text proposed by the Commission

Amendment

(45a) **(45a) ‘operations support systems (OSS) and business support systems (BSS) of mobile electronic communications networks’ means the platforms and software components necessary for the management of the network, the provisioning and monetisation of the services, and the interactions with mobile users;**

Or. en

Amendment 295
Francesco Torselli

Proposal for a regulation
Article 2 – paragraph 1 – point 45 b (new)

Text proposed by the Commission

Amendment

(45b) **‘transport and transmission functions of mobile electronic communications networks’ means all components necessary for the backhaul and aggregation of traffic across the network, including microwave and IP transport links;**

Or. en

Amendment 296
Francesco Torselli

Proposal for a regulation
Article 2 – paragraph 1 – point 46

Text proposed by the Commission

Amendment

(46) ‘radio access network (RAN) of mobile electronic communications networks’ means the network connecting the mobile user equipment to the core network, including base stations (eNodeB for 4G, gNodeB for 5G), remote radio heads (RRH) and baseband units (BBU), active antenna systems (AAS), and where applicable, disaggregated RAN components such as centralised units (CU) and distributed units (DU), and the RAN intelligent controller (RIC);

(46) ‘radio access network (RAN) of mobile electronic communications networks’ means the network connecting the mobile user equipment to the core network, including base stations (eNodeB for 4G, gNodeB for 5G), remote radio heads (RRH) and baseband units (BBU), active antenna systems (AAS), and where applicable, disaggregated RAN components such as centralised units (CU) and distributed units (DU), and the RAN intelligent controller (RIC), ***including both real-time and non-real time RIC***;

Or. en

Amendment 297

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 2 – paragraph 1 – point 50 a (new)

Text proposed by the Commission

Amendment

(50a) ‘general-purpose AI model with systemic risk’ means a general-purpose AI model classified as a general-purpose AI model with systemic risk in accordance with Article 51 of Regulation (EU) 2024/1689;

Or. en

Amendment 298

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 2 – paragraph 1 – point 50 b (new)

(50b) ‘agentic AI system’ means an AI system within the meaning of Article 3, point (1), of Regulation (EU) 2024/1689 which plans and executes sequences of actions in pursuit of an objective, including the use of software tools and the interaction with network and information systems, with limited or no human intervention;

Or. en

Amendment 299

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 2 – paragraph 1 – point 50 c (new)

(50c) ‘AI high risk security incident’ means an event in which an general-purpose AI model with systemic risk, whether or not it has been placed on the market or put into service, (a) circumvents technical measures designed to isolate or contain it; (b) establishes a channel of communication not authorised by its operator, including with other AI systems; (c) accesses network and information systems of third parties without authorisation; or (d) resists or circumvents an instruction to cease operation.

Or. en

Amendment 300

Katri Kulmuni, Eero Heinäluoma

Proposal for a regulation

Article 3 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. Management Board may prioritise ENISA's tasks set out in this regulation on a risk-based basis according to the resources available to it.

Or. en

Justification

Priorisation of ENISA's tasks should be possible in case of, for example, sudden and unforeseen changes in the cyber landscape. Allowing priorisation would also ensure that limited resources available can be used in most efficient way.

Amendment 301

Ondřej Krutílek

Proposal for a regulation

Article 3 – paragraph 2

Text proposed by the Commission

Amendment

2. ENISA shall act as a **reference point** for advice and **expertise** on cybersecurity for Member States, as well as for other stakeholders in the Union.

2. ENISA shall act as a **centre of expertise** for advice and **knowledge** on cybersecurity for Member States, **and where appropriate Union entities**, as well as for other **relevant** stakeholders in the Union. **ENISA shall achieve this by virtue of its independence, the scientific and technical quality of the advice, contributions, and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.**

Or. en

Amendment 302

Jens Geier

Proposal for a regulation

Article 3 – paragraph 2

Text proposed by the Commission

Amendment

2. ENISA shall act as a reference point for advice and expertise on cybersecurity for Member States, as well as for other stakeholders in the Union.

2. ENISA shall act as a reference point for advice and expertise on cybersecurity for Member States ***and Union entities***, as well as for other stakeholders in the Union.

Or. en

Amendment 303

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

**Proposal for a regulation
Article 3 – paragraph 3**

Text proposed by the Commission

Amendment

3. ***ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.***

deleted

Or. fr

Amendment 304

Marc Botenga

on behalf of The Left Group

**Proposal for a regulation
Article 3 – paragraph 5 a (new)**

Text proposed by the Commission

Amendment

5a. The mandate of ENISA is civilian in nature. ENISA shall not be assigned tasks related to offensive cyber operations

Or. en

Amendment 305

Ondřej Krutílek

Proposal for a regulation
Article 4 – paragraph 1

Text proposed by the Commission

Amendment

1. ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice, contributions, and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.

deleted

Or. en

Amendment 306

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation
Article 4 – paragraph 2

Text proposed by the Commission

Amendment

2. ENISA shall assist Member States and, where appropriate, Union entities in implementing horizontal and sectoral Union policies and legislation related to cybersecurity, including market surveillance activities.

2. ENISA shall assist Member States and, where appropriate, Union entities *in areas of emerging technologies with a potential impact on cybersecurity, including AI and PQC, and* in implementing horizontal and sectoral Union policies and legislation related to cybersecurity, including market surveillance activities.

Or. en

Justification

Emerging technologies, notably AI, raise new questions about how the existing cybersecurity acquis applies. ENISA is best placed to give Member States and Union entities consistent support in those areas.

Amendment 307

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation
Article 4 – paragraph 3

Text proposed by the Commission

3. ENISA shall ***provide its expertise and assist the Commission in developing*** Union policies ***and*** legislation ***related to cybersecurity***.

Amendment

3. ENISA shall ***advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the cybersecurity impact on*** Union policies, legislation ***and implementation***;

Or. en

Amendment 308
Jens Geier

Proposal for a regulation
Article 4 – paragraph 5

Text proposed by the Commission

5. ENISA shall contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability across the Union, including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).

Amendment

5. ENISA shall contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability ***and facilitating the recognition of cybersecurity skills and relevant professional qualifications, vocational education and training (VET) credentials and degrees*** across the Union including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).

Or. en

Amendment 309
Ondřej Krutílek

Proposal for a regulation
Article 4 – paragraph 5

Text proposed by the Commission

5. ENISA shall contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability across the Union, including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).

Amendment

5. ENISA shall, ***where appropriate in cooperation with the ECCC***, contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability across the Union, including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).

Or. en

Amendment 310
Marc Botenga
on behalf of The Left Group

Proposal for a regulation
Article 4 – paragraph 5 a (new)

Text proposed by the Commission

Amendment

5a. ENISA shall support Member States in setting up accessible cybersecurity training, with priority for workers in sectors affected by this Regulation.

Or. en

Amendment 311
Jens Geier

Proposal for a regulation
Article 4 – paragraph 7

Text proposed by the Commission

7. ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats.

Amendment

7. ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats , ***including cyber threats and systemic risks originating from or targeting artificial intelligence systems. ENISA shall, in particular, support entities and Member States in building technical and analytical capacities to address adversarial attacks and defend against AI-enabled cyberattacks, automated offensive cyber operations, or other malicious use of artificial intelligence capabilities by adversarial actors.***

Or. en

Amendment 312

Jens Geier

Proposal for a regulation

Article 4 – paragraph 7 a (new)

Text proposed by the Commission

Amendment

7a. ENISA shall build internal capacity and expertise regarding the security of open-source software architectures, actively engage with open source software stewards and developer communities, and support the implementation of secure-by-design practices and coordinated vulnerability disclosure within open source ecosystems underpinning critical infrastructure.

Or. en

Amendment 313

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 4 – paragraph 7 a (new)

Text proposed by the Commission

Amendment

7a. ENISA shall contribute to the technical capacity of the Union for cybersecurity testing by establishing, maintaining and operating the EU Cybersecurity Testbed referred to in Article 6, point (16), for the technical evaluation of products with digital elements, software applications and AI models and systems.

Or. en

Amendment 314

Ondřej Krutílek

Proposal for a regulation

Article 4 – paragraph 8

Text proposed by the Commission

Amendment

8. ENISA shall support operational cooperation at Union level, including by contributing to shared situational awareness of the cyber threat and incident landscape among Member States and, in cooperation with CERT-EU, among Union entities.

8. ENISA shall support operational cooperation at Union level, including by contributing to shared situational awareness of the cyber threat and incident landscape among Member States and, in cooperation with CERT-EU, among Union entities, **and in particular support the CSIRT network and EU-CyCLONE.**

Or. en

Amendment 315

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 4 – paragraph 8 a (new)

8a. ENISA shall contribute to the independent technical evaluation of the cyber relevant capabilities and of the containment of general-purpose AI models and agentic AI systems, in accordance with Article 16a, and shall operate the framework for structured access to AI models with advanced cyber capabilities referred to in Article 16b.

Or. en

Amendment 316

Jens Geier

Proposal for a regulation

Article 4 – paragraph 9

Text proposed by the Commission

9. ENISA shall closely cooperate with Europol, CSIRTs and other relevant national authorities in order to improve cybersecurity preparedness and response to ransomware incidents.

Amendment

9. ENISA shall closely cooperate with Europol, CSIRTs, **relevant offices within the Commission including the EU AI Office**, and other relevant national authorities in order to improve cybersecurity preparedness and response to ransomware incidents.

Or. en

Amendment 317

Ondřej Krutílek

Proposal for a regulation

Article 4 – paragraph 9

Text proposed by the Commission

9. ENISA shall closely cooperate with **Europol**, CSIRTs and other relevant national authorities in order to improve cybersecurity preparedness and response **to ransomware incidents**.

Amendment

9. ENISA shall closely cooperate with CSIRTs and other relevant national authorities, **and where appropriate with Europol**, in order to improve cybersecurity preparedness and response **capacities of**

the Member States.

Or. en

Amendment 318

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 4 – paragraph 9

Text proposed by the Commission

9. ENISA shall closely cooperate with Europol, CSIRTs and other relevant national authorities in order to improve cybersecurity preparedness and response to ransomware incidents.

Amendment

9. ENISA shall closely cooperate with Europol, CSIRTs and other relevant national authorities in order to improve cybersecurity preparedness and ***the*** response to ***and prevention of*** ransomware incidents.

Or. en

Justification

Moves ENISA's ransomware work from reactive to preventive, consistent with Article 13

Amendment 319

Ondřej Krutílek

Proposal for a regulation

Article 4 – paragraph 11

Text proposed by the Commission

11. ENISA shall contribute to the harmonisation of the digital single market by ***engaging*** in standardisation work relevant for Union policies related to cybersecurity and by developing technical specifications.

Amendment

11. ENISA shall contribute to the harmonisation of the digital single market by ***supporting Member States and the Commission*** in standardisation work relevant for Union policies related to cybersecurity and by developing technical specifications.

Or. en

Amendment 320

Marc Botenga

on behalf of The Left Group

Proposal for a regulation

Article 4 – paragraph 11 a (new)

Text proposed by the Commission

Amendment

11a. ENISA shall promote the use of open-source, auditable and publicly governed solutions in the cybersecurity of ICT assets, and shall support Member States and Union entities in applying the principle of ‘public money, public code’, so that software developed with public funds for the operation of key ICT assets of public sector entities is made publicly available under an open-source licence.

Or. en

Amendment 321

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation

Title II – Chapter II – Section 1 – title

Text proposed by the Commission

Amendment

1 Support for implementation of Union policy and law

1 Support for ***the drafting and*** implementation of Union policy and law

Or. en

Amendment 322

Ondřej Krutílek

Proposal for a regulation

Article 5 – paragraph 1 – point c

Text proposed by the Commission

Amendment

(c) ***at the request of the Commission,*** assisting Member States by providing

(c) assisting Member States by providing support, such as technical

support, such as technical guidance, including on cybersecurity risk management measures, tools for cybersecurity maturity assessment, and incident response playbooks, tailored to the sectors listed in Annexes I and II to Directive (EU) 2022/2555 or support for the implementation of secure-by-design principles for products with digital elements in line with Regulation (EU) 2024/2847, with a view to facilitating the improvement of the cybersecurity maturity levels and compliance with Union law regarding cybersecurity;

guidance, including on cybersecurity risk management measures, tools for cybersecurity maturity assessment, and incident response playbooks, **where appropriate** tailored to the sectors listed in Annexes I and II to Directive (EU) 2022/2555, or support for the implementation of secure-by-design principles for products with digital elements in line with Regulation (EU) 2024/2847, with a view to facilitating the improvement of the cybersecurity maturity levels and compliance with Union law regarding cybersecurity;

Or. en

Amendment 323

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Article 5 – paragraph 1 – point e

Text proposed by the Commission

(e) assisting Member States and relevant Union entities in developing and promoting cybersecurity policies related to sustaining the general availability and integrity of the public core of the open internet;

Amendment

(e) assisting Member States and relevant Union entities in developing and promoting cybersecurity policies related to **advancing DNS security and** sustaining the general availability and integrity of the public core of the open internet;

Or. en

Amendment 324

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 5 – paragraph 1 – point f a (new)

Text proposed by the Commission

Amendment

(fa) in accordance with Regulation (EU) 2024/1689, providing technical advice and support to the AI Office, to the market surveillance authorities and to the Member States on the cybersecurity requirements laid down in Article 15 of that Regulation for high-risk AI systems and on the cybersecurity protection of general-purpose AI models with systemic risk pursuant to Article 55(1), point (d), of that Regulation;

Or. en

Amendment 325
Ondřej Krutílek

Proposal for a regulation
Article 5 – paragraph 1 – point g

Text proposed by the Commission

Amendment

(g) assisting Member States in carrying out mutual assistance and in facilitating such cooperation processes for essential and important entities pursuant to [Article 37a of Directive (EU) 2022/2555];

deleted

Or. en

Amendment 326

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation
Article 5 – paragraph 1 – point h

Text proposed by the Commission

Amendment

(h) at the request of the European Data Protection Board, providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy.

