BRIEFING
EU Legislation in Progress

Managed security services

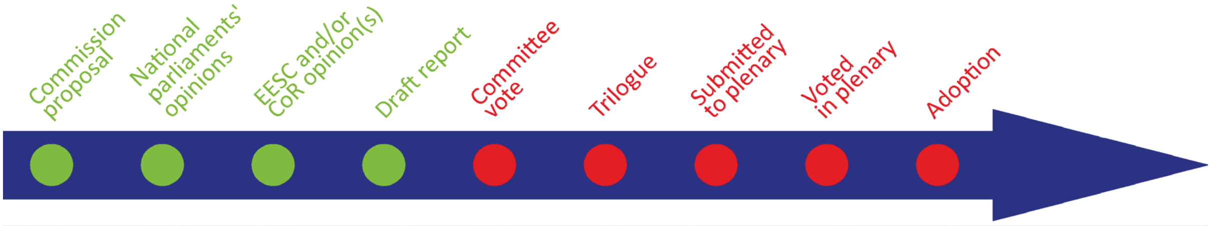
OVERVIEW

Managed security services are services carrying out or providing assistance for activities relating to customers' cybersecurity risk management. They are gaining increasing importance in the prevention and mitigation of cybersecurity incidents. Yet they were not included in the scope of the EU cybersecurity certification framework within the Cybersecurity Act from 2019. As some Member States have begun adopting certification schemes for managed security services that are divergent or inconsistent, there is a need to avoid fragmentation in the internal market. The present proposal therefore includes targeted amendments to the scope of the Cybersecurity Act, seeking to enable managed security services schemes by means of Commission implementing acts.

In Parliament, the file has been assigned to the Committee on Industry, Research and Energy (ITRE), where the rapporteur published her report on 7 September 2023. The amendments tabled in the ITRE committee were published on 21 September 2023. The vote in committee is scheduled for 25 October 2023.

Regulation amending Regulation (EU) 2019/881 as regards managed security services

Committee responsible:	Industry, Research and Energy (ITRE)	COM(2023)0208 18.4.2023
Rapporteur:	Josianne Cutajar (S&D, Malta)	2023/0108(COD)
Shadow rapporteurs:	Angelika Niebler (EPP, Germany) Bart Groothuis (Renew, the Netherlands) Ville Niinistö (Greens/EFA, Finland) Evzen Tošenovský (ECR, Czechia)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Vote in committee on draft report	



EPRS | European Parliamentary Research Service

Author: Mar Negreiro
Members' Research Service

PE 754.556 – October 2023

EN

Introduction

Cybersecurity attacks are on the rise. It is estimated that ransomware attacks hit organisations every 11 seconds around the globe. Cybersecurity Ventures predicts that the general global cost of cybercrime (e.g. ransomware, malware and cryptocrime) will reach US$10.5 trillion annually by 2025. The latest ENISA report on the threat landscape in the EU revealed that 10 terabytes of data are stolen every month. Ransomware scored highest on the list of cyber-attacks in the EU, followed closely by distributed denial of service attacks (DDoS). For instance, the largest DDoS attack ever was launched in Europe in July 2022. These attacks are getting larger and more complex, with mobile networks and the internet of things (IoT) now being used in cyberwarfare. ENISA's report further reveals that all sectors are under threat, including the health sector, with public administration, online service providers and the general public being most exposed to cyberthreats. According to a Eurobarometer survey, the majority of citizens believe that there is a growing risk of falling victim to cybercrime, through personal data abuse or theft, malicious software or phishing.

Cyber-attacks, besides being among the fastest-growing form of crime worldwide, are also growing in scale, cost and sophistication. According to Cybersecurity Ventures, ransomware alone will cost its victims around US$265 billion annually by 2031, with a new attack (on a consumer or business) every 2 seconds. As a result, businesses have to invest more money to make cyberspace safer for themselves and their customers. Not only businesses but also citizens and entire countries have been affected by cyber-attacks. The first known cyber-attack on a country was mounted on Estonia in April 2007, affecting the online services of banks, media outlets and government bodies for weeks. Since then, many other countries have suffered cyber-attacks, including on critical infrastructure, such as on electric power systems, hospitals and water plants.

Given the growing number and cost of cyber-attacks, spending on information security is also increasing worldwide. Critical sectors, such as transport, energy, health and finance, have become increasingly dependent on digital technologies to run their core business. While growing digital connectivity brings enormous opportunities, it also exposes economies and societies to cyberthreats. As the number, complexity and scale of cybersecurity incidents grows, so does their economic and social impact.

The growing challenges in the cybersecurity landscape have led the EU to reflect on how to enhance the protection of its citizens and companies against cyberthreats and attacks.

