CR^2
COALITION TO REDUCE
CYBER RISK

March 18, 2021

Submitted via the Better Regulation Portal

European Commission
Directorate-General for Communications Networks, Content & Technology
1049 Bruxelles
Belgium

RE: Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union

The Coalition to Reduce Cyber Risk, Inc. ("CR2") submits these comments in response to the invitation for public comments issued by the European Commission ("the Commission") regarding the Adopted Act of the Proposal for a Directive on Measures for a High Common Level of Cybersecurity across the Union ("NIS2 Proposal"). CR2 appreciates the opportunity to comment on the review and looks forward to working with the European Parliament, European Council and European Commission to further improve the NIS2 Proposal, ensuring that robust cybersecurity underpins the Commission's Digital Single Market initiative.

CR2 members include global organizations that represent numerous sectors, including financial services, IT, and telecommunications, that are committed to security, trust, and economic growth and opportunity. CR2 members have deep expertise in cybersecurity and enterprise risk management, as well as unique insights into cross-sector independences and global interconnectivity, which drive the need for consistent, foundational approaches to cybersecurity risk management across sectors and geographies. As such, CR2 has set out to work collaboratively with public and private sector entities to improve cybersecurity risk management practices that will both enhance cybersecurity and support economic growth.

CR2 commends the Commission for its work on the NIS2 Proposal, which addresses many of the concerns raised by industry experts during the prior public consultation period. These include:

- Clarifying that maintaining accurate WHOIS data is a lawful activity under European data protection law (Recital 59)
- Promoting the use of a risk management-based approach to security measures requirements, grounded in international standards (Article 18)
- Supporting the development of enhanced information sharing mechanisms among important and essential entities (Article 26)

We are nevertheless concerned that parts of the NIS2 Proposal will undermine the Commission’s objectives of enhancing cybersecurity and reducing fragmentation of the internal market. These concerns include:

- Important and essential entities may be subject to conflicting Member State requirements for implementing the Directive
- Misalignment between GDPR and NIS2 Proposal reporting requirements and timelines will introduce unnecessary complexity for companies, result in misleading or inaccurate information, and distract from immediate investigation and remediation efforts
- The broad scope of reportable incidents will create unnecessary ‘noise’ and increase circulation of non-authoritative, secondhand information, which could not only cloud the identification of significant risks but also delay coordination on incident response and mitigation activities
- The significant expansion of critical infrastructure, to encapsulate new sectors and all large- and medium-sized companies in those sectors, will dilute government and industry resources away from the most critical assets

CR2 appreciates your willingness to engage constructively and seek outside expertise and input on this vitally important issue. We have provided more detailed recommendations for your consideration below, and we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that the NIS2 Proposal meets its dual objectives of improving cybersecurity and preserving the Digital Single Market.

Respectfully Submitted,

The Coalition to Reduce Cyber Risk, Inc.

Coalition to Reduce Cyber Risk
Detailed Comments on the NIS2 Proposal

Potential for Overlapping Regulations

Throughout the NIS2 Proposal, there is a theme of cooperation between Member States and the Commission. The Commission clearly recognizes that steps to ensure security must be taken throughout the EU for the goals of the NIS2 Proposal to be accomplished. Without a method for determining a single country of oversight for each critical entity, however, such that different Member States do not impose conflicting or overlapping requirements, there is the potential for companies to receive conflicting requirements. For example, *Article 3* allows Member States to adopt additional provisions calling for a higher level of cybersecurity and *Article 7* calls for each Member State to adopt a national cybersecurity incident and crisis response plan.

While we believe that the Commission's goal in these articles is to empower Member States to increase security levels, many essential and important entities provide services across multiple Member States. Different cybersecurity strategies, incident response plans, and provisions for additional requirements can quickly lead to conflicting requirements on designated companies. Conflicting regulations across Member States could inhibit essential and important entities' ability to deploy security best practices seamlessly across borders. Additionally, varying laws could potentially place them in legal jeopardy where legal requirements conflict.

Adequate security risk management practices are consistent everywhere, as the Commission frequently references when mentioned international standards in the NIS2 Proposal, therefore Member States should not impose conflicting requirements on essential and important entities.

CR2 recommends that the NIS Cooperation Group set consistent risk management practices across the Union for those sectors that are in scope of the NIS2 IT risk regime. Even if adoption by Member States remains voluntary, alignment among participant countries would reduce variation among Member States' laws and make supervision and audits of designated companies possible at the Commission level.

In addition, CR2 recommends that the Commission and Member States explore the use of mutual recognition agreements for oversight or audits of critical infrastructure entities. This would reduce the cost and complexity of compliance, and avoid wasteful duplication, enhancing the ability of companies to investment in security.

Need stronger alignment with best in class international standards

In *Article 5*, the NIS2 Proposal outlines the requirements for Member State's national cybersecurity strategies and in *Article 18*, the NIS2 Proposal outlines risk management measures that each Member State should take to ensure a secure network. While the Proposal makes reference to the use of European and international standards, both sections miss an opportunity to reference *specific* international standards, leaving potential scope for divergence at the Member State level.

Cybersecurity best practices are consistent no matter where you operate. The consistent use of international standards globally is critical both to the seamless deployment of security best practices across borders and the preservation of the digital single market. Divergence, meanwhile, inhibits security and trade.

The NIS2 Proposal, or subsequent work by the NIS Cooperation Group, should reference international standards such as ISO/IEC 27001, 27103 and 27110, or globally utilized standards such as the *NIST Framework for Improving Critical Infrastructure Cybersecurity,* as being adequate for meeting security measures requirements anywhere in the Union, to provide companies with confidence that they can deploy these standards consistently across Europe. Referencing these specific international standards will help reduce variation across Member States' national security strategies and enhance security risk management efforts.

