Comments on the Draft Proposal of the Cyber Security Act

Zagreb, November 2023

AmCham

American Chamber of Commerce in Croatia Američka gospodarska komora u Hrvatskoj

Introduction

Given the extremely strong digital transformation of all spheres of our lives, especially the digitization of business and the management of public institutions, cyber security has surpassed the point of 'reputational and financial' responsibility and has become a key factor of security. Nowadays, cyber security is a strategic, operational issue not only of business entities and state institutions but also of our way of life.

The American Chamber of Commerce in Croatia (AmCham) recognizes the importance of cyber security and welcomes the efforts of the European Union and Croatia to update existing legislation and respond to numerous challenges.

AmCham welcomes Croatia's efforts in the part of transposing the Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive) into national legislation.

The NIS2 Directive (Directive EU2022/2555) is legislation on cyber security within and at the level of the European Union, establishing the legal framework for increasing the overall level of EU security. The directive encourages mutual cooperation in the field of cyber security at the level of member states and requires the member states to be appropriately equipped with technology, teams and national authorities that monitor and influence the speed, quality and response to computer security incidents. What is more, it encourages the development of a culture of cyber security across all economic sectors essential for the economy of individual members but also of the entire European Union.

Companies that have been identified as essential and key by the member states will have to be part of a system that will work closely with national authorities to implement the Directive.

In this context, the Proposal of the Cyber Security Act emerged as part of the transposition of the NIS2 Directive (Directive EU2022/2555) into national legislation.

Comment on the Act

AmCham believes that the Cyber Security Act will have a significant impact on the Croatian economy and institutions. Therefore, it is of particular importance to remove all potential ambiguities of definitions and terms and to avoid legal uncertainties in implementing the Act. The adoption of an accompanying Regulation was also announced, which should define all the details and eliminate all ambiguities. Considering the importance of the aforementioned legislation and the impact it will have on the business sector as well as the country in general, AmCham believes that the process of adopting the Regulation requires the inclusion of a certain number of independent cyber security experts as members of the working group, as well as entrepreneurs whose business is significantly related to and will be affected by the entry into force of the Act and the adoption of the related Regulation.

The role of the Security and Intelligence Agency and the structure of the National Cyber Security Center

Article 63 foresees the establishment of the National Cyber Security Center (NCSC) as part of the Security and Intelligence Agency (SIA), at the same time outlining the tasks of the competent authority for the implementation of cyber security requirements (i.e. SIA for the sectors listed in Annex III of the proposed Act) and the tasks of the central state authority for cyber security transferred to NCSC. Further review of the act, especially the implementation part in Art. 114 points to the fact that NCSC will be organized as an internal organizational unit of SIA and, as such, will not have a separate character, nor will it be formally and legally separate from SIA.

In connection with the above, we point to the proposal to list the NCSC in Annex III of the Draft Act as the competent CSIRT for certain sectors, while at the same time listing the central state authority for cyber security, i.e. the SIA, as the competent authority for the implementation of cyber security requirements for most of the same sectors. In the specific case, the question arises as to with which body and in what way should the individual entity, i.e. the one subject to the Act, communicate? Will formal communication with the NCSC be considered as communication with the SIA in the role of the central state authority for cyber security, and will communication with the central state authority for cyber security also be considered as notification to the NCSC as the CSIRT? Please note that the provisions of Art. 37 and 38 of the proposal of the Act, as well as the aforementioned provisions, only raise additional questions because the procedural issues of notifying the competent authorities are planned to be technically and legally and procedurally regulated in the future, while at the same time the draft proposal of the Act (Articles 101 and 102) foresees extremely severe sanctions for entities, as well as for responsible persons in entities.

The legislative decision in question creates uncertainty and ambiguity for the addressee of the law regarding the body or bodies with which the addressee is obliged to communicate, as well as which competences and powers under the Act are to be exercised by the SIA, and which by the NCSC as a nominal (but not legally and formally) separate body.

If the intention of the legislator is to establish the NCSC as a separate and independent body with powers different from those of the SIA, it would be more suitable to separate the NCSC as a separate body within the security and intelligence system, modeled after the Information Systems Security Bureau. On the other hand, should the legislator insist on the proposal of the NCSC as an integral part of the SIA, we certainly suggest additional and clearer arrangement of the mutual relationship and coordination between the NCSC and the SIA in the context of the Cybersecurity Act, particularly clearer arrangement of the mutual relationship between entities subject to the Act and the NCSC/SIA when it comes to sectors where they are listed as the competent CSIRT and the competent authority for the implementation of cyber security requirements.

Adoption and implementation of the Cyber Security Act

In addition to the mentioned NIS2 Directive at the EU level, there is currently a whole set of regulations that represent a new legislative framework for information security and protection of critical entities at the EU level. Some of these regulations have already entered into force and will need to be transposed into the legislation of the Republic of Croatia (CER directive), while some regulations are already directly applicable in the Republic of Croatia (CSA regulation and DORA regulation). Furthermore, it is important to highlight the CRA (Cyber Resilience Act), which is in the adoption process and will build on the framework set by the NIS2 directive in the part that refers to issues of certification and protection of the supply chain in relation to digital products and products with digital components.

Since the deadline for the transposition of the CER directive is the same as for the NIS2 directive (October 2024) and since these are related regulations that build on and complement each other, we believe that it is necessary to additionally and unequivocally establish the mutual relationship between the NIS2 directive implementing act (Act) and the future CER directive implementing act. The above is particularly important to avoid mutual inconsistencies or contradictions, especially since the CER directive implementing authority (MI) is different from the NIS2 directive implementing authority (Ministry of Croatian Veterans).

In relation to the mentioned CRA, it is to be expected that the final text of the said regulation, which is expected in the year to come, will also have an impact on the enforcement and implementation of the Cyber Security Act in terms of the

certification of ICT products, services and systems, as well as the issue of securing supply chains in entities covered by the Cyber Security Act. Since it is not certain when the CRA regulation will enter into force, i.e., it being probable that the issues of certification of ICT products, services and systems and establishing uniform security standards will be successively regulated over the following years in accordance with the adoption of new regulations (CRA regulation) and establishment of the EU security scheme for ICT products, services and systems, we believe that by the time of the adoption of the CRA regulation and the EU scheme for ICT products, services and systems, the Act, implementing act or other by-laws or equivalent regulations (Act on the Implementation of Cybersecurity Certification) should unequivocally regulate the criteria and standards (ISO or similar) that would serve as a stable basis for the implementation of technical and organizational measures by persons subject to the Act in the future.

For additional information, please contact:
American Chamber of Commerce in Croatia
Andrea Doko Jelušić,
Executive Director T: 01 4836 777
E: andrea.doko@amcham.hr