AmCham EU

SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

The EU Cybersecurity Act proposal

Building an effective response to strengthen Europe's cyber resilience

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive Summary

With the publication of the EU Cybersecurity Act proposal, the European Commission aims at increasing the cyber resilience of the digital economy by empowering the European Union Agency for Network and Information Security (ENISA) and creating an EU cybersecurity certification framework.

ENISA

- AmCham EU welcomes the European Commission's proposal to convert ENISA into a **permanent EU cybersecurity agency**, to strengthen its powers and increase its resources. As the responsibilities of ENISA grow, it should aim to continuously reinforce its **stakeholder engagement**, well beyond the established Permanent Stakeholder Group. It will be very important for ENISA to keep and enhance its ability to cooperate with industry, in an inclusive and transparent way.

- **Raising awareness** on the need for cybersecurity amongst the entire community – vendors, service providers, industry, employees and consumers – is essential. While American business is prepared to do its fair share, public bodies including ENISA should also provide the necessary resources and investments in initiatives such as education and awareness raising campaigns on cybersecurity best practices.

Cybersecurity certification framework

- The framework should be **voluntary and market-driven in nature** as companies should be able to develop the security system features best for their unique risk situation. In order to ensure this flexibility for companies, the proposal should build on a clear approach whereby schemes are defined against standards which are identified to meet certain defined requirements and which are implemented and developed by stakeholders. The proposal should also take into account the possibility of **self-declaration**.
- In order to achieve **harmonisation** of security certificates, the possibility of mutual recognition and single conformity assessment could significantly reduce administrative costs. Furthermore, the relationship with existing national schemes needs to be further clarified.
- A **strong public-private partnership** is needed in the development of European certification. The proposed process lacks provisions for adequate transparency and openness, and is ultimately not reflecting the provisions and best practices under the WTO Agreement on Technical Barriers to Trade.
- ENISA and the European Commission need to work with stakeholders to continue to **prioritise and refine** any scope of categories and corresponding requirements under a certification scheme to accurately reflect a **risk-based approach**. The focus should be on areas where there are currently gaps and no existing schemes. Furthermore, any duplication should be avoided in sectors where a certification process is under development.
- This framework should clearly differentiate a certification scheme and the **technical requirements** against which the scheme assesses products or services. We believe certification must firmly rely on standards in place and in particular on **international standards**. Where there are gaps, standards should be defined through the European standardisation procedure.
- The compatibility of EU certificates with **international mutual recognition agreements** needs to be clarified. We recommend that the proposal includes provisions to ensure continued compatibility with international mechanisms such as the CCRA (Common Criteria Recognition Agreement) and warn against any attempt replace them.

- The set of **security objectives** seems too prescriptive compared to the broad scope of the framework. Certain of the objectives do not seem to fit very well with existing product requirements. Furthermore, the limitation of the **applicability** of certifications to a maximum of three years under Article 48.6 is problematic given the length of certification procedures.

Security by design and duty of care

- Next to certification, we believe in the potential of **security by design** to enhance cyber resilience, and look forward to supporting the work of the European Commission to promote this concept. Security by design can significantly reduce security risks and long-term costs of development.

Contents

Introduction

The presence of Internet of Things (IoT) objects is rapidly expanding, connecting humans with technology and increasing the efficiency of industrial operations. In order to make this ecosystem thrive, it is fundamental to make privacy, security, and trust a priority. Since the publication of the cybersecurity strategy in 2013, several significant legislative steps have been taken to improve network (and information) security in the Digital Single Market. Through the adoption of the eIDAS Regulation[1], the second Payment Services Directive (PSD2)[2], the Directive on security of network and information systems (NIS Directive)[3] and the Genderal Data Protection Regulation (GDPR)[4], a comprehensive set of requirements has been introduced for network and information system operators.

