Briefing
Initial Appraisal of a European Commission Impact Assessment

European Parliament

December 2017

EU Cybersecurity Agency and cybersecurity certification

Impact assessment (SWD(2017) 500, SWD(2017) 501 (summary)) of a Commission proposal for a regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on information and communication technology cybersecurity certification ('Cybersecurity Act') (COM(2017) 477 final/2)

Background

This note seeks to provide an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above proposal, which is the main part of the 'Cybersecurity package', submitted on 13 September 2017 and referred to Parliament's Committee on Industry, Research and Energy (ITRE). As announced in the State of the Union Address 2017 and the Commission's communication on Europe's Cyber Resilience System and Cybersecurity Industry,[1] the initiative aims to reform the European Union Agency for Network and Information Security (ENISA or 'Agency') in order to enhance its supporting functions for Member States in achieving cybersecurity resilience and to acknowledge the Agency's responsibilities under the new directive on security of network and information systems (NIS Directive).[2] In addition, the proposal establishes a voluntary European cybersecurity certification framework to promote such certification schemes for specific information and communication technology (ICT) products and services, and to allow for mutual recognition of certificates so as to avoid further market fragmentation.[3]

Problem definition

The IA highlights the Agency's overall positive performance following its evaluation, but also underlines gaps and challenges for the future of cybersecurity in the EU. To demonstrate the importance of the identified problems, the IA emphasises the increase in cyber-attacks and security incidents, as well as their economic impact.[4] It identifies six problem drivers: (i) an incomplete regulatory framework; (ii) immature cooperation mechanisms; (iii) a lack of EU-wide reliable data and analyses; (iv) limited efficiency and suitability of current certification mechanisms; (v) insufficient and uneven resources allocated at national and EU level; and (vi) insufficient education and awareness programmes. Subsequently, the IA identifies three main problems concerning ENISA and cybersecurity certification in the EU (which appear to be identical to the problem drivers):

[1] European Commission communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410, 5 July 2016, pp. 4 ff; see also the Commission's mid-term review on the implementation of the Digital Single Market (DSM) Strategy of May 2017, in which it identified cybersecurity as a key priority.
[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security and information systems across the Union; ENISA is expected to play an important role in the implementation of the NIS Directive: ENISA inter alia provides the secretariat for the Computer Security Incident Response Team (CSIRT) network and assists the Member States and the Commission by providing expertise and advice (IA, p. 12).
[3] Proposal, p. 10; see also M. Negreiro, New ENISA and the Cybersecurity Act, EU legislation in progress, EPRS, December 2017; A. Zygierewicz, European Union Agency for Network and Information Security (ENISA), implementation appraisal, EPRS, May 2017.
[4] For instance, Internet of Things (IoT) Security and Privacy Recommendations, Broadband Internet Technical Advisory Group Report, 2016; 'Cyber risk is an Internet of Things world', Flashpoint Report, Deloitte, 2015; Global State of Information Security Survey, PWC, 2016; 'Counting the cost - Cyber exposure decoded', Lloyd's and Cyence, 2017.

Author: Katharina Eisele with Malte Krumm
Ex-Ante Impact Assessment Unit
PE 615.633

- fragmentation of cybersecurity policies and approaches across Member States;
- dispersed resources and approaches of EU institutions, agencies and bodies;
- insufficient awareness and information of citizens and companies concerning cyber threats and security properties of ICT products and services (IA, pp. 17-42).

The IA claims that ENISA is the only organisation with 'some preventive operational capabilities'[5] (IA, p. 35). However, one may wonder how this claim fits with the mission statement of Europol's European Cybercrime Centre (EC3), which includes 'outreach & cooperation', 'public awareness & prevention' and 'training & capacity building' in its strategy.[6] The IA appears to ignore a potential overlap and stresses that the evaluation of ENISA as well as the stakeholder consultations qualified the relations between EC3 and ENISA as a good cooperation.[7] However, it seems that this cooperation can be improved, as demonstrated by the call for a 'structured' cooperation with EC3 in the context of option 2 ('Reformed ENISA') (IA, p. 53). The IA predicts that the problems identified will get worse, as the number of cybercrimes and the associated costs for businesses are expected to increase. Certification schemes could become even more national and sectorial. This implies a need for increased common effort of Member States, EU institutions and private stakeholders to face cybersecurity threats. The interrelations between drivers, problems and consequences are displayed in a detailed problem tree (IA, p. 27).