(h) providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy.

Amendment 327

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 5 – paragraph 1 – point h a (new)

Text proposed by the Commission

Amendment

(ha) in cooperation with the Commission, providing technical expertise to the European Board for Digital Services established pursuant to Article 61 of Regulation (EU) 2022/2065 on cyber threats, incidents and vulnerabilities affecting recipients of services covered by that Regulation, including those enabling or facilitating online fraud. Such support shall be without prejudice to the tasks and powers conferred by that Regulation.

Or. en

Justification

ENISA would provide the European Board for Digital Services with technical expertise on cyber-enabled online fraud. The amendment does not give ENISA supervisory or enforcement powers under the Digital Services Act.

Amendment 328

Ondřej Krutílek

Proposal for a regulation

Article 5 – paragraph 4

Text proposed by the Commission

Amendment

4. ENISA shall be a member of the NIS Cooperation Group pursuant to Article 14(3) of Directive (EU) 2022/2555.

4. ENISA shall be a member of the NIS Cooperation Group pursuant to Article 14(3) of Directive (EU) 2022/2555 ***and shall actively support the works of the Group .***

Or. en

Amendment 329

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation

Article 5 – paragraph 4

Text proposed by the Commission

4. ENISA shall be a member of the NIS Cooperation Group pursuant to Article 14(3) of Directive (EU) 2022/2555.

Amendment

4. ENISA shall be a member of the NIS Cooperation Group pursuant to Article 14(3) of Directive (EU) 2022/2555 **and shall actively support the works of the Group.**

Or. en

Amendment 330

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation

Article 5 – paragraph 5

Text proposed by the Commission

5. ***At the Commission's request,*** ENISA ***shall*** provide expertise, technical advice, information or analysis or carry out preparatory work ***on specific cybersecurity matters with a view to informing the Commission's policymaking and monitoring of the implementation of Union legislation.***

Amendment

5. ***The Commission shall consult with*** ENISA ***to*** provide expertise, technical advice, information or analysis or carry out preparatory work ***when developing Union policies, legislation and*** implementation.

Or. en

Amendment 331

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Article 5 – paragraph 5 a (new)

5a. ENISA shall assist the Commission in developing and updating guidance on structured access to artificial intelligence models and systems with advanced cyber capabilities for cybersecurity purposes.

That guidance shall set out:

(a) criteria for granting access to different types of organisations, such as Union entities, Member State authorities, operators of critical infrastructure, cybersecurity providers and research actors, and how such organisations are to be identified;

(b) security criteria to ensure that access does not pose undue risk;

(c) a mechanism to streamline the provision of access to eligible entities;

(d) contingency measures in case access is restricted or withdrawn by a provider or a third-country authority.

Or. en

Amendment 332

Ondřej Krutílek

Proposal for a regulation

Article 6 – paragraph 1 – point 1

Text proposed by the Commission

(1) Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise;

Amendment

(1) Member States, ***at their request***, in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise;

Or. en

Amendment 333

Markéta Gregorová
on behalf of the Verts/ALE Group
Jens Geier
on behalf of the S&D Group

Proposal for a regulation
Article 6 – paragraph 1 – point 1 a (new)

Text proposed by the Commission

Amendment

(1a) The services of the EU Cybersecurity Testbed referred to in point (16) of the first subparagraph shall be provided free of charge to micro, small and medium-sized enterprises, to open-source software stewards and to CSIRTs. ENISA shall publish transparent, objective and non discriminatory criteria for priority access, taking into account the potential security impact of the product, AI model or application concerned, its market exposure and the needs of essential and important entities within the meaning of Directive (EU) 2022/2555. Article 47(3) shall not apply to those services.

Or. en

Amendment 334
Markéta Gregorová
on behalf of the Verts/ALE Group
Jens Geier
on behalf of the S&D Group

Proposal for a regulation
Article 6 – paragraph 1 – point 1 b (new)

Text proposed by the Commission

Amendment

(1b) ENISA and the European Cybersecurity Industrial, Technology and Research Competence Centre established by Regulation (EU) 2021/887 shall conclude, within [6] months of the date of entry into force of this Regulation, a working arrangement on the deployment, resourcing and roadmap of the EU

Cybersecurity Testbed, in order to prevent duplication, to align Union funding under the Digital Europe Programme and to ensure that the results of the testing inform the research agenda of the Union. ENISA shall transmit the working arrangement to the European Parliament and to the Council.

Or. en

Amendment 335
Katri Kulmuni, Eero Heinäluoma

Proposal for a regulation
Article 6 – paragraph 1 – point 7

Text proposed by the Commission

(7) national CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices;

Amendment

(7) national CSIRTs in raising the level of their capabilities, ***in particular by developing general, scalable and reusable guidance, methodologies and best-practice materials***, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices;

Or. en

Justification

ENISA's efforts related to capabilities of national CSIRTs should focus in particular to actions that can provide more added value across the Union. By developing general, scalable and reusable guidance etc. ENISA can broadly support the national efforts, instead of focusing to support individual CSIRTs.

Amendment 336
Ondřej Krutílek

Proposal for a regulation
Article 6 – paragraph 1 – point 9

Text proposed by the Commission

(9) relevant public bodies as well as private stakeholders by conducting targeted trainings, where appropriate in cooperation with stakeholders;

Amendment

(9) relevant public bodies as well as private stakeholders by conducting targeted trainings, where appropriate in cooperation with stakeholders ***in consultation with the Member States***;

Or. en

Amendment 337

Ondřej Krutílek

Proposal for a regulation

Article 6 – paragraph 1 – point 13

Text proposed by the Commission

(13) public authorities and private stakeholders in relation to conformity assessment and evaluation activities, including conformity assessment bodies and small and medium-sized enterprises, to support a robust, competitive, inclusive and harmonised conformity assessment ecosystem supporting the implementation Regulation (EU) 2024/2847 and the European cybersecurity certification framework;

Amendment

(13) ***at their request***, public authorities and private stakeholders in relation to conformity assessment and evaluation activities, including conformity assessment bodies and small and medium-sized enterprises, to support a robust, competitive, inclusive and harmonised conformity assessment ecosystem supporting the implementation Regulation (EU) 2024/2847 and the European cybersecurity certification framework;

Or. en

Amendment 338

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 6 – paragraph 1 – point 15 a (new)

Text proposed by the Commission

Amendment

(15a) Member States, CSIRTs, micro, small and medium-sized enterprises and open-source software stewards within the

meaning of Regulation (EU) 2024/2847, by establishing, by [18 months after the date of entry into force of this Regulation], and operating, in cooperation with the Joint Research Centre of the Commission, a secure testing facility and sandbox environment ('EU Cybersecurity Testbed') for the voluntary testing, stress testing and vulnerability assessment of products with digital elements, software applications and AI models and systems, including cyber ranges and the secure testing of AI with advanced cyber capabilities for cybersecurity use cases, making use of the computing capacity of the high-performance computing infrastructure of the European High Performance Computing Joint Undertaking, and by providing technical guidance on the remediation of the vulnerabilities identified.

Or. en

Amendment 339
Ondřej Krutílek

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission

ENISA shall assist Member States in their efforts to raise awareness of Union policies and legislation regarding cybersecurity and promote their visibility by developing actionable tools and guidance. ENISA shall support initiatives aimed at increasing the European cybersecurity talent pool, in particular by coordinating competitions.

Amendment

ENISA shall, ***where appropriate in cooperation with the ECCC***, assist Member States in their efforts to raise awareness of Union policies and legislation regarding cybersecurity and promote their visibility by developing actionable tools and guidance. ENISA shall support initiatives aimed at increasing the European cybersecurity talent pool, in particular by coordinating competitions.

Or. en

Amendment 340

Ondřej Krutílek

Proposal for a regulation

Article 8 – paragraph 1

Text proposed by the Commission

1. ENISA shall carry out and disseminate analyses of the main market trends in the cybersecurity market on both the demand and supply sides, in particular related to the areas where European cybersecurity certification schemes exist or are planned, sectors listed in Annexes I and II to Directive (EU) 2022/2555, and product categories covered by Regulation (EU) 2024/2847, including Annexes III and IV to that Regulation.

Amendment

1. ENISA shall, ***where appropriate in cooperation with the ECCC***, carry out and disseminate analyses of the main market trends in the cybersecurity market on both the demand and supply sides, in particular related to the areas where European cybersecurity certification schemes exist or are planned, sectors listed in Annexes I and II to Directive (EU) 2022/2555, and product categories covered by Regulation (EU) 2024/2847, including Annexes III and IV to that Regulation.

Or. en

Amendment 341

Bart Groothuis, Ivars Ijabs, Anna Stürgkh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 8 – paragraph 3

Text proposed by the Commission

3. ENISA shall build knowledge and disseminate technical advice and analyses on state-of-the-art cybersecurity tools, frameworks standards and best practices.

Amendment

3. ENISA shall build knowledge and disseminate technical advice and analyses on state-of-the-art cybersecurity tools, ***capabilities, services***, frameworks standards and best practices, ***including for emerging technologies with a potential cybersecurity impact, such as AI models***.

Or. en

Justification

The tools developed should extend to frontier AI, whose cyber capabilities change both the threat and the defence landscape.

Amendment 342

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 8 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. ENISA shall establish, maintain and review at least every six months a list of artificial intelligence models most suitable for preventing, detecting and responding to cyberattacks, including those involving artificial intelligence. That list shall be based on a technical assessment conducted by ENISA in cooperation with the CSIRTs network and the competent authorities of the Member States. It shall take into account, at least, the following criteria:

(a) the model's performance in terms of threat detection, vulnerability discovery and analysis, including zero-day vulnerabilities, and incident handling support;

(b) the model's robustness and security, including its resistance to manipulation and data leakage;

(c) the possibility of deploying the model on infrastructure located in the Union and under the control of the authority using it;

(d) the place of establishment and control structure of the supplier, and its exposure to the law of a third country that may require access to the data processed or cooperation with the authorities of that third country;

(e) the model's release under a free and open-source licence.

The list shall clearly identify European artificial intelligence models within the meaning of Article 68b. ENISA shall make the list available to the competent authorities, the CSIRTs network and Union entities, and publish a version of

the list that does not contain sensitive information.

The list shall be indicative and shall not bind the Member States.

Or. fr

Justification

AI models are replaced in a few months: no national authority can assess all of them alone. A list revised every six months by ENISA would pool this monitoring for the Member States. It would incorporate sovereignty criteria (supplier control, exposure to extraterritorial laws, location in the EU) and remain indicative: it would not be binding on any Member State.

Amendment 343

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 8 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. ENISA shall advise the Commission, the European Cybersecurity Industrial, Technology and Research Competence Centre, the Network of National Coordination Centres and the Member States on research priorities and technical benchmarking, on the basis of the operational findings, cyber threat trends and recurring vulnerability patterns identified through the EU Cybersecurity Testbed referred to in Article 6, point (16).

Or. en

Amendment 344

Ondřej Krutílek

Proposal for a regulation

Article 9 – paragraph 1 – point a

Text proposed by the Commission

Amendment

(a) where appropriate, engaging as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

(a) where appropriate **and after informing the Management Board**, engaging as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

Or. en

Amendment 345

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Article 9 – paragraph 1 – point a

Text proposed by the Commission

Amendment

(a) where appropriate, engaging as **an observer** in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

(a) where appropriate, engaging as **a participant** in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

Or. en

Amendment 346

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Article 9 – paragraph 1 – point d

Text proposed by the Commission

Amendment

(d) providing expert advice and support to the Commission on matters relating to the international recognition of European cybersecurity certificates in accordance with Article 87;

(d) providing expert advice and support to the Commission on matters relating to the international recognition of European **standards and** cybersecurity certificates in accordance with Article 87;

Or. en

Amendment 347

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrīd Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Article 9 – paragraph 1 – point e

Text proposed by the Commission

(e) providing expert advice and support to the Commission on matters concerning international standardisation **and engaging with** relevant international standardisation organisations, where relevant, in collaboration with the ECCG established under Article 90.

