Computer & Communications Industry Association
Tech Advocacy Since 1972

Computer & Communications Industry Association (CCIA Europe) Submission to ANSSI on the revised SecNumCloud security scheme

15 November 2021

The Computer & Communications Industry Association ('CCIA Europe') welcomes the opportunity to provide comments on the updated version of the SecNumCloud certification. CCIA Europe represents both service providers and customers of cloud services in France, Europe, and around the world. We commend ANSSI's efforts to bolster cybersecurity and trust in cloud services given the expected growth of cloud service provision and use in Europe.

CCIA Europe supports the development of open standards and voluntary certifications that provide cloud customers assurances about their vendors' organizational and technical capabilities to ensure the availability, authenticity, integrity, and confidentiality of customer data and their information systems.

Moreover, we support the effort by the European Union towards the harmonisation of cloud security practices through the adoption of the EU Cloud Security scheme due next year, in accordance with Article 57 and Recital 94 of the Cybersecurity Act. We see an opportunity for a European approach that can deliver greater trust, better security, and reduced costs for both cloud providers and customers. Leveraging the EU single market can also open new opportunities for European and global vendors alike. While the French government and ANSSI have defined specificities of the French market that are captured in the SecNumCloud since 2016, we believe it is important that a forthcoming EU Cloud Security scheme reflects a consistent cybersecurity vision across all Member States in line with the spirit of the EU Cybersecurity Act.

CCIA Europe agrees with the need to protect customer data from foreign government interference. While the updated SecNumCloud scheme seeks to address this issue through new provisions beyond core security controls considerations (e.g., foreign ownership limitations), we believe that the same objective could also be achieved by implementing contractual, operational and technical measures as the recent ruling of the Court of Justice of the EU in "Schrems II" (C-311/18) underlined. At the same time, we believe that it is important to acknowledge the pressing need to reform (European) law enforcement and intelligence communities' investigatory arsenal, adapting it to a borderless digital age so that they can carry out the public interest missions entrusted to them. Extraterritorial government and data access laws are a global issue that can be best resolved through bilateral and/or multilateral agreements with third country partners.

Finally, we caution against a data localisation requirement which appears at odds with the EU's recent unilateral and multilateral commitments against data localisation requirements,[1] and is not required under the relevant EU rules (GDPR, Cybersecurity Act, NIS Directive).

For further information, please contact Alexandre Roure, CCIA Europe Senior Manager, Public Policy: aroure@ccianet.org

[1] G7 Members' commitments (June 2021): "Championing data free flow with trust, to better leverage the potential of valuable datadriven technologies while continuing to address challenges related to data protection. To that end we endorse our Digital Ministers' Roadmap for Cooperation on Data Free Flow with Trust"; G20 Digital Ministers' commitments (August 2021): "Digital Economy Ministers, in 2020, recognised the opportunities and challenges of data free flow with trust and cross-border data flows and the need to address these challenges such as those related to privacy, data protection, intellectual property rights and security, in accordance with the relevant applicable legal frameworks, including by identifying commonalities between existing approaches and instruments used to enable data to flow with trust across borders"; European Commission communication on an Open, Sustainable and Assertive Trade Policy (February 2021): "The Commission will work towards ensuring that its businesses can benefit from the international free flow of data in full compliance with EU data protection rules and other public policy objectives, including public security and public order. In particular, the EU will continue to address unjustified obstacles to data flows while preserving its regulatory autonomy in the area of data protection and privacy".