Objectives of the legislative proposal

The overall objective of the Commission proposal is 'to increase resilience and enhance (the EU's) cybersecurity preparedness'.[8] The three **general** objectives of this initiative are:

- to increase cyber resilience of Member States businesses and the EU as a whole;
- to ensure a proper functioning internal market for ICT products and services;
- to increase the global competitiveness of EU companies operating in the ICT field.

Although presented as a core element and used in multiple contexts of the IA, the term 'cyber(security)-resilience' has not been further defined and remains vague.[9] The IA identifies six **specific** objectives: (i) cooperation & coordination of Member States and EU institutions; (ii) capabilities & preparedness of Member States; (iii) avoiding fragmentation of certification schemes; (iv) EU level capabilities; (v) awareness of citizens and businesses; (vi) transparency of cybersecurity assurance. According to the Commission's own guidelines, objectives should be SMART (specific, measureable, achievable, realistic and time-bound).[10] It seems that the above-defined objectives are neither very specific nor time-bound.

Range of options considered

The IA presents four policy options concerning ENISA's future status and five options related to an EU-wide ICT product and service certification framework, including the baseline options. The Commission discards two options at an early stage: option 1 on the expiry of ENISA's mandate and option 4 on ICT security internal market legislation.[11] This latter option 4 would establish an obligatory conformity assessment based on the 2008 internal market new legislative framework. Tables 2 and 3 below provide the specificities of each option. The Commission's preferred options are marked in grey.

[5] For example, the organisation of cyber exercises, the support to the CSIRT capacity building and the development of national cybersecurity strategies (see footnote 78 in IA, p. 35).
[6] Europol, European Cybercrime Centre - EC3 website, last accessed on 29 November 2017.
[7] IA, p. 38: 'There is almost no overlap between the two organisations, which seem to cooperate well'.
[8] Proposal, explanatory memorandum, p. 2; the operational objectives are specified in the section on monitoring indicators.
[9] Further criticising the vagueness, A. Bendiek et al., 'Die erneuerte Strategie der EU zur Cybersicherheit', SWP-Aktuell 72, October 2017.
[10] See Tool #16 of the Better Regulation Toolbox on 'how to set objectives'.
[11] The Commission discards option 1 because of its incoherence with ENISA's role as laid down in the NIS Directive and in the EU Cybersecurity Strategy and blueprint, missing stakeholder support, significant implementation costs of alternative services, and the co-legislators' decision to assign specific tasks to an independent agency. Option 4 is discarded due to its disproportionate burden and costs for industry, Member States and SMEs (IA, pp. 60-62).

Table 2: Options related to ENISA

Option	Substance & functions
Option 0 (baseline)	• continuance of ENISA after scheduled expiry in 2020; new fixed term mandate on equal terms • supporting tasks as provided by NIS Directive • secretariat of the Computer Security Incident Response Team (CSIRT) network
Option 2	• reformed ENISA with permanent mandate • clarified role of ENISA as EU agency for cybersecurity; structured cooperation with the Computer Emergency Response Team for EU institutions (CERT-EU), EC3 and other EU bodies • moderate review of governance architecture • stronger mandate with regard to NIS Directive, EU Cybersecurity Strategy, EU Blueprint for cyber crisis cooperation and ICT security certification • EU hub for cybersecurity information and best practices • functions as cybersecurity 'market observatory' supporting ICT standardisation and security certification • coordination of research and innovation in the field of cybersecurity • secretariat of the CSIRT network

Option 3	• ENISA with permanent mandate and with full operational capabilities covering the entire cybersecurity lifecycle
	• functions as described above under option 2
	• additionally, Computer Emergency Response Team (CERT) under ENISA's auspices, including prevention, detection and responses to cyber incident
	  ○ active technical operational assistance (expertise, human resources) to Member States CSIRTs
	  ○ new legal basis required
	  ○ produce real-time situational awareness and dynamic (live) threat intelligence feeds

Source: authors, based on IA, pp. 49-54.

