



ELECTRICITY
ASSOCIATION
OF IRELAND

127 Baggot Street Lwr.

Dublin, D02 F634

Date: 19th March 2021

By email to: cybersecurityconsultations@decc.gov.ie

Cc: lta.OFarrell@decc.gov.ie

RE: EAI response to consultation on NIS 2.0

Dear Cyber Security team at DECC,

On behalf of the members of the EAI, I am writing to you in response to the consultation on the Directive on Security of Network and Information Systems (NIS Directive). The Electricity Association of Ireland (EAI) is the representative body for the electricity industry and gas retail sector operating within the Single Electricity Market (SEM) on the island of Ireland. Our members range in size from single plant operators and independent suppliers to international power utilities. EAI members have a significant presence in NI, ROI and GB across the sector value chain.

To begin, the EAI and its members recognise the growing importance of cybersecurity and we welcome this review of the NIS Directive and efforts to strengthen the EU's cybersecurity capability. In strengthening and harmonising the approach to cybersecurity, it is important that risk management principles and proportionality continue to guide the development of the NIS.

We welcome the following acknowledgement on page 20 of the proposal that *“cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned”*. We would caution against taking the NIS down an overly prescriptive route which could prove detrimental to the overall intended objectives.

In regard to the specific provisions being proposed we would like to highlight the following areas for consideration:

Article 29 - Supervision and enforcement for essential entities

The new supervision and enforcement powers under Articles 29 are a significant step up in comparison to what is in place currently. Some of these proposals are too wide ranging as currently drafted. Certain aspects of the proposed powers need be either refined, clarified or reconsidered.

A decarbonised future powered by electricity

Electricity Association of Ireland

Registered Office: 127 Baggot St Lower, Dublin 2, Ireland D02 F634

Registered No. 443598 | VAT No. IE9682114C

T +353 1 524 1046 | E info@eaireland.com | [@ElectricityAI](https://twitter.com/ElectricityAI)

www.eaireland.com



- The proposal to permit “*security scans*” needs to be reconsidered. We are concerned that these powers are inappropriate, invasive and could potentially pose a risk to the operations of essential services. Wholesale authority to conduct invasive testing could not be accommodated in its current form and any right to access the Operational Technology (OT) environment would require a considerable collaborative effort to undertake securely.
- The proposal to permit “*On-site inspections and off-site supervision, including random checks*” also needs to be defined. Access to site would need to be carefully controlled and managed to ensure continuity of service. We would have concerns regarding the control measures which would be required to permit random checks in an OT environment. Random or unannounced site inspections or supervision could pose a risk to continued operation of essential services. Collaboration in advance of such checks would be required. We would ask for clarity on how these inspections will work and how much notice will be provided for onsite inspections.
- In relation to enforcement, we note the significant enhancement of powers and sanctions. It is critical that these enforcement powers are proportionate and appropriate to each sector. Article 29(5.a) states that Members States shall have the power to “*suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity*”. This raises questions about the nature of the “*certification*” and “*authorisations*” being referred to. It also suggests potential links to licencing conditions which would need to be carefully considered in terms of the practicalities and appropriateness of applying such a provision. It is important that provisions here are consistent with the overall intention of the Directive which is to ensure security of essential services.

Role of certification

- The requirements and articles of the Directive need to be proportionate and appropriate, in line with any form of risk management framework, and this should also apply to certification, which is mentioned in several articles. We believe that overemphasis on certification could be detrimental to the guiding principle of managing risks. Clarity is needed as to the type and purpose of certification. It is important that certification does not detract from focus on risk management. We would caution against use of a compliance standard like North American Energy Reliability Corporation Critical Infrastructure Protection (NERC CIP).
- Article 21 provides that the “*Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate*”

and under which specific European cybersecurity certification schemes". This describes a wide-ranging power. Clarity is needed as to the role, type and purpose of certification. Clarity is also needed as to whether it is intended that certification will extend beyond ICT devices, applications and systems into the broader OES environment.

- EAI members support a role for the right type of certification but have questions of the extent of the work involved to obtain cybersecurity certification under the EU-wide cybersecurity certification framework (envisaged by the EU Cybersecurity Act (Regulation 2019/881)) as it is currently unclear what is involved e.g., reports, visits, scans.

International cooperation – absence of Article 13 in NIS2

- International cooperation needs to be part of the NIS approach. Article 13 of NIS1 has been omitted from this proposed draft. It is of critical importance that this be reinstated particularly in the context of Brexit. Clear mechanisms need to be in place for cooperation with third countries. We need to understand how compliance with NIS2 can be applied cross-border with a non-EU country i.e., Northern Ireland.

Article 4 – Definitions

- NIS 2 defines cloud computing services as *"a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources"*. There is a need for further clarity on what types of cloud providers should be covered by the draft Directive to avoid unintentionally covering entities that are not envisioned to be captured.

Article 17 – Training requirements

- Further information is required in on the training requirements referenced in Article 17. Clarity is required as to who is expected to be trained and on what basis we will declare the status of named individual's training.

Article 20 – Reporting Obligations

- Further information is needed in relation to incident reporting thresholds such as what constitutes a reportable incident and clarity is required in terms of definitions e.g. *"Risk"*, *"Near Misses"* etc. The current draft could capture a wide range of incidents. Further information is also needed in regard to frequency and level of detail that would be required. Care needs to be taken with this proposed requirement to ensure

it does not place a disproportionate burden on obligated entities that may divert scarce resources from operational cyber security requirements which may limit the ability to achieve the overall policy goals of the draft Directive.

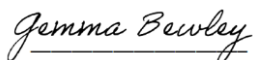
- The terms '*significant incident*' and '*significant threat*' are important as reporting of a significant incident would be expected but reporting on significant threats would not be expected. Hence, these terms need clarifying.
- EAI members would also have concerns about how they are to manage reporting obligations and how are these obligations to be scoped.
- We note that the Directive proposes to reduce the incident reporting timeframe from 72 hours to 24 hours which is a much tighter timeframe and could pose challenges if not implemented appropriately. Further information is needed on the information that needs to be shared and the mechanism through which this should be shared. It is important that this requirement does not inadvertently increase risks or divert resources away from dealing with the cyber incident.

Conclusion

As highlighted above, some of the proposals are wide ranging and need to be clarified or reconsidered. The Directive emphasises the importance of risk management. It is important that this emphasis is maintained throughout the articles and that requirements are proportionate and appropriate. It is also important that any new requirements be phased in appropriately over a realistic timeframe. This is important for Competent Authorities and OESs. It is important to ensure NIS is meaningful and CAs have the capability and resources to manage this sufficiently. It is also important for OESs who will need to invest to increase capability and who will already have supply chain agreements in place. Our members' requirements for compliance with NIS 2 should be clear so that any necessary changes can be carried out easily and effectively before adoption takes effect.

We look forward to engagement on these issues and to receiving a response to this communication.

Yours Sincerely

A handwritten signature in black ink that reads 'Gemma Bewley' in a cursive script.

Gemma Bewley



Policy Analyst

Electricity Association of Ireland