Existing situation

Cybersecurity is one of the EU's top priorities for a digital and connected Europe, as stated in the Commission's EU cybersecurity strategy for the digital decade and the EU cybersecurity strategy for 2020 to 2025. It is also in line with the EU's priorities to create a Europe fit for the digital age in which digital transformation will benefit both people and businesses. The cybersecurity strategy acknowledges that improving cybersecurity is essential in order both to benefit from innovation, connectivity and automation and safeguard fundamental rights and freedoms (e.g. protection of personal data and freedom of expression). The existing EU cybersecurity framework comprises several pieces of legislation that cover specific aspects of cybersecurity from different angles.

The Directive on Security of Network and Information Systems across the EU (NIS Directive) entered into force in 2016, bringing in horizontal legal measures to boost the overall level of cybersecurity in the EU, with a focus on protecting critical infrastructure. The threat landscape has changed considerably since the NIS Directive came into force in 2016, and the scope of the directive needed updating and expanding to meet current risks and future challenges such as ensuring that 5G technology is secure. In addition, its transposition and implementation brought to light inherent flaws in certain provisions and approaches. Thus, the NIS Directive has been replaced by the recently adopted Directive on the Security of Network and Information Systems (NIS2), which tackles its predecessor's limitations and needs to be transposed into national law by 17 October 2024. In addition, sectoral legislation, such as the Directive on the Resilience of Critical Entities (CER) and the Regulation on Operational Resilience of the Financial Sector (DORA) set specific security and reporting requirements in their fields.

As far as information and communication technology (ICT) products, services and processes are concerned, back in 2019 the EU Cybersecurity Act strengthened the powers of the European Union Agency for Cybersecurity (ENISA) and introduced the cybersecurity certification framework for the creation of voluntary certification schemes to apply to the cybersecurity features of an ICT product, service or process.[1] Although the schemes remain voluntary for businesses, they could be used for compliance with the mandatory safety requirements of other legal acts, for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

The joint communication 'EU Policy on Cyber Defence' adopted by the Commission and the High Representative on 10 November 2022, announced that the Commission would explore the development of EU-level cybersecurity certification schemes for the cybersecurity industry and private companies. It would also explore other actions, such as the EU cyber-solidarity initiative to support the gradual setting-up of an EU-level cyber reserve with services from trusted private providers to strengthen preparedness and response actions across the EU.

Parliament's starting position

In its 10 June 2021 resolution, the Parliament called for security by design and cyber-resilience for all internet-connected products along the entire supply chain. More specifically, Parliament welcomed the 'Commission's plans to propose horizontal legislation on cybersecurity requirements, with a view to harmonising national laws and preventing fragmentation of the single market.

Council starting position

In its conclusions of 2 December 2020, the Council acknowledged the increased cybersecurity risks for connected devices. Furthermore, it expressed the need to minimise cybersecurity risks to protect consumers as well as to increase the EU's cyber-resilience to foster competitiveness and innovation.

In its conclusions of 23 May 2022 the Council called upon the Commission to propose common EU cybersecurity proposal for EU cybersecurity emergency response mechanisms and processes and called for an increase in the overall level of cybersecurity in the EU by facilitating the emergence and development of trusted cybersecurity service providers.

Preparation of the proposal

Given its limited scope, the Commission did not conduct any preparatory studies, impact assessments or public consultations in advance of the proposal. It did however carry out targeted consultations with Member States and ENISA. As stated in the proposal, Member States described their current activities and views regarding certification of managed security services. While ENISA explained its views and its findings from discussions with Member States and stakeholders. The comments and information received from Member States and ENISA have fed into the proposal.

The changes the proposal would bring

The proposal contains two articles: Article 1 contains the amendments to the Cybersecurity Act regulation while Article 2 concerns the entry into force.

Article 1 contains targeted amendments to amend the scope of the European cybersecurity certification framework in the Cybersecurity Act to include 'managed security services'. It introduces a definition of those services, which is very closely aligned to the definition of 'managed security services providers' under the NIS 2 Directive. It also adds a new article 51(a) on the security objectives of EU cybersecurity certification adapted to 'managed security services'. Lastly, the proposal contains a number of technical amendments to ensure that the relevant articles apply also to 'managed security services'.

The proposed targeted amendments to the scope of the European cybersecurity certification framework in the Cybersecurity Act seek to enable the adoption of European cybersecurity certification schemes for 'managed security services' by means of Commission implementing acts. Therefore, 'managed security services' will be covered by the EU certification framework along with information and communication technology (ICT) products, ICT services and ICT processes, that were already covered under the Cybersecurity Act adopted in 2019.

This proposal aims to prevent fragmentation in the single market, as some Member States have already begun adopting certification schemes for managed security services that are divergent or inconsistent.

Managed security services are services carrying out or providing assistance for activities relating to customers' cybersecurity risk management. They are gaining increasing importance in the prevention and mitigation of cybersecurity incidents. Managed security service providers in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in helping entities prevent, detect, respond to or recover from incidents. They have, however, also themselves been the target of cyberattacks. In addition, they pose a particular risk because of their close integration in the operations of their customers to ensure cybersecurity.