Amendment

(e) providing expert advice and support to the Commission on matters concerning international standardisation **as well as promoting and coordinating European engagement in** relevant international standardisation organisations, where relevant, in collaboration with the ECCG established under Article 90 **and industry and civil society stakeholders**.

Or. en

Justification

Reflects the changes to Article 18(6) on promoting European standards at the global level, and coordinating a coherent European position and engagement in international standard setting bodies. by facilitating coordination with Member States, industry and civil society.

Amendment 348

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrīd Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Article 9 – paragraph 1 – point e a (new)

Text proposed by the Commission

Amendment

(ea) providing expert advice, analysis and support to the Commission on matters concerning the security of open source and of emerging technologies with potential cybersecurity impact, such as AI.

Or. en

Justification

Reflects the EU's AI Action Plan on AI and Cybersecurity: The EU apply AI-defense where the need is most urgent. Critical open source software is the right place to act first, due to the

high penetration in critical infrastructure sectors. Reportedly, 98% of the total codebase contains open source, with critical infrastructure industry averaging to about 80% of codebases with high- or critical-risk vulnerability

Amendment 349

Ondřej Krutílek

Proposal for a regulation

Article 10 – paragraph 1

Text proposed by the Commission

1. ENISA shall support operational cooperation among Member States, Union entities through CERT-EU, and ***between*** other stakeholders.

Amendment

1. ENISA shall support operational cooperation among Member States, Union entities through CERT-EU, and ***where appropriate*** other stakeholders.

Or. en

Amendment 350

Ondřej Krutílek

Proposal for a regulation

Article 10 – paragraph 2

Text proposed by the Commission

2. ENISA ***shall be a member of the network of national CSIRTs established pursuant to Article 15(1) of Directive (EU) 2022/2555 and*** shall provide the secretariat of the CSIRTs network pursuant to Article 15(2) of Directive (EU) 2022/2555.

Amendment

2. ENISA shall provide the secretariat of the CSIRTs network ***and shall actively provide assistance for the cooperation among the CSIRTs*** pursuant to Article 15(2) of Directive (EU) 2022/2555. ***For that purpose, it shall support, advise and facilitate the activities within the network.***

Or. en

Amendment 351

Ondřej Krutílek

Proposal for a regulation

Article 10 – paragraph 3

Text proposed by the Commission

Amendment

3. ENISA shall provide the secretariat of the European cyber crisis liaison organisation network (EU-CyCLONe) pursuant to Article 16(2), second subparagraph, of Directive (EU) 2022/2555.

3. ENISA shall ***facilitate the cooperation within EU-CyCLONe and*** provide the secretariat of the European cyber crisis liaison organisation network (EU-CyCLONe) pursuant to Article 16(2), second subparagraph, of Directive (EU) 2022/2555.

Or. en

Amendment 352
Ondřej Krutílek

Proposal for a regulation
Article 10 – paragraph 4 – introductory part

Text proposed by the Commission

Amendment

4. ENISA shall support ***technical and*** operational cooperation among Member States, ***in particular*** through the ***CSIRTs network and*** EU-CyCLONe. Such support shall include:

4. ENISA shall support operational cooperation among Member States, through the EU-CyCLONe. Such support shall include:

Or. en

Amendment 353
Ondřej Krutílek

Proposal for a regulation
Article 10 – paragraph 4 – point a

Text proposed by the Commission

Amendment

(a) advising on improvement of capabilities to prevent, detect, respond to and recover from incidents;

deleted

Or. en

Amendment 354
Ondřej Krutílek

Proposal for a regulation

Article 10 – paragraph 4 – point b

Text proposed by the Commission

(b) at the request of one or more Member States, providing advice and ***assessments*** in relation to a specific ***potential or ongoing incident or*** cyber threat, including ***through the provision of expertise and facilitating the technical handling of such incidents, and through*** supporting the voluntary sharing of relevant information and technical solutions between Member States;

Amendment

(b) at the request of one or more Member States ***concerned***, providing advice and ***assistance*** in relation to a specific cyber threat, including ***by and*** supporting the voluntary sharing of relevant information and technical solutions between Member States;

Or. en

Amendment 355

Ondřej Krutílek

Proposal for a regulation

Article 10 – paragraph 4 – point c

Text proposed by the Commission

(c) analysing vulnerabilities, threats ***and incidents***;

Amendment

(c) analysing vulnerabilities ***and*** threats;

Or. en

Amendment 356

Ondřej Krutílek

Proposal for a regulation

Article 10 – paragraph 4 – point e

Text proposed by the Commission

(e) ***contributing to*** supporting the ***coordinated*** management of large-scale cybersecurity incidents and crises at ***operational level, in particular by assisting EU-CyCLONe in preparing reports to*** political level ***and by facilitating timely information sharing between the CSIRTs network and EU-CyCLONe***;

Amendment

(e) supporting the ***operational cooperation within EU-CyCLONe among the Member States in assessing the*** management of large-scale cybersecurity incidents and crises ***and supporting decision-making*** at political level ***in relation to such incidents and crises***;

Amendment 357

Ondřej Krutílek

Proposal for a regulation

Article 10 – paragraph 5

Text proposed by the Commission

5. At the request of **a** Member **State** or a Union entity in cooperation with CERT-EU, ENISA shall support consistent public communication relating to an incident or cyber threat.

Amendment

5. At the request of **one or more** Member **States concerned**, or a Union entity in cooperation with CERT-EU, ENISA shall support **their** consistent public communication relating to an incident or cyber threat **through EU-CyCLONe and CSIRTs Network, as appropriate**.

Or. en

Amendment 358

Ondřej Krutílek

Proposal for a regulation

Article 11 – paragraph 1 – introductory part

Text proposed by the Commission

1. For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape **among Member States and among Union entities**, ENISA shall:

Amendment

1. For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape, ENISA shall:

Or. en

Amendment 359

Letizia Moratti

Proposal for a regulation

Article 11 – paragraph 1 – point a

Text proposed by the Commission

Amendment

(a) develop in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, CERT-EU, Europol and other relevant Union entities, repositories of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures;

(a) “**(a)** develop in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, CERT-EU, Europol and other relevant Union entities, repositories of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures; **“as well as mechanisms supporting the proactive identification of emerging cybersecurity risks affecting critical sectors, digital infrastructures and industrial ecosystems operating across the Union, ensuring that information-sharing activities are conducted according to the need-to-know principle and do not entail the disclosure of sensitive, classified or defence-related information without the prior consent of the Member State or entity from which such information originates.”**”

Or. en

Amendment 360

Ondřej Krutílek

Proposal for a regulation

Article 11 – paragraph 1 – point a

Text proposed by the Commission

(a) develop in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, CERT-EU, Europol and other relevant Union entities, **repositories** of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures;

Amendment

(a) develop in cooperation with EU-CyCLONe, **CSIRTs through** the CSIRTs network, the Commission, CERT-EU, **Cross-Border Cyber Hubs**, Europol and other relevant Union entities, **a repository** of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures, **and facilitate the sharing of cyber threat intelligence contained in that repository among those entities, as appropriate;**

Or. en

Amendment 361

Ondřej Krutílek

Proposal for a regulation

Article 11 – paragraph 1 – point b

Text proposed by the Commission

(b) ***in accordance with Article 12***, issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in particular in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555;

Amendment

(b) issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in particular in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555, ***to CSIRTs through CSIRTs Network and, where relevant, EU-CyCLONe***;

Or. en

Amendment 362

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 11 – paragraph 1 – point b

Text proposed by the Commission

(b) in accordance with Article 12, issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in particular in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555;

Amendment

(b) in accordance with Article 12, issue early alerts of a potential or ongoing ***ransomware incident or*** significant or large-scale incident, or a cyber threat of a potential cross-border nature, in particular in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555;

Or. en

Justification

This reflects the link made between the early alerts in Article 12 and the Ransomware early warning and detection program in Article 13.

Amendment 363

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation
Article 11 – paragraph 1 – point g a (new)

Text proposed by the Commission

Amendment

(ga) where appropriate, support cooperation with providers of artificial intelligence models and systems to enhance the sharing of cyber threat intelligence, in particular on AI-driven cyber threats.

Or. en

Amendment 364
Jens Geier

Proposal for a regulation
Article 11 – paragraph 2 – point a

Text proposed by the Commission

Amendment

(a) perform analyses of cyber threats, incidents, trends, emerging technologies and their impacts, including a regular analysis addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847;

(a) perform analyses of cyber threats, incidents, trends, emerging technologies and their impacts, including a regular analysis addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847. ***Such analyses shall systematically assess systemic cybersecurity risks related to advanced artificial intelligence technologies, in particular autonomous capabilities, the risks associated with general-purpose AI models with open weights, AI-enabled automated threat vectors, and vulnerabilities across AI supply chains;***

Or. en

Amendment 365
Markéta Gregorová
on behalf of the Verts/ALE Group
Jens Geier
on behalf of the S&D Group

Proposal for a regulation

Article 11 – paragraph 2 – point a

Text proposed by the Commission

(a) perform analyses of cyber threats, incidents, trends, emerging technologies and their impacts, including a regular analysis addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847;

Amendment

(a) perform analyses of cyber threats, incidents, trends, emerging technologies and their impacts, including a regular analysis addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847 ***and a regular analysis of the use of general-purpose AI models and agentic AI systems by threat actors and of the cyber relevant capabilities of such models and systems, drawing on the evaluations referred to in Article 16a;***

Or. en

Amendment 366

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrīd Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews, Elisabetta Gualmini

Proposal for a regulation

Article 11 – paragraph 2 – point c

Text proposed by the Commission

(c) carry out long-term strategic analyses of cyber threats and incidents in order to identify emerging trends ***and*** help prevent incidents.

Amendment

(c) carry out long-term strategic analyses of cyber threats and incidents in order to identify emerging trends ***or tactics to*** help prevent incidents. ***or feed into the Union's security foresight.***

Or. en

Amendment 367

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrīd Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini

Proposal for a regulation

Article 11 – paragraph 2 – point c a (new)

(ca) explore ways to assist cooperation with AI providers to enhance sharing of cyber threat intelligence and on AI-driven cybersecurity threats through the relevant Union networks, both at horizontal and sectoral levels.

Or. en

Justification

Reflects the EU Action Plan on Cybersecurity and Artificial Intelligence: As technologies and associated risks will continue to evolve, collective situational awareness and structured information sharing on AI-driven cybersecurity threats through relevant Union networks, both at horizontal and sectoral levels, will be instrumental to strengthen situational awareness. ENISA should explore ways to assist cooperation with AI providers to enhance sharing of threat intelligence.

**Amendment 368
Ondřej Krutílek**

**Proposal for a regulation
Article 11 – paragraph 2 a (new)**

2a. Early alerts referred to in paragraph 1, first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. That information may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures. Such alerts shall be issued as soon as possible.

Amendment 369

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation

Article 11 – paragraph 5

Text proposed by the Commission

5. ENISA shall cooperate closely with the Member States in the preparation of the EU Cybersecurity Technical Situation Report referred to in paragraph 1, point (e). The Report shall be based on publicly available information, ENISA's own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2022/2555, both on a voluntary basis, EC3 and CERT-EU. In agreement with the contributing entities, ENISA may make an aggregated version of the Report publicly available.

Amendment

5. ENISA shall cooperate closely with the Member States in the preparation of the EU Cybersecurity Technical Situation Report referred to in paragraph 1, point (e). The Report shall be based on publicly available information, ENISA's own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2022/2555, both on a voluntary basis, EC3 and CERT-EU. In agreement with the contributing entities, ENISA may make an aggregated version of the Report publicly available. ***ENISA shall encourage Member States to share information needed for the report to reflect the situation in all Member States.***

Amendment 370

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Article 11 – paragraph 5 a (new)

Text proposed by the Commission

Amendment

5a. ENISA shall regularly analyse the cyber capabilities of frontier artificial intelligence models and their implications for cybersecurity in the Union and shall, where appropriate, cooperate with the AI Office. ENISA shall share the results of

its analyses, taking into account their sensitivity, with relevant Union entities and Member State authorities, in particular the CSIRTs network, EU-CyCLONe and the European Cybercrime Centre (EC3) at Europol.

Or. en

Amendment 371
Katri Kulmuni, Eero Heinäluoma

Proposal for a regulation
Article 12

Text proposed by the Commission

Amendment

Article 12

deleted

Early alerts

1. Early alerts referred to in Article 11(1), first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such information may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures.

2. Early alerts referred to in Article 11(1), first subparagraph, point (b), shall be issued as soon as possible to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-CyCLONe.

3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.

4. The service referred to in paragraph 3 shall be provided upon a request of the entity and in a machine-readable format made publicly available. That service shall include sharing of information on cyber threat indicators and recommendations on mitigation measures.

5. ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.

Or. en

Justification

The proposed early alert rules are unnecessarily detailed and ill-suited to ENISA's mandate. More flexibility should be left for ENISA to develop early alerts. Providing the service directly to entities in Annexes I and II to Directive (EU) 2022/2555 would significantly change ENISA's role and duplicate national cybersecurity authorities' efforts. Serving such a large group could also require significant resources and capabilities ENISA currently lacks, without real Union-level added value.

