ECIS European Committee for Interoperable Systems

ECIS ivzw-aisbl
Louizalaan 65 avenue Louise Box 2
B-1050 Brussels, Belgium

T/F +32 (0)2 706 24 15
info@ecis.eu
www.ecis.eu

29 March 2023

ECIS TWO-PAGER ON EUCS AND CYBERSECURITY

1. BACKGROUND ON ECIS

The European Committee for Interoperable Systems ("**ECIS**") is an international, non-profit association of information technology companies founded in 1989 which endeavours to promote a favourable environment for interoperable ICT solutions. For three decades ECIS has actively represented its members on issues relating to interoperability and competition before European, international, and national fora, including the EU institutions and WIPO. ECIS' members include both large and small information and communications technology hardware and software providers. For further information, please see ECIS' website at www.ecis.eu.

2. RECOMMENDATION

Governments should be sensitive to the risk of confusing security certification with other policy objectives such as data sovereignty or immunity. Cyber technical requirements should be kept strictly separate from industrial policy rules to avoid the unintended consequence of weakening cyber resilience and thereby undermining the core of what is understood by sovereignty, *i.e.* national security. This advice applies not only to the European Union Cybersecurity Certification Scheme on Cloud Services ("**EUCS**") within the Cyber Security Act but also regulatory frameworks that will reference it and will be impacted such as the NIS 2 Directive and the Cyber Resilience Act.

3. THE IMMUNITY REQUIREMENTS IN THE DRAFT EUCS WILL HAVE AN ADVERSE EFFECT ON EUROPE'S CYBERSECURITY RESILIENCE

ENISA's EUCS scheme aims to establish an EU-wide certification regime for cloud services with three levels of assurance: "*basic,*" "*substantial,*" and "*high.*" For high level assurance certification, the European Commission has asked ENISA to add "*immunity*" (or "*sovereignty*") requirements, with the political objective to ensure immunity from foreign jurisdictions.

Although the EUCS scheme itself is foreseen as voluntary, the high assurance level is expected to become mandatory for the essential and important services listed under the NIS2 Directive.

Localisation undermines information sharing for cybersecurity purposes, which policy leaders have emphasised as vital to effective cybersecurity

ECIS point of view on EUCS and cybersecurity draws on previous research and policy analysis such as the June 24, 2022 "The Effects of Data Localization on Cybersecurity"
Peter Swire & DeBrae Kennedy-Mayo, Georgia Institute of Technology

The cybersecurity threat landscape is global. Threats originate from bad actors that are statistically most often neither located within the EU or associated or allied countries, such as in North America. One the most effective proven ways to counter the spread of threats is for governments and industry to work closely together and share threat and incident information rapidly within shared confidential networks. This cooperation allows for threats that manifest themselves in different global regions to be identified and nipped in the bud at an early stage. The capability to do so relies on two factors: (i) uninhibited data flows which may contain personal and non-personal data in combination with the ability to share threat intelligence rapidly and (ii) the availability of cybersecurity support or expertise from outside in acute situations.

The above-mentioned information exchange is facilitated by industry providers, many of which have a large footprint in Europe but are not EU headquartered nor majority locally owned. Excluding such players from EU Member State cloud markets will lead to these markets going partly dark, excluding them from full access to intelligence and cloud services that rely on the availability of data – whether this data be related to state sponsored malicious actors, cyber criminals, zero day exploits or the exploitation of other vulnerabilities. Restrictions on data flows or data localisation creates a larger attack surface for malicious hackers and a slower uptake on attacker's information may, for instance, delay or block non-personal telemetric data in a cyber system using artificial intelligence. In addition, operators will struggle to navigate between global cyber security management controls which reach beyond EU borders and data localisation requirements or data transfer restrictions for personal and non-personal data under the EUCS.

How can risks be mitigated? Technology is inherently global ... Policy is always jurisdictional (see here)

ECIS recommends that that the technology and jurisdictional requirements in the EUCS scheme be separated as a good hygiene measure. Cyber certification frameworks such as EUCS should:

1. Harmonise (or at least embrace) global cybersecurity standards incorporating ISO 27002 – recent research has shown that data localisation and data minimisation in cyber can threaten an organisation's ability to achieve integrated management of cybersecurity risks.

2. Enhance risk based approaches such as those enshrined in NIS2 for certifying cloud services and remove restrictions such as ownership, establishment, nationality or security clearance.

3. Be strictly focused on requirements and controls which are technical. The inclusion of non-technical requirements – such as where headquarters are located or immunity declarations – runs the risk of introducing levels of legal and technical ambiguity into the certification scheme that render the scheme itself weaker, lessening the effectiveness of cyber resilience in EU markets.

Moreover, the risk of compromising cybersecurity resilience is even more acute since the high level 3 assurance scheme will most likely incorporate non-technical requirements and level 3 is relevant and applicable to critical infrastructures which represent the highest risk to society.

ECIS point of view on EUCS and cybersecurity draws on previous research and policy analysis such as the June 24, 2022 "The Effects of Data Localization on Cybersecurity"
Peter Swire & DeBrae Kennedy-Mayo, Georgia Institute of Technology