BRIEFING

EU Legislation in Progress

High common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

OVERVIEW

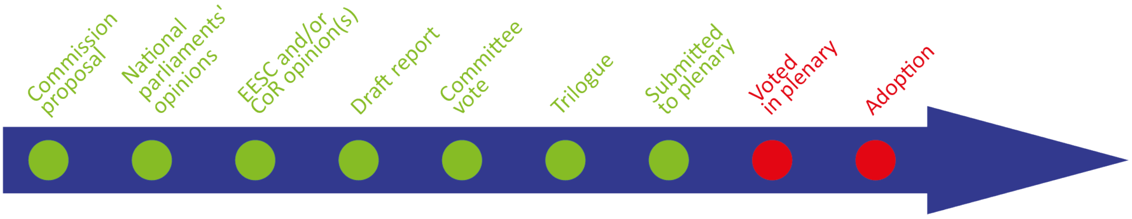
The digital transformation is making the EU institutions and administration more vulnerable to cyber-threats and incidents. Their number has surged dramatically in recent years: there were as many incidents during the first half of 2021 as in the whole of 2020, for instance. Yet an analysis of 20 Union institutions, bodies and agencies showed that their governance, preparedness, cybersecurity capability and maturity vary substantially, weakening the system.

This proposal for a regulation would establish a common framework to ensure that similar cybersecurity rules and measures are applied within all Union institutions, bodies, offices and agencies, to improve their resilience and incident-response capacities and rapidly improve the existing situation.

In the European Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE). The report was adopted unanimously in the ITRE meeting on 9 March 2023. The committee's decision to enter into interinstitutional negotiations was confirmed by the plenary on 15 March 2023. A provisional agreement was reached during the trilogue on 26 June 2023. ITRE confirmed the political agreement at its meeting on 18 September 2023 and Parliament is expected to adopt the text as agreed during its plenary session in November 2023.

Proposal for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

Committee responsible:	Industry, Research and Energy (ITRE)	COM(2022)0122 22.3.2022
Rapporteur:	Henna Virkkunen (EPP, Finland)	2022/0085(COD)
Shadow rapporteurs:	Miapetra Kumpula-Natri (S&D, Finland) Izaskun Bilbao Barandica (Renew, Spain) Mikuláš Peksa (Greens/EFA, Czechia) Evžen Tošenovský (ECR, Czechia) Markus Buchheit (ID, Germany) Marc Botenga (The Left, Belgium)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Vote in plenary	



EPRS | European Parliamentary Research Service

Author: Mar Negreiro
Members' Research Service

PE 733.625 – October 2023

EN

Introduction

While growing digital connectivity brings enormous opportunities, it also exposes economies and societies to cyber-threats, and cybersecurity issues are becoming a day-to-day struggle in the EU. Cyber-attacks, besides being among the fastest-growing form of crime worldwide, are also growing in scale, cost and sophistication. The annual cost of cybercrime to the global economy in 2020 was estimated at €5.5 trillion, double the figure for 2015. In a 2019 Eurobarometer survey, three quarters (76 %) of respondents believed that they were facing a growing risk of falling victim to cybercrime. According to monitoring reports from the EU Agency for Network Information Security (ENISA), cybercrime is becoming increasingly monetised, particularly in the case of major cyber-attacks that use ransomware. Increased e-commerce and cashless payments are meanwhile bringing heightened risks of cybercrime attacks and cybersecurity breaches. With payments becoming increasingly cashless, online theft – of money and also of personal data – has been on the rise. Moreover, critical sectors, such as transport, energy, health and finance, and also public sector agencies and governments are under threat. Another major source of concern are supply chain attacks, such as the 2020 SolarWinds Hack. In that instance, a sophisticated hack into software at source enabled cyber-attackers to spy – undiscovered for nine months – on users of the software, including private companies and the US government.