It is important though to stress that measures taken to improve trust and security are market-driven: It is in the industry's best interest to incorporate the highest possible levels of security in products and services, baked in through security by design and assured through stringent security standards such as the ISO 27000 series. Furthermore, cybersecurity is a responsibility of government and industry alike and the most effective way of advancing it is through public-private partnerships involving open dialogue and trusted collaboration[5].

With the publication of the EU Cybersecurity Act proposal, the European Commission aims at increasing resilience and market confidence by empowering the European Union Agency for Network and Information Security (ENISA) and creating an EU cybersecurity certification framework.

The Commission is right in proposing to make the mandate[6] of ENISA permanent, strengthen its powers and increase its resources so it can contribute even more substantially to raising cybersecurity awareness[7]. As a pan-European body, ENISA has great potential to contribute to the integration and completion of the Digital Single Market (DSM) for cybersecurity. However, as the responsibilities of ENISA grow, the agency should also aim to continuously reinforce its stakeholder engagement. The agency should also get a substantial role in building skills and raising awareness.

Furthermore, security certification is a well-established practice to enhance security of product and services. Reducing and preventing fragmentation across the EU will certainly benefit to consumers and business. However, in order for the EU framework to truly enhance cyber resilience, it is fundamental that, amongst other:

- EU certificates are voluntary;
- The certification process is inclusive;
- The scope is targeted;
- Schemes are defined against existing European and international standards.

[1] Regulation (EU) N°910/2014

[2] Directive (EU) 2015/2366

[3] Directive (EU) 2016/1148

[4] Regulation (EU) 2016/679 - in particular its provisions on the security of processing and the notification of personal data breaches

[5] Important initiatives are for instance the contractual public-private partnership on cyber (Cyber cPPP), the Network and Information Security Platform (NISP), the European Multi Stakeholder Platform on ICT Standardisation (MSP), the existing Cloud Select Industry Groups (C-SIGs) and the Alliance for IoT Innovation (AIOTI).

[6] Regulation (EU) N°526/2013

[7] AmCham EU's reply to the public consultation on ENISA, here.

This paper outlines hereafter detailed comments on both parts of the Commission proposal. Furthermore, it gives some views on security by design and the notion of duty of care as other tools that can play an important role in increasing cyber resilience, in reaction to the European Commission communication on *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*.

ENISA – the 'EU Cybersecurity Agency'

AmCham EU supports the Commission's proposal to convert ENISA into a permanent EU cybersecurity agency, strengthen its powers and increase its resources. It will enable the agency to contribute even more substantially and effectively to awareness-raising on cybersecurity in the EU and strengthening collaboration between public and private stakeholders across the EU and beyond to tackle cyber threats.

1. Maintaining and deepening stakeholder involvement

ENISA plays a key role in further integrating the DSM from a cybersecurity standpoint. As its responsibilities grow, it will be very important for the agency to sustain and enhance its ability to cooperate in an inclusive and transparent way with the private sector as well as international partners and standards certification bodies such as the US National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO). A close partnership with industry is critical to achieve higher levels of cybersecurity. In many cases, industry plays a leading role in providing software, services and hardware that protect public and private organisations from cyber threats.

This inclusive cooperation goes much further than the established Permanent Stakeholder Group (PSG) and is of critical importance for the proposed EU cybersecurity certification framework. ENISA should play a central role in defining EU cybersecurity schemes in close partnership with relevant stakeholders. While **Article 44** of the draft regulation states that 'When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders and closely cooperate with the Group', the processes and rules of engagement of ENISA with 'relevant stakeholders', including industry, should be clearly defined in the Regulation.

