

*OFE's response to the Inception
Impact Assessment on ICT
security certification*

August 2017



***OFE's response to the Inception Impact Assessment
on ICT security certification ¹***

Security is a core priority for the Information Communication Technology ('ICT') sector, in order to prevent abuse, cyber crime, and attacks on critical infrastructure, to protect personal information, and thereby to mitigate related socio-economic cost. The ICT sector has a vested interest in supporting these aims in terms of bolstering trust, which translates into high levels of market acceptance and increased uptake of innovation. Moreover, such adoption plays a major role in the context of Europe's digitisation and global competitiveness.

OpenForum Europe ('OFE') has long addressed this topic, and runs a cybersecurity task force, which investigates needs and best practices as well as on strategic and technical directions for improving cybersecurity, educates around the key issues, promoting the use of standards and providing input into policy discussions and analyses. Therefore, OFE wishes to contribute by responding to the latest Impact Assessment, and appreciates the Commission's invitation to stakeholders to provide further input and comments.

OFE would like to offer the following thoughts and recommendations as inputs for further discussion and exchanges. We believe that further discussion and analysis are required before any decision as to the best methods for further improving cybersecurity is taken. Especially, decisions about whether certification should be mandatory, whether trust labels would help, and whether regulation – and if so, in what respect – would be a promising way to pursue an in-depth analysis on the expected benefits and on innovation in the area of cybersecurity.

***Further discussion and analysis are required before any
decision as to the best methods for further improving
cybersecurity is taken***

”

¹ Ares(2017)3436811 ("Proposal for a Regulation revising ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework")

1. The importance of cybersecurity for the Digital Single Market

The Digital Single Market ('DSM') mid-term review re-confirmed the importance of cybersecurity within the context of digital priorities for the region. In the 2016 Cybersecurity communication², the European Commission announced that it would develop a proposal for a European ICT security certification framework to be presented in 2017. Specifically, the Commission undertook to explore ICT security certification within critical infrastructure sectors, such as in aviation, railways, automotive, and within specific certification and validation mechanisms of ready-to-be-deployed technology. In this regard, the Commission committed to address identified gaps under the European ICT security certification scheme mentioned above. To the extent possible, efforts are to build on internationally recognised standards. In this context, the Commission also expressed its intention to explore options related to how best to integrate ICT security in future sector-specific legislation, which also relates to safety aspects.

Parallel to the evaluation of possible regulatory options, the Commission said that it would explore the creation of a European, commercially oriented, voluntary and lightweight labelling scheme for the security of ICT products. This has since been further elaborated in policy discussions, e.g. in the context of the Internet of Things ("IoT"), and has been suggested as a potential item for a Trust in the Digital Single Market³ package in Spring 2017.

Finally, by way of background, on 6 June 2017 the Commission (I) published an Inception Impact Assessment: (a) of the Proposal for a Regulation revising ENISA Regulation (No 526/2013); and (ii) laying down a European ICT security certification and labelling framework; and (ii) sought stakeholder inputs in response to four specific options that the Commission is considering in the area of ICT security certification. Below, these options are considered.

² COM(2016) 410 final (COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry).

³ COM(2011) 942 (COMMISSION COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A coherent framework for building trust in the Digital Single Market for e-commerce and online services).

2. Comments on the Policy Options

In its inception report, the Commission emphasises that the final option will need to ensure that European standards should be compatible with or based on international standards, whenever that is possible. This is extremely important, because cyber attacks know no borders, and therefore global standards and related certifications play an even more significant role in increasing the security of networks and devices. Moreover, the Commission pledges that in case a policy option establishing a certification framework is chosen, such framework should not stifle innovation and competition, and should be within reach for small and medium enterprises (SMEs). For OFE, this means that the solution being considered by the Commission will need to be flexible and adaptable. In order to effectively combat malicious attackers, industry must be able to invent, develop and deploy new tools to protect IT technologies against ever-changing cyber risks. Having the aforementioned principles in mind, which solution best fulfils the objective so as best to secure Europe's digital transformation?

Cyber attacks know no borders, and therefore global standards and related certifications play an even more significant role in increasing the security of networks and devices



General consideration: security – public versus private responsibility

A basic and overriding theme – as reflected in the Impact Assessment and the different options – is to analyse the extent to which: (i) regulation should be enacted in the area of cyber crime; (ii) cybersecurity represents a public good where the regulator must be active to protect the people, and their way of interaction; and (iii) such protection is a private responsibility with no role for the regulator to play? In this context, a major step has been taken with the definition of critical infrastructures and the respective requirements outlined in the Network Information Security (NIS) Directive. On that basis, the discussion now concerns whether there is any need for further regulation around cybersecurity.