These problems have been exacerbated by the pandemic, which triggered an unprecedented rise in malicious cyber-activity. The war in Ukraine meanwhile has generated more hybrid threats. As a result, the EU is exploring the need to adopt additional measures in the field of global technology politics to counter Chinese and Russian influence in the technology realm.

Evolving digital technology and the increased complexity and interconnectedness of digital systems are amplifying cybersecurity risks, and the EU institutions, bodies and agencies (EUIBAs) are not immune; they have experienced a dramatic surge in cyber threats and incidents. For instance, in the first half of 2021 alone, there were as many cyber-attacks on Union institutions as in the whole of 2020. Despite this, an analysis of 20 EU institutions, bodies and agencies has shown that their governance, cyber-hygiene, overall capability and maturity vary enormously. As they are all closely interconnected, weaknesses in one can expose others to security threats and espionage.

Existing situation

In this context, in 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy put forward a new EU 'cybersecurity strategy for the digital decade', which included a reinforced cybersecurity framework. The strategy was in line with the Commission's priorities to make Europe fit for the digital age and achieve the digital decade targets. The pandemic has more than confirmed the importance of preparing the EU for the digital decade, as well as the need to continually improve cyber-resilience, particularly for those who operate essential services such as public sector entities, healthcare and energy grids.

The reinforced cybersecurity framework includes a review of the Directive on the Security of Network and Information Systems (NIS Directive)[1] and the implementation of the Cybersecurity Act, to improve the EU's operational capacity at ENISA.

The strategy also announced the establishment of 'new horizontal rules' for connected products and associated services placed on the internal market. This would be included in the proposed cyber-resilience act, subsequently released in September 2022.

Similarly, funding for EU cybersecurity initiatives has increased in the 2021-2027 programming period through a mix of instruments, such as the Digital Europe programme, Horizon Europe, the European Defence Fund, and the EU Recovery and Resilience Facility. The objective is to reach up to €4.5 billion of combined investment, to be allocated notably to SMEs under the recently established Cybersecurity Competence Centre and network of national coordination centres.

When it comes to protecting the EUIBAs, the Computer Emergency Response Team (CERT-EU) established a decade ago and ENISA are the two main entities tasked with offering them cybersecurity support.[2] Although independent in its operations, CERT-EU remains a task force, with no legal personality. It is administratively placed within the European Commission (DG DIGIT), from which it receives logistical and administrative support. CERT-EU's aim is to make the EUIBAs' information and communications technology (ICT) infrastructure more secure, by enhancing their capacity to deal with cyber-threats and vulnerabilities, and so enable them to prevent, detect and respond to cyber-attacks. CERT-EU has around 40 staff organised in teams of specialists focusing, for example, on cyber-threat intelligence, digital forensics and incident response. In 2020, CERT-EU's steering board set a new strategic aim for the task force, of guaranteeing a comprehensive level of cyber-defence for all EUIBAs, given the increase in threats. The strategic aim also includes broad-spectrum security operations centres (SOCs) that monitor networks, and non-stop monitoring for high-severity threats. CERT-EU supports the information technology (IT) security teams of the larger EUIBAs, including with first-line 24/7 monitoring. For smaller and medium-sized EUIBAs, CERT-EU provides all the related services.

Parliament's starting position

On 10 June 2021, the European Parliament adopted a resolution on the EU's cybersecurity strategy for the digital decade, in which it called for EU-funded digitalisation projects to include cybersecurity requirements. It also welcomed support for research and innovation, especially in disruptive technologies (such as quantum computing and quantum cryptography), and called for further research into post-quantum algorithms as a standard for cybersecurity.

On 9 March 2022, the Parliament's plenary called for new counter- and deterrence measures to ensure cybersecurity and resilience against cyber-attacks.

Council starting position

On 24 January 2022, the Council of the EU called on the Commission to strengthen the EU's resilience and ability to fight back against cyber-attacks.

