ENCS

WP-020-2020

Response to the EU consultation on network codes

Version 1.0

13 May 2020

Version History

Date	Version	Description
13 May 2020	1.0	Reply to EU consultation

TLP White – Public

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training.

ENCS

EU consultation on network codes

In May 2020, the Directorate-General for Energy of the European Commission had a targeted stakeholder consultation for a priority list for the development of network codes and guidelines on electricity for the period 2020-2023 and on gas for 2020 (and beyond). In the consultation, they asked stakeholders to provide input on the need and adequate scope of new electricity network codes on cyber security.

ENCS considers a network code on cyber security as an important regulation to protect the internal market for electricity against cyber-attacks. This can be done by:

- Ensuring that each party sufficiently mitigates risks to the common electricity grid
- Protecting information shared between parties in the market
- Set up means to detect and respond to cross-border cyber security incidents
- Establishing a process to define minimum security requirements for products, systems, and services

Mitigating risks to the common electricity grid

The impact of a cyber-attack against parties in the internal electricity market can be much larger than the damage to the party itself. It may affect the entire electricity system. If the attack for instance causes a large enough electrical load to be disconnected, this could lead to issues balancing demand and supply in Europe.

It is hence important that each party in the market takes sufficient measures to mitigate such risks. ENCS thinks the best way to ensure this is to use a risk-based approach based on the ISO / IEC 27000 standard.

ENCS agrees with the SGTF EG 2 recommendation that DSO and TSOs conform to the ISO/IEC 27001 standard with a specified scope. ISO/IEC 27000 provides a mature framework to assure the cyber security of organizations. It is designed to work on organizations of different sizes. Many grid operators are already using it. And there is infrastructure available to support the implementation and audits on many organizations.

ENCS would recommend that other market parties are made to conform to ISO/IEC 27001 if cyber-attacks against them may disrupt the grid. Electricity producers or parties that offer demand-side flexibility, such as electric vehicle charge point operators, can be as important to the stability of the grid as DSOs and TSOs. Threat actors aiming at grid sabotage will look to attack the weakest parties to achieve their goal. So, all relevant market parties should have some minimal level of cyber security.

The network code should include cyber security risk criteria. ISO/IEC 27001 is risk-based. Organizations using it need to set their own risk criteria based on the requirements of stakeholders. To ensure that risks to the EU internal electricity market are properly

addressed, the network code should include such requirements**. ENCS would recommend that requirements should cover how the risk assessments are performed to ensure their quality. It should also include criteria on when risks may be accepted.** These criteria can be based on a risk-impact matrix as recommended in the SGTF EG2 report.

ENCS would recommend against including detailed minimum requirements in the network code. The requirements can become outdated quickly when new threats arise. Moreover, a risk-based approach allows for smarter more cost-effective solutions.

Protecting shared information

The network code should ensure that information that is shared to enable the internal market is properly protected. ENCS would recommend setting up a classification scheme for such information. The classification could be based on the potential impact if the confidentiality, integrity, or availability of the information is compromised. Minimum security measures can be defined to protect information of a certain classification level.

The network code could define the classification levels. ENCS **would recommend not to include the security measures themselves, but instead to define a process to define and update them, so that they can evolve with new threats.**

Detecting and responding to cyber security incidents

The network code should set up the means to collaborate to detect and respond to cross-border cyber security incidents. Cyber security incident response is now organized mostly nationally. But if an incident would affect the electricity supply in different member states, quick and effective supranational collaboration would be needed.

An early warning system as proposed in the SGTF EG2 report can help to detect incidents. **ENCS would however favor voluntary participation, as this would make it easier to build a trusted community**. Mandatory reporting of incidents is already included in the NIS directive.

More critical however would be to set up groups or organizations for responding to major incidents. **ENCS recommends that the network code provides a framework for a crisis management organization for cyber security incidents.** It should, if possible, address the risk that in case of a cyber-attack important information needed to counter it is classified at a national level and not shared across borders.

Supply chain security

ENCS agrees with the SGTF EG2 recommendations on minimum security requirements for products, systems, and services and supply chain security. Such requirements would be a particularly effective way to increase the security of smaller market parties. Often smaller parties need to rely on their suppliers for their security. By setting minimum requirements through the network code, it can be ensured that they will get secure systems.

ENCS does think it is important that operators of essential services are allowed to follow a risk-based approach, as it is recommended in the SGTF EG2 report. So, they would be allowed to use products, systems, and services that do not meet the minimum requirements if they can show that cyber security risks are sufficiently mitigated. Such a risk-based approach leaves larger market parties free to choose the most cost-effective measures to mitigate risks.