Further regulation does not seem per se to lead to better security in the area of ICT. Regulatory measures can only create a basis for the IT market to make sure that security is considered in an adequate way in IT technologies and solutions. To make sure that the best technologies are used and are state-of-the-art will largely remain a private responsibility of users and customers of IT technologies.

Further regulation does not seem per se to lead to better security in the area of ICT



Thus whilst some basic requirements around cybersecurity may be set in the form of regulation, what remains most important is to promote innovation, so that new methods and ways for constantly improving cybersecurity are developed. Initiatives to improve guidance on how to achieve best-of-class security should be provided (the associated development and drafting may be done in standards bodies with the involvement of all stakeholders).

A major flaw in the options put forward by the European Commission is the absence of a holistic approach for combating cyber threats. Most importantly, the development and adoption of a voluntary framework profoundly reduces the instances and scale of financial loss and the impact and severity of security breaches that arise from cyber-attacks against critical infrastructure, government assets, private sector businesses, and the academic and not for profit sectors.

This is best accomplished through a ‘risk management’ approach which seeks to move to and maintain a desired, optimal cybersecurity state based on the unique needs, considerations, and best practices of the organization’s industry and business model. Traditionally, cyber risk management relied heavily on the development of “checklists” that can be used by public or private entities to measure compliance. Events in recent years have made it clear that individuals and organizations of all sizes, including businesses, governments and NGOs, must learn to more effectively manage their cyber risks in order to avoid catastrophic consequences to their own well-being as well as the well-being of the economy and national security⁴.

⁴ An example for such ‘risk management’ is the voluntary risk-based approach is provided by the NIST Framework. It consists of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, which provide detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework aims to help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources. The Framework Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

Specific comments on the preliminary policy options: Certification

(0) On the baseline scenario

OFE agrees with the analysis and the risk of further fragmentation. Many certification schemes are already in existence, including those in a variety of Member States. The goal should be focused on reducing fragmentation and promoting a consistent approach, thus reducing confusion. In particular, rather than looking for various certification or labelling schemes, methods should be explored that are less fragmented and that build on well-established processes used in Europe, e.g., methods similar to the New Approach / New Legislative Framework, which work well in other critical areas, where there is some public responsibility in protecting users and consumers, such as product safety.

Unfortunately, no such discussion and analysis have yet taken place, partly because the discussion about certification and labelling has taken precedence, with a lot of vested interests involved (e.g., in groups and organisations expecting to make business out of any certification scheme).

The goal should be focused on reducing fragmentation and promoting a consistent approach, thus reducing confusion. Unfortunately, no such discussion and analysis have yet taken place, partly because the discussion about certification and labelling has taken precedence, with a lot of vested interests involved

”

(i) On Option 1: Support Industry led-initiatives

Option 1 proposes that more Member States be encouraged to join the Senior Officials Group – Information Systems Security (SOG-IS), and actively to promote/support its activities (i.e., to support voluntary sector-specific industry-led initiatives). A possible role for ENISA would be to contribute (by means of technical expertise) to the development of technical specifications and standards relevant to ICT security certification. This option has many positive points. For a long time, industry and other stakeholders have taken up the topic of cybersecurity in standardisation. Respective standards are available and standardisation activities are ongoing in a number of organisations. These include first and foremost ISO/IEC JTC 1 SC27, which can be seen as the global focal point for

cybersecurity standards. But extremely important activities are also underway in relevant global standards bodies that have leading roles for the internet and the world wide web, most notably in the IETF, W3C and OASIS. Recently also the European Standardisation Organisations (ESOs) have started work in the area of cybersecurity, which may add to the portfolio of high-quality standards available and under way.

There seems to be a need for solid information about all available standards, including those from global standards bodies - with particular emphasis on the latter, which are sometimes not considered in EU policy contexts. Therefore, some action should be taken to identify and map all standards and provide information about the issues they address, including with respect to compliance with the NIS Directive and to the General Data Protection Regulation ('GDPR'). Such information is best gathered through the application of an open and transparent process, in and across standards bodies.

The key focus should be on promoting, through education and a voluntary framework, a 'risk management' approach to cybersecurity. Standards are a piece of that strategy. However, standards alone will not be sufficient. Cybersecurity also very much depends on technologies implemented on top of the standards. Competitive technologies are available and new ones will continue to be developed. Addressing the increasing, complex, and unavoidable cyber risks in the modern world requires organizations to develop and implement a risk management programme that identifies, assesses, and prioritizes cyber risks, and incorporating it into their overall enterprise risk management. It is important to increase the awareness about the different elements – or building blocks – for implementing cybersecurity technologies.

