Briefing
EU Legislation in Progress

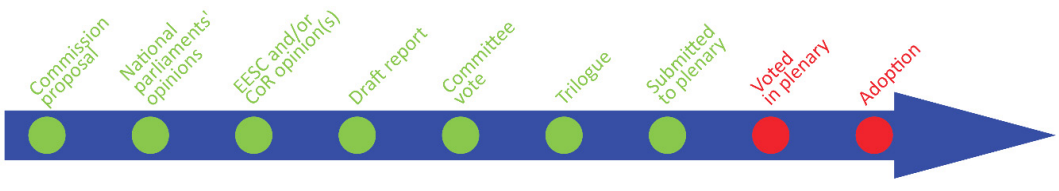
European Parliament

CONTENTS

ENISA and a new cybersecurity act

In September 2017, the Commission adopted a cybersecurity package with new initiatives to further improve EU cyber-resilience, deterrence and defence. As part of these, the Commission tabled a legislative proposal to strengthen the EU Agency for Network Information Security (ENISA). Following the adoption of the Network Information Security Directive in 2016, ENISA is expected to play a broader role in the EU's cybersecurity landscape but is constrained by its current mandate and resources. The Commission presented an ambitious reform proposal, including a permanent mandate for the agency, to ensure that ENISA can not only provide expert advice, as has been the case until now, but can also perform operational tasks. The proposal also envisages the creation of the first voluntary EU cybersecurity certification framework for ICT products, where ENISA will also play an important role. Within the European Parliament, the Industry, Research and Energy Committee adopted its report on the proposal in July. A agreement was reached with the Council during the fifth trilogue meeting, on 10 December 2018, and this was approved by ITRE committee on 14 January. The vote in plenary on this text is scheduled in March 2019.

Regulation on ENISA, the 'EU Cybersecurity Agency', and on information and communication technology cybersecurity certification (the 'Cybersecurity Act')	
COM(2017) 477, 13.9.2017, 2017/0225 (COD), Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')	
Committee responsible:	Industry, Research and Energy (ITRE)
Rapporteur:	Angelika Niebler (EPP, Germany)
Shadow rapporteurs:	Peter Kouroumbashev, (Evžen Tošenovský (ECR, Czech Republic), Pavel Telička (ALDE, Czech Republic), Marisa Matias (GUE/NGL, Portugal), Jakop Dalunde (Greens/EFA, Sweden), Dario Tamburrano (EFDD, Italy), Christelle Lechevalier (ENF, France)
Next steps expected:	First-reading vote in plenary



26 February 2019
Third edition

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

Please note this document has been designed for on-line viewing.

Print

EPRS | European Parliamentary Research Service
Author: Mar Negreiro
Members' Research Service

PE 614.643

EN

Introduction

In light of the significant changes that have occurred in the cybersecurity landscape in recent years and the increasing risks coming from a connected world expected to number over 20 billion connected devices by 2020, the Commission has decided to reinforce the EU's resilience, deterrence and response to cyber-attacks. At the same time the number and diversity of cyber threats is growing unabated.

According to monitoring reports from the EU Agency for Network Information Security (ENISA) there is a trend towards increasing monetisation of cybercrime, with an estimated global loss of US$ 1 billion for 2016 alone. Major cyber-attacks, using ransomware for instance,[1] were among ENISA's top 2016 cyber threats. Since 2016 more than 4 000 ransomware attacks have occurred every day, a 300 % increase compared with 2015. Recent large-scale attacks, such as WannaCry (a type of ransomware attack) in May 2017, have shown how massive the impact can be. This attack affected over 230 000 systems in 150 countries, in this case mainly computers. Another major cyber-attack that took place in October 2016 poured through a network of internet of things (IoT) devices (such as digital cameras and DVR players, but not computers) infected with special malware (a malicious software called the Mirai botnet). As a result businesses are having to invest more money to make cyberspace safer for themselves and their customers.

According to the Commission, the economic impact of cybercrime rose five-fold between 2013 and 2017, and could further rise by a factor of four by 2019, while 80% of European companies were affected in 2016. Not only companies but also citizens and entire countries are affected: the first known cyber-attack on a country happened in Estonia in April 2007, affecting the online services of Estonian banks, media outlets and government bodies for weeks. Since then many other nations have suffered cyber-attacks also affecting critical infrastructure. According to a recent Eurobarometer survey 87 % of EU citizens regard cyber-crime as an important challenge to the EU's internal security and a majority are concerned about being victims of various forms of cybercrime. In the United States of America (USA) about 64 % of the population has experienced a data breach.

