
WP-034-2020

# Update on the revised NIS directive

Version 1.0

18 December 2020

This document is shared under the Traffic Light Protocol classification:

**TLP WHITE - public**


The European Network for Cyber Security (ENCS) is a non-profit membership 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.

# Revised NIS directive

On 16 December 2020, the European Commission adopted a proposal for a revised NIS directive: the directive on *measures for a high common level of cybersecurity across the Union* [1]. The directive is meant to repeal the directive *concerning measures for a high common level of security of network and information systems across the Union* [2] from 2016, also known as the NIS directive .

The goal of the revised NIS directive is to achieve a harmonized, high level of cybersecurity across the European Union by incorporating feedback from the most recent consultations and filling some gaps found in the NIS version from 2016. The new directive, which focuses on enabling resilient infrastructure and critical services, is a key component of the Union's new Cybersecurity Strategy for the Digital Decade. It was released alongside a proposal for a Directive on the Resilience of Critical Entities, which is the successor of the 2008 European Critical Infrastructure Directive.

The most important changes for grid operators seem to be:

- The scope was extended to include many parties important to grid stability
- Supervision and enforcement of the implementation is made stricter
- It may become mandatory to use of products, services, and processes certified under the Cybersecurity Act
- Provisions are added to integrate the upcoming network code on cybersecurity

## Extended scope

The revised NIS directive extends the scope of entities that should comply with it. Previously, in the electricity sector only TSOs, DSOs, and suppliers were covered. Under the revised NIS directive, the scope also includes (Annex I):

- Producers
- Electricity market operators
- Electricity market participants providing aggregation, demand response, or energy storage services

It is no longer up to member states to designate parties as operators of essential services. Instead, all entities of the above types are considered *essential entities*, and should fall under the revised NIS directive. Only micro and small enterprises are excluded as long as they are not seen as having a high security risk profile, which can be determined by member states individually. This can be the case for example if the entity is the sole provider of a service or a trust service provider (Article 2).

With this extended scope, most parties that pose a risk to the security of electricity supply would now come under the NIS directive. For instance, operators of wind and solar farms

(identified as critical infrastructures in the DER member project [3]) would be considered producers. Electric vehicle charge point operators would be considered as a market participant offering demand response, if they provide smart charging. Still some critical parties seem not to be covered yet, such as the installers of wind and solar farms and the manufacturers of consumer solar panels.

The choice to only exclude micro and small enterprises should lead to a more harmonized application of the NIS directive throughout the EU. Under the current NIS directive member states identify the operators of essential services, and there are large differences between which parties they take in scope. Under the revised NIS directive, member states only have discretion over micro and small enterprises. All larger enterprises are automatically in scope.

## Stricter supervision

The revised directive gives national competent authorities more power to supervise and enforce the implementation at essential entities. They can conduct random on-site inspections, regular audits and security scans, and they can request cybersecurity policies and audit results (Article 29).

Based on these, the competent authority can issue warnings, binding instructions, order entities to seize conduct and even issue public statements identifying the legal and natural persons responsible for the infringement. They can also set deadlines for actions needed to remedy deficiencies (Article 29).

Given the previous reluctance of member states to impose penalties, a list of administrative sanctions is established for breach of the cybersecurity risk management and reporting obligations. These include fines of up to 10 million euros or 2% of annual turnover (Article 31).

## Use of European certification schemes

Under the revised directive, member states may require essential entities to use products, services, or processes that are certified under the Cybersecurity Act. This could for instance mean that member states require grid operators to use smart meters certified under the EU Common Criteria scheme [4], RTUs and IEDs certified under the ICS cybersecurity certification framework [5], or cloud service certified under the cloud certification scheme [6]. This requirements could seriously restrict the options of grid operators during procurement.

## Integration with the network code on cybersecurity

The revised NIS directive contains two changes that should make it easier to integrate with the planned network code on cybersecurity:

- The Commission is empowered to adopt delegated acts (such as network codes) for instance to address sectoral specificities. The delegate acts may require additional measures (Article 18(2)) or certification of products, services or processes (Article 21(2)). This allows the network code on cybersecurity to add to the network code in these areas.
- Members states should allow essential entities to share information about threats and incidents among themselves in trusted communities. This would open the way for direct information sharing between grid operators, as planned in the fifth pillar of the network code on cybersecurity.

## Other changes

The revised NIS directive includes several other changes meant to increase information sharing between government bodies. These changes will not directly affect grid operators. The major changes in this area are:

- Information sharing and cooperation between member state authorities is increased with an enhanced role for the Cooperation Group. Entities outside the scope of the Directive are also allowed to contribute on a voluntary basis (Articles 26 and 27).
- Increased collaboration between national CSIRTs and competent authorities is introduced. By its own admission, the EU lacks collective situational awareness of cyber threats. The directive helps with building the operational capacity to prevent, deter, and respond to cyber threats, ultimately contributing to the establishment of a European cyber shield.
- A European Cyber crises liaison organization network (EU- CyCLONe) is created to support the coordinated management of large-scale cybersecurity incidents and crises and to ensure the regular exchange of information among member states and EU institutions (Articles 12 to 16).
- A framework for Coordinated Vulnerability Disclosure is established for newly discovered vulnerabilities across the EU with CSIRTs acting as trusted intermediaries and facilitators (Articles 5 to 11). A vulnerability registry operator by ENISA is created.
- The Cooperation group will perform coordinated risk assessments for the supply chain for key information and communication technologies (Article 19).

## Next steps

The proposed NIS 2 Directive will now be negotiated in the Council of the EU and the European Parliament. Upon final adoption, member states will have 18 months to implement the changes. The next round of review and revision of the NIS 2 Directive will begin 54 months after adoption.

# References


[1] European Commission, „Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148," 16-12-2020.

[2] European Parliament and the Council of the European Union, „Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 6-7-2016.

[3] ENCS, „WP-029-2020: Why DER cybersecurity is critical and how to protect DER systems," 2020.

[4] ENISA, „Cybersecurity Certification - EUCC, a candidate cybersecurity scheme to serve as the successor to the existing SOG-IS," 2020.

[5] Joint Research Center, „Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)," 2020.

[6] CSPCert, „Recommendations for the implementation of the CSP Certification scheme," 2019.