Table 3: Options related to ICT certification

Option	Substance
Option 0 (baseline)	• non-EU intervention • expected market fragmentation in the coming 5 to 10 years • missing trust of market operators in ICT products and services hampering the DSM • missing economic incentive to establish high security standards • uneven levels of protection among Member States' critical infrastructure leading to increased risk of cross-border proliferation of attacks • (if existent) uncoordinated, inefficient and resource-intensive establishment of agreements for mutual acceptance of certificates
Option 1	• non-legislative option • ENISA performs awareness raising activities and functions as a platform for public and private stakeholders for exchange of views • Commission provides Member States with guidance on national and sectorial certification schemes, including certification authorities and conformity assessment bodies • support of EU-wide co- or self-regulatory initiatives and of standardisation activities

Option 2	• legislative act; incorporating the Senior Official Group – Agreement of Mutual Recognition of Information Technology Security Certificates (SOG-IS MRA)[12] into a mandatory system for all Member States • new Management Committee composed of Member State representatives, supported by ENISA, to coordinate the standardisation process as well as certification policies between national certification authorities and testing facilities
Option 3	• legislative act; new EU ICT Security Certification Framework • framework with common provisions and procedures for national certification schemes, including specific sets of security objectives and minimum content of schemes, as for instance three different level of assurance, ranging from 'basic', 'substantial' to 'high' • mutual recognition of certificates issued under these schemes • Commission can order ENISA and the European Cyber-certification Group (ECCG), composed of representatives from national certification authorities, to prepare specific European schemes, adopted by means of either delegated or implementing acts • EU schemes are initially voluntary, but future EU or national legislation can have recourse to the schemes and set them as mandatory standards for specific ICT products and services • Member States each establish one supervisory authority for complaint handling, information sharing and EU-wide cooperation

Source: authors, based on IA, pp. 54-59

Scope of the Impact Assessment

The IA assesses first the effectiveness of the options with regard to the specific objectives and analyses the different impacts in terms of economic, social and environmental impact, impact on fundamental rights and on innovation. These results are then compared and summarised in two tables (IA, pp. 86 ff., Tables 5 and 6). Finally, the Commission presents a **preference for option 2 with regard to ENISA.** According to the IA, options 2 and 3 have similar positive impacts, it seems the strong stakeholder support of option 2 was decisive. **With regard to certification, the Commission prefers option 3**.

Options related to ENISA (IA, pp. 62-70, 82-93)

In respect of **effectiveness**, option 3 is deemed to be more effective than the other options concerning EU level capabilities to support Member States and the EU's overall preparedness. Various services[13] add to the positive impacts of option 2. With regard to option 2, the IA states that it is 'reasonable to assume that the clear position of ENISA in the EU-cybersecurity ecosystem and the better definition of the links and 'bonds' with other EU institutions, agencies and bodies would result into a stronger cooperation (...)' (IA, p. 63). However, the concrete form of such a 'clear position', including relevant links and bonds to other actors in the field of cybersecurity, in particular Europol's EC3, is not further specified and remains unclear. Concerning **economic impact**, options 2 and 3 are considered as equally efficient in regard as far as a 'high value for money' is concerned. By additionally providing operational support to Member States and operators of critical infrastructures, option 3 is expected to reach more economic benefit than option 2. However, these benefits are reflected in the higher financial contribution required for implementation (option 3: €28 million per year; option 2: €23 million per year) and the higher number of additionally required staff (option 3: 70 staff, 44 full-time equivalents (FTE) in permanent positions, 26 FTE in contractual positions; option 2: 50 staff, 36 FTE in permanent positions, 14 FTE in external positions). Despite these figures, it should be borne in mind that a precise impact on the EU economy has not been estimated due to lack of reliable data and analysis; the assumption of a positive economic impact is based

[12] SOG-IS MRA is the main certification mechanism existing at European level, which includes 12 Member States plus Norway and has developed only a few protection profiles regarding digital products.

[13] For instance, the support for less equipped Member States, EU level flash reports, and real-time situational awareness reports.

on the presumed reduction of the costs of cybersecurity and -crime incidents which are estimated to stand at 0.41% of EU GDP (approx. €55 billion).[14]

The IA assumes that both options have a positive, indirect **social impact**, as they contribute to increased security and trust of EU citizens and businesses in the digital society. The IA expects a positive impact on **fundamental rights**. A positive impact is also expected with regard to **innovation** due to, among other things, ENISA's practical expertise and information sharing. No significant **environmental impact** is expected.