In May 2017, under the Digital single market strategy midterm review, the Commission therefore identified tackling cybersecurity threats as one of its three key priority areas for further EU action in the years to come, and announced a legislative proposal for the second half of 2017 and the review of the 2013 EU cybersecurity strategy.

On 13 September 2017, coinciding with President Juncker's State of the Union speech, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy proposed to reinforce the EU's resilience and response to cyber-attacks. Among the initiatives to improve EU resilience, the Commission tabled a proposal for a regulation on ENISA (the EU Cybersecurity Agency) and on information and communication technology cybersecurity certification (the Cybersecurity Act), which proposes a permanent mandate for ENISA and the creation of a voluntary EU certification framework for ICT security products.

1 Ransomware is a subset of malware in which the data on a victim's computer is locked and payment is demanded before the ransomed data is decrypted and access returned to the victim.

Existing situation

ENISA was established in 2004, based on Regulation (EC) No 460/2004. Regulation (EC) No 1007/2008 and the Regulation (EC) 580/2011 extended ENISA's mandate.[2] The agency was established for a period of seven years beginning on 19 June 2013, and its mandate will therefore end in June 2020.

In light of the significant changes that have occurred in the cybersecurity landscape since the adoption of the ENISA Regulation, the Commission decided to bring forward the evaluation and review of the mandate of the agency (otherwise due by 20 June 2018). So far, ENISA's role has mainly been to provide expertise and advice rather than dealing operationally with cybersecurity.[3] Until now this has been largely the competence of the Member States. This began to change with the adoption in 2016 of the Directive on the Security of Network and Information Systems (known as the NIS Directive), which formally created a network of Member State computer security incident response teams (CSIRTs).[4] The secretariat for this network is provided by ENISA. ENISA has therefore assisted Member States with the implementation of the NIS Directive, the deadline for which was 9 May 2018.

The agency will also play a key role in information and communication technologies (ICT) security certification. ICT security certification plays an important role in increasing trust and security in products and services that are crucial for the smooth functioning of the digital single market in the light of the increasing growth of the internet of things and connected devices. At the moment, a number of different security certification schemes for ICT products exist in the EU[5] and some are only valid within their national territories. While these initiatives confirm the importance of certification, the Commission has identified that multiple certification initiatives lead to the fragmentation of the single market. In addition, the Commission has noted that there are few national schemes available and that these differ considerably by country and by sector. For example, according to the European Commission, a smart meter manufacturer who wants to sell its products in three Member States, e.g. Germany, France and the UK, currently needs to comply with three different certification schemes.[6]

Parliament's starting position

In its resolution of 12 September 2013 on the cybersecurity strategy of the European Union: an open, safe and secure cyberspace the European Parliament called for the development of increased cyber-resilience for critical infrastructures while it noted the growing cyber-security challenges. In its resolution of 16 January 2016 Towards a Digital Single Market Act it asked the Commission to put in place a strong

2 With Regulation (EU) No 526/2013 on ENISA finally repealing Regulation (EC) No 460/2004 on 21 May 2013.
3 It also coordinates one of the biggest pan-European cybersecurity exercises, Cyber Europe, which happens every two years.
4 Effective and adequately resourced national computer security incident response teams (CSIRTs) across the EU in accordance with Article 9 of the NIS Directive, which are crucial for increasing the Member States' preparedness against growing cyber-threats. For this ENISA has issued a number of documents and studies describing good practices and recommendations at a technical level for various CSIRT capabilities and services.
5 For instance the *Certification Sécuritaire de Premier Niveau* in France (CSPN), Commercial Product Assurance in the UK, the Dutch Baseline Security Product Assessment (BSPA) or the SOG-IS MRA which includes 12 Member States plus Norway and has developed protection profiles for various digital products.
6 These are the CPA in the UK, the CSPN in France and a specific protection profile based on common criteria in Germany.

cybersecurity agency to fight cybersecurity attacks. More specifically, it called for efforts to be made to improve resilience against cyber-attacks, with an increased role for ENISA.

More recently, in its resolution of 3 October 2017 on the fight against cybercrime, in the light of the increasing number of connected appliances Parliament asked for attention to be drawn to the safety of all devices and for action to promote the security-by-design approach. It asked Member States to speed up the setting-up of computer emergency response teams to which businesses and consumers can report malicious emails and websites, as envisaged by the NIS Directive.

