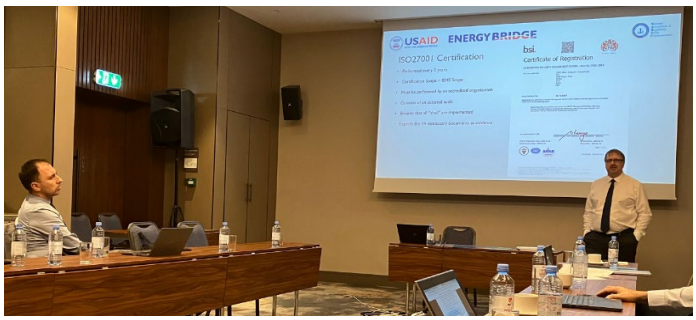
North Macedonia Regulator Adopts Cybersecurity Rules, Takes on Leading Role in Securing Energy Sector Protection and Resilience



June 2023 – This month, the Energy and Water Services Regulatory Commission (ERC) of North Macedonia adopted new Cybersecurity Rules, which will be integral to implementing cybersecurity standards in the energy sector, strengthening the sector's resilience, and protecting critical energy infrastructure. With funding from the United States Agency for International Development (USAID) Bureau for Europe and Eurasia, the National Association of Regulatory Utility Commissioners (NARUC) has worked with the Energy and Water Services Regulatory Commission (ERC) of North Macedonia since 2018 to strengthen and improve its cyber preparedness capabilities through the Europe and Eurasia Cybersecurity Initiative ("the Initiative").

The Initiative supports USAID's U.S.-Europe Energy Bridge goal of critical infrastructure protection by supplying national regulatory authorities in Europe and Eurasia with the information needed to prevent and respond to cyberattacks as well as establish regulatory frameworks to improve critical infrastructure resilience. USAID's Energy Bridge is anchored in the belief that a country's long-term energy security is indivisible from its sovereignty, its economic prospects, and the strength of its democracy.

The ERC has been an active participant of the Initiative – for example, it created a cybersecurity working group that engages in USAID and NARUC cybersecurity activities and provided comments on national-level primary legislation relating to cybersecurity energy rules. Following participation in USAID and NARUC activities, the ERC also developed a regulator-level cybersecurity strategy and associated action plan, for which NARUC volunteer experts reviewed and provided comments. In particular, the cybersecurity strategy has helped the ERC to better organize its internal processes, affirm its position regarding cybersecurity, and improve its ability to navigate conversations around cybersecurity with other energy sector stakeholders. Together, these actions convey the ERC's role as a proactive leader on cybersecurity and the effective management of cybersecurity procedures for entities in North Macedonia's electricity sector.

The progress that the ERC has made under the Initiative is in line with efforts by the Government of North Macedonia to improve its ability to protect critical infrastructure and ensure that systems and structures are in place to meet the future requirements of international allies like the European Union (EU) and the North Atlantic Treaty Organization (NATO).[1] Cyberattacks are on the rise throughout Europe and have been compounded by the Russian Federation's war on Ukraine, which has made protecting the energy sector more vital than ever.[2]

In addition to geopolitical factors, the energy sector is an attractive target for attackers for multiple reasons, including that it relies on inherently complex infrastructure and there is a shortage of cybersecurity expertise in the workforce.[3] With this in mind, the ERC is using its credibility and authority to work with other energy sector stakeholders in North Macedonia to respond proactively to cyber threats and ensure the grid is resilient and well-protected.

Amending North Macedonia's Energy Law and Drafting the Cybersecurity Rules

In 2018, North Macedonia's Parliament adopted a new Energy Law, developed with USAID assistance, which harmonized the energy legislation of North Macedonia with the EU Third Energy Package.[4] The ERC and other national energy sector stakeholders drafted amendments to align the recently adopted law with international cybersecurity standards for energy organizations and create a more secure digital ecosystem. USAID Connect for Growth activity assisted in drafting the amendments, and NARUC assisted by providing feedback on this draft as well as customized support in developing the accompanying Cybersecurity Rules – which are bylaws that the ERC will adopt for internal management – and procedures for implementing the amended Energy Law after its adoption.[5]

In November 2022, North Macedonia's Parliament adopted the amended Energy Law, effectively assigning the responsibility of overseeing cybersecurity in the energy sector to the ERC, providing a testament to the ERC's leadership in the energy sector and the importance of cybersecurity hygiene in the sector. Following this development, in December 2022 NARUC delivered a set of draft Cybersecurity Rules, which USAID Connect for Growth helped to finalize by ensuring consistency with the local legal format in North Macedonia. NARUC then trained the ERC and relevant energy sector stakeholders on the associated implementation steps required. During the training, ERC staff identified critical decision points around implementing the rules as well as a draft timeline for internal review and future use.

On June 8, 2023, the ERC Board fully adopted the Cybersecurity Rules, which will aid it in: 1) implementing cybersecurity standards in the energy sector of North Macedonia, 2) setting reporting requirements agreed upon with energy sector stakeholders to ensure cyber preparedness, and 3) strengthening energy sector resiliency. Per the ERC's press release, the Rules will ensure that "operators and manufacturers are obliged to appoint a cyber security officer and prioritize measures to protect critical infrastructure, for which there will be an appropriate procedure for monitoring, reporting and dealing with cyberattacks." In doing so, they will help to maintain security of supply, protect market participants and consumers, and enhance the efficiency, competitiveness, and transparency of North Macedonia's energy market.