In its conclusions of 22 March 2021 on the EU's cybersecurity strategy for the digital decade, the Council stressed that cybersecurity is vital for the functioning of the public administration and institutions, at both national and EU levels, and for the EU's society and economy.

In its conclusions of 2 December 2020 on the security of connected devices, the Council encouraged the Commission to assess the complementary sector-specific regulations that should define what level of cybersecurity should be met by the connected devices to ensure that specific security and privacy requirements are put in place for devices with higher security risks.

In its conclusions of 2 October 2020, the Council called for acceleration of the deployment of very high capacity and secure network infrastructure (including fibre and 5G) all over the EU, and for measures to enhance the EU's ability to protect itself. It furthermore called on the EU and the Member States to make full use of the 5G cybersecurity toolbox adopted on 29 January 2020.

Preparation of the proposal

The Commission did not perform an impact assessment to accompany this proposal,[3] but it did conduct various stakeholder consultations. These were internal rather than external consultations and there was no public consultation.

The internal consultations included a written consultation of the EUIBA directors-general responsible for IT security. This took place between 10 December 2021 and 10 January 2022. There was also a Commission inter-service consultation in February 2022, including an inter-service steering group, in the cybersecurity subgroup of the Interinstitutional Committee on Digital transformation of the Union institutions, bodies and agencies.

In addition, on 25 June 2021, representatives of Member States in the Council, representatives of the European Parliament and relevant stakeholders from the Union institutions, bodies and agencies participated in a workshop organised by the Commission to discuss the content of the future proposal for a regulation.

CERT-EU has meanwhile analysed the main cyber-threats to which the EUIBAs are currently exposed or are likely to be exposed in the near future given current trends such as the increase in teleworking, the migration of systems to the cloud and the increased outsourcing of IT services.

The analysis shows that CERT-EU has not been able to provide the EUIBAs with all the support they need, particularly in relation to capacity-building for less mature EUIBAs. Although CERT-EU is highly valued by the EUIBAs, its effectiveness is compromised by an increasing workload, unstable funding and staffing, and insufficient cooperation from some EUIBAs, which do not always share timely information on vulnerabilities and on significant cybersecurity incidents that have affected them or may affect others.

In addition to the CERT-EU threat analysis, the Commission carried out an evaluation of the IT security functioning of 20 EUIBAs: this evaluation showed that their governance, cyber-hygiene, overall capability and maturity vary very widely. It concluded that all EUIBAs should be required to implement a baseline of cybersecurity measures in order to address this disparity and fragmentation and to bring them all to a common level of cybersecurity.

The changes the proposal would bring

The proposal aims to increase the level of cyber-resilience among the EUIBAs to reduce inconsistencies in their resilience and improve their level of joint situational awareness and collective capacity to prepare and respond. For that, the proposal would modernise CERT-EU's mission and tasks, taking account of changed and increased digitalisation trends in recent years and the evolving cybersecurity threat landscape.

In practical terms, the proposal would establish a common cybersecurity framework to ensure common rules and measures on cybersecurity to improve all EUIBAs' resilience and incident-response capacities. The proposed regulation would:

- oblige the EUIBAs to: i) establish an internal framework for the management, governance and control of cybersecurity risks, ensuring effective and prudent management of all such risks; ii) adopt a cybersecurity baseline to address the risks identified through this framework; iii) carry out a cybersecurity maturity assessment covering all elements of its IT environment at least every three years; and iv) adopt a cybersecurity plan;
- strengthen the mandate and funding of CERT-EU, which would be renamed the 'Cybersecurity Centre' for the Union institutions, bodies and agencies and provide the resources it would need to fulfil its role;
- set up a new interinstitutional cybersecurity board to drive and monitor the implementation of the regulation and to steer CERT-EU;
- define the task and missions of CERT-EU as an autonomous interinstitutional cybersecurity centre;
- promote coordination and cooperation in response to significant incidents, in order to ensure the exchange of information among CERT-EU and the EUIBAs, such as incident-specific information to facilitate detection of similar cyber-threats or incidents. It would introduce the obligation to share (non-classified) IT information with CERT-EU and to report significant threats, vulnerabilities and incidents;
- oblige all EUIBAs to notify CERT-EU of significant cyber-threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them.