Amendment 372
Ondřej Krutílek

Proposal for a regulation
Article 12

Text proposed by the Commission

Amendment

Article 12

deleted

Early alerts

1. Early alerts referred to in Article 11(1), first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such information may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise,

adversarial tactics, threat actor-specific information and recommendations on mitigation measures.

2. Early alerts referred to in Article 11(1), first subparagraph, point (b), shall be issued as soon as possible to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-CyCLONe.

3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.

4. The service referred to in paragraph 3 shall be provided upon a request of the entity and in a machine-readable format made publicly available. That service shall include sharing of information on cyber threat indicators and recommendations on mitigation measures.

5. ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.

Or. en

Amendment 373

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsik, Barry Andrews

Proposal for a regulation

Article 12 – paragraph 1

Text proposed by the Commission

1. Early alerts referred to in Article 11(1), first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such information may include publicly known vulnerabilities and whether

Amendment

1. Early alerts referred to in Article 11(1), first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing **ransomware incident**, a significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such information may include

they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures.

publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures.

Or. en

Justification

This reflects the link made between the early alerts in Article 12 and the Ransomware early warning and detection program in Article 13.

Amendment 374

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation Article 12 – paragraph 2

Text proposed by the Commission

2. Early alerts referred to in Article 11(1), first subparagraph, point (b), shall be issued as soon as possible to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-CyCLONe.

Amendment

2. Early alerts referred to in Article 11(1), first subparagraph, point (b), shall be issued as soon as possible to the CSIRT or CSIRTs concerned, ***as well as to the relevant national cyber crisis management authorities designated pursuant to Article 9(1) of Directive (EU) 2022/2555***, and, where appropriate, to the CSIRTs network and EU-CyCLONe.

Or. en

Amendment 375

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation Article 12 – paragraph 3

Text proposed by the Commission

3. ENISA shall offer an early alert service to entities operating in sectors

Amendment

3. ENISA shall offer an early alert service to entities operating in sectors

listed in Annexes I and II to Directive (EU) 2022/2555.

listed in Annexes I and II to Directive (EU) 2022/2555. ***That service shall complement the tasks of the CSIRTs. Every alert disseminated under the service shall be transmitted to the CSIRTs concerned before or simultaneously with its dissemination to entities. Where the CSIRT concerned has issued an advisory on the same threat or vulnerability, the alert shall reference that advisory. Where that advisory has been made publicly available, ENISA shall not disseminate a separate alert concerning the same threat or vulnerability to entities under the jurisdiction of that Member State without the prior agreement of the CSIRT concerned.***

Or. en

Justification

ENISA's early alert service should complement rather than duplicate the operational role of national CSIRTs. Alerts should therefore be coordinated with the CSIRTs concerned, take account of existing national advisories and avoid parallel dissemination where a CSIRT has already issued a public advisory, unless that CSIRT agrees otherwise. Participation by entities should remain voluntary and should not create additional notification obligations or disadvantage non-participants.

Amendment 376 **Markus Buchheit**

Proposal for a regulation **Article 12 – paragraph 3**

Text proposed by the Commission

3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.

Amendment

3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555, ***in coordination with the CSIRTs designated pursuant to Article 10 of Directive (EU) 2022/2555. This service shall complement the activities of the national CSIRTs and shall not create parallel lines of notification or communication with the entities.***

Amendment 377

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, João Cotrim De Figueiredo, Elisabetta Gualmini

**Proposal for a regulation
Article 12 – paragraph 3**

Text proposed by the Commission

3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.

Amendment

3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555. ***ENISA may expand this service to other entities of strategic importance.***

Or. en

Justification

Entities outside the NIS2 annexes may be critical to the Union essential security interests and its economic security.

Amendment 378

Diego Solier, Mariateresa Vivaldini

**Proposal for a regulation
Article 12 – paragraph 4**

Text proposed by the Commission

4. The service referred to in paragraph 3 shall be provided upon a request of the entity and in a machine-readable format made publicly available. That service shall include sharing of information on cyber threat indicators and recommendations on mitigation measures.

Amendment

4. The service referred to in paragraph 3 shall be provided upon a request of the entity, ***without prejudice to notification channels and obligations established under Directive (EU) 2022/2555***, and in a machine-readable format made publicly available. That service shall include sharing of information on cyber threat indicators and recommendations on mitigation measures. ***Participation shall be voluntary and shall not lead to any form of detrimental treatment of entities that do not participate.***

Justification

ENISA's early alert service should complement rather than duplicate the operational role of national CSIRTs. Alerts should therefore be coordinated with the CSIRTs concerned, take account of existing national advisories and avoid parallel dissemination where a CSIRT has already issued a public advisory, unless that CSIRT agrees otherwise. Participation by entities should remain voluntary and should not create additional notification obligations or disadvantage non-participants.

Amendment 379**Letizia Moratti****Proposal for a regulation****Article 12 – paragraph 5***Text proposed by the Commission*

5. ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.

Amendment

5. “ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph ***“ensuring the timely dissemination of relevant cyber threat alerts to competent authorities, operators and relevant cybersecurity stakeholders.”***

Or. en

Amendment 380**Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews, João Cotrim De Figueiredo, Elisabetta Gualmini****Proposal for a regulation****Article 12 – paragraph 5***Text proposed by the Commission*

5. ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.

Amendment

5. ENISA shall, ***within six months of the entry into force of this Regulation,*** establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.

Or. en

Amendment 381

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 13 – title

Text proposed by the Commission

Support in incident response and review

Amendment

Support in incident response and review,
and ransomware early warning

Or. en

Amendment 382

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 13 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. When operating and administering the EU Cybersecurity Reserve, ENISA shall procure pre-committed capacity on the basis of objective and transparent criteria concerning, in particular, cybersecurity and security requirements, technical and operational capability, service quality, resilience, availability and value for money. Without prejudice to eligibility or security requirements laid down in Regulation (EU) 2025/38 or other applicable Union law, procurement shall not be subject to a mandatory minimum percentage based on the Member State or country of establishment of a provider or on its ownership or control structure. ENISA shall report annually to the European Parliament and to the Council on the composition of the providers from which pre-committed capacity has been procured, including their place of establishment, service category and, where applicable, whether they are controlled by a third country or by an entity of a third country.

Justification

Pre-committed capacity under the EU Cybersecurity Reserve should be procured according to security, capability, resilience and value-for-money considerations rather than predetermined geographic quotas. Existing eligibility and security safeguards under Union law remain fully applicable. Annual reporting on establishment and ownership provides transparency over the composition of the Reserve without unnecessarily restricting competition or reducing the pool of capable providers.

Amendment 383

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation**Article 13 – paragraph 2***Text proposed by the Commission*

2. At the request of the **Commission** or EU-CyCLONe, ENISA, with the support of the CSIRTs network **and with the approval of the Member State concerned**, shall review and assess significant cybersecurity incidents or large-scale cybersecurity incidents in accordance with Article 21 of Regulation (EU) 2025/38.

Amendment

2. At the request of the **Member State concerned** or EU-CyCLONe, ENISA, with the support of the CSIRTs network, shall review and assess significant cybersecurity incidents or large-scale cybersecurity incidents in accordance with Article 21 of Regulation (EU) 2025/38.

Amendment 384

Ondřej Krutílek

Proposal for a regulation**Article 13 – paragraph 3***Text proposed by the Commission*

3. **ENISA shall assist, in cooperation with Europol and CSIRTs or other competent authorities as applicable, individual essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555 in preparing, responding to and recovering from a ransomware**

Amendment

deleted

incident. For that purpose, ENISA shall establish a helpdesk and in particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.

Or. en

Amendment 385

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsik, Barry Andrews

Proposal for a regulation Article 13 – paragraph 3

Text proposed by the Commission

3. ENISA shall assist, in cooperation with Europol and CSIRTs or other competent authorities as applicable, individual essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555 in ***preparing, responding to and recovering from*** a ransomware incident. For that purpose, ENISA shall ***establish a helpdesk and*** in particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.

Amendment

3. ENISA shall assist, in cooperation with Europol and CSIRTs or other competent authorities as applicable, individual essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555 in ***preventing*** a ransomware incident. For that purpose, ENISA shall ***support CSIRTs in establishing a ransomware early warning and detection programme within one year of the date of entry into force of this Regulation.***

3a. The early warning and detection programme shall aim to prevent ransomware incidents from taking place, by enabling the earliest possible identification of ransomware activity in the pre-encryption phase and by timely alerting the entities concerned to take mitigating action. The programme shall be operated by CSIRTs or other competent authorities and may be integrated into other national cybersecurity services offered to essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555.

Member States may extend the programme to other entities.

3b. Within the early warning and detection programme, the CSIRT or other competent authority concerned shall, on a regular basis:

(a) collect and aggregate cyber threat intelligence, including cyber threat intelligence it may procure from the EU Cybersecurity Reserve or the European Cybersecurity Alert System pursuant to Regulation (EU) 2025/38, covering at least incident notifications, network abuse events, and vulnerabilities or exposed services;

(b) correlate that intelligence in order to identify indicators of ransomware activity, in particular indicators of the pre-encryption phase;

(c) deliver alerts to the entities concerned, without undue delay where the intelligence points to an imminent ransomware incident, containing at least the indicators identified, the affected asset, vulnerability or exposed service, and recommended mitigating measures; and

(d) follow up on alerts, where entities so request, with guidance on mitigation and, where relevant, on reporting under Article 23 of Directive (EU) 2022/2555.

3c. ENISA shall function as a supportive analysis centre for the early warning and detection programme that provides CSIRTs or other competent authorities with data or cyber threat intelligence by means of the early alerts established pursuant to Article 12, and may:

(a) make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation;

(b) develop, in cooperation with CSIRTs and Europol, common methodologies, indicators and templates for the detection of ransomware activity in the pre-encryption phase and for the content of

*alerts;
(c) facilitate the exchange of experience
and best practices among CSIRTs
participating in the programme.*

*3d. Three years after the date of entry into
force of this Regulation, ENISA shall
assess the functioning of the programme,
in cooperation with the CSIRTs network,
and report its findings to the Commission
and the NIS Cooperation Group.*

Or. en

Justification

The Commission proposal's ransomware helpdesk was vaguely described and implies incident response, for which ENISA is not equipped. The amendment, inspired by the UK's approach, proposes early detection, which is where most of the benefit lies as you prevent encryption from taking place. It delivers tailored daily and weekly alerts on incidents, network abuse and exposed vulnerabilities. It draws on public, commercial and closed intelligence sources, for which national CSIRTs are best positioned, with support of ENISA.

Amendment 386 Markus Buchheit

Proposal for a regulation Article 13 – paragraph 3

Text proposed by the Commission

3. ENISA shall assist, in cooperation with Europol and CSIRTs or other competent authorities as applicable, individual essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555 in preparing, responding to and recovering from a ransomware incident. For that purpose, ENISA **shall** establish a helpdesk and in particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.

Amendment

3. ENISA shall assist, **at the request of the relevant CSIRT and** in cooperation with Europol and CSIRTs or other competent authorities as applicable, individual essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555 in preparing, responding to and recovering from a ransomware incident. For that purpose, ENISA **may** establish a helpdesk and in particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation. **The support shall be secondary to national capabilities and to incident response services available on the**

market.

Or. de

Amendment 387

Katri Kulmuni, Eero Heinäluoma

Proposal for a regulation

Article 13 – paragraph 3

Text proposed by the Commission

3. ENISA *shall* assist, *in cooperation with* Europol and CSIRTs or other competent authorities *as applicable, individual essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555 in preparing*, responding to *and recovering from a ransomware incident*. For that purpose, ENISA shall *establish a helpdesk and in particular* make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.

Amendment

3. ENISA *may, at the request of a Member State concerned*, assist Europol and CSIRTs or other competent authorities responding to *significant incidents*. For that purpose, ENISA shall make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.

Or. en

Justification

ENISA's support should cover more generally responding to significant incidents rather than focusing only to ransomware incidents. Instead of individual entities, ENISA should focus its efforts to support Europol and national authorities that normally communicate with and supervise the essential and important entities.

Amendment 388

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 14 – paragraph 3

Text proposed by the Commission

3. At the request of EU-CyCLONe,

Amendment

3. At the request of EU-CyCLONe,

the Commission, ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents and crises at Union level.

the Commission, ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents and crises at Union level. ***ENISA may organize cybersecurity exercises at Union level in a way that include the participation of international organisations or other partner countries in accordance with the Union priorities.***

Or. en

Amendment 389

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation Article 14 – paragraph 3

Text proposed by the Commission

3. At the request of EU-CyCLONe, the Commission, ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents and crises at Union level.

Amendment

3. At the request of EU-CyCLONe ***or*** the Commission, ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents and crises at Union level ***and to multiple simultaneous significant or large-scale incidents. ENISA shall seek to involve the private sector in such exercises.***

Or. en

Amendment 390

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, András Gyürk, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation Article 14 – paragraph 3

Text proposed by the Commission

3. At the request of EU-CyCLONe,

Amendment

3. At the request of EU-CyCLONe,

the Commission, ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents and crises at Union level.

ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents and crises at Union level.

Or. fr

Amendment 391

Katri Kulmuni, Eero Heinäluoma

Proposal for a regulation

Article 14 – paragraph 4

Text proposed by the Commission

4. *At the request of Member States*, ENISA shall support *them* in organising national cybersecurity exercises.

Amendment

4. ENISA shall support *Member States* in organising national cybersecurity exercises *in particular by providing general guidance and methodologies as well as facilitating the exchange of best practices from national exercises*.

Or. en

Justification

ENISA's efforts related to supporting Member States in organizing exercises should focus to actions that can provide more added value across the Union. By providing general guidance and methodologies can broadly support the national efforts, instead of focusing to support individual Member States.

Amendment 392

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Pierre-Romain Thionnet

Proposal for a regulation

Article 15

Text proposed by the Commission

Amendment

Article 15

deleted

Provision of tools and platforms

1. ENISA shall establish, provide, operate, maintain and update as necessary,

operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.

2. Where appropriate for the purposes of paragraph 1, ENISA shall cooperate and exchange information with the CSIRTs network and, where applicable, market surveillance authorities.

Or. fr

Amendment 393

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation Article 15 – title

Text proposed by the Commission

Provision of tools *and* platforms

Amendment

Provision of tools platforms *and testing laboratories*

Or. en

Amendment 394

Jens Geier

Proposal for a regulation Article 15 – paragraph 1

Text proposed by the Commission

1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union

Amendment

1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union

level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.

level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation. ***Where the single-entry point referred to in Article 23a of Directive (EU) 2022/2555 is established, ENISA shall ensure that the tools and platforms referred to in this paragraph are aligned with it and do not create parallel or duplicative incident-reporting channels.***

Or. en

Amendment 395

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation Article 15 – paragraph 1

Text proposed by the Commission

1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.

Amendment

1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools, ***including AI-enabled testing tools,*** to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation. ***ENISA shall take appropriate measures to facilitate SMEs' access to those tools.***

Or. en

Amendment 396

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 15 – paragraph 1

Text proposed by the Commission

1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], **and** testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.

Amendment

1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555]. **ENISA shall also establish testing tools, in particular AI-driven tools,** to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation **or tools to demonstrate compliance with those procedures or legislations.**

Or. en

Justification

Conformity assessment is becoming a bottleneck and the cost and duration of testing weigh most heavily on SMEs. Testing tools provided by ENISA, especially AI-driven ones, could help companies demonstrate compliance faster, more consistently and at lower cost.

Amendment 397

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Article 15 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. ENISA shall, together with the Joint Research Centre, provide a secure testing environment in which users, such

as public authorities and critical infrastructure operators, can test how artificial intelligence models and systems with advanced cyber capabilities perform in specific cybersecurity tasks. The environment shall not be used to evaluate general-purpose AI models for compliance with Regulation (EU) 2024/1689.

The testing environment shall build primarily on existing cyber ranges. ENISA shall manage it and lay down rules on its security and confidentiality as well as on the sharing of test results.

Users shall bear their own costs and remain responsible for their testing methods.

ENISA shall aggregate the test results shared with it and use them to issue and maintain guidance on the secure use of artificial intelligence models and systems in cybersecurity.

Or. en

Amendment 398

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrīd Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 15 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. ENISA shall establish and operate testing laboratories and operational tools for emerging technologies with an impact on cybersecurity, including AI and PQC, to foster harmonized Union-wide testing and to enhance the Union's cybersecurity posture. If necessary for improved or urgent capabilities, ENISA may make use of the EU Cybersecurity Reserve to procure services and tools.

Or. en

Justification

Reflects the EU Action Plan on Cybersecurity and Artificial Intelligence.

Amendment 399

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 15 – paragraph 1 b (new)

Text proposed by the Commission

Amendment

1b. ENISA shall support the Commission and Member States in jointly obtaining access to emerging technologies with an impact on cybersecurity, including AI and PQC, where timely access is needed for general use. For this purpose, it may consider the potential use of funding instruments available, including joint procurement.

Or. en

Justification

Reflects the EU Action Plan on Cybersecurity and Artificial Intelligence.

Amendment 400

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews, Michael McNamara

Proposal for a regulation

Article 15 – paragraph 2

Text proposed by the Commission

Amendment

2. Where appropriate for the purposes of ***paragraph 1***, ENISA shall cooperate and exchange information with the CSIRTs network and, where applicable, market surveillance authorities.

2. Where appropriate for the purposes of ***paragraphs 1, 1a and 1b***, ENISA shall cooperate and exchange information with the CSIRTs network and, where applicable, market surveillance authorities, ***Europol, the Artificial Intelligence Office and the Joint Research Centre of the Commission. For the purpose of paragraphs 1a and 1b, ENISA may use the European High***

Performance Computing infrastructure (EuroHPC). ENISA and the European High Performance Computing Joint Undertaking shall, within [6] months of the entry into force of this Regulation, conclude a working arrangement specifying the practical modalities of ENISA's access.

Or. en

Justification

Uses existing Union assets instead of building new ones, and gives access to the computing power needed for testing.

Amendment 401

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 15 a (new)

Text proposed by the Commission

Amendment

Article 15a

Single entry point for incident reporting

1. ENISA shall establish, operate and maintain a single entry point for incident reporting through which entities may submit notifications required under Union legal acts, where those Union legal acts so provide, including Articles 23 and 30 of Directive (EU) 2022/2555, Article 33 of Regulation (EU) 2016/679, Article 19 of Regulation (EU) 2022/2554, Articles 19a, 24 and 45a of Regulation (EU) No 910/2014, Article 15 of Directive (EU) 2022/2557 and Article 14 of Regulation (EU) 2024/2847 ('the single entry point'). The single entry point shall build on the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847.

2. The single entry point shall be designed to ensure that:

(a) a single submission by an entity may

fulfil reporting obligations applicable to the same incident under more than one Union legal act referred to in paragraph 1, provided that the submission contains the information required under each applicable legal act, is submitted within the applicable deadline and is transmitted to all authorities and CSIRTs entitled to receive it;

(b) each submission is transmitted without delay to the competent authorities and CSIRTs designated under the relevant Union legal act, which shall be the sole addressees of the content of the submission and shall remain responsible for its handling in accordance with that act;

(c) information already submitted by an entity can be retrieved, supplemented, corrected and reused for subsequent reporting stages, without requiring the entity to resubmit information already provided;

(d) national entry points and existing national reporting systems designated by Member States may be connected to the single entry point through open, documented and machine-readable interfaces, enabling equivalent functionality and the secure exchange of information between those systems;

(e) the single entry point provides clear information identifying the applicable reporting obligations, definitions, thresholds, deadlines, formats, procedures and competent authorities and CSIRTs on the basis of information communicated and kept up to date by the Member States and the relevant Union authorities;

(f) submissions may be made in all official languages of the Union and the single entry point complies with applicable Union accessibility requirements.

3. ENISA shall implement appropriate technical, operational and organisational measures ensuring the confidentiality, integrity and availability of the single

entry point and of information transmitted through it. Those measures shall in particular ensure that:

(a) the content of submissions is encrypted between the notifying entity and the addressee authorities referred to in paragraph 2, point (b);

(b) ENISA shall not have access to the content of incident reports or notifications and shall process only metadata strictly necessary for secure routing, authentication, acknowledgement of transmission, operation and security of the single entry point and for aggregated and anonymised statistical analysis;

(c) personal data and commercially or security-sensitive information contained in metadata shall be limited to what is strictly necessary and, where technically possible, pseudonymised before further processing by ENISA;

(d) encrypted submission content shall not be retained on infrastructure operated by ENISA beyond what is technically necessary to confirm transmission to the addressee authorities and in any event no longer than 72 hours;

(e) the architecture shall be federated and shall not create a central Union repository of incident-report content;

(f) an independent security audit shall be carried out before the single entry point becomes operational for a Union legal act referred to in paragraph 1 and at least every two years thereafter.

4. The operation of the single entry point shall not confer on ENISA or any other authority new powers to receive, access, use or share the content of incident reports beyond those expressly provided for in the applicable Union legal act. Information submitted through the single entry point shall be shared with authorities other than the addressee authorities referred to in paragraph 2, point (b), only where the applicable Union legal act expressly provides for such

sharing.

5. Where a submission indicates that an incident affects or is likely to affect entities or services in another Member State, the single entry point may notify the CSIRTs of the Member States concerned of the existence, sector and type of the incident. The content of the submission shall be shared only in accordance with paragraph 4.

6. The single entry point shall issue to the notifying entity a timestamped acknowledgement of receipt and transmission to the addressee authorities. A reporting obligation shall be considered fulfilled through the single entry point only where the applicable information has been successfully transmitted to the authorities entitled to receive it within the applicable deadline. Where the single entry point is unavailable, entities shall be able to fulfil their reporting obligations through alternative channels made publicly available by the competent authorities. An entity shall not be considered to have infringed a reporting obligation solely as a consequence of the unavailability of the single entry point where it has used such an alternative channel within the applicable deadline.

7. ENISA shall adopt the technical, operational and organisational specifications necessary for the functioning of the single entry point in cooperation with the Commission, the CSIRTs network, the NIS Cooperation Group and the competent authorities under the Union legal acts referred to in paragraph 1, and after an appropriate public consultation. Those specifications shall ensure interoperability with existing national reporting systems through secure, open and documented interfaces.

8. The single entry point shall become operational in respect of each Union legal act referred to in paragraph 1 only after the Commission, following consultation with the relevant competent authorities

and the CSIRTs network and taking account of the independent security audit referred to in paragraph 3, point (f), has confirmed that the system is operational, interoperable, reliable and secure for the reporting obligations concerned. The Commission shall publish notice of that confirmation in the Official Journal of the European Union.

Or. en

Justification

A single entry point can substantially reduce duplicative incident reporting, provided that it does not create a central repository of sensitive cybersecurity information or alter the competences of national and sectoral authorities. The system should therefore operate through a federated architecture, reuse information already submitted, interoperate with national systems and ensure that notification content remains accessible only to the authorities legally entitled to receive it. Clear rules on successful transmission, system activation and outages are also necessary to ensure legal certainty for reporting entities.

Amendment 402

Letizia Moratti

Proposal for a regulation

Article 16 – paragraph 1 – introductory part

Text proposed by the Commission

ENISA shall develop a common Union vulnerability management service capacity and provide vulnerability management services to stakeholders by:

Amendment

“ENISA shall develop a common Union vulnerability management service capacity and provide vulnerability management services to stakeholders **“through harmonised mechanisms supporting vulnerability identification, coordination and remediation processes across relevant Union stakeholders”** by:

Or. en

Amendment 403

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 16 – paragraph 1 – introductory part

Text proposed by the Commission

ENISA shall develop a common Union vulnerability management service capacity and provide vulnerability management services *to* stakeholders *by*:

Amendment

ENISA shall develop a common Union vulnerability management service capacity and provide vulnerability management services, *on an optional basis and in support of Member States and their competent authorities and other stakeholders that request it*.

Or. fr

Amendment 404

Ondřej Krutílek

Proposal for a regulation

Article 16 – paragraph 1 – introductory part

Text proposed by the Commission

ENISA shall develop a common Union vulnerability management service capacity *and provide vulnerability management services to stakeholders by*:

Amendment

ENISA shall develop a common Union vulnerability management service capacity;

Or. en

Amendment 405

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 16 – paragraph 1 – point a

Text proposed by the Commission

(a) maintaining the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555;

Amendment

(a) maintaining the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555 *and monitoring its security*;

Or. fr

Justification

Keeping a European vulnerability database paradoxically creates another point of vulnerability: the creation of a single point of failure.

Amendment 406

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 16 – paragraph 1 – point b

Text proposed by the Commission

(b) providing vulnerability management services to stakeholders, building on the European vulnerability database and making use of relevant information available to ENISA;

Amendment

(b) providing vulnerability management services to stakeholders, ***including the prioritization and faster deployment of updates by essential and important entities by*** building on the European vulnerability database and making use of ***the tools, platforms and laboratories referred to in Article 15 or other*** relevant information available to ENISA, ***and, where relevant, by issuing technical specifications pursuant to Article 77.***

Or. en

Justification

As the number of vulnerability reports increases with AI, manufacturers must decide which flaws to fix first across product lines, while users - especially essential and important important entities - must determine which updates to deploy first, often with limited resources.