The key focus should be on promoting, through education and a voluntary framework, a 'risk management' approach to cybersecurity

”

Therefore, option 1, by going one step further than the baseline scenario, offers a potential approach that recognizes the need for flexibility and efficiency, whilst creating global solutions. However, it lacks recognition that, first and foremost, a 'risk management' approach is a primary goal for organizations. Moreover, in the technical field, formal standards development organizations are not the only way that cybersecurity standards are set and maintained. In this regard, OFE

encourages Member States to continue their work (and join, if not currently a member) to harmonize approaches through the Common Criteria Recognition Arrangement, instead of the SOG-IS (which is just a subset of the former, and useful only for high assurance products). Moreover, the European Commission should ask the ESOs to set up a joint activity for the development of a European Cybersecurity Framework. Follow-on activities to a Cybersecurity Framework could be (e.g.) guides and use cases.

On Option 2: European ICT certification and labelling

Option 2 proposes a European institutional framework for ICT certification and labelling through a legislative instrument, without however introducing new ICT security requirements for specific products and services.

Certification and labelling are traditional instruments for checking technology against a pre-defined set of criteria and so testify that the criteria are fulfilled (e.g. energy consumption labelling on a fridge). This is a rather static way and the set of criteria against which certification is done can only be a basic minimum level set of measures. But cyber crime is fast-moving, ever changing, and creating new challenges all the time. Thus no basic set of minimal measures will provide security. Therefore, any certification along these lines, and any respective labels, run a high risk of suggesting that appropriate security is in place, and thus of creating “pseudo-trust”. This may have the reverse effect that IT users are made to believe that there is security in the technologies, systems and tools they use and thus neglect to take further action themselves, which would however be an absolutely pre-requisite to achieving the levels of protection and security level which users require.

Certification and labelling are traditional instruments for checking technology against a pre-defined set of criteria and so testify that the criteria are fulfilled

”

At the same time, this does not mean that it would make no sense for a provider of IT technologies to certify that it has taken a number of specified measures to ensure cybersecurity. A number of standards are already available which describe the steps that need to be taken in the area of cybersecurity. Confirming that the respective standards have been implemented can lay a certain foundation.

Yet, it is questionable whether this is a task for certification and labelling. Under the EU New Legislative Framework / New Approach, Europe has a well-working system in place for regulated domains, such as product safety: the legal requirements laid down in a Regulation or a Directive can be met through standards. Today, technology vendors can give a 'Supplier's Declaration of Conformity' (SDoC) that they implement in the respective standard(s), and thus may operate under the Presumption of Conformity. This system has worked well for decades, has become a role model for other regions and has helped to ensure a high level of safety and consumer protection in many different technology areas.

In a similar way, for a precise set of products the regulator could request industry to confirm that certain standards in the area of cybersecurity have been implemented. But everyone needs to be aware that this will only be a starting point: real security can only be achieved if proper technologies are then implemented on top of these standards. As a first step, however, it will be important to identify the full set of standards that could be used in this context, and to analyse with stakeholders (i) the extent to which they provide security, and (ii) what is needed on top - which is not a matter for standardisation. Further discussion and analysis is needed to fully address these questions.

New technologies - such as cognitive technologies and artificial intelligence - will increasingly be used to raise the level of cybersecurity and to provide better services to IT users at every level. It is important to provide room for such innovation, rather than to level down security to a basic minimum

”

The European Commission should work with ESOs and relevant global fora/ consortia in order to identify and better understand the role of standards in the context of an ever more complex and dynamic cybersecurity threat landscape. The European Commission might consider implementing a process similar to the well-established New Approach, relying on close collaboration with IT technology vendors and other stakeholders and users on the well-established and proven process of Supplier's Declaration of Conformity and the Presumption of Conformity. Moreover, given the technology challenges of today, certification and labelling, with their naturally static approach, are rather “old-fashioned” and it is questionable whether such a process is capable of addressing the real issues. New technologies - such as cognitive technologies and artificial intelligence - will increasingly be used to raise the level of cybersecurity and to provide better services

to IT users at every level. It is important to provide room for such innovation, rather than to level down security to a basic minimum.

On Option 3: Propose an ICT security legislation based on the 2008 New Legislative Framework

Option 3 proposes the creation of ICT specific legislation based on the 2008 New Legislative Framework. As shown in option 2, this option is to be preferred over that of creating labels and certification schemes. Indeed, in the area of ICT it may be said that eventually the European Commission will need to consider implementing a process similar to the well-established New Approach, relying on close collaboration with IT technology vendors and other stakeholders and on the well-established and proven process of the Supplier's Declaration of Conformity and the Presumption of Conformity.

Cybersecurity users and providers do not need Europe-specific standards. Solutions in the area of cybersecurity must be global



As the Commission points out in its inception document, this would require the adoption of a new legislative instrument setting out mandatory harmonised requirements and conformity assessment mechanisms to ensure the security of specific ICT products and services. Compliance with harmonised standards published in the Official Journal of the EU would give a presumption of conformity with the security requirements set out in the legislative instrument. ENISA could cooperate with standardisation bodies in developing these standards that are in line with the state-of the art in the field of ICT security. The drawback of this option is timing, due to its lengthy process.

Cybersecurity users and providers do not need Europe-specific standards. Solutions in the area of cybersecurity must be global. However, it may be beneficial to transpose existing international and global standards - including CC protection profiles - into European standards, so as to reduce the number of standards in play.

3. Conclusions: right solution for the right time

Of the four options proposed by the Commission, option 2 could seriously harm the current ICT cybersecurity framework and the Commission's leadership role in this increasingly global policy arena. No label will ever be able to certify that a necessary level of security has been reached. Certification and labelling risk giving a wrong impression, in turn leading to greater damage in the end. Therefore, option 2 should decisively be ruled out. Too much time and too many resources have already been absorbed by option 2, at the cost of assessing other more effective approaches.

Option 1 is worthy of further discussion, as noted above. If the problem identified in the option baseline scenario is that there is fragmentation, then the solution envisaged here is to create an ecosystem where there is further collaboration and alignment. Moreover, as suggested above, the European Commission could double down on its role within the Union to direct and orchestrate effective interaction and collaboration between the different stakeholders. For this, Member States, if not involved already, should join the Common Criteria Recognition Arrangement (as opposed to only engaging in SOG-IS activity). Moreover, the Commission should ask ESOs to set up a joint activity for developing a European Cybersecurity Framework that would describe how the respective standards address security requirements laid down in EU regulation and would address further issues like risk management.

There is a clear need for further and on-going discussion and analysis before deciding on the methods for further improving cybersecurity in a sustained and effective manner, and focusing attention on furthering the voluntary adoption of a 'risk management' model

”

Option 3 presents a number of pitfalls, described above. Regulation would increase the rigidity of the cybersecurity ecosystem without a clear case for benefits or increased clarity. At best this could be considered for products where market access issues already exist, such as smart meters. Moreover, it is a lengthy process, and some initiatives (such as those proposed in option 1) could contribute in a more timely fashion to the achievement of the right legislative framework. Europe-specific standards are not and cannot be the solution to a global threat. Transposing existing international and global standards into European standards

will create the benefit of relying on the best possible, international technology and of adopting them in a consistent way for Europe – ideally within the context of a European CyberSecurity Framework as proposed above.

There is a clear need for further and on-going discussion and analysis before deciding on the methods for further improving cybersecurity in a sustained and effective manner, and focusing attention on furthering the voluntary adoption of a 'risk management' model. Such discussion and analysis should further put the user needs into focus and avoid being overshadowed or even precluded by attempts from certain groups to push for certification and labelling without addressing the flip-side of such an approach and the risks that it would bring. Indeed, significant caution should be used with respect to any decision as to whether certification is the right instrument and should become mandatory, whether trust labels will help, and whether regulation – and if so, in what respect – could better secure Europe's citizens and organisations. The publication of the Inception Report by the European Commission is an important part of that on-going process. We welcome the opportunity to provide input on the solutions advanced by the European Commission and we look forward to assisting further in this important work.

For more information, please contact OFE's CEO Sachiko Muto at sachiko@openforumeurope.org or OFE's Director for Policy and Research Diana Cocoru at +32 485 21 76 07 or diana@openforumeurope.org

OpenForum Europe (OFE) is a not-for-profit, independent European based think tank which focuses on openness within the IT sector. We draw our support not only from some of the most influential global industry players, but most importantly from across European SMEs and consumer organisations and the open community. OFE also hosts a global network of OpenForum Academy Fellows, each contributing significant innovative thought leadership on core topics. Views expressed by OFE do not necessarily reflect those held by all its supporters.

OFE Limited, a private company
with liability limited by guarantee
Registered in England and Wales with
number 05493935

Registered office: Claremont House,
1 Blunt Road, South Croydon, Surrey
CR2 7PA, UK