Options related to ICT certification (IA, pp. 70-82, 82-93)

The IA finds that a co- or self-regulatory regime under option 1 would improve the **effectiveness** regarding the above-mentioned objectives only in a limited and indirect way. Voluntary activities in the field of cybersecurity certification would establish a low incentive to invest resources to develop required expertise. By comparison**,** option 2, building on SOG-IS MRA, is supposed to establish an international fora for Member States. The IA assumes that fragmentation of certification schemes will increase under option 2 due to the limited scope of SOG-IS MRA (only used for products, not services; requiring a high level of assurance). The IA states that an EU-wide framework under option 3 would remove the co-existence of national certification schemes for products and services covered by a European scheme. Also, option 3 would give businesses a strong incentive to comply, as they could market their products more widely due to mutual recognition of certificates. According to the IA, this benefit would compensate the absence of a mandatory requirement to certify which would have improved transparency of cybersecurity assurance.[15] As regards **economic impact**, the IA ranks options 1 and 2 as equally positive, while option 3 is predicted to be the most efficient option (IA, p. 87, Table 6; see Table 4 below).

Table 4: Economic impact of ICT certification policy options

	Option 1	Option 2	Option 3
Commission	• 2 Administrators + 1 Assistant • Awareness raising campaign (€250-400 000 per year)	• 2 Administrators + 1 Assistant	• 3 Administrators • Expert Group (€16-17 000 per year) *(other costs borne by ENISA, see above)*
Member States	• 3 meetings per year (€2 500-7 000) • 2 meetings on coordinated enforcement per year (€1 700-4 700) • new implementation/soft law measures (€1 000)	• Involvement of national certification authority in meetings (€58 000 per year)	• National certification authority (€1 600 000 per year) • Enforcement and supervision (€290-300 000 per year; lower impact on present SOG-IS MRA members)
Industry	• no indication due to voluntary participation • potentially significant resources for consensus efforts	• no indication due to voluntary participation • reduced cost for present users due to EU-wide recognition	• no indication due to voluntary participation • reduced cost for users due to EU-wide recognition

Source: authors, based on IA, pp. 62-93

Regarding **social impact**, the IA states that under option 1, the incentive to encourage ICT certification would be low, and thus the support to foster trust in the DSM limited. In contrast to this, the one-stop shop mechanism for certification under option 2 could lead to a new chain of trust among vendors and operators of critical infrastructures. Yet, asymmetries with regard to products requiring medium and low level of assurance would persist due to the limited scope of SOG-IS MRA. The IA finds that option 3 would 'enable end-users to make

[14] IA, pp. 21, 65 referring to a 2014 study from McAfee & Center for Strategic and International Studies, 'Net Losses: Estimating the Global Cost of Cybercrime'.
[15] See also Table 5, IA, p. 87.

more informed purchase decisions', as it offers various level of assurances for products and services. In addition, the 'chain of trust' would be extended to the final end-user.

The IA assigns all options a positive **impact on fundamental rights**. With regard to **innovation**, the IA states that the focus of SOG-IS MRA on products requiring a high level of security under option 2 could result in firms considering 'more agile certification schemes' for their products and services requiring a low level of assurance. Under option 3, ENISA could cooperate with standardisation bodies and ensure an adequate level of security and technological innovation in a European scheme. No option has any significant **environmental impact**.

Subsidiarity / proportionality

The legal basis of the proposal is Article 114 TFEU. The IA points out that this legal basis has been recognised by the Court of Justice[16] and was confirmed by the 2013 Regulation establishing ENISA's current mandate. Referring to ENISA's task under the NIS Directive, the IA clarifies that the Agency's operational activities promote the objectives of an increased cooperation and coordination and EU level capabilities. With regard to the fragmentation of national certification schemes and the missing EU framework, the IA states that both '[hinder] the creation of an internal market for ICT products and services and [hamper] competitiveness of the European industry in this sector' (IA, p. 46). The IA identifies cybersecurity as a matter of common interest to the Union and finds that, due to interdependencies between national networks and information systems, EU intervention is necessary. In addition, this intervention is supposed to provide positive 'spill-over effects' based on the sharing of good practices and address the current fragmented certification systems. For these reasons, the IA confirms the necessity as well as the added value of EU action. Regarding proportionality, the IA finds that 'none of the options analysed (...) go beyond what is necessary to achieve the objectives (...) in a satisfactory manner' and additionally do not impede national actions in the field of national security matters (IA, p. 47). The French Senate submitted a reasoned opinion before the submission deadline of 7 December 2017. It criticised inter alia that ENISA's new mandate and the certification framework were put together in one legal text and considered that the proposal's legal base should be Article 114 TFEU, together with Article 5 TEU on security issues.

