BDEW e.V.
German Association of
Energy and Water Industries
Reinhardtstraße 32
10117 Berlin

Opinion Statement

Proposal for a Regulation on ENISA („Cybersecurity Act“)

Proposal for a Regulation on ENISA, the „EU Cybersecurity Agency“, and repealing Regulation (EU) 526/2013 and on Information and Communication Technology cybersecurity certification (2017/0225 (COD))

Berlin, 15th January 2018
Transparency-Register ID: 20457441380-38

Executive Summary

The German Association of Energy and Water Industries (Bundesverband der Energie- und Wasserwirtschaft - BDEW) represents operators of essential services in the sectors energy and water / waste water as defined in point (4) of Article 4 of Directive (EU) 2016/1148 (NIS-Directive).

The availability of essential services is a central requirement for the confidence of citizens in the functioning of their economy, governments and society as a whole. Effective protection of essential services can only succeed with a functioning cooperation between public institutions and private or municipal operators of essential services, such as the energy and water industries. In doing so, the jurisdiction and competencies both on European level as well as in Member States need to be established and common strategies and standards coordinated.

BDEW welcomes the Commission's goal to strengthen cybersecurity in Member States and to foster cooperation in this context by means of the present proposal. However, BDEW believes the following elements in the proposal for a regulation require modification or should be considered in the future legislative process:

1. Clear delimitation of competencies and jurisdictions between ENISA and national authorities: Member States are responsible for the implementation of the NIS-Directive
2. Open and transparent development of the proposed European certification and labeling framework: involvement of Member States and European standardization bodies CEN, CEN ELEC and ETSI
3. Securing compatibility to existing systems when standardising different certification schemes
4. Improved consistency and explicit differentiation between legislative proposals on privacy (e.g. General Data Protection Regulation GDPR, ePrivacy Regulation), cybersecurity (e.g. NIS-Directive, Cybersecurity Act) and authenticity (e.g. eIDAS Regulation)

1 Introduction

The German Association of Energy and Water Industries (Bundesverband der Energie- und Wasserwirtschaft - BDEW) represents operators of essential services in the sectors energy and water / waste water as defined in point (4) of Article 4 of Directive (EU) 2016/1148 (NIS-Directive). The 1,800 companies represented by BDEW differ widely in terms of their size and forms of organization. The spectrum of the association's members ranges from local and municipal utilities to regional and inter-regional suppliers. They represent around 90 percent of the electricity production, over 60 percent of local and district heating supply, 90 percent of natural gas supply as well as 80 percent of drinking water extraction and around a third of waste water disposal in Germany. This large variety in the German energy and water markets as well as in terms of drinking water supply and waste water disposal is unique within the European Union.

On 13th September 2017, the European Commission published a Cybersecurity Package, including a new Cybersecurity Strategy, a proposal for a regulation on ENISA, as well as a communication on the implementation of the NIS-Directive. The regulation proposal has been corrected on 4th October 2017.

The ambitious Cybersecurity Package aims to update the digital security architecture in the European Union to a new level. This is an important step in the right direction, because the requirements for cybersecurity are steadily increasing with growing digitization and the energy revolution (Energiewende) becoming more and more decentralized. The availability of essential services is a central requirement for the confidence of citizens in the functioning of economy, governments and society. Many advantages of digitisation can only be effectively harnessed with a corresponding common level of security both on the level of processes as well as products and services in EU Member States. Therefore, essential service operators are notably reliant on common national and international standards, secure products and services as well as an effective and efficient cooperation between the Commission and Member States.

While the NIS-Directive sets a clear direction for common standards and increased cooperation between Member States, the state of its implementation currently varies considerably across the EU. Transposing the NIS-Directive consistently across the EU therefore remains a high priority, while making sure that Member States are responsible for the implementation in national law.

2 Remarks on key positions

The following further remarks on aforementioned key positions should be considered in the upcoming legislative process from BDEW's point of view:

2.1 Clear delimitation of competencies and jurisdictions between ENISA and national authorities: Member States are responsible for the implementation of the NIS-Directive

Strengthening ENISA's mandate, especially in the area of supporting Member States in the implementation of the NIS-Directive must not lead to rivalries over competencies between ENISA and national authorities or unclear roles, responsibilities and contact partners for operators of essential services.