Council and European Council starting position

In the conclusions of 15 December 2016, the European Council called for action to ensure complementarity between EU and NATO as regards various threats, including cyber security.

In its conclusions of 19 October 2017 the European Council called for the adoption of a common approach to EU cyber security following the reform package proposed by the European Commission on 13 September 2017. To that end, the Commission's cybersecurity proposals should be developed in a holistic and timely manner, on the basis of an action plan to be set up by the Council. The EU leaders regarded cyber security reform as one of the main ongoing aspects on the road to completing the EU digital single market.

Similarly, the Council, in its conclusions on the joint communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, welcomed the proposal for a strong and permanent mandate for ENISA with the primary objective of supporting and developing closer cooperation between Member States, to increase their capacities and to increase confidence in a digital Europe.

Proposal

Preparation of the proposal

To underpin the proposal and collect evidence the Commission ran two public consultations and commissioned three dedicated studies: one on the evaluation of ENISA and two on the role of certification and labelling that fed into the impact assessment accompanying the legislative proposal. The main results are briefly described below.

The public consultations

The main public consultation took place between 18 January and 12 April 2017. It was conducted in the context of the evaluation and review of ENISA in accordance with Article 32 of Regulation (EU) No 526/2013. 90 replies were received, including 88 responses to the questionnaire and two position papers.

98 % of respondents saw a need for an EU body to respond to the needs and gaps identified (see above) and identified ENISA as the appropriate organisation to help the EU respond to those needs and gaps.

The overall performance of ENISA during the 2013 to 2016 period was assessed positively by the majority of respondents (74 %) as contributing to network and information security in the EU. A majority of respondents furthermore considered ENISA to be achieving its various objectives. However a majority of respondents considered ENISA's size in terms of staff members to be insufficient.

In particular, the respondents judged that ENISA, if sufficiently mandated and resourced, could play an important role in improving EU's resilience against cyber-attacks.

An earlier public consultation took place between 18 December 2015 and 11 March 2016 (12 weeks) on the contractual public-private partnership (PPP) on cybersecurity. This focused on the possible establishment of the cybersecurity contractual public-private partnership and also called for contributions on potential additional policy measures that could stimulate cybersecurity industry in the EU. These included a section devoted to ICT security certification. The consultation received 241 responses. On the related certifications questions the majority of respondents stressed the importance of cybersecurity certification schemes for the development of the digital single market in Europe. However, many (37.9 %) thought the current certification schemes did not support the needs of Europe's industry while 44.6 % did not know how to answer the question. A large share of respondents (50.4 %) stated that they did not know whether certification schemes were mutually recognised. Among those who answered more than half felt that current certification schemes were not widely recognised across the EU.

Impact assessment

The impact assessment (IA) conducted for this proposal is substantial, including six different documents (12 annexes in total). The IA explores three different policy options for the review of ENISA and four policy options for ICT security certification (and two options that were discarded at an early stage)[7], including the baseline options.

The IA assesses which policy option could best improve ENISA's capacities in its new operational role while mitigating identified problems.[8] The analysis on ICT certification meanwhile identifies additional problems such as the growing emergence of multiple national and sectorial certification schemes that increase costs for companies operating across borders in the EU.

The analysis leads to the conclusion that a reformed and enhanced ENISA in combination with a general but voluntary EU ICT cybersecurity certification framework was the preferred option. It concludes that a one-size-fits-all mandatory approach to cybersecurity certification would not work across the large variety of ICT products and services, as needs vary considerably according to sectors.

The creation of this framework should provide companies with a single procedure for cybersecurity certification, reducing costs, facilitating cross-border operations and avoiding fragmentation. Moreover, it is intended to increase cybersecurity assurance for ICT products and services of pivotal sectors (transport, energy, health, the automotive sector and finance, among others) and raise consumers' trust.

The EPRS initial appraisal of the impact assessment has highlighted that the Commission recognises the overall lack of evidence in the field of cybersecurity, as companies are reluctant to share information in this field, as it could potentially harm them. The Commission therefore had to follow some key assumptions for the economic estimates of the options relating to ENISA (see Annex 6 of the IA). It appears that a no cost-benefit analysis was conducted. The EPRS initial appraisal also points out that the Commission did not carry out a dedicated public consultation on ICT security certification. However the Commission argues that stakeholders were able to express their views on this issue in the two open public consultations as well as in two surveys regarding ICT security certification organised in 2017.