Budgetary or public finance implications

According to the IA, under option 2 (the preferred option), the current EU budget for ENISA (€11 million) would need to be increased to about €20-23 million per year. Member States would still be able to provide voluntary financial contributions to the Agency (IA, p. 65).[17] The creation of an expert group envisaged under option 3 on certification (the preferred option) would entail costs for the EU budget of €16 000 to €17 000 annually. Member States appointing a competent certification authority are expected to bear costs that would amount to approximately €1 600 000 per year (IA, pp. 79-80; see also IA, Annex 7, p. 71).

SME test / Competitiveness

The IA specifies the impact on competitiveness, competition and SMEs for each option. Under options 2 and 3 regarding ENISA, the Agency would perform several functions that 'could lead to increased competitiveness of EU businesses, in particular SMEs.' The access to free, high quality and independent information, analyses and recommendations could ease the budgets of SMEs and micro-enterprises provided that linguistic barriers can be overcome (IA, pp. 65-66). Concerning certification, the impact of option 1 on SMEs would depend on their willingness to participate in the development of guidelines, certification schemes, standards and best practices recognised across Member States (IA, p. 73). The IA states that option 2 'may have a positive effect on SMEs that already rely on the SOG-IS mechanism as they can use certificates throughout the entire EU' (IA, p. 76). Option 3 would have a very positive effect on competitiveness, as it would significantly reduce costs and administrative burden for SMEs that already certify their products and services at various level of assurance, or are willing to do so. This option would also eliminate a potential market-entry barrier (for new businesses and SMEs) (IA, p. 80). The Commission conducted a survey on certification aimed at SMEs in 2017 (IA, Annex 2, pp. 133-135).

[16] C-216/04 *UK v Parliament and Council*, ECLI:EU:C:2006:279 (judgment of 2 May 2006).
[17] See also legislative financial statement attached to the proposal, p. 82.

Simplification and other regulatory implications

The Commission notes that the proposed regulation is without prejudice to the certification of data processing operations under the General Data Protection Regulation.[18] Also, it would ensure compatibility with Regulation 765/2008 on accreditation and market surveillance requirements.[19]

Quality of data, research and analysis

The Commission used a wide variety of quantitative and qualitative research and data to underpin its IA. In addition to the ex-post evaluation on ENISA, which was conducted by the external contractors Ramboll and Carsa for the period 2013-2016 (IA, Annex 5), two studies were finalised in 2017 on ICT security certification, one conducted by the Joint Research Centre (IA, Annex 8), and the other by the external contractor Pricewaterhouse-Coopers (IA, Annex 7). The Commission also conducted two public consultations, various meetings and a series of surveys (see section below). The Commission seems generally open about data limitations. The IA further admits that 'the quality of the studies is impacted by the overall lack of evidence in the field of cybersecurity as a whole' (IA, Annex 1, p. 111). In particular, companies are reluctant to share information in this field that could potentially harm them. The IA specifies the key assumptions and sources for the economic estimates of the options relating to ENISA in Annex 6. It appears that no cost-benefit analysis was conducted.

Stakeholder consultation

The IA identifies the stakeholders affected by the problem, such as businesses, public authorities and citizens (IA, pp. 42-44).[20] The Commission organised a number of stakeholder activities, including workshops and surveys. In addition, two 12-week online open public consultations were conducted, one on public-private partnership on cybersecurity (about 240 respondents) and the other on the evaluation and review of ENISA (about 90 respondents). According to the Commission's summary report of the first public consultation, most respondents welcome the set-up of a contractual public-private partnership on cybersecurity, and ask for a few clear priority areas with strategic focus. Out of the 90 respondents to the second public consultation, 15 were Member States and 27 came from the private sector. A majority of the respondents (74 %) assessed ENISA's overall performance during 2013 to 2016 as positive. Respondents also identified some challenges for the future of cybersecurity in the EU, and a large majority (88 %) considered the current instruments and mechanisms available at EU level to be insufficient, or only partially adequate, to address these (see summary report). The IA points out that no dedicated public consultation on the ICT security certification in the EU was carried out (IA, p. 105). It argued that stakeholders were able to express their views on this issue in the two public consultations, as well as in two surveys[21] regarding ICT security certification organised in 2017. The Commission also held interviews with 50 key players in the cybersecurity community. The IA provides a general, non-exhaustive list of stakeholders consulted. However, neither the identity of these 50 key players, nor the results of the interviews, are clearly indicated (IA, Annex 2, pp. 114-115).