As the responsibilities of ENISA grow, it should continuously reinforce its stakeholder engagement beyond the PSG. Where appropriate, this could take place through regular public consultations with adequate response timing to allow private stakeholders to efficiently contribute to ENISA activities. In order to enhance its accountability, ENISA should also streamline its consultation policy and publish periodic reports summarising how stakeholders' views have been taken into account. Furthermore, ENISA could build upon positive experiences of multi-stakeholder dialogue, such as the Stakeholder Forum of the Body of European Regulators for Electronic Communications (BEREC). For instance, the agency could set up a platform for strategic dialogue enabling active participation by all key stakeholders to reflect on key developments and future challenges for the cybersecurity sector.

2. Raising awareness and developing critical skills

Raising awareness on the need for cybersecurity amongst the entire community – vendors, service providers, industry, employees and consumers – is essential. American companies are willing to support such efforts. However, it is critical for ENISA and other public actors to commit resources for initiatives such as education and awareness-raising campaigns on cybersecurity best practices. These can help to increase the scale and impact of efforts such as the proposed certification framework.

The challenge security brings is not just technical, but also deeply human. Indeed, it very much relates to issues such as awareness, best practice, usability and exploitation of human weaknesses. Particularly with the exponential growth of IoT, even small improvements in public awareness of and attitudes towards cybersecurity can help improve security. Therefore building and improving cybersecurity skills is critical.

It is also fundamental to ensure that ENISA itself is in a position to attract and retain top talent in cybersecurity from across the EU. We welcome that the proposal foresees additional staff capacity for the agency. However, filling those positions could become a real challenge if adequate incentives are not in place.

In this context, with additional powers and resources, ENISA's role could evolve to become:

- The standing institutional custodian of cyber-policy dialogue between EU policy-makers, the private sector and civil society;
- A center of excellence to develop awareness raising, education and training;
- An authoritative and neutral point of reference for cybersecurity good practices and benchmarking;
- A capacity building and capability validation services provider on a commercial basis to both public and private sector customers.

The EU Cybersecurity Certification Framework

Security certification is a well-established practice that can play a role in increasing resilience and awareness for business users and consumers. However, the certificates should be voluntary, the process needs to be inclusive, the schemes must be international in nature and closely linked to standards.

If not developed carefully, certification risks giving customers and consumers a false sense of security and safety. Effective security requires a strong and on-going commitment to security governance which includes the continuous assessment of defenses against emerging threats.

Additionally, there is a strong risk that schemes that are not based on international standards and existing certification approaches could have a negative impact on the European cybersecurity market by creating market entry barriers or raising costs for non-EU headquartered companies.

1. A voluntary and market-driven approach

Any European security certification system should follow a voluntary and risk-based approach to cybersecurity which encourages companies to innovate while developing secure systems at the same time. Individual companies will also retain the flexibility to best determine and mitigate their own risks, which will vary by sector, size and sophistication.

Government mandates for specific security features may force companies to focus their efforts on meeting a standard that may or may not be right for their risk level, instead of developing the most adequate security system features for their unique risk situation. They will also tend to limit the ability of companies to react in comparison to the agility of threat actors.

In order to ensure this flexibility for companies, the proposal should build on a clear approach where:

- Requirements are defined in the certification scheme and standards are identified with which those requirements may be met;
- Standards are implemented – and, if needed, new standards are developed – by the stakeholders to meet those requirements;
- Certification is done against these standards.

The Regulation should also take into account self-assessment for analysing the compliance with requirements. Such a model follows well established processes in Europe where standards are at the centre of achieving compliance. This enables to provide industry and all stakeholders with clarity about the requirements and standards to be implemented and which can be taken into account for in the planning of development and technology innovation.

In order to define EU-wide cybersecurity standards for classes of products and services, the existing European standardisation system embodied in Regulation 1025/2012 should be used, building on global standards where possible. This will be the best way to achieve EU-wide reconciliation of technical requirements into a single standard recognised by all Member States.

