FEDIL

Publication

PROJECT GROUP ON THE NEW EUROPEAN CYBERSECURITY STRATEGY

Call for participation

In the framework of the new European Cybersecurity Strategy released end of December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy proposed (1) a review of the NIS directive of 2016 and (2) a Directive on the Resilience of Critical Entities.

1. The EU Cybersecurity Strategy for the Digital Decade.
   This communication includes among others the launch of a network of security operations centres across the EU, powered by artificial intelligence (AI), which will constitute a real « cybersecurity shield » for the EU and the creation of a new joint « cyber unit », to strengthen cooperation between EU bodies and Member State authorities.
2. A Proposal for a Directive on measures for high common level of cybersecurity across the Union (« NIS 2.0 »), review of the NIS directive of 2016, which :
   - expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope;
   - eliminates the distinction between operators of essential services and digital service providers;
   - classifies entities upon their importance and devides them repectively in essential and important categories with the consequence of being subject to different supervisory regime;
   - strengthens and streamline security and reporting requirements for the companies by imposing a risk management approach providing a minimum list of basic security elements that have to be applied;
   - adresses security of supply chains and supplier relationships.
3. A Report on the impact of the Commission Recommandation on the Cybersecurity of 5G networks.
4. A proposal for a Directive on the resilience of critical entities which expands both the scope and depth of the 2008 European Critical Infrastructure Directive. 10 sectors are now covered.

Essential entitites: Energy (Electricity, District heating and cooling, Oil, Gas, Hydrogen) – Transport (Air, Rail, Water, Road) – Banking – Financial market

infrastructures – Health – Drinking water – Waste water – Digital infrastructures (IXP providers, DNS services providers, TLD name registries, Cloud computing services providers, Content delivery network providers, Trust services providers, Providers of electronic communications networks or services) – Public administration – Space (Operators of ground-based infrastructure, owned, managed and operated by MS or by private parties).

Important entitites: Postal courier and services – Waste management – Manufacturing, production and distribution of chemicals – Food production, processing and distribution – Manufacturing (Manufacture of medical devices and in vitro diagnostic medical devices, Manufacture of computer, electronic and optical products, Manufacture of electrical equipment, Manufacture of machinery and equipment, Manufacture of motor vehicles, trailers and semi-trailers, Manufacture of other transport equipment – Digital providers (Providers of online marketplaces – Providers of online search engines – Providers of social networking services platform).

Please, find more details on entities' definition on the document below:

LIST OF SECTORS, SUBSECTORS & TYPE OF ENTITIES UNDER THE SCOPE OF THE « PROPOSAL FOR A DIRECTIVE ON MEASURES FOR HIGH LEVEL OF CYBERSECURITY ACROSS THE UNION » (NIS 2.0) & « THE PROPOSAL FOR A DIRECTIVE ON THE RESILIENCE OF CRITICAL ENTITIES »

New sectors and entities covered are highlighted in blue.

Should your activity falls under the areas mentioned and your knowledge and/or experiences are linked to **security, cybersecurity, risk management and analysis, compliance and reporting obligations** among others, we kindly invite you to join the dedicated project group aiming at analysing the proposed directives and new measures to be taken by concerned entities and how they will impact your security policy and elaborate a position paper together with the project group members.

In order to participate to the project, please contact celine.tarraube@fedil.lu.