The changes the proposal would bring

Essentially the proposal would reinforce the EU cybersecurity agency and establish a voluntary ICT cybersecurity certification framework. Each of these changes are described below.

7 Option 1 on the expiry of ENISA mandate and option 4 on ICT security internal market legislation introducing a mandatory scheme (see pp. 60-62 of the impact assessment main report).

8 Such as the fragmentation of policies and approaches to cybersecurity across Member States, dispersed resources and fragmentation of approaches to cybersecurity across EU institutions, agencies and bodies, and insufficient awareness and information of citizens and companies.

The reform of ENISA

The Commission proposes to reform ENISA into a stronger EU cybersecurity agency with a permanent mandate, greater operational resources and a stable footing for the future. Thus new tasks and resources will be given to the agency in areas such as operational cooperation and ICT security certification in order to reflect the new reality and needs in cybersecurity, along with the role of assisting Member States in implementing the NIS Directive in developing their CSIRTs.

At present ENISA is based in Heraklion, Crete, Greece, and has a branch office in Athens. Its budget is €11.2 million for 2017. Under the proposal, it would grow considerably in terms of both budget and human resources.

Table 1 – Current and future resources foreseen to enhanced ENISA

ENISA resources	Now	Future
Staff	84 people	125 people
Budget	€11 million	€23 million
	gradual increase: starting with +5 million 1st year and fully achieved 4 years after entry into force.	

Source: European Commission 2017.

Concretely, ENISA would be in charge of six different types of activity, as listed below:

1. Market-related tasks within the cybersecurity certification framework, including to prepare candidate European cybersecurity certification schemes, with the expert assistance and close cooperation of national certification authorities: these schemes would be adopted by the Commission. ENISA would also support policy development in information and communication technology (ICT) standardisation.

2. Policy development and implementation: the aim would be to do more to support to the Commission and Member States in the development, implementation and review of general cybersecurity policy and in key strategic sectors identified by the NIS Directive e.g. energy, transport and finance.

3. Capacity building: ENISA would reinforce support for Member States in order to improve capabilities and expertise, for instance on the prevention of and response to incidents.

4. Knowledge and information: ENISA would provide analyses and advice and raise awareness, so as to become the one-stop shop for cybersecurity information from the EU institutions and bodies.

5. ENISA would be in charge of the incident response teams (CSIRTs) secretariat at EU level and would provide assistance on request to Member States to handle incidents.

6. ENISA would handle large scale cybersecurity incidents.

The new agency's mandate, objectives and tasks would be subject to regular reviews.

The agency would also organise annual EU-wide cybersecurity exercises and improve the sharing of threat intelligence and knowledge by setting up information sharing and analysis centres. It would also play a role in the upcoming cybersecurity blueprint for cyber crisis cooperation and the European cybersecurity research and competence centre, to which the agency would link its advice on EU research needs.

The creation of a European cybersecurity certification framework

ENISA's new mandate would also include assisting with the development of a voluntary EU certification framework recognised in all the Member States and confirming that products and services are cyber-secure. The proposed certification framework would provide for EU-wide certification schemes with a comprehensive set of rules, technical requirements, standards and procedures. This would be based on agreement at EU level on the evaluation of the security properties of a specific ICT-based product or service. The resulting certificates confirming compliance with such requirements would be recognised in all Member States, as the proposal establishes the primacy of EU schemes above existing national schemes.

The European cybersecurity certification schemes would be prepared by ENISA, with the assistance, expert advice and close cooperation of a European cybersecurity certification group (ECCG),[9] and adopted by the Commission by means of implementing acts. When a need for a cybersecurity certification scheme is identified, the Commission will ask ENISA to prepare a scheme for specific ICT products or services. ENISA will work on the scheme in close cooperation with national certification supervisory authorities represented in the group. Member States and the group may also propose to the Commission that it ask ENISA to prepare a particular scheme.

Once a European cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services would be able to submit an application for certification of their products or services to a conformity assessment body of their choice. Accreditation would be issued for a maximum of five years and could be renewed on the same conditions provided that the conformity assessment body meets requirements.