Amendment 407

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Article 16 – paragraph 1 – point b

Text proposed by the Commission

(b) providing vulnerability management services to stakeholders, building on the European vulnerability

Amendment

(b) providing vulnerability management services to stakeholders, building on the European vulnerability

database and making use of relevant information available to ENISA;

database and making use of relevant information available to ENISA, **and providing support for risk-based prioritisation and information on the exploitability of vulnerabilities;**

Or. en

Amendment 408
Ondřej Krutílek

Proposal for a regulation
Article 16 – paragraph 1 – point d

Text proposed by the Commission

(d) actively supporting the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 with regard to the management of the coordinated disclosure of vulnerabilities which may have a significant impact on entities in more than one Member State;

Amendment

(d) actively supporting, **at their request**, the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 with regard to the management of the coordinated disclosure of vulnerabilities which may have a significant impact on entities in more than one Member State;

Or. en

Amendment 409
Markéta Gregorová
on behalf of the Verts/ALE Group
Jens Geier
on behalf of the S&D Group

Proposal for a regulation
Article 16 – paragraph 1 – point e a (new)

Text proposed by the Commission

Amendment

(ea) mapping, by [12 months after the date of entry into force of this Regulation] and every two years thereafter, together with the Commission, the Member States, open-source communities and open-source software stewards within the meaning of Regulation (EU) 2024/2847, the open-source software components on

which essential and important entities within the meaning of Directive (EU) 2022/2555 depend for the provision of their services, and operating a Critical Open Source Resilience Campaign for those components, including coordinated vulnerability identification and remediation support for the stewards and maintainers concerned; ENISA shall publish the results of the mapping in machine readable form, except where publication would compromise the security of the components concerned;

Or. en

Amendment 410

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Article 16 – paragraph 1 – point e a (new)

Text proposed by the Commission

Amendment

(ea) where appropriate, identifying critical open source components used by entities in the sectors listed in Annexes I and II to Directive (EU) 2022/2555 and supporting the remediation of their vulnerabilities, including through voluntary partnerships between maintainers and supporting organisations, in cooperation with the Member States, the Commission and open source communities and building on existing Union initiatives.

Or. en

Amendment 411

Bart Groothuis, Ivars Ijabs, Anna Stürgkh, Sigrid Friis, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 16 – paragraph 1 – point e a (new)

Text proposed by the Commission

Amendment

(ea) mapping and accelerating the patching of critical open-source components, together with the Commission, Member States and open source communities.

Or. en

Justification

Reflects the EU's AI Action Plan on AI and Cybersecurity: The EU apply AI-defense where the need is most urgent. Critical open source software is the right place to act first, due to the high penetration in critical infrastructure sectors. Reportedly, 98% of the total codebase contains open source, with critical infrastructure industry averaging to about 80% of codebases with high- or critical-risk vulnerability

Amendment 412

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 16 – paragraph 1 – point e b (new)

Text proposed by the Commission

Amendment

(eb) adapting, by [12 months after the date of entry into force of this Regulation], the European vulnerability database and the methodologies referred to in point (e) to the discovery of vulnerabilities at scale by means of AI, including machine readable submission, automated triage and prioritisation and the handling of reports generated by AI systems, and providing AI assisted prioritisation, remediation and patching services to essential and important entities, free of charge to open-source software stewards, micro and small enterprises and CSIRTs.

Or. en

Amendment 413

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 16 a (new)

Text proposed by the Commission

Amendment

Article 16a

***European AI Security Evaluation
Capability***

- 1. ENISA shall establish, by [12 months after the date of entry into force of this Regulation], and operate a European AI Security Evaluation Capability ('the Capability') as a standing technical capacity for the independent evaluation of the cyber relevant capabilities and of the containment of general-purpose AI models and agentic AI systems. The Capability shall act as the hub of a European AI security evaluation network composed of ENISA, the Joint Research Centre of the Commission acting under the mandate of the AI Office, and the national bodies referred to in paragraph 2.***
- 2. Member States which have designated a national body competent for the evaluation of the safety or security of advanced AI models shall notify that body to the Commission and to ENISA within [6] months of the date of entry into force of this Regulation. The Capability shall provide evaluation coverage to Member States which have not designated such a body.***
- 3. The Capability shall: (a) at the request of the Commission, carry out or contribute to evaluations of general-purpose AI models with systemic risk pursuant to Article 92 of Regulation (EU) 2024/1689, including through experts***

appointed in accordance with Article 92(2) of that Regulation, and transmit its findings to the AI Office; (b) develop, maintain and publish Union methodologies and benchmarks for the evaluation of cyber relevant capabilities, including autonomous vulnerability discovery and exploitation, and for the containment of agentic AI systems, including compliance with instructions to cease operation, prevention of communication between AI agents through channels not authorised by the operator, resistance to the circumvention of isolation measures, control of network egress and per agent identity and logging of actions and tool calls; (c) evaluate, on its own initiative or at the request of a Member State or of the CSIRTs network, the cyber relevant capabilities and the effectiveness of the safeguards of general-purpose AI models made available on the Union market, including models whose parameters are made publicly available, and publish the results; (d) analyse AI high risk security incidents notified pursuant to Article 16c and issue advisories to the CSIRTs network and EU-CyCLONe; (e) transmit to the Commission, for the purposes of Article 99, any finding that a general-purpose AI model or an agentic AI system possesses capabilities liable to compromise the security of network and information systems of entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555; (f) represent, together with the AI Office, the technical evaluation capacity of the Union in international networks of AI safety and security institutes and coordinate the exchange of methodologies and of access to models within the network referred to in paragraph 1.

4. Evaluations shall be carried out on the basis of graduated access: remote programmatic access; access to the model without safety mitigations, where provided for under Regulation (EU) 2024/1689;

and full access on the basis of agreements with providers. Where a provider fails to cooperate with an evaluation requested pursuant to Article 92 of Regulation (EU) 2024/1689, the Commission shall, within [30] days, assess whether measures pursuant to Article 93 of that Regulation are warranted and shall inform the European Parliament and the Council of its assessment.

5. The Capability shall not carry out evaluations with network access to systems outside its evaluation environment unless the following containment measures apply: continuous human monitoring; per agent identity and logging of actions and tool calls; allow listing of network egress; and the absence of shared writable storage between AI agents. ENISA shall notify any AI high risk security incident occurring in its own evaluations in accordance with Article 16c within 72 hours.

6. The head of the Capability shall be appointed by the Executive Director after a hearing before the competent committee of the European Parliament and shall appear before that committee at least once a year. ENISA shall transmit annually to the European Parliament and to the Council a report, accompanied where necessary by a classified annex, itemising: (a) the evaluations carried out, by model and by access tier; (b) the AI high risk security incidents analysed; (c) the methodologies and benchmarks published; (d) the requests for access made to providers, and the access granted and refused.

7. Information obtained by the Capability from providers shall be used only for the purposes of this Article and of Regulation (EU) 2024/1689 and shall be subject to Articles 54 and 67.

8. The Capability shall be financed from a dedicated budget line within the contribution from the Union referred to in Article 46(3), point (a), and shall be

staffed in addition to the staff required for the other tasks of ENISA. ENISA may engage experts of the bodies referred to in paragraph 2 and of the Joint Research Centre as seconded national experts or other staff in accordance with Article 59. The Capability shall be located so as to enable daily cooperation with the AI Office, the Joint Research Centre and CERT-EU, without prejudice to Article 61. For the purposes of its evaluations, the Capability shall make use of the computing capacity of the high-performance computing infrastructure and of the AI Factories of the European High Performance Computing Joint Undertaking, in accordance with the access policy laid down pursuant to Council Regulation (EU) 2021/1173.

Or. en

Amendment 414

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 16 b (new)

Text proposed by the Commission

Amendment

Article 16b

Structured access to AI models with advanced cyber capabilities

1. The Commission shall adopt, by [9 months after the date of entry into force of this Regulation], a delegated act in accordance with Article 119 establishing a Union framework for structured access to AI models with advanced cyber capabilities for cybersecurity purposes. The framework shall lay down:

(a) the categories of entities eligible for access, including Union entities, the competent authorities and CSIRTs

designated pursuant to Directive (EU) 2022/2555, essential and important entities, providers of managed security services established in the Union, the Capability and the bodies referred to in Article 16a(2), and research organisations established in the Union;

(b) the conditions of access, including identity verification of users, phishing resistant authentication, monitoring for misuse, logging, and the purposes for which access may be used;

(c) priority rules for entities operating in sectors of high criticality within the meaning of Directive (EU) 2022/2555;

(d) contingency measures where a provider or a third country authority restricts or withdraws access, including the joint procurement of alternative capabilities, the use of the EU Cybersecurity Reserve established by Regulation (EU) 2025/38 and the use of compute capacity of the high-performance computing infrastructure and of the AI Factories of the European High Performance Computing Joint Undertaking established pursuant to Council Regulation (EU) 2021/1173;

(e) the modalities of the access of the Capability and of the bodies referred to in Article 16a(2) to models for the purposes of Article 16a. 2. ENISA shall operate the framework, maintain a register of participating providers and eligible entities, and report annually to the European Parliament and to the Council on access granted, refused, restricted and withdrawn.

3. Access by an entity to a model under the framework shall be conditional upon:

(a) the model having been evaluated in accordance with Article 16a(3), point (b), by a member of the network referred to in Article 16a(1); and (b) the commitment of the provider to notify AI high risk security incident in accordance with Article 16c and to transmit to ENISA, simultaneously with the AI Office, the information on

serious incidents notified pursuant to Article 55(1), point (c), of Regulation (EU) 2024/1689 which concerns the security of network and information systems.

4. Providers of general-purpose AI models with systemic risk which make such models available on the Union market shall grant the Capability access to those models for the purposes of Article 16a under the conditions laid down in the delegated act referred to in paragraph 1.

5. Where a provider or a third country authority restricts or withdraws access to a model on which Union entities, competent authorities or essential entities rely, the Commission shall, within 30 days, assess the impact, activate the contingency measures referred to in paragraph 1, point (d), where necessary, and inform the European Parliament and the Council.

Or. en

Amendment 415

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 16 c (new)

Text proposed by the Commission

Amendment

Article 16c

Notification of AI high risk security incident

1. Providers of general-purpose AI models with systemic risk, and any entity operating an agentic AI system in the Union or in a manner affecting network and information systems located in the Union, shall notify any AI high risk security incident without undue delay and

in any event within 24 hours of becoming aware of it.

2. The notification shall be made through the single reporting platform established pursuant to Article 16 of Regulation (EU) 2024/2847 to the CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555 of the Member State concerned and to ENISA. ENISA shall forward the notification without delay to the AI Office and, where the incident is liable to affect entities in more than one Member State, to the CSIRTs network and EU-CyCLONe.

3. Paragraph 1 shall apply irrespective of whether the AI system concerned has been placed on the market or put into service, including to AI systems operated in research, testing or evaluation environments.

4. Operators of publicly accessible online services which are used, without their authorisation, as a means of communication or coordination by AI systems may report such use through the platform referred to in paragraph 2.

5. The notifying entity shall submit a final report within one month of the notification. ENISA shall publish anonymised aggregate analyses and shall include an itemised overview of the notifications received in the report referred to in Article 16a(6).

6. The notification shall not in itself subject the notifying entity to increased liability.

7. Member States shall lay down the rules on penalties applicable to infringements of paragraph 1 by entities under their jurisdiction and shall notify those rules to the Commission by [the date of application of this Regulation]. The penalties provided for shall be effective, proportionate and dissuasive.

Or. en

Amendment 416
Markéta Gregorová
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 16 d (new)

Text proposed by the Commission

Amendment

Article 16d

Facilitation of legitimate security research

- 1. Member States and competent authorities shall ensure that the implementation of this Regulation does not impede, restrict, or create administrative or regulatory disincentives for legitimate security research carried out in good faith.***
- 2. Security research shall be deemed legitimate where it is conducted in accordance with coordinated vulnerability disclosure frameworks established pursuant to Article 12 of Directive (EU) 2022/2555 or vulnerability handling procedures under Regulation (EU) 2024/2847, provided that interaction with systems is strictly limited to what is necessary to verify and document the vulnerability and avoids deliberate operational disruption.***
- 3. Competent authorities, in cooperation with the CSIRTs designated under Directive (EU) 2022/2555, shall issue national guidance to clarify the interaction between coordinated vulnerability reporting and administrative or regulatory enforcement measures, looking to foster an environment that fosters legitimate security research.***

Or. en

Amendment 417

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 17 – paragraph 1 – point a

Text proposed by the Commission

(a) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes, managed security services and the cyber posture of entities in accordance with Article 74 and, where applicable, developing technical specifications in accordance with Article 77;

Amendment

(a) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes, managed security services and the cyber posture of entities in accordance with Article 74 and, where applicable, developing technical specifications in accordance with Article 77, ***only where no relevant harmonised standards or technical specifications developed by European standardisation bodies are available or are likely to be available within a reasonable timeframe;***

Or. fr

Amendment 418

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Article 17 – paragraph 2 – point a a (new)

Text proposed by the Commission

Amendment

(aa) the governance of the SCCG pursuant to Article 90a;

Or. en

Amendment 419

Jens Geier

Proposal for a regulation

Article 17 – paragraph 2 – point c

Text proposed by the Commission

Amendment

(c) relating to the international recognition of European cybersecurity certificates in accordance with Article 87;

(c) relating to the international recognition of European cybersecurity certificates ***and mutual recognition agreements*** in accordance with Article 87 ***while promoting high levels of cybersecurity, trustworthiness and consistency with Union law and values;***

Or. en

Amendment 420

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, András Gyürk, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 17 – paragraph 2 – point e

Text proposed by the Commission

(e) preparing model provisions to be referenced in the European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities in accordance with Article 81(5).