To learn more about this development, NARUC spoke with Apostolcho Ramov, Head of Information Technology (IT) at the ERC, on the role of the regulator when it comes to cybersecurity in the energy sector, how the ERC has grown its cybersecurity capacity over the years, and how the Cybersecurity Rules will impact both national and regional energy security.

Q&A

Can you tell us about yourself and your role at the ERC?
My name is Apostolcho Ramov, and I have been working as the head of the IT department at the ERC for almost 14 years. I am very pleased to be part of the project provided by USAID and NARUC; it has enabled us to keep pace with developments related to cybersecurity issues in the energy sector. Our dedicated team at the ERC has used this opportunity to learn about the current trends, approaches, strategies, and activities in the United States and the EU that address the preparation of an adequate response by regulatory bodies to the risks arising from potential cyberattacks on energy networks and facilities.

How long have you been part of USAID and NARUC's regional cyber working group? Can you name the most memorable results of your participation in the Initiative?
I have been part of USAID and NARUC's regional cyber working group for almost four years. For me, the most memorable result of my participation in the Initiative is the ERC's preparation of a cybersecurity strategy for the electricity sector. From 2018-2020, the ERC, in consultation with NARUC, prepared this regulator-level strategy as well as a draft list of recommendations for the transmission system operator, distribution system operator, and large generation companies as well

as a draft action plan for the implementation of the strategy. These milestones have helped guide the direction the ERC has taken toward our most recent achievement of adopting the Cybersecurity Rules.

In your point of view, what is the role of the energy regulator when it comes to critical infrastructure protection and cybersecurity?
Often, cyber resilience and cybersecurity is thought of solely as an IT issue. However, this is not the case as energy companies' resilience to cyberattacks has significant implications for energy markets and final consumers, thereby linking it to ERC statutory objectives. The ERC has a strategic role, which is to ensure the well-functioning of the national energy markets. Key operational objectives in this respect are to provide security of supply and customer protection as well as strengthen the efficiency, competitiveness, and transparency of the energy markets. In order to provide security of supply, the ERC aims to ensure the soundness of regulated companies, and in so doing reduce the risk of disruption to the continuity of electricity supply.

Since 2018, USAID and NARUC have supported the ERC with regard to cybersecurity regulation, including peer reviewing the ERC cybersecurity strategy, providing training on cybersecurity maturity models, and sharing the five publications in the USAID and NARUC Europe and Eurasia Cybersecurity Initiative Toolkit. Can you give us some examples of how the ERC has used this assistance to grow its cybersecurity capacity and how it has become a leader in ensuring cybersecurity in North Macedonia?
The ERC added USAID and NARUC's framework for cybersecurity investment to its current tariff approval system, which requires utilities to provide detailed information on their planned costs for security/cybersecurity. If an evaluation shows that the costs are reasonable and realistic, they are approved as part of the utilities' investment plans for the following regulatory period.

Some parts of the Revenue Cap Regulation Methodology, which the ERC uses for tariff approval, resulted from USAID and NARUC assistance. Additionally, we incorporated some examples from the USAID and NARUC document "*Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators*" in the methodology. The ERC is also using some methods from performance-based regulation, which NARUC gave presentations on in the past, especially for defining cybersecurity requirements, recommendations, and indicators for utilities.

Can you explain what the new Cybersecurity Rules will implement and how they will strengthen North Macedonia's energy security?
The ERC sees the Cybersecurity Rules as a new and very important regulatory instrument that will strengthen its regulatory competencies in the segment of cybersecurity issues. With the adoption of the Energy Law Amendments, the ERC gained the legal basis to enforce secondary legislation. The Cybersecurity Rules will lead to improvements in the security of supply by ensuring that critical energy infrastructure is ultimately well protected. They will clearly define the role of the ERC in terms of cybersecurity and the effective management of cybersecurity procedures for entities in the electricity sector, as well as generate a specific set of measures that other entities should undertake.

Given the increasing number of cyberattacks in Southeast Europe, do you think the adoption of the Cybersecurity Rules will also impact regional cybersecurity?
Definitely. The adoption of the Cybersecurity Rules will also impact regional cybersecurity in all Balkan countries because we are all connected through the electrical grid. If there is a cyberattack on the power grid in one country, there is a possibility for a cascading effect, and through interconnections, neighboring countries will also be affected by that attack.

What do you think the significance of regional collaboration and cooperation is when it comes to adopting cybersecurity standards and regulations?
To achieve a high level of confidence in the security of the electricity sector in North Macedonia, a high degree of cooperation is needed between the ERC and other local stakeholders in the electricity

sector. Regional collaboration is also key, as well as the willingness of countries to respond proactively to threats in the sector and enhance the resilience of their own systems against cyberattacks.

Having said that, we would like to point out that the ERC is going to use its credibility and authority to strengthen that confidence and provide an environment in which all relevant stakeholders will act accordingly with this key aim – to provide a secure and reliable electricity system in the country and through interconnections with neighboring countries.

What best practices would you share with