The IA provides a breakdown of the stakeholder support for the various options proposed. Concerning the options on ENISA, the IA reports that the vast majority of stakeholders across all categories appear to welcome option 2 (the preferred option), whereas stakeholder expressed divergent views regarding option 3 (IA, pp. 67, 69-70). With regard to certification, the IA informs that the majority of stakeholders (without specifying which) would welcome soft-law initiatives under option 1, while acknowledging that this alone would not be sufficient (IA, p. 74). Stakeholders generally praised the work of SOG-IS MRA under option 2 (IA, p. 77). A majority of stakeholders support option 3 (the preferred option); however, the need to provide adequate staff was also emphasised (IA, p. 82).

---

[18] See explanatory memorandum to the proposal, p. 13.

[19] Ibid; as far as supervisory authorities are concerned, 'the proposed regulation will require Member States to designate national certification supervisory authorities with responsibilities for supervision, monitoring and enforcement of the rules. Those bodies will remain separate from conformity assessment bodies, as prescribed by Regulation 765/2008'.

[20] See also Annex 10 on the affected stakeholders of the preferred option.

[21] The two surveys were addressed to the certification community and SMEs (IA, Annex 2, p. 105).

Monitoring and evaluation

The IA presents a number of monitoring and evaluation activities, which include the organisation of meetings with ENISA, Member States' representatives and stakeholders. Regarding certification, the Commission envisages inter alia the widening of the product and services scope covered by the EU certification scheme. The IA points out that the first evaluation should take place five years after entry into force of the legal instrument 'provided sufficient data is available' (IA, p. 97). Further evaluation should take place every five years. The IA provides a list with monitoring indicators[22] specifying the respective data sources (Table 8, IA, pp. 98-103). The monitoring indicators, which relate to the operational objectives, provide benchmarks.

Commission Regulatory Scrutiny Board

The Commission's Regulatory Scrutiny Board (RSB) first issued a negative opinion dated 24 July 2017, which the IA does not mention.[23] The RSB subsequently issued an opinion marked 'positive with reservations' on 25 August 2017. This identified persisting deficiencies and called for: (i) a better description of the context; (ii) the inclusion of the evaluation findings on ENISA weaknesses; (iii) a better explanation of the preferred option regarding certification; and (iv) the identification of monitoring criteria and benchmarks for evaluation purposes. The final IA lists in Annex 1 the RSB's main recommendations along with the modifications undertaken (IA, pp. 105-110), as required by the Better Regulation Guidelines. Overall, it seems that the RSB's criticisms have been addressed. However, more specific information on why ENISA's new mandate and the certification framework were dealt with under one umbrella would have been useful (as criticised by the RSB in its negative opinion).

Coherence between the Commission's legislative proposal and IA

It appears that the legislative proposal of the Commission follows the recommendations expressed in the IA.

Conclusions

Generally, the IA seems to provide a sound basis on which to change the current mandate for ENISA and to introduce a new cybersecurity certification framework. It appears that the IA's assumptions are based on solid research and analysis, and the Commission was open about data limitations. However, it would have been useful if the IA had provided further clarification regarding ENISA's operational role and the envisaged cooperation with Member States and other EU actors, for example, Europol's EC3. In addition, a public consultation specifically on ICT security certification in the EU could have been helpful.

To contact the Ex-Ante Impact Assessment Unit, please e-mail: EPRS-ImpactAssessment@europarl.europa.eu

Manuscript completed in December 2017.

[22] For example, one monitoring indicator relates to the number of Member States having made use of ENISA recommendations and opinions in their policy making process (Table 8, IA, p. 99).

[23] See, however, explanatory memorandum, p. 18. Unusually, the two opinions have been issued together in one document and with the same RSB meeting date.