2. A harmonised approach to certification

A matter of concern for industry is the potential for a patchwork of inconsistent national laws in this area that will divert resources towards complex compliance efforts and away from innovation. AmCham EU therefore welcomes the Commission's objective to reduce administrative costs and ensure there is a stronger and more harmonised approach to cybersecurity certification. In order to achieve harmonisation, the following elements are particularly important:

- Resources should be based on mutual recognition as outlined in **Article 48**. This would allow for a certification received in one Member State to be applicable in other Member States, reducing compliance costs.
- A specific recognition should be included in the proposal that applications can be made to any Conformity Assessment Body of choice.
- **Article 49** states that national schemes will cease to exist from the moment a European certification will be in place. It is unclear how this process will work precisely and needs further elaboration.

3. An inclusive governance model

AmCham EU is concerned that the proposed process for creating certification schemes lacks transparency and openness and is ultimately not taking into account the provisions and best practices under the WTO Agreement on Technical Barriers to Trade (WTO TBT Agreement). As it stands, the proposed framework gives full and sole discretion to the Commission to decide what cybersecurity schemes are required within the EU, whether standards apply to a scheme and what types of products or services are covered by a scheme. **Article 44(2)** requires ENISA to consult with stakeholders but does not specify how this is to be achieved, nor whether stakeholders can participate in the drafting of a scheme. This ignores the value of standardisation and creates uncertainty in the market place regarding the adoption of high cybersecurity standards.

A strong public-private partnership is needed for the development of European certification. The private sector is well-positioned and already encouraged today to both secure its own technologies and share best practices with others to promote a secure digital ecosystem. Governments can often develop the best security policies by collaborating with the private sector and obtaining cooperation and 'buy-in' from all stakeholders. This is much more effective than pursuing mandates which will only have the effect of driving industry to the lowest common denominator and taking away resources for actually performing security.

Industry is also well positioned not only to build and maintain the security of its own technologies but to share best practices and to join with others in helping to secure the digital ecosystem. The private sector has vast capability to spur capacity building through training and awareness, and to enhance collaboration operationally resulting in shared best practices, better threat detection technology, and better threat analysis capability. Industry collaboration internationally continues to grow rapidly, and these networks, as well as those developing between governments and industry will establish better lines of communication when dealing with cross-border cybersecurity incidents.

4. A clear scope reflecting a risk-based approach

While the proposed framework recognises that one-size-does-not-fit-all, AmCham EU is concerned about the broad scope of 'ICT products and services' (**Articles 43 & 47 (1.a)).** The draft Regulation refers to 'ICT products and services,' defined as 'any element or group of elements of network and information systems' (**Article 2(11)**), while also referring to 'processes […] systems, or a combination of those' (**Recital 47**).

The elements in the scope of a proposed EU-wide scheme should be decided taking a risk-based approach. Not all applications and systems pose the same level of cybersecurity threats to the economy. Any tiered levels of requirements and/or controls should be defined based on the risk profile of applications. However, they are generally problematic as they are not used in international standards and certification schemes, since you either fulfil certain requirements or you do not. Furthermore, a low tier level is not likely to increase trust.

As the categories proposed by the Commission remain broad, it is important for ENISA and the Commission to work actively with stakeholders to continue to prioritise and refine any scope of categories and corresponding requirements under a certification scheme to accurately reflect a risk-based approach.

We understand that one driver for the proposal is the focus on IoT. If this is the case, further clarification is needed. The proposal should define whether all objects connected to the internet would be subject to the framework (from autonomous vehicles and smart phones to fridges and baby toys) or only a subset of this group. An option could be to create categories based on the impact of cyber breach. If these schemes do not define clearly which products and services they cover and how they relate to standards, then they will create ambiguity, be difficult to implement and monitor, and thus fall short of improving cybersecurity resilience.

The proposal should focus on areas where there are currently gaps and no existing schemes, such as consumer-oriented IoT devices. In this area, a voluntary industry-led approach such as a code of conduct laying out processes and adherence to relevant standards would be a more effective approach than top-down regulation. There are already some proposals for such a scheme and these should be examined at EU level. In addition, any schemes should carefully define which objects fall into the category of consumer-oriented IoT devices. The specific challenges of consumer device security, which must balance effectiveness with usability, should also be taken into account.

