Alliance for IoT and Edge Computing Innovation

Brussels, 25 July 2024

AIOTI Response to the public consultation on the NIS2 Implementing Act

Background

The Network and Information Security Directive (NIS2 Directive) strengthens cybersecurity risk-management measures and streamlines incident-reporting obligations for a large number of operators across the EU.

From the point of view of the Internet of Things and Edge computing that are among the key technologies of interest for the Alliance for IoT and Edge Computing Innovation (AIOTI), we would like to submit comments to the draft Implementing Act that is subject of this public consultation.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.

Alliance for IoT and Edge Computing Innovation

Comments and proposals

Theme	Part	Problems	Proposal	Rationale
Supply chain security	Annex 5.1. Supply chain security policy 5.1.3. When establishing their supply chain security policy, relevant entities shall take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555, where applicable.	1. "Where applicable" is not defined which creates legal uncertainty and it should be further clarified; 2. Until now, there is limited information about "the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555". Due to lack of information and non-transparent procedure, the results of such coordinated security risks are not predictable.	**To add "in accordance with national law"** 5.1.3. When establishing their supply chain security policy, relevant entities shall take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555, where applicable **in accordance with national law.**	"The coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555" shall be in line with national, EU and international legal principles such as equal treatment/non-discrimination, free movement of goods and services, principle of proportionality and legal certainty enshrined in the TFEU.
Recurring incidents	Article 4 Recurring incidents Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where they meet all of the following criteria: (a) they have occurred at least twice within 6 months; (b) they have the same apparent root cause.	Recurring incidents in Article 4 refer to the threshold for reporting security incidents that occur repeatedly. There may be a large number of cloud service incidents that affect individual tenants, but these incidents can be resolved in a timely manner. Therefore, it is recommended that the threshold be raised. Currently, events with the same root cause are reported as long as they occur twice within six months. If the number of affected users exceeds 100,000, the events need to be reported. or the total number of affected CSC customers or the total contract value of affected cloud services of affected CSCs.		This requirement does not comply with the actual situation of the industry. There may be many accidents that affect a single tenant. Generally, the accident is handled according to the contract with the customer. It is recommended to raise the threshold.

Theme	Part	Problems	Proposal	Rationale
Cloud service provider	Art. 7 significant incidents with regard to cloud computing service providers (b) for one or more of the cloud computing services provided, the customer service level agreement is not met for more than 5 % of the cloud computing service users in the Union, or for more than 1 million of the cloud computing service users in the Union, whichever number is smaller, for a duration of more than one hour; (c) the availability of the cloud computing service of a provider that has no customer service level agreement in place is limited for more than 5 % of the cloud computing service users in the Union, or for more than 1 million of the cloud computing service users in the Union, whichever number is smaller, for a duration of more than one hour; d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the cloud computing service is compromised as a result of a suspectedly malicious action, e) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the cloud computing service is compromised with an impact on more than 5 % of the cloud computing service users in the Union.	We believe that the scale of cloud service providers varies greatly, especially for small cloud service providers. 5% of their users may be very small and have little impact, which has huge differences compared to the impact of 5% of users or 1 million users of large cloud service providers. If data compromise affects the CIA of data, it is recommended that the minimum threshold be set. For example, if data compromise affects more than 100,000 users, the data needs to be reported. Either the total number of customers of the affected CSC or the total contract value of the affected cloud services of the affected CSC is used as the trigger criteria.		With regard to Article 7 obligations for cloud providers, It is recommended that a threshold be defined for the minimum number of affected users. For example, the incident needs to be reported only when at least 100,000 users are affected. The scale of cloud service providers varies greatly. The burden on the small CSPs shall be reduced to the minimum.

Theme	Part	Problems	Proposal	Rationale
Content delivery network providers (CDN)	Article 9 Significant incidents with regard to content delivery network providers	The threshold is not explicit and low.		The scale of cloud service providers varies greatly. The burden on the small CSPs should be reduced to the minimum.