CERT-EU would therefore require additional resources to fulfil its expanded role. These resources would be reallocated from the EUIBAs benefitting from CERT-EU's services. According to studies, direct cybersecurity spending tends to vary between 4 and 7 % of organisations' aggregated IT expenditure. Moreover, the threat analysis undertaken by CERT-EU in support of this legislative proposal indicates that international bodies and political organisations face increased risks and therefore a level of 10 % of IT spending on cybersecurity would seem a realistic target.

However, according to the Commission the exact cost of such efforts cannot be determined due to the lack of detailed information on the IT expenditure of the EUIBAs and the relevant share of cybersecurity spending.

Advisory committees

Neither the European Economic and Social Committee (EESC) nor the European Committee of the Regions (CoR) adopted an opinion on the proposal.

National parliaments

The proposal is open to review by the national parliaments of Member States. However as it falls under exclusive EU competence, the submission of reasoned opinions on grounds of subsidiarity does not apply, and only eight Member States have begun or completed the scrutiny procedure.

Stakeholder views[4]

As there was no open public consultation, most stakeholders did not put forward position papers on this proposed legislation.

The European Data Protection Supervisor (EDPS) strongly advises that the proposal[5] provide clear, legal grounds for the processing of personal data by CERT-EU and the EU institutions, including, in particular, the purposes of processing and the categories of personal data that may be processed. The EDPS believes that this proposal needs to be improved in order to align it with the substantive rules of the NIS2 Directive, so that consistent and homogeneous rules for EU Member States and the EU institutions are achieved.

In May 2022, the European Court of Auditors (ECA) published an extensive analysis on the issue in a special report. The objective of the audit was to determine whether the EUIBAs, as a whole, have established adequate arrangements to protect themselves against cyber-threats.

According to the report, even though EUIBAs have established mechanisms for cooperation in the area of cybersecurity, the report noted that potential synergies were not fully exploited. Although there is a formalised structure for information exchange, with actors and committees having complementary roles, participation in interinstitutional forums by smaller EUIBAs is hindered by limited resources, and the representation of decentralised agencies and joint undertakings on the CERT-EU steering board is not optimal. The report also revealed that EUIBAs do not systematically share information on cybersecurity-related projects, security assessments and other service contracts with each other. This could lead to duplication of efforts and increased costs. The report also noted operational difficulties in the exchange of sensitive, non-classified information, via encrypted email or in videoconference, due to the lack of interoperability of IT solutions, inconsistent guidelines on their allowed use and a lack of common information markings and handling rules.

The ECA report concluded that the EUIBA community has not achieved a level of cyber-preparedness commensurate with the threats. The report established that key cybersecurity good practices were not always implemented, including some essential controls, and that a number of EUIBAs are clearly underspending on cybersecurity. Furthermore, sound cybersecurity governance is not yet in place in some EUIBAs: IT security strategies are in many cases lacking support or are not endorsed by senior management, security policies are not always formalised, and risk assessments do not cover the entire IT environment. Not all EUIBAs have their cybersecurity regularly subject to independent assurance. Moreover, cybersecurity training is not always systematic.

Based on these conclusions, the ECA recommended that:

- the Commission improve the cyber-preparedness of EUIBAs through a legislative proposal introducing common binding rules on cybersecurity for all EUIBAs and increased resources for CERT-EU;
- the Commission, in the context of the Interinstitutional Committee on Digital Transformation, promote further synergies among EUIBAs in selected areas;
- CERT-EU and ENISA increase their focus on EUIBAs that are less mature in cybersecurity.