9 The ECCG will be composed of the national certification supervisory authorities of Member States.

Views

Advisory committees

The European Economic and Social Committee (EESC) adopted an opinion on 14 February 2018, in which it supports the proposals and asks the European Commission to consider a number of additional recommendations. It questions if the resources allocated to ENISA are enough to accomplish its new tasks. It also asks for ENISA to support e-government actions and to provide regular reports on the cyber-readiness of Member States, focusing on the sectors identified in the NIS Directive. Likewise, it considers that ENISA should also monitor the performance and decision-making processes at the national certification supervisory authorities.

The EESC also supports the proposal to increase awareness on cyber-hygiene measures for individuals and businesses and to create a cybersecurity competence network and related cybersecurity research competence centres.

On the cybersecurity certification framework, the EESC believes that it is necessary for the achievement of the digital single market to have a homogeneous interpretation of the rules for cybersecurity, including mutual recognition between Member States with certification schemes by different sectors as a common baseline. To achieve this, it recommends that sectorial EU agencies[10] are involved in the process, as well as European standardisation bodies[11] which would set minimum European standards for IT security.

Thus, the envisaged European Cybersecurity Certification Group supported by ENISA should be made up of national certification supervisory bodies, private-sector stakeholders, scientific and civil society actors. As certification is a key method of providing a higher level of security, more emphasis should be given to IoT security in the new EU certification approach. The EESC also believes that the certification process must include a proper labelling system both for hardware and software, to be applied also to imported products.

The Committee of the Regions has not adopted an opinion specifically on this proposal. However in its opinion of 31 January 2018 on the digital single market mid-term review, it asked among other things for the Commission to set up an EU cybersecurity agency with full operational capacities and a stable operational framework. It also supported the development of standards, instruments and mechanisms to ensure the security of networks and information systems to guarantee a high level of protection in all Member States.

National parliaments

The deadline for national parliaments to submit reasoned opinions on the grounds of subsidiarity was 7 December 2017.

10 Such as EASA, ERA, EMA, etc.
11 Such as CEN, CENELEC and ETSI.

The French Senate adopted a reasoned opinion on 27 November 2017 that considers that the proposal does not comply with the principle of subsidiarity. Among other things, it criticises the fact that ENISA's new mandate and the certification framework were put together in one legal text and that the proposal's legal base should be Article 114 of the Treaty on the Functioning of the European Union, together with Article 5 of the Treaty on European Union on security issues. The Senate notes that 'European cooperation on cybersecurity matters must continue to be done on the basis of the Member States' participation and voluntary provision of sensitive information, even those related to national security on which the ENISA cannot therefore dispose of further investigatory powers as planned in the Article 7, point 5 of the Regulation proposal'. On the cybersecurity certification framework it points out that the proposed regulation places ENISA at the heart of the certification process, whereas this agency has no expertise on the matter.

The Spanish Cortes Generales adopted a resolution on 8 November, concluding that the text does comply with the principle of subsidiarity.

The Czech Senate also adopted a resolution on 22 November. This supports the proposal but asks for further encouragement of digital literacy activities to change the attitudes and responses of individuals and businesses to cyber threats and to deepen cooperation and coordination with NATO in this field. It supports the proposed reinforcement of ENISA and the extension of its mandate for an indefinite period. However, it considers that it should complement the activities of the Member States in the field of cybersecurity and not seek to take over their competences in this area.

Stakeholders' views[12]

During the public consultation a large majority of stakeholders agreed that EU legislative action was needed to enhance ENISA's role and back the EU's fight against cyber-attacks.

On the certification framework, stakeholders recognised that in the absence of an EU-wide cybersecurity certification scheme, products and services have to be certified individually in each Member State, leading to market fragmentation. Most importantly, in the absence of EU harmonisation legislation for ICT products and services, differences in cybersecurity certification standards and practices in Member States are liable in practice to create 28 separate security markets in the EU, each with its own technical requirements, testing methodologies and cybersecurity certification procedures, impeding the completion of the digital single market.

The industry associations Business Europe and Digital Europe are in favour of a non-mandatory certification framework based as much as possible on international standards. Digital Europe is concerned that labelling could create a false sense of security in consumer products. Business Europe calls for encryption to be encouraged to protect intellectual property and highlights that this proposal does not address cyber-attacks aimed at businesses to protect them against cyber-theft of critical technologies, trade secrets and other confidential business information.

12 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 'EP supporting analysis'.