Finally, it is important to avoid duplicating efforts in certain sectors where a certification process is under development, such as:

- Under the UNECE World Forum for Harmonisation of Vehicle Regulations for the automotive sector;
- Under International Civil Aviation Organization (ICAO) for the aviation sector;
- Under the International Telecommunication Union (ITU) for telecommunications service.

5. A strong reliance on European and international standards

This framework should clearly differentiate between a certification scheme and the technical requirements against which the scheme assesses products or services. Those requirements should be embodied in a standard and the development of such standards should follow requirements and recommended practices under the WTO TBT Agreement.

Codifying technical requirements into a scheme itself risks by-passing transparent and open standardisation processes. European Standardisation Organisations' (ESOs) processes are structurally set up with these characteristics. AmCham EU welcomes the strong involvement of ENISA in defining cybersecurity schemes and understands that this is not part of the proposal. However, we wish to draw attention to the fact that ENISA is not a standards body, and thus processes and rules of engagement with ENISA are not defined in a similar manner.

The established standardisation system with its full-consensus process gives control to ESOs' and national standards bodies, allows for industry representation and has a track record of supporting EU legislation. Moreover, the ESOs, national standards bodies and international standards organisations have processes in place to adequately cover intellectual property rights that may be related to technologies used in standardisation.

Certification should rely to the extent possible on standards in place and in particular on international standards (for example ISO 27001 and its extensions). If there is a need to define new standards and thereby new certifications, ENISA should consider in the first place if international standards exist. Standards such as ISO 27017 may, if needed, be transposed into European standards.

Where there are gaps, European standards should be defined through the normal procedure. The process of developing such certification schemes at European level should not be circumvented using the argument that the standards development process in Europe is too slow. International and European cybersecurity standardisation should not take the approach of defining certification schemes which differ from international and European standards.

Standardisation bodies have already produced cybersecurity standards for ICT technologies and ICT infrastructure, products, hardware and software. In the proposals the schemes should reference recognised international standards. European standards can help reduce fragmentation across Member States, but these should also reflect international, consensus-driven standards when possible.

6. A compatible framework with international mutual recognition agreements[8] (MRAs)

The Common Criteria Recognition Agreement (CCRA) is an international mutual recognition agreement that ensures international mutual recognition for IT product certifications. User communities (either national or multinational groupings) specify security requirements for classes of IT products – e.g. firewalls or smart cards – known as Protection Profiles (PPs). Certifications against such PPs are recognised internationally. Where PPs have been established by national supervisory authorities and are subject to replacement by a European cybersecurity certification scheme, it is not clear how or whether the broader international recognition of such a scheme is to be maintained. Likewise, where Member States recognised international PPs, we are concerned how these may be superseded by the European scheme without proper consultation.

Within Europe, SOG-IS (Senior Official Group – Information Systems Security)[9] develops its own set of PPs. Certifications against them are mutually recognised across a number of Member States. Given that the certification framework has the potential to develop schemes that cover the same ground, it is essential that the national supervisory authorities that take part in SOG-IS buy into the concept of the framework. If not, we risk parallel certification activities or requirements for testing outside the scope of official certification and the goal to reduce certification fragmentation will not be met.

We recommend that the proposal includes provisions to ensure continued compatibility with international mechanisms such as the CCRA as opposed to attempting to replace them, which would have the opposite effect to the stated aim to reduce fragmentation.

7. Non-prescriptive security objectives

The framework is trying to cover a wide-range of certifications and types of devices and services and these may not easily boil down to one set of security objectives, as listed in **Article 45**. In general, it is better to set an overarching goal as opposed to prescribing how to get there – which is the realm of the certifications themselves. In addition, adding specific security objectives to the legal text is the wrong approach, these should be in a technical annex.