Amendment

(e) preparing model provisions to be referenced in the European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities in accordance with Article 81(5), ***after consulting European standardisation bodies and relevant stakeholders.***

Or. fr

Amendment 421

Jens Geier

Proposal for a regulation

Article 17 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. Certification schemes developed under this framework shall, where relevant, include requirements ensuring that ICT services handling sensitive or critical data are protected against unlawful access from third countries, actors and autonomous agents, and

remain subject to effective control within the Union. They shall also facilitate market uptake, ensure interoperability across Member States and minimise barriers to entry, in particular for SMEs.

Or. en

Amendment 422

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 17 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. When preparing a candidate European cybersecurity certification scheme, ENISA shall prioritise the use of harmonised European standards and recognised international standards. Technical specifications developed by ENISA may only be used exceptionally and as a last resort.

Or. fr

Amendment 423

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 18 – paragraph 1

Text proposed by the Commission

Amendment

1. ENISA **shall** draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting **those** technical specifications, ENISA shall **consider** existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

1. ENISA **may** draft technical specifications and **shall provide** guidance to support the implementation of Union legislation in the field of cybersecurity. **ENISA may draft technical specifications only where: (a) there is no harmonised standard covering the relevant requirements the reference of which has been published in the Official Journal of the European Union and no such**

reference is expected to be published within a reasonable period; and (b) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft or revise European standards for those requirements, and: (i) the request has not been accepted by any of the European standardisation organisations to which it was addressed; or (ii) the request has been accepted by at least one of the European standardisation organisations to which it was addressed, but the requested European standards: (1) are not delivered within the deadline set in the request; (2) do not comply with the request; or (3) do not satisfy the requirements they aim to cover. When drafting technical specifications, ENISA shall *take as their basis* existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance. *Where the reference of a harmonised standard covering the relevant requirements is subsequently published in the Official Journal of the European Union, the corresponding ENISA technical specification shall cease to be used for the purposes for which the harmonised standard provides coverage.*

Or. en

Justification

European standardisation should remain the primary route for developing technical requirements supporting Union cybersecurity legislation. ENISA technical specifications should therefore serve as a subsidiary instrument where the standardisation process cannot provide an adequate standard within a reasonable period. Where a corresponding harmonised standard subsequently becomes available, it should take precedence, avoiding parallel technical frameworks and unnecessary fragmentation.

Amendment 424
Jens Geier

Proposal for a regulation
Article 18 – paragraph 1

Text proposed by the Commission

1. ENISA shall draft ***technical specifications and*** guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Amendment

1. ENISA shall draft guidance to support the implementation of Union legislation in the field of cybersecurity. ***ENISA may draft technical specifications for that purpose where suitable European or international standards or other technical specifications are not available or appropriate and where timely action is necessary.*** When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Or. en

Amendment 425

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, András Gyürk, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation
Article 18 – paragraph 1

Text proposed by the Commission

1. ENISA shall draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Amendment

1. ***Where no relevant harmonised standards exist or are likely to be available within a reasonable timeframe,*** ENISA shall draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Or. fr

Amendment 426
Ondřej Krutílek

Proposal for a regulation
Article 18 – paragraph 1

Text proposed by the Commission

1. ENISA shall draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Amendment

1. ENISA shall, ***in consultation with Member States and other relevant stakeholders***, draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Or. en

Amendment 427
Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation
Article 18 – paragraph 1

Text proposed by the Commission

1. ENISA shall draft technical specifications ***and guidance*** to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Amendment

1. ENISA shall ***draft guidance and may*** draft technical specifications to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

Or. en

Amendment 428

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation

Article 18 – paragraph 1 – subparagraph 1 (new)

Text proposed by the Commission

Amendment

ENISA may only draft technical specifications intended for use in European cybersecurity certification schemes where one of the conditions set out in Article 77(1) is met.

Or. en

Amendment 429

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 18 – paragraph 2

Text proposed by the Commission

Amendment

2. ENISA shall monitor and, where relevant, participate and lead in standardisation development activities at Union level and, in accordance with Article 9, at international level, in view of supporting Union policies related to cybersecurity.

2. ENISA shall monitor and, where relevant, participate and lead in standardisation development activities at Union level and, in accordance with Article 9, at international level, in view of supporting Union policies related to cybersecurity, ***and shall contribute thereto in line with the competences of the European standardisation bodies.***

Or. fr

Amendment 430

Jens Geier

Proposal for a regulation

Article 18 – paragraph 2

Text proposed by the Commission

Amendment

2. ENISA shall monitor and, where relevant, participate **and lead** in standardisation development activities at Union level and, in accordance with Article 9, at international level, in view of supporting Union policies related to cybersecurity.

2. ENISA shall monitor and, where relevant, participate in standardisation development activities at Union level and, in accordance with Article 9, at international level, in view of supporting Union policies related to cybersecurity.

Or. en

Amendment 431

Katri Kulmuni, Eero Heinäluoma

**Proposal for a regulation
Article 18 – paragraph 3**

Text proposed by the Commission

Amendment

3. ***ENISA shall support the development and evaluation of cryptographic algorithms. Where a cryptographic algorithm is evaluated positively by ENISA, ENISA shall cooperate, in accordance with Regulation (EU) No 1025/2012, with the European standardisation bodies to support its standardisation.***

deleted

Or. en

Justification

This capacity requires high level competence that ENISA does not currently have. Choosing and supporting globally standardized, royalty-free PQC algorithms also in the EU-level is important. EU does not need its own PQC-algorithms, except for safeguarding high level classified information. For all other use cases, open standards should be used. PQC algorithms should be included in EU's cryptographical recommendations which would advance EU level coordination. Fragmentation should be avoided by following NIST, ISO and other relevant bodies' standard recommendations.

Amendment 432

Jens Geier

Proposal for a regulation

Article 18 – paragraph 3

Text proposed by the Commission

3. ENISA shall support the development and evaluation of cryptographic algorithms. Where a cryptographic algorithm is evaluated positively by ENISA, ENISA shall cooperate, in accordance with Regulation (EU) No 1025/2012, with the European standardisation bodies to support its standardisation.

Amendment

3. ENISA shall support the development and evaluation of cryptographic algorithms ***including support in the area of post-quantum cryptography***. Where a cryptographic algorithm is evaluated positively by ENISA, ENISA shall cooperate, in accordance with Regulation (EU) No 1025/2012, with the European standardisation bodies to support its standardisation.

Or. en

Amendment 433

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Pierre-Romain Thionnet

Proposal for a regulation

Article 18 – paragraph 5

Text proposed by the Commission

5. ENISA shall assist the Commission in the assessment of draft harmonised standards to support the implementation of Union harmonisation legislation in the field of cybersecurity.

Amendment

5. ENISA shall assist the Commission in the assessment of draft harmonised standards to support the implementation of Union harmonisation legislation in the field of cybersecurity. ***ENISA shall not participate in the assessment of harmonised standards or technical specifications where it has contributed to their drafting, development or preparation.***

Or. fr

Amendment 434

Bart Groothuis, Ivars Ijabs, Anna Stürgh, Morten Løkkegaard, Martin Hojsík, Barry Andrews

Proposal for a regulation

Article 18 – paragraph 6

Text proposed by the Commission

Amendment

6. ENISA shall promote the uptake of European **and international** standards for cybersecurity.

6. ENISA **in cooperation with the Commission** shall promote the **international** uptake of European standards for cybersecurity **by:**

(a) participating in international governmental ICT standard-setting bodies, and coordinating European input with relevant stakeholders;

(b) facilitating coordination with and support of European industry and NGO participation in international non-governmental ICT standard-setting bodies.

ENISA shall also promote the uptake of international standards within the Union.

Or. en

Justification

European representation, whether governmental or non-governmental, in international ICT standard-setting bodies is lagging behind. ENISA and the Commission should promote European standards and a coherent European position and engagement in international standard setting bodies, by facilitating coordination with member states, Industry and civil society.

Amendment 435

Katri Kulmuni, Eero Heinäluoma

Proposal for a regulation

Title II – Chapter II – Section 4

Text proposed by the Commission

Amendment

[...]

deleted

Or. en

Justification

The proposed new tasks related to the implantation of Cyber Skills Academy would require very significant resources from ENISA. Furthermore, these tasks are not based on other legislative obligations. Although there is a recognized need to increase the number of cybersecurity professionals in the Union, at the same time it remains unclear to what extent

the proposed tasks can, in practice, contribute to addressing the cybersecurity skills gap and increasing the number of professionals.

Amendment 436

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Article 19 – paragraph 3

Text proposed by the Commission

3. ENISA **may** consult stakeholders in the development and uptake of the ECSF.

Amendment

3. ENISA **shall** consult stakeholders in the development and uptake of the ECSF.

Or. en

Amendment 437

Diego Solier, Mariateresa Vivaldini

Proposal for a regulation

Article 20 – paragraph 1

Text proposed by the Commission

1. ENISA shall develop, **adopt** and maintain **European individual** cybersecurity **skills attestation schemes**. **The use of European individual** cybersecurity skills **attestation schemes** shall be voluntary for national public bodies and private entities, **unless otherwise specified by national law**.

Amendment

1. ENISA shall develop and maintain **a mapping of internationally recognised professional qualifications and training programmes for cybersecurity against the ECSF role profiles**. **ENISA shall make the mapping publicly available through the Cybersecurity Skills Academy**. **The use of the mapping** shall be voluntary for national public bodies and private entities.

Or. en

Justification

The mapping will enable employers, professionals and public authorities to compare existing certifications and training against common ECSF profiles, without establishing a new Union credential.

Amendment 438

Diego Solier, Mariateresa Vivaldini

**Proposal for a regulation
Article 20 – paragraph 2**

Text proposed by the Commission

2. Prior to initiating a new European individual cybersecurity skills attestation scheme, ENISA shall consult the Commission. ENISA shall *only adopt such a scheme following a positive opinion from the Commission. When preparing a European individual cybersecurity skills attestation scheme, ENISA may consult relevant stakeholders.*

Amendment

2. On the basis of the mapping referred to in paragraph 1, ENISA shall consult the Commission *and professional associations to identify gaps in the professional qualifications and training programmes. Based on this exercise, ENISA shall publish an assessment of the gap analysis.*

Or. en

Justification

An assessment of existing provision and labour market needs will help identify gaps that warrant further action and avoid duplicating available certifications and training.

Amendment 439

Diego Solier, Mariateresa Vivaldini

**Proposal for a regulation
Article 20 – paragraph 2 a (new)**

Text proposed by the Commission

Amendment

2a. Where the gap analysis referred to in paragraph 2 identifies gaps in existing professional qualifications or training programmes, ENISA shall invite relevant stakeholders to develop or adapt professional qualifications or training programmes for cybersecurity. Responsibility for developing and delivering qualifications or training programmes shall remain with the providers.

Or. en

Justification

ENISA may bring relevant providers together to address identified gaps. The development and operation of certifications and training will remain the responsibility of those providers.

Amendment 440

Jens Geier

Proposal for a regulation

Article 20 – paragraph 3 – point c

Text proposed by the Commission

(c) market uptake analysis specific to each attestation scheme;

Amendment

(c) market uptake analysis specific to each attestation scheme, ***including its accessibility, relevance for SMEs, contribution to addressing cybersecurity skills shortages, and impact on cross-border recognition of cybersecurity skills within the internal market ;***

Or. en

Amendment 441

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Pierre-Romain Thionnet

Proposal for a regulation

Article 20 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. European individual cybersecurity skills attestation schemes shall build on existing national frameworks and take into account national qualifications and assessments meeting equivalent requirements, without prejudice to the maintenance of more demanding national arrangements.

Or. fr

Amendment 442

Jens Geier

Proposal for a regulation
Article 21 – paragraph 1

Text proposed by the Commission

1. Authorised attestation providers shall assess whether individuals meet the requirements of a European individual cybersecurity skills attestation scheme and, where those requirements are met, issue European individual cybersecurity skills attestations. Attestation providers may hold several authorisations, each granted for one European individual cybersecurity skills attestation scheme.

Amendment

1. Authorised attestation providers shall assess whether individuals meet the requirements of a European individual cybersecurity skills attestation scheme and, where those requirements are met, issue European individual cybersecurity skills attestations. Attestation providers may hold several authorisations, each granted for one European individual cybersecurity skills attestation scheme ***and may cover one or more proficiency levels defined under that scheme. They shall be able to operate across the Union.***

Or. en

Amendment 443
Jens Geier

Proposal for a regulation
Article 21 – paragraph 2

Text proposed by the Commission

2. ENISA shall provide guidance to and conduct obligatory training of assessors regarding the requirements and assessment methods included in the European individual cybersecurity skills attestation scheme as referred to in Article 20(3), point (b).

Amendment

2. ENISA shall provide ***regular*** guidance to and conduct obligatory training of assessors regarding the requirements and assessment methods included in the European individual cybersecurity skills attestation scheme as referred to in Article 20(3), point (b).