The FIEEC and ZVEI industry associations welcomed the fact that the European cyber security certification schemes would be defined at European level in order to minimise the fragmentation between Member States and the fact that these schemes remained voluntary, and called for coordinated action on cyber security standardisation. While Deutsche Telekom has stated that to substantially raise the security standards for IoT devices would require much more than voluntary product certification, including mandatory labelling based on clear product characteristics as well as new product liability legislation in the case of insufficient security measures. It also criticises the fact that NIS legislation would need to broaden to other sectors as it would become outdated before the conclusion of the implementation period.

The industry association Eurosmart supports the Commission's proposal while putting forward a number questions, regarding for instance how a fair and transparent process can be assured for the preparation of the certification scheme and how it would be governed. It also criticises one of the Commission studies undertaken for the IA.[13]

The associations IFIA and CEOC meanwhile ask for a clear distinction to be made between critical mandatory certification and voluntary duty of care. As certain high risk products should be subject to mandatory certifications, such as connected cars, smart grids, etc. it also asks for higher security levels for ICT products (i.e. cybersecurity by design and throughout the product/service lifecycle) and for the scheme to be based on international standards.

In this sense the director of operations at ENISA mentioned in a recent interview that binding standards for cybersecurity certification could be beneficial in some areas, such as for critical infrastructure. However, in other areas, binding standards could hamper innovation. For instance in the internet of things area lightweight certification was relevant. He also argued that labels could be developed to complement lightweight certification and highlighted the need for more discussion about how to deal with liability for cyber-attacks.

A research paper from a German think-tank criticised ENISA's governance of the ICT framework and a number of questions that have been left pending. For these researchers the EU has neither defined resilience or deterrence properly nor made sufficiently clear how it intends to overcome institutional fragmentation and lack of legal authority in cybersecurity issues. Moreover, a key criticism is that controversial topics – such as the harmonisation of criminal law or the use of encryption – have been entirely omitted. It asks for Member States to abandon their stand-alone efforts and to speed up the legal regulation of cybersecurity at EU level.

For the European Cockpit Association (ECA), the body that represents European pilots, there are four areas of concern as regards certification:

> certificate 'shopping': the possibility for the manufacturer to select the organisation where the chances of acquiring the certificate are the highest.

13 See their technical document on the PricewaterhouseCoopers study.

> subsidiarity: the idea that Member States will have to endorse certificates issued in other Member States, even when the certifying organisations they have appointed themselves nationally would have denied that certificate, undermining more stringent national standards.

> capacity building: as ENISA will be required to set up an information sharing analysis centre (ISAC), they are concerned in terms of the exchange of sensitive/restricted information by ENISA.

> operational cooperation: the agency will contribute to the CSIRT network in various ways. Under Article 7.4(c), ENISA will be analysing vulnerabilities, artefacts and incidents. The NIS Directive does not so far require Member States to share this information, and since ENISA doesn't collect incident data itself, it is not clear how the activities envisaged under this article will materialise, unless mandatory sharing of information is considered.

Some other concerns were raised by the European banking association and the UK's International Regulatory Strategy Group (IRSG) regarding the fragmentation arising from different regulations coming from different regulators and supervisors. For instance the NIS Directive, Infrastructure Act, PSD2 and the ECB are all asking for to incidents to be reported using different taxonomies and templates. Similarly they see a need to avoid overlapping requirements, such as a possible duplication of responsibilities, for instance between the General Data Protection Regulation and the NIS Directive in the context of incident reporting. Also both FIEEC and ZVEI are calling for better consistency and explicit differentiation between European privacy and security regulations.

Legislative process

Within the European Parliament, the file has been assigned to the Industry, Research and Energy Committee (ITRE) (rapporteur: Angelika Niebler, EPP, Germany). The Internal Market and Consumer Protection Committee (IMCO), as associated committee under Rule 54 of Parliament's rules of procedure, and the Budgets, Foreign Affairs and Civil Liberties committees (BUDG, AFET and LIBE) were asked for opinions. The AFET committee subsequently decided not to give an opinion on the proposal.

On 12 October 2017, the European Commission presented the legislative proposal and impact assessment to the IMCO committee, and did so on 22 January 2018 to the ITRE committee, which had held a public hearing on the issue in November 2017.