For example, some of the objectives do not seem to match very well with existing product requirements. **Article 45 (f)** is an objective to restore availability – which is largely the domain of the entity operating the devices rather than the device itself. **Article 45 (d) and (e)** also presume ongoing management of products in their operational environment, which is not something under the control of the device manufacturer.

Article 45 (g) requires that ICT products and services are provided with software that does not include known vulnerabilities. It is not unusual, however, for products to be shipped with vulnerabilities that do not represent a specific risk in their common operational environment. In other words, the product may only need to be resistant against attacks performed to a particular level of sophistication and one

[8] The Mutual Recognition Agreements between the EU and a third country lay down the conditions under which one Party will recognise the conformity assessment results of the other Party's conformity assessment bodies. See: https://ec.europa.eu/growth/single-market/goods/international-aspects/mutual-recognition-agreements_en

[9] https://www.sogis.org/

needs to assess the attack vector needed to take advantage of the vulnerability. As such, this security objective would be better worded as a requirement to assess vulnerabilities.

8. A point-in-time certification

There are several provisions that presume a continuous compliance approach in the framework, including in **Article 47.1(g), 47.1(j)** and **Article 48.6**. This fails to recognise certifications that amount to the assessment of a specific product at a particular point-in-time.

The limitation of the applicability of certifications to a maximum of three years under Article 48.6 is particularly problematic. Given that existing product assurance certifications can take 12 to 18 months to achieve, and the diversity of products and of vulnerability patterns, the validity period should be made optional in the proposal and decided on a case-by-case basis.

Security by design and duty of care

Besides cybersecurity certification – which assesses the security of a product at a particular point in time – other tools can play an important role in increasing cyber resilience, such as security by design and the notion of duty of care. AmCham EU strongly welcomes the focus on security by design as outlined in the Communication *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. In today's fast paced digitised economy organisations need to focus on speed to deliver optimal user experiences. This also means that security needs to be integrated in the overall process and cannot be a mere afterthought. Organisations across all sectors, including the public sector, must therefore integrate security throughout their development processes. This will allow organisations to significantly reduce the security risks and long-term costs of development. A security by design approach should be cultivated throughout the organisation. It should start with strong governance models, so that organisations are aware of cybersecurity responsibilities and roles, and move down to secure development methods. A voluntary multi-stakeholder approach to define essential building blocks in promoting those is the right way forward.

Conclusion

The EU Cybersecurity Act lays down important measures to strengthen Europe’s cyber resilience. The empowerment of ENISA is critical in order to strengthen the Digital Single Market from a cybersecurity standpoint. ENISA should evolve to be the standing institutional custodian of cyber-policy dialogue between EU policy-makers, the private sector and civil society, and be the center of excellence to develop awareness raising, education and training. As its responsibilities grow, it is crucial that the agency continuously reinforces its stakeholder engagement, well beyond the established Permanent Stakeholder Group. Furthermore, the agency needs to be equipped with adequate resources as well as be able to attract and retain highly qualified workforce.

EU security certificates can provide an effective tool to increase market confidence in products and services. The framework for defining EU certificates needs to be voluntary and closely involve the privacy sector. The proposal should build on a clear approach whereby schemes are defined against standards identified to meet certain requirements and implemented and developed by stakeholders. Furthermore, in order to provide an effective tool, EU security certificates should be truly harmonised and rely on a single conformity assessment. Their scope of categories and corresponding requirements should accurately reflect a risk-based approach and focus on areas where there are no existing schemes. It is fundamental that the requirements under each scheme are fully defined against international and – if not available - European standards. Also, the broader international recognition of such a scheme needs to be ensured as currently different international mutual recognition agreements are in place.

Security by design and duty of care should be promoted as effective tools to increasing cyber resilience. Integrating security in their overall development process, will allow organisations to significantly reduce security risks and long-term development costs.