ITI Promoting Innovation Worldwide

8 December 2021

RE: Global industry concerns in European Cloud Security Certification

We are writing to you on behalf of the Information Technology Industry Council (ITI) regarding the recent developments in the context of the development of European cloud security certification, as well as the parallel work at national level in France on its SecNumCloud scheme.

ITI is the premier global advocate and thought leader for the ICT industry. ITI's membership is comprised of 80 leading technology and innovation companies headquartered around the world from all corners of the ICT sector and beyond, including hardware, software, digital services, semiconductor, network equipment, and Internet companies.

ITI appreciates the efforts to protect data, systems and infrastructure from anomalous behavior and prevent unauthorized access. We believe that a harmonized European approach would be most beneficial for users and service providers. As it stands now, the current French SecNumCloud initiative conflicts with the EU objective to address Member States' fragmented approach to cloud security practices in accordance with article 57 of the Cybersecurity Act (Regulation 2019/881/EC) and replace national schemes with the EU Cloud Security Scheme (EUCS) of ENISA in the future.

While ITI agrees with the French government that offering cloud computing service providers a stable framework is essential for guaranteeing the quality of their service and fostering trust, a harmonized, EU-wide initiative will provide more clarity to cloud providers and users on the security assurance levels for cloud services. This will also allow all cloud providers to streamline their risk assessments and management measures across the EU.

In addition, a number of specific elements of SecNumCloud raise substantive concerns, making the potential alignment between the draft ENISA EU Cloud Security Scheme (EUCS) and the French initiative highly problematic.

SecNumCloud contains provisions that go beyond cybersecurity requirements

We understand the French Government's concerns around foreign government's access to sensitive information, and our industry is working with policymakers to address these issues. This is also being addressed in global fora such as the ongoing OECD work on Trusted Government Access to Private Sector Data. As a long-term solution can only be achieved through intergovernmental engagement, a cybersecurity standard-setting context is not the right way forward.

Cybersecurity certifications should focus on attesting implementation of the objective and universal goal of keeping data secure from cybersecurity threats. Considerations around foreign jurisdiction and control over data relate to more subjective considerations over "sovereignty" than to cybersecurity. Every organization has its own risk profile – or conducts its own risk assessment when it comes to sovereignty. This takes into account the sensitivity of their data, the level of control needed and acceptable compromise in terms of functionality. Providers are already offering tools that allow for varying levels of sovereign controls. Customers should be allowed to use the solutions that reflect their specific needs - while maintaining access to the best security features.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

More sovereignty requirements lead to less choice and fewer security options

Unfortunately, the overly strict SecNumCloud sovereignty requirements would also mean that customers who do not require sovereign controls would suffer from reduced choice, as only a few providers will be able to comply with them. Tying a high level of cybersecurity to a high level of sovereignty controls doesn't seem fit for today's diverse cloud demand. In addition, limiting the number of providers available is in turn a cybersecurity threat, as it makes the ecosystem less diversified and thus more vulnerable to attacks, malfunctions and other adverse events. Such an approach would actually undermine security rather than strengthen it.

Clearly, these problems would only be exacerbated should the "sovereignty-focused" SecNumCloud approach be replicated at European level through the EUCS.

Data localization

Section 19.2 of SecNumCloud introduces a requirement to process and host all data solely within the EU, including data necessary to operate services on the Internet. This not only limits cloud services and cloud providers' eligibility to SecNumCloud, but also affects cybersecurity, making it more difficult for organizations to exchange datasets stored outside borders; increasing costs for maintaining state-of-the-art solutions; and reducing alternative storage in cases of data losses or network outage.

If a provision having the same effect as section 19.2 were to be expanded to a European cybersecurity scheme, it would significantly limit the eligibility of third country cloud providers' to the EUCS, with no legal justification for such a restriction under the EU General Data Protection Regulation (GDPR), or under any EU cybersecurity law (e.g., Cybersecurity Act or NIS Directive).

WTO commitments

Finally, ITI is concerned about provisions that appear to contravene World Trade Organization (WTO) commitments, namely SecNumCloud's article 19.6 (*Immunité au droit extracommunautaire*) which would require cloud service providers to have immunity from non-EU laws. This provision would subject cloud service providers to explicit foreign corporate ownership structure limitations. More specifically, a shareholder outside the EU as an individual could not possess, directly or indirectly, more than 24% of the company's rights, and, collectively, shareholders outside the EU could not hold more than 39% of the value and voting rights of the company. Shareholders outside the EU would also lose veto rights and the ability to nominate a majority of the members of the boards.

Article 19.6 would violate France's commitment to national treatment and most-favoured nation rules under the WTO Agreement on Government Procurement (GPA). If the European cybersecurity scheme contained similar provisions, it would contravene the WTO GPA's non-discrimination commitments (Article III), which stipulate that parties to an agreement "shall not treat a locally established supplier less favorably on the basis of the degree of foreign affiliation or ownership".[1]

In other words, as there are clear questions about the French SecNumCloud compatibility with WTO commitments, implementation of these new requirements should be postponed, and article 19.6 should be removed. Finally, a potential inclusion of equivalent provisions in the EUCS would create even greater concerns.

Conclusion

Many of the proposed SecNumCloud requirements relate to legal aspects, organizational structure, and investment and ownership, that are unrelated to technical-based certification of cloud services or improving of cybersecurity. These requirements will have a direct impact on the usability, affordability, and eligibility of SecNumCloud and should not serve as inspiration for a European certification scheme.

Our comments regarding commitments to WTO rules and the global trade system, sovereignty requirements, and the indirect creation of requirements for back door localization are intended to help raise cyber security protection while leveraging the benefits of cloud innovation and economic growth.

Thank you for considering these concerns. ITI remains at your disposal to further discuss these issues.
Sincerely,

Guido Lobrano, ITI Vice President and Director General for Europe