The LIBE and BUDG committees adopted their opinions on 16 March and 23 April 2018 respectively. The IMCO committee adopted its opinion as associated committee on 22 May 2018. It welcomed the proposals, calling for the strengthening of ENISA's powers and involvement of stakeholders. It underlined that 'certificate shopping' should be avoided, and recommended strengthening ENISA's surveillance powers to make sure that the cybersecurity certificate's implementation is consistent across Member States. It also made other recommendations, such as the introduction of a mandatory EU Trust Label for certified ICT products and services, as well as security-by-design and privacy-by-design principles throughout their lifecycle.

In total, 631 amendments and 24 compromise amendments were tabled on this file. The ITRE committee adopted its report on 10 July, with 56 votes in favour, 5 against and 1 abstention. It also voted to enter into interinstitutional negotiations with the Council and the Commission, a decision confirmed during the September plenary session.

The ITRE report supported both the new mandate for ENISA and the creation of a voluntary cybersecurity certification framework to improve the EU's resilience to cyber-attacks and deliver a better coordinated EU response. It was also in favour of increasing cyber-hygiene awareness among citizens and businesses, and strengthening trust in ICT products and services.

On the new ENISA, the report proposed to give it additional tasks, broadening its role even further to improve the coordination and exchange of best practices among Member States on cybersecurity education, in order to increase cyber-hygiene awareness for citizens, educators and businesses and to improve digital literacy and security by design. It also sought to clarify the limits of the ENISA mandate regarding the competences of the Member States.

It would also establish a notification system for national certification schemes, and introduce audits. The certification schemes needs to include not only ICT products and services but also 'processes' to consider their whole life-cycle. The report also highlighted the priority of focusing on developing schemes for the Internet of Things (IoT), given the increasing number of connected ICT products and services.

In addition, the report called for the Commission to be empowered to adopt the European cyber-certification schemes by means of *delegated acts* (rather than *implementing acts*[14] as stated in the Commission proposal) and insisted on predictability for the markets through establishing a rolling work programme for European cybersecurity certification schemes. It also stressed the need to increase consumers' trust by offering transparent information on the level of security of ICT products, services and processes, while clarifying that even a high level of cybersecurity certification cannot guarantee that an ICT product or service is completely safe.

On 25 May 2018, Member States agreed on a general approach, and on 8 June 2018 the Council adopted its position and a mandate to begin negotiations with the European Parliament as soon as possible. In its position, the Council also supported the new mandate for ENISA. However, it specified that the operational activities to be carried out should support and complement the actions taken by Member States in order to fulfil their obligations arising from the NIS Directive. Member States, for their part, should not introduce any new national certification schemes for services already covered by an existing European cybersecurity certification scheme. However, they should not be prevented from adopting or maintaining national certification schemes for national security purposes.

The Council text provided for the creation of a National Liaison Officers Network, composed of representatives of all Member States, to facilitate the exchange of information between ENISA and the Member States. It also supported the creation of a voluntary cybersecurity certification framework. It specified that the certification would be voluntary, unless otherwise specified in EU or Member State law.

The first trilogue meeting took place on 13 September 2018, a second on 1 October, the third on 5 November, the fourth on 22 November and the fifth on 10 December 2018. During the fifth trilogue meeting, agreement was reached on the text. The deal was then approved in the ITRE meeting on 14 January 2019. Now it is due to be voted by Parliament during the March I 2019 plenary session, and thereafter by the Council.

The agreed text reinforces the mandate of ENISA, and establishes the first EU framework for cybersecurity certification.

The text seeks to increase the agency's regular reporting activities. Among other things, 'state of cybersecurity' reports on the number of incidents and threats across the EU are to be produced together with the EU Member States, and ENISA is to organise twice-yearly large-scale EU cybersecurity simulation exercises, to improve the Union's resilience and coordinated response to attacks. The agency should contribute to responses at Union level in the case of large-scale cross-border cybersecurity incidents, and test the arrangements for such cooperation during its regular cybersecurity simulation exercises.

On the cybersecurity act, for the creation of a voluntary[15] cybersecurity certification framework, the agreed text emphasises that ENISA needs to play a stronger role in establishing European cybersecurity schemes, together with the Member States and relevant stakeholders. The text reinforces the role of industry in

14 Implementing acts include solely implementation measures, whereas delegated acts allow amending, supplementing, or deleting of non-essential elements of the basic legislative act.
15 According to the text cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.

the scheme's development, and redefines the assurance levels. Certification schemes need to include not only ICT products and services but also 'processes', to consider their whole life-cycle, as the Parliament had requested. The agreed text broadens the composition of the agency's advisory groups so as to have more industry participation. It creates an additional advisory group named the 'Stakeholder Cybersecurity Certification Group' – to help ENISA and the Commission consult relevant stakeholders – composed of members from both demand and supply sides of ICT products and services, including SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection authorities and conformity assessment bodies and academia, as well as consumer organisations on the demand side. It also provides for the creation of a European Cybersecurity Certification Group of representatives of national cybersecurity certification authorities to oversee its implementation.