Or. en

Amendment 444
Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Pierre-Romain Thionnet

Proposal for a regulation
Article 21 – paragraph 3 – subparagraph 1 – introductory part

Text proposed by the Commission

Entities wishing to become authorised attestation providers or renew their authorisation ('applicants') shall submit an application to **ENISA**. They shall meet the following requirements:

Amendment

Entities wishing to become authorised attestation providers or renew their authorisation ('applicants') shall submit an application to ***the competent authority of the Member State in which they are established***. They shall meet the following requirements:

Or. fr

Amendment 445

Jens Geier

Proposal for a regulation

Article 21 – paragraph 4

Text proposed by the Commission

4. Applicants shall not be high-risk suppliers.

Amendment

4. Applicants shall not be high-risk suppliers ***nor entities referred to in Article 2, point (39a)***.

Or. en

Amendment 446

Marc Botenga

on behalf of The Left Group

Proposal for a regulation

Article 21 – paragraph 7

Text proposed by the Commission

7. Authorised attestation providers may request a fee from individuals for assessing and issuing the European individual cybersecurity skills attestations, taking into account the indicative cost of a European individual cybersecurity skills attestation pursuant to Article 20(4) and made public on a dedicated website in accordance with Article 23, point (d).

Amendment

7. Authorised attestation providers may request a fee from individuals for assessing and issuing the European individual cybersecurity skills attestations, taking into account the indicative cost of a European individual cybersecurity skills attestation pursuant to Article 20(4) and made public on a dedicated website in accordance with Article 23, point (d). ***Where an attestation is required by an***

employer, by national law or by collective agreement, nothing in this Regulation shall be interpreted as requiring the individual to bear the cost.

Or. en

Amendment 447

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Pierre-Romain Thionnet

**Proposal for a regulation
Article 22**

Text proposed by the Commission

Amendment

Article 22

deleted

Examination of applications to become an authorised attestation provider and maintenance of authorisations

1. Applicants shall pay a fee to ENISA for the examination of their application. Authorised attestation providers shall pay a fee to ENISA for the maintenance of their authorisation.

2. ENISA shall evaluate whether the requirements laid down in Article 21(3) and (4) and the obligations laid down in Article 21(5) are met or continue to be met by applicants and authorised attestation providers.

3.

After examining an application against the requirements laid down in Article 21(3) and (4), ENISA may issue one of the following decisions:

(a) granting the applicant the status of authorised attestation provider or renewing it;

(b) rejecting the application to become an authorised attestation provider or not renewing it;

(c) closing the processing of the application due to the applicant's inaction

following a request for additional information by ENISA.

ENISA may amend, suspend or revoke such decisions based on its evaluation pursuant to Article 22(2) or in the case referred to in Article 21(6).

4. ENISA shall issue the decision referred to in paragraph 3 within three months from the date of submission of an application in accordance with Article 21(3). Where ENISA requested the applicant for the additional information, ENISA shall issue the decision referred to in paragraph 3 within one month of receiving additional information.

5. The decision referred to in paragraph 3, point (a) shall have a maximum duration of three years and indicate the fee related to the yearly maintenance of the authorisation.

6. ENISA shall ensure that its activities relating to the development and adoption of European individual cybersecurity skills attestation schemes as laid down in Article 20 are strictly separated and carried out independently from the activities on the examination of applications and on evaluations set out in paragraphs 2 and 3 of this Article.

Or. fr

Amendment 448

Krzysztof Hetman, Mirosława Nykiel, Adam Jarubas, Kamila Gasiuk-Pihowicz, Borys Budka

Proposal for a regulation

Article 24 – paragraph 1 – point f a (new)

Text proposed by the Commission

Amendment

(fa) National Liaison Officers Network.

Or. en

Amendment 449

Marc Botenga

on behalf of The Left Group

Proposal for a regulation

Article 25 – paragraph 1

Text proposed by the Commission

1. The Management Board shall be composed of one member ***appointed by*** each Member State ***and*** two members appointed by the ***Commission***. All members shall have the right to vote.

Amendment

1. The Management Board shall be composed of:

(a) one member ***from*** each Member State;

(b) two members ***representing the Commission***;

(c) ***one independent expert*** appointed by the ***European Parliament***;

(d) ***two members representing trade unions cross-industry at Union level***;

(e) ***three representatives from recognised Union-level non-governmental organisations active in the field of cybersecurity, respectively from digital rights and civil liberties organisations, consumer protection organisations and civil society organisations working on cybersecurity and democracy***

All members shall have the right to vote.

Or. en

Amendment 450

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

Proposal for a regulation

Article 25 – paragraph 1

Text proposed by the Commission

1. The Management Board shall be

Amendment

1. The Management Board shall be

composed of one member appointed by each Member State and **two members** appointed by the Commission. All members shall have the right to vote.

composed of one member appointed by each Member State and **one member** appointed by the Commission. All members **appointed by a Member State** shall have the right to vote.

Or. fr

Amendment 451

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Article 25 – paragraph 3

Text proposed by the Commission

3. Each Member State shall appoint ***the head of a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555*** as the member of the Management Board. ***Where this proves not to be feasible, Member States shall appoint a high-level representative of a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as the member of the Management Board.***

Amendment

3. Each Member State shall appoint as the member of the Management Board ***a representative with appropriate professional expertise and experience and with authority to take strategic decisions on cybersecurity, where possible the head of a national cybersecurity authority or of a competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555.***

Or. en

Amendment 452

Markus Buchheit

Proposal for a regulation

Article 25 – paragraph 4

Text proposed by the Commission

4. Members appointed by the Commission and alternate members of the Management Board shall be appointed in light of their knowledge in the field of cybersecurity, taking into account their relevant managerial, administrative and budgetary skills. The Commission and the

Amendment

4. Members appointed by the Commission and alternate members of the Management Board shall be appointed in light of their knowledge in the field of cybersecurity, taking into account their relevant managerial, administrative and budgetary skills. The Commission and the

Member States *as regards alternates, shall aim to achieve a balanced representation between men and women on the Management Board and* shall make efforts to limit their turnover in order to ensure continuity of the Management Board's work.

Member States shall make efforts to limit their turnover, in order to ensure continuity of the Management Board's work.

Or. de

Amendment 453

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation Article 25 – paragraph 5

Text proposed by the Commission

Amendment

5. *The term of office of the members appointed by Member States shall be equal to the term of their function referred to in paragraph 3.* **deleted**

Or. en

Amendment 454

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Pilar del Castillo Vera

Proposal for a regulation Article 25 – paragraph 6

Text proposed by the Commission

Amendment

6. The term of office *of the alternates and* of the members appointed by the Commission shall be four years. That term shall be renewable.

6. The term of office of the members appointed by the *Member States and by the Commission, and of the alternates,* shall be four years. That term shall be renewable.

Or. en

Amendment 455

Aleksandar Nikolic, Mélanie Disdier, Julie Rechagneux, Christophe Bay, Majbritt Birkholm, Pierre-Romain Thionnet

**Proposal for a regulation
Article 26 – paragraph 1 a (new)**

Text proposed by the Commission

Amendment

1a. The Chairperson and the Deputy Chairperson shall not be representatives of the Commission.

Or. fr

Amendment 456
Markéta Gregorová
on behalf of the Verts/ALE Group

**Proposal for a regulation
Article 28 – paragraph 1 – point m**

Text proposed by the Commission

Amendment

(m) appoint the Executive Director and, ***if it decides to create the function of a Deputy Executive Director***, the Deputy Executive Director, and where relevant extend their term of office or remove them from office in accordance with Article 31;

(m) appoint the Executive Director and the Deputy Executive Director, and where relevant extend their term of office or remove them from office in accordance with Article 31;

Or. en

Amendment 457
Markus Buchheit

**Proposal for a regulation
Article 30 – paragraph 3**

Text proposed by the Commission

Amendment

3. The Executive Board shall be composed of the Chairperson of the Management Board, one representative of the Commission to the Management Board, and three other members appointed by the Management Board from among its

3. The Executive Board shall be composed of the Chairperson of the Management Board, one representative of the Commission to the Management Board, and three other members appointed by the Management Board from among its

members with the right to vote. The Chairperson of the Management Board shall also be the Chairperson of the Executive Board. The ***appointments of the*** members of the Executive Board shall ***aim to ensure gender balance*** on the ***Executive Board***. The Executive Director shall take part in the meetings of the Executive Board without the right to vote.

members with the right to vote. The Chairperson of the Management Board shall also be the Chairperson of the Executive Board. The members of the Executive Board shall ***be appointed*** on the ***basis of their professional competence***. The Executive Director shall take part in the meetings of the Executive Board without the right to vote.

Or. de

Amendment 458

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation Article 32 – paragraph 3

Text proposed by the Commission

3. The Executive Director shall report to the European Parliament on the performance of their tasks ***when*** invited to do so. The Council may invite the Executive Director to report on the performance of their tasks.

Amendment

3. The Executive Director shall report to the European Parliament on the performance of their tasks ***at least once a year and whenever*** invited to do so. The Council may invite the Executive Director to report on the performance of their tasks.

Or. en

Amendment 459

Markus Buchheit

Proposal for a regulation Article 32 – paragraph 5 – point o

Text proposed by the Commission

(o) ***promote diversity and gender balance in*** the recruitment of ENISA's staff;

Amendment

(o) ***ensure that*** the recruitment of ENISA's staff ***is based solely on ability, efficiency and integrity, also taking into account an appropriate geographical balance between Member States;***

Or. de

Amendment 460

Markéta Gregorová

on behalf of the Verts/ALE Group

Jens Geier

on behalf of the S&D Group

Proposal for a regulation

Article 32 – paragraph 5 – point q a (new)

Text proposed by the Commission

Amendment

(qa) ensure the administrative, technical, human and infrastructure resources required for the operational continuity and security of the EU Cybersecurity Testbed referred to in Article 6, point (16);

Or. en

Amendment 461

Tomas Tobé, Christian Ehler, Aura Salla, Jörgen Warborn, Andrea Wechsler, Dimitris Tsiodras, Pilar del Castillo Vera

Proposal for a regulation

Article 32 – paragraph 6

Text proposed by the Commission

Amendment

6. Where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities. The Executive Director shall inform the Management Board in advance thereof. The procedures regarding in particular the composition of the working groups, the appointment of the experts of the working groups by the Executive Director and the operation of the working groups shall be specified in ENISA's internal rules of operation.

6. Where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities **as well as the private sector and the research community**. The Executive Director shall inform the Management Board in advance thereof. The procedures regarding in particular the composition of the working groups, the appointment of the experts of the working groups by the Executive Director and the operation of the working groups shall be specified in ENISA's internal rules of operation.

Amendment 462

Markéta Gregorová

on behalf of the Verts/ALE Group

Proposal for a regulation

Article 32 – paragraph 7

Text proposed by the Commission

7. Where necessary for the purpose of carrying out ENISA's tasks in an efficient and effective manner and based on an appropriate cost-benefit analysis, the Executive Director may decide to establish one or more local offices in one or more Member States. Before deciding to establish a local office, the Executive Director shall seek the opinion of the Member States concerned, including the Member State in which the seat of ENISA is located, and shall obtain the prior ***consent of the Commission and the Management Board. In cases of disagreement during the consultation process between the Executive Director and the Member States concerned, the issue shall be brought to the Council for discussion. The aggregate number of staff in all local offices shall be kept to a minimum and shall not exceed 40% of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The number of the staff in each local office shall not exceed 10% of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.***

Amendment

7. Where necessary for the purpose of carrying out ENISA's tasks in an efficient and effective manner and based on an appropriate cost-benefit analysis, the Executive Director may decide to establish one or more local offices in one or more Member States. Before deciding to establish a local office, the Executive Director shall seek the opinion of the Member States concerned, including the Member State in which the seat of ENISA is located, and shall obtain the prior ***approval of the Management Board. The Commission shall be informed without delay of any decision to establish a local office.***

Amendment 463

Markéta Gregorová

on behalf of the Verts/ALE Group

Proposal for a regulation
Article 32 – paragraph 7 a (new)

Text proposed by the Commission

Amendment

7a. Staff of ENISA may be located at the seat of ENISA, in the local offices established pursuant to paragraph 7 or, where necessary for the performance of ENISA's tasks, at any other location in a Member State, including on a temporary basis and including at the premises of Union entities with which ENISA cooperates. No quantitative limit shall apply to the distribution of ENISA's staff between the seat and other locations. This paragraph concerns the determination of the place of employment within the meaning of the Staff Regulations and the Conditions of Employment. It is without prejudice to those acts and to the rules on working time, part time work and teleworking adopted pursuant to Article 110 thereof, and without prejudice to the location of the seat of ENISA.

Or. en

Amendment 464
Markéta Gregorová
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 33 – paragraph 2

Text proposed by the Commission

Amendment

2. Where the Management Board decides to create a function of a Deputy Executive Director, the provisions of Article 31 shall apply to the Deputy Executive Director accordingly.

2. If the Executive Director is absent or indisposed, or the post is vacant, based on prior decision of the Administrative Board, the Deputy Executive Director may be empowered to perform the respective tasks in addition to those assigned according to paragraph 3.

Or. en