Accordingly, the providers of managed security services are considered as 'essential or important entities' belonging to a sector of high criticality pursuant to the NIS2 Directive.

Managed security services providers will also play an important role in the EU-level cybersecurity reserve, the gradual setting-up of which is supported by the cyber solidarity act proposal, tabled in parallel to the present proposed regulation. An EU-level cybersecurity reserve[2] is envisaged, to be used to support response and immediate recovery actions in the event of significant and large-scale cybersecurity incidents. The relevant cybersecurity services provided by 'trusted providers' referred to in the cyber solidarity act, correspond to the 'managed security services' in the proposal for a regulation amending Regulation (EU) 2019/881 as regards managed security services.

The provisions to be amended by the proposal will be evaluated as part of the periodic evaluation of the Cybersecurity Act to be carried out by the Commission.[3]

Advisory committees

The European Economic and Social Committee (EESC) opinion of 14 July 2023 emphasises the concerns that, 4 years after the adoption of the EU Cybersecurity Act, no cybersecurity scheme has yet been adopted by the European Commission through implementing acts and no product has yet been cyber-certified. The EESC argues that the EU's sectoral agencies should be involved in the process of developing EU cybersecurity schemes and a minimum EU standard should be adopted, in cooperation with the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI), including for internet of people (IoP) devices and the IoT.

The EESC emphasises the vital need to procure only Europe-based technology for equipping EU cyber shield members. It is 'in the EU's strategic interest to ensure that the Union retains and develops the essential capacities to secure its digital economy, society and democracy, to achieve full digital sovereignty as the only way to protect critical technologies, and to provide effective key cybersecurity services'.

The Committee of the Regions has yet to submit an opinion on this initiative.

National parliaments

The subsidiarity deadline for national parliament was 21 July 2023. Eleven Member States started or concluded contributions, with the Czech Chamber of Deputies and the Portuguese Assembleia da República issuing opinions on the proposal.

The Czech Chamber of Deputies questions mainly the cyber solidarity act proposal, with its provision to exchange sensitive information concerning national security at EU level, as well as subsidiarity compliance.

Stakeholder views[4]

Given its limited scope, the Commission did not hold a public consultation of stakeholders in advance of the proposal and there are no major reactions or position papers about it.

Legislative process

In Parliament, the file has been assigned to the Committee on Industry, Research and Energy (ITRE) and Josiane Cutajar (S&D, Malta) has been appointed as rapporteur. The Committees on Internal Market and Consumer Protection (IMCO) and on Civil Liberties, Justice and Home Affairs (LIBE) have been asked for their opinions. IMCO published its specific opinion on 21 September 2023, stressing that the certification of managed security services is essential for building trust in the quality of those services and achieving a high level of consumer protection. It recommends requiring managed security service providers to adhere to relevant cybersecurity standards. It also calls for the introduction of a voluntary EU trust label for certified ICT products and a specific funding instrument for a cybersecurity research and development programme. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) decided not to provide an opinion.

The rapporteur published her report on 7 September 2023 and presented it during the ITRE committee meeting on 18 September 2023. The rapporteur supports the Commission proposal to prevent individual Member States from continuing to adopt different certification schemes for managed security services so as to avoid fragmentation and further divergences. She seeks complementarity between the proposal for a regulation amending Regulation (EU) 2019/881 as regards managed security services and the cyber solidarity act proposal, to allow for managed security services (i.e. 'trusted providers' in the cyber solidarity act) to play an important role in the future EU cybersecurity reserve.

In her report, Cutajar seeks to clarify the definition of managed security services and their scope. In addition, she places a stronger emphasis on addressing the skills gap and helping SMEs to get the financial support they need to address such challenges.

The amendments tabled in the ITRE committee were published on 21 September 2023. The committee is expected to vote on the draft report on 25 October 2023.

Work at the Council has started and is ongoing.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Car P. and De Luca S., EU cyber-resilience act, EPRS, European Parliament, May 2023.

Madiega T., Artificial intelligence act, EPRS, European Parliament, June 2023.

Negreiro M., The NIS2: A high common level of cybersecurity in the EU, EPRS, European Parliament, February 2023.

Negreiro M., ENISA and a new cybersecurity act, EPRS, European Parliament, July 2019.

Vikolainen V., Strengthening cyber resilience, Initial appraisal of a European Commission impact assessment, EPRS, December 2022.

OTHER SOURCES

European Parliament, Managed security services 2023/0108(COD), Legislative Observatory (OEIL).

ENDNOTES

[1] It should be noted that no EU cybersecurity certification scheme has been published yet since the Cybersecurity Act was adopted in 2019.

[2] The EU-level cybersecurity reserve should, inter alia, take into account whether those providers have obtained EU or national cybersecurity certification. Future certification schemes for managed security services will thus play a significant role in the implementation of the cyber solidarity act.

[3] In accordance with Article 67 of that act.

[4] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2023.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

First edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.