ENISA and CERT-EU support the key observations established by the Court of Auditors, while also bringing some clarifications. For instance, existing actions by ENISA and/or CERT-EU are not considered by ECA in its report, nor are planned future activities. Both ENISA and CERT-EU support the recommendation by ECA to focus on less mature EUIBAs.

On 21 June 2022, the Council also published some conclusions on the ECA special report. Among other things it stated that the EUIBAs should allocate a sufficient budget to ensure the implementation of protection measures against cyber-threats and to improve the cooperation and exchange of information on cybersecurity, as well as improved interoperability of secure communication channels between each other. It also invited the Commission to take into account the recommendations of the special report when designing the cybersecurity policies of the EUIBAs, and to advocate more synergies between them. It stated that the EUIBAs should have a risk management framework for cybersecurity and systematise the use of cybersecurity awareness and training programmes for staff.

Legislative process

In the European Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE) (rapporteur: Henna Virkkunen, EPP, Finland). The Committees on Constitutional Affairs (AFCO), on Justice and Home Affairs (LIBE), and on Budgets (BUDG) were asked for their opinions.

The European Commissioner for Budget and Administration, Johannes Hahn, presented the proposal on 2 June 2022 to the ITRE committee. After the presentation, the members of the ITRE committee discussed with the Commissioner the key elements of the proposal, such as the governance framework, the interinstitutional cybersecurity board and CERT-EU's reinforced mandate.

In the same context, and on the same day, Bettina Jakobsen, Member of the European Court of Auditors, presented the special report on the cybersecurity of EUIBAs (mentioned in the stakeholders section of this briefing).

The BUDG committee adopted its opinion on 12 July 2022, AFCO adopted its opinion on 1 February 2023 and LIBE adopted its opinion on 1 March 2023.

The rapporteur published her draft report on 7 October 2022. The deadline for tabling amendments was 27 October 2022. The report was adopted unanimously in the ITRE meeting on 9 March 2023, with 57 votes in favour, no abstentions and no votes against. The ITRE committee decision to enter into interinstitutional negotiations was confirmed in plenary the following week.

In its report, ITRE supports the key elements of the proposed regulation, such as strengthening the mandate of CERT-EU, setting up a new interinstitutional cybersecurity board (IICB) to drive the implementation of the new regulation and promoting coordination and cooperation in response to cyber-incidents together with CERT-EU. The report also further develops the risk-management measures to be implemented by the entities. Where the IICB finds that a Union entity (i.e. an EUIBA) has not applied or implemented the proposed regulation effectively, it could, among other things and without prejudice to the internal procedures of the Union entity concerned: i) request relevant and available documentation relating to the effective implementation of the provisions of this regulation, ii) communicate a reasoned opinion with observed gaps in the implementation of this regulation, iii) invite the Union entity concerned to provide a self-assessment on its reasoned opinion, and iv) issue, in cooperation with CERT-EU, guidance to clarify the EUIBA's risk management, governance and control framework, cybersecurity risk-management measures, cybersecurity plans and reporting obligations.

The report also introduces additional responsibilities for CERT-EU, such as playing a coordinating role in the disclosure of vulnerabilities and tasking it with proposing the criteria and scale for the cybersecurity frameworks to be adopted by EU entities. There is also a provision to establish CERT-EU as an autonomous interinstitutional service provider for all Union entities, with regular assessments of its functioning. These would allow for changes to its structure. There is the intention also to reorganise the timeframe for reporting significant cyber incidents, aligning the notification timing requirements with those of the NIS2 Directive.

The Council approved its general approach on 18 November 2022. It supports the key elements of the proposed regulation and further strengthens the mandate and funding of CERT-EU and the creation of the IICB. In addition, Council's general approach aligns the proposal with the NIS2 Directive and removes references to the joint cyber unit, as it has not yet been defined. It also strengthens the mechanisms for ensuring EU entities' compliance with the new regulation, while respecting their institutional autonomy.