Scope Expansion

In *Article 2*, the NIS2 Proposal states, "*This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation.*" This definition of scope, while excluding micro and small enterprises, includes medium-sized and large enterprises. Medium-sized enterprises are defined by the European Commission as an organization with more than 50 employees and more than 10 million in revenue; a large enterprise is defined as having more than 250 employees and 50 million in revenue.[1] The capture of all medium and large companies is overly broad and unnecessarily expands the scope of companies defined as either essential or important.

The designation of critical infrastructure should be appropriately narrow. From a risk perspective, the 10,000th most critical company doesn't need to meet the same standards as the 1st. From a government perspective, the broader the scope, the harder it is to enforce and manage. Many, if not most, Member States will not be able to adequately monitor and provide oversight of this number of companies. According to data from 2017, there are roughly 48,000 large companies and 236,000 medium companies in the EU.[2] Accordingly, this would place a burden on medium

[1] https://ec.europa.eu/growth/smes/sme-definition_en

[2] http://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-297817_QID_50E8F4DC_UID_-3F171EB0&layout=TIME,C,X,0;INDIC_SB,L,X,1;SIZE_EMP,L,Y,0;NACE_R2,L,Z,0;GEO,L,Z,1;INDICATORS,C,Z,2;&zSelection=DS-297817GEO,EU28;DS-297817INDICATORS,OBS_FLAG;DS-297817NACE_R2,B-N_S95_X_K;&rankName1=INDICATORS_1_2_-1_2&rankName2=NACE-R2_1_2_-1_2&rankName3=GEO_1_2_0_1&rankName4=TIME_1_0_0_0&rankName5=INDIC-SB_1_2_1_0&rankName6=SIZE-EMP_1_2_0_1&sortC=ASC_-1_FIRST&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=ROLLING&time_most_recent=false&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23

companies without sufficient administrative capacity to provide the support and oversight needed for implementation.

CR2 recommends that ‘essential’ or ‘important’ designations be based upon the potential impact of a disruption to service, rather than an arbitrary measure, such as having more than 50 employees. Council Directive 2008/114/ec provides precedent for designating *critical infrastructure* according to the potential impact of an incident on vital societal functions, such as health, safety, security and economic or social well-being.

Recital 16 and *Recital 18* further expand the scope of the NIS2 Proposal by stating “*Cloud computing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources*,” and *“this Directive should cover also providers of such data centre services that are not cloud computing services,” respectively.*

The definitions of cloud and data center services are too broad and as a result will encompass a myriad of different types of services. While many cloud service providers and data centers play an important role in the cybersecurity ecosystem, as the NIS2 Proposal is written, it will capture many providers that otherwise do not meet the criteria to be essential or important, such as gaming services.

We recommend aligning the cloud computing definition in NIS2 with those that have been internationally agreed upon in the context of ISO/IEC 17788 and ITU-T Y.3500, as well as further refinement of the scope of companies that are captured in this sector.

CR2 recommends, given that supply chain dependencies are already address in the proposal, that the scope of cloud services and data center services coverage be reduced to only capture the truly essential providers.

Potential for New Complexity in Terms of Essential vs Important Designations

The NIS2 Proposal creates two categories: essential and important entities. While the two categories should be held to the same risk management requirements, the different categories are held to differing levels of supervisory and different penalties – meaning ultimately there will be different responsibilities depending on the classification of an entity.

While the degree to which a company is important or essential may be different in different countries, it is counterproductive to the digital single market and cybersecurity to have them meet different practices in different countries. If the same services were to be designated differently across the EU it would cause confusion and complexity. Whether or not a service is designated as essential or important, it should not be able to be designated differently in different countries for consistency purposes. CR2 recommends the NIS Cooperation Group create a process for single country designation so that companies are not recipients of conflicting Member State requirements.

Need to align reporting & timelines with GDPR

Article 20 of the NIS2 Proposal states, *"Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT: (a) without undue delay and in any event within 24 hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action."*

The notification timeline of 24 hours is far too short of a deadline to report an incident to authorities. Furthermore, it is not in line with GDPR's requirements and many incidents could fall under both NIS2's reporting timeline and GDPR's. The hours immediately after an entity becomes aware of an incident are very challenging from an operational perspective, as company representatives investigate the cause and scale of activities, assess legal ramifications, and ensure the continued confidentiality, integrity and availability of information. Beyond the administrative burden that short timelines for reporting place on critical infrastructure entities, they increase the risk of companies unintentionally sharing information that is either inaccurate or lacks sufficient context to be useful.

CR2 recommends changing the notification period to 72 hours – aligning with GDPR.

Need to narrow scope of reportable incidents

Additionally *Article 20* states an incident is significant and needs to be reported if an: *"incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned and/or the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses."*

This threshold for reportable incidents as written is too low. The description of "potential to cause…" is overly broad, as companies may be the subject of millions of such attempts per day. As a result, the volume of information that is subject to reporting will both overwhelm industry and government. This short reporting timeline will force industry to divert valuable resources away from operational activities and make the aggregation of incident data more challenging. The government would also be overwhelmed with data and would have to sift through millions of reports to find incidents that are actually worth government involvement. Threat information sharing is valuable only to the extent that it provides security professionals with timely, actionable information. Accordingly, we recommend that events with the "potential" to cause damage be removed from the scope of the proposal.