Member states are responsible for the implementation of the NIS-Directive, especially regarding security requirements and incident notifications as set out in Article 14 of the NIS-Directive. For operators of essential services, the primary contact partner needs to remain the competent national authority. Increased cooperation between Member States can subsequently be managed similar to a cascade by the respective national authorities with ENISA's support.

Furthermore, BDEW deems it necessary to define at a suitable place, how ENISA or the CSIRT-Network ensures the confidentiality of security-related information during information exchange for cross-border incidents.

2.2 Open and transparent development of the proposed European certification and labelling framework: involvement of Member States and European standardisation bodies CEN, CEN ELEC and ETSI

A common European certification and labelling framework can contribute to an effective protection of citizens and companies. However, the proposed framework needs to be developed in an open and transparent process, and involving Member States as well as European standardisation bodies **CEN, CEN ELEC and ETSI**.

In particular, BDEW would like to express its concern that the Commission, according to the proposal, will have the sole authority to decide which schemes are deemed necessary and which are not. According to the proposal, neither Member States, the European Council, European Parliament, nor national standardization bodies, associations or the industry will have a say in this matter. Member States and the newly established "Cybersecurity Certification Group" can only propose candidate schemes to the Commission according to the present proposal. Making certification under the new schemes voluntary, unless otherwise specified in Union law cannot sufficiently mitigate this shortcoming.

Furthermore, in the view of BDEW, no certification requirements or requirements for the use of certified products for operators of essential services should be laid down without a qualified evaluation if these requirements are suitable and applicable for their specific field of application. This can only be accomplished by involving the relevant standardisation bodies in Member States as well as the European standardisation bodies CEN, CEN ELEC and ETSI.

2.3 Securing compatibility to existing systems when standardising different certification schemes

Furthermore, the proposed certification and labelling framework needs to consider existing security standards and requirements in the field of cyber- and information security and ensure compatibility to these systems. This includes, amongst others, the ISO 2700x standards as well as specific standards such as ISO/IEC 27019 for the energy industry or IEC 62443 for industrial automation and control system standards.

In addition, requirements set out by Member States and their respective regulatory authorities also need to be taken into account. For instance in Germany, during implementation of Article 14 of the NIS-Directive, the regulatory authority posed specific certification requirements to the energy sector in its "IT-Security Catalogue" according to § 11 (1) *Energiewirtschaftsgesetz*. In other sectors, such as water and waste water, industry specific security standards are being implemented, and should be considered, respectively.

Furthermore, the German Institute for Standardisation (DIN, Deutsches Institut für Normung) promotes security in the industrial sector in its projects "IoT Security" and "Secure Identities". Sector-specific standardisation work is also being promoted at DKE (German Commission for Electrical, Electronic & Information Technologies of DIN and VDE). Cybersecurity not only concerns the digital single market, but also Member States; especially regarding questions of security standards and certifications.

For an analysis on a European level, regarding which standards already exist and where preparatory work has already been carried out, the know-how of CEN/CENELECs Cyber Security Coordination Group (CSCG) should also be incorporated, to effectively avoid inefficiencies or duplicate work.

2.4 Improved consistency and explicit differentiation between legislative proposals on privacy (e.g. General Data Protection Regulation GDPR, ePrivacy Regulation), Cybersecurity (e.g. NIS-Directive, Cybersecurity Act) and authenticity (e.g. eIDAS Regulation)

In the wake of increasing digitalization of the economy, governments and society and with the associated technical progress and societal realities, the requirements in the areas of cyber- and information security, authenticity and privacy are increasing rapidly. Although these areas have intersections and potentials for synergies, BDEW recommends, to lay down more consistent requirements in common areas, and ensure explicit differentiation in other areas. Enhanced cooperation and coordination between the involved Directorates-General (e.g. DG CONNECT, DG GROW, DG HOME, DG ENERGY) can contribute to this.