Trilogue negotiations started on 27 April 2023 and the positions were closely aligned. Thus, an agreement was reached during the trilogue on 26 June 2023. The ITRE committee confirmed the political agreement during its meeting on 18 September 2023 and Parliament is expected to vote on it during its November 2023 plenary session.

Under the agreement, the new rules would require Union entities to establish a governance, risk management and control framework in the area of cybersecurity. They would also have to implement cybersecurity measures addressing the identified risks, conduct regular cybersecurity maturity assessments and put in place a cybersecurity plan. The agreement also envisages the stronger CERT-EU and its enhanced coordination role. CERT-EU would be renamed the 'Cybersecurity Service for the Union institutions, bodies, offices and agencies', while keeping the current acronym. It would advise all EU institutions, bodies, offices and agencies and help them to prevent, detect and respond to incidents. It would also act as a hub for information exchange and coordination on cybersecurity and incident response. All EU entities would be required to share non-classified incident-related information with CERT-EU without undue delay.

Under the agreement, the new interinstitutional Cybersecurity Board would also be established to monitor the implementation of the regulation and supervision of CERT-EU. The board would consist of representatives of all the EU institutions and advisory bodies, the European Investment Bank, the European Cybersecurity Competence Centre, ENISA, the European Data Protection Supervisor, the EU Agency for the Space Programme, and representatives of the EU Agencies Network. The secretariat of the board would be provided by the European Commission.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Negreiro M., The NIS2 Directive, EPRS, European Parliament, February 2023.

Kononenko V., Improving the common level of cybersecurity across the EU, EPRS, European Parliament, February 2021.

Zygierewicz A., Directive on security of network and information systems (NIS Directive), EPRS, European Parliament, November 2020.

Negreiro M. with Belluomini A., The new European cybersecurity competence centre and network, EPRS, European Parliament, July 2020.

Negreiro M., The NIS2 directive, EPRS, European Parliament, February 2023.

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

Erbach G. with O'Shea J., Cybersecurity of critical energy infrastructure, EPRS, European Parliament, October 2019.

OTHER SOURCES

European Court of Auditors, Cybersecurity of EU institutions, bodies and agencies – Level of preparedness overall not commensurate with the threats, Special report, May 2022.

European Parliament, High common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, Legislative Observatory (OEIL).

Europol, Internet organised crime threat assessment (IOCTA) 2021, 2021.

ENDNOTES

[1] The NIS 2 directive on measures for a high common level of cybersecurity across the Union should further improve the cybersecurity resilience and incident response capacities of public and private entities, national competent authorities and bodies and the Union as a whole. It is therefore necessary that the EUIBAs follow suit by applying rules that are consistent with the proposed NIS 2 directive and mirror its level of ambition.

[2] CERT-EU was originally established in May 2011, when the secretaries general of the Union institutions and bodies decided to establish a pre-configuration team for a CERT-EU supervised by an inter-institutional steering board. In September 2012, CERT-EU was established as a taskforce of the European Commission with an inter-institutional mandate of cooperation in cybersecurity. In December 2017, the Union institutions and bodies concluded an interinstitutional arrangement on the organisation and operation of CERT-EU.

[3] An informal impact assessment – 'Threat Landscape Analysis and an IT Security Maturity Assessment of the Union institutions, bodies and agencies' – was nevertheless performed. Three options were considered, ranging from no action to policy option 1 – non-legislative measures to align the Union institutions, bodies and agencies, policy option 2 – an interinstitutional cybersecurity board and a cybersecurity framework, and policy option 3 – a far-reaching central authority and extensive common binding cybersecurity rules. Option 2 was chosen as it achieves most of the intended objectives and is the only viable option, given the prevailing legal boundaries under which the EU can 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'.

[5] Together with the other related proposal that was published on the same date on classifying information security.

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)

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