Once a European cybersecurity certification scheme is adopted, manufacturers or providers of ICT products, ICT services or ICT processes should be able to submit applications for certification of their ICT products or ICT services to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national accreditation body. Accreditation should be issued for a maximum of five years and should be renewable on the same conditions, provided that the conformity assessment body still meets the requirements.

The certification scheme would specify three risk-based assurance levels:

1. **basic**, where the ICT product, service or process is protected from the known basic risks of cyber-incidents;

2. **substantial**, where known risks of cyber-incidents are prevented and there is also capability to resist cyber-attacks with limited resources; and

3. **high**, where risks of cyber-incidents are to be prevented and the ICT product, service or process is able to resist state-of-the-art cyber-attacks with significant resources.

The agreed text develops further the criteria for these three different assurance levels. For the 'basic' level, if a European cybersecurity certification scheme sets out provisions for self-assessment of conformity, it proposes that it be possible for manufacturers or service providers to carry out the conformity assessment themselves.[16]

As a priority, the Commission shall focus on the sectors listed in the NIS Directive which are to be assessed at the latest two years after the adoption of the first European cybersecurity certification scheme.[17] The text underlines the particular importance of certifying critical infrastructure, including energy grids, water, energy supplies and banking systems. Under this agreement, the Commission is set to draft the scope of products that might require obligatory certification, with a list to be finalised by the end of 2023. ENISA should also strive to provide consumers with relevant information on applicable certification schemes, for example by providing guidelines and recommendations. As requested by Parliament, manufacturers must

16 See Articles 50(1) and 51 respectively.
17 See sectors listed in Annex II of Directive (EU) 2016/1148.

provide detailed information including guidance on installation and on the period for security support, including information about security updates.

As was requested by the Parliament, the Commission should prepare a rolling work programme for European cybersecurity certification schemes, that would allow industry, national authorities and standardisation bodies to prepare in advance for future European cybersecurity certification schemes. The first EU rolling work programme would be published no later than 12 months after the entry into force of the regulation. It would be updated at least once every three years, and more often if necessary. ENISA is to maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes

The Commission, on the basis of the candidate scheme prepared by ENISA, should then be empowered to adopt European cybersecurity certification schemes by means of implementing acts.

Member States should not introduce new national cybersecurity certification schemes for ICT products, ICT services or ICT processes already covered by an existing European cybersecurity certification scheme. However, Member States should not be prevented from adopting or maintaining national cybersecurity certification schemes for national security purposes.

Finally the text requires an evaluation by the Commission no later than five years after entry into force of the regulation, and every five years thereafter. The evaluation should consider among other things the impact, effectiveness and efficiency of ENISA, and the possible need to modify its mandate and resources further. Moreover, any increased role and scope of the agency should be reflected in its allocated budget and also in the functioning of the European certification system.

The new regulation would enter into force on the 20th day following that of its publication in the Official Journal of the European Union. Articles 58, 60, 61, 63, 64 and 65 would however apply 24 months later than that.

References

EP supporting analysis

EU Cybersecurity Agency and cybersecurity certification, initial appraisal of a European Commission impact assessment, EPRS, December 2017.

The European Union Agency for Network and Information Security (ENISA), implementation appraisal, EPRS, May 2017.

Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU, EPRS, 2017.

Cybersecurity in the European Union and beyond: Exploring the threats and policy responses, Policy Department for Citizens' Rights and Constitutional Affairs, 2015.

Other sources

EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act), Legislative Observatory (OEIL), European Parliament.

Cybersecurity in the European Digital Single Market, High Level Group of Scientific Advisors Scientific Opinion No 2/2017, European Commission.

ENISA Threat Landscape Report, European Commission, 2016.

The EU's revised Cybersecurity Strategy, SWP Comments, German Institute for International Security Affairs, November 2017.

eprs@ep.europa.eu | EPRS (intranet) | Thinktank (internet) | Blog