



September 30, 2019

EU Cyber Security Team (4/48)
Department for Digital, Culture, Media and Sport
100 Parliament Street
London
SW1A 2BQ

Subject: EU Cyber Security Certification (EU Exit) Call for Views

Dear EU Cyber Security Team:

The U.S. Chamber of Commerce welcomes the Department for Digital, Culture, Media and Sport's (DCMS') September 11, 2019, Call for Views on European Union (EU) Cyber Security Certification and its expressed desire to maintain a close relationship with the EU on cyber security. The Chamber supports the government's preference to enter into negotiations with the EU on mutual recognition arrangements, where it seems reasonable to do so and subject to agreement with the EU.

The EU Cyber Security Act (the Regulation) is intended to harmonize cyber security certification schemes across the Union in order to strengthen the digital single market and enhance the security and resilience of the information and communications technology (ICT) ecosystem. The certification framework envisioned under the Regulation spares U.S. businesses from having to certify products and services with multiple national certification authorities. Importantly for the Chamber and its members is the applicability of EU certifications across all member states.

The Chamber appreciates that the U.K. government was an active participant in shaping the Regulation and its goal of preventing fragmentation of the digital economy. We continue to work with international stakeholders to fashion consensus and industry-driven policy approaches to security.

The Chamber offers the following principles for considering certification schemes:

- Leveraging a multistakeholder process that is open, transparent and consensus-driven and does not place trusted companies at a disadvantage.
- Promoting the use of industry-led international standards.
- Assessing potential schemes according to risk- and environment-based requirements.
- Preserving industry third-party certification and conformity self-assessments based on risk.
- Promoting voluntary certification, mandating only in limited circumstances.

Leveraging a multistakeholder process that is open, transparent and consensus-driven and does not place trusted companies at a disadvantage. In recent years, cyber attacks against public and private institutions have undermined the security of the digital economy. The Chamber believes that multistakeholder processes contribute to the security of the internet architecture. Our goal is to foster a more resilient ecosystem through the creation of industry-led, market-based cyber security solutions. A key tenet of the multistakeholder process is that it is not biased toward one company, sector of the economy, or nation. The collective expertise of public and private stakeholders, combined with sophisticated risk mitigation tools and technologies, have the potential to unleash the next wave of security- and resiliency- enhancing innovations.

Promoting the use of industry-led international standards. The Regulation—Article 8.5—smartly recognizes the role that international standards have for the risk management and security of ICT products and services. The Chamber believes that cyber efforts are most effective if they reflect international standards and industry-driven practices. Standards, guidance and best practices relevant to cyber security are typically led by the private sector and adopted on a voluntary basis; they are optimal when developed and recognized globally.

The Chamber has championed efforts in duly recognized standards bodies, like ISO/IEC, to promote common, global approaches to information security that can be scaled to meet market needs. Such approaches avoid burdening multinational enterprises with the overlapping, and often conflicting, requirements of multiple jurisdictions.

Over the past year, the Chamber has been engaged in the Convening the Conveners (C2) initiative. C2 brings together 20 major cyber security and technology organizations in a precedent-setting effort to develop a consensus baseline set of security capabilities for the rapidly expanding IoT marketplace. The baseline of core capabilities is intended to meet the market's expectation for security and align policies around the world. The Chamber urges U.K. and EU policymakers to leverage the C2 Consensus on [IoT Device Security Baseline Capabilities](#) and align standards, best practices and frameworks to it.

Assessing potential schemes according to risk- and environment-based requirements. The Chamber strongly agrees with expert views that because IoT devices and their uses and needs are so varied, few recommendations can be made that apply uniformly. Depending on a variety of factors—from device complexity, managed or unmanaged, communications requirements, use and context—security-enhancing measures can be achieved in a variety of ways. For example, a connected lightbulb has a different risk profile than an industrial flow meter. Both devices should meet a common set of core security capabilities, but they will differ in how to meet that capability just as the risk profile for each device differs. The Regulation smartly recognizes this distinction in offering three levels of assurance for cyber security certification (i.e., basic, substantial and high). Future U.K. and EU cyber security schemes should take into account risk and environment based assessments prior to applying security mandates.

Preserving industry third-party certification and conformity self-assessments based on risk. The Chamber appreciates the view of policymakers that cybersecurity certification on its own cannot guarantee that an ICT product or service is completely secure. It is our view that certification is a tool that manufacturers and service providers can deploy as part of a multilayered, comprehensive risk management plan for the lifecycle management of a product or service. Article 53 of the Regulation permits the use of conformity self-assessment. The Chamber believes that industry groups have in-house subject matter and technical experts capable of evaluating ICT products and services in certain cases. As cyber security certification schemes are developed, we urge UK and EU policymakers to leverage the robust testing and evaluation capabilities of industry experts as both third-party certifiers and self-assessors.

Promoting voluntary certification, mandating only in limited circumstances. The Chamber is concerned about policies at home and abroad that require specific, top-down approaches to security. Such mandates are unlikely to keep up with malicious actors or align with international best practices—outcomes that the Chamber presses the public and private sectors to pursue. The Chamber wants device makers, service providers, and buyers to gain from the business community leading the development of state-of-the-art IoT components and sound risk management practices. Next steps include facilitating a process in the marketplace that generates both security and value for buyers and sellers. Market and/or policy incentives may be needed to jump-start this circle. The Chamber acknowledges that governments may require mandatory certification for products and services but urges policymakers to consider these mandates only in limited circumstances.

Public and private organizations have been working diligently for years to establish policies and frameworks to support a digital economy based on the rapid deployment of connected devices. These technologies have the promise to enhance safety, increase efficiencies, and enable new actions. This new ubiquitous connectivity is not without its challenges to security, privacy and trust.

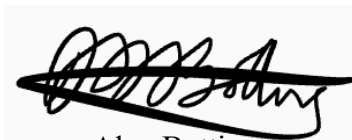
The Chamber shares the U.K.'s and EU's interest in deploying and securing ICT infrastructure domestically and globally. There is a clear need for closer international cooperation to improve cyber security standards and promote a common global approach to these issues. We look forward to supporting both the U.K. and EU governments' cooperation on an interoperable, mutually recognized approach to cyber security certification.

Please contact Vincent M. Voci (email: vvoci@uschamber.com or work: +1-202-463-5553) or Alex Botting (email: abotting@uschamber.com or work: +1-202-463-3179) if you have any questions or need more information.

Sincerely,



Vincent M. Voci
Cyber Policy Director
U.S. Chamber of Commerce



Alex Botting
Director
Global Regulatory Cooperation
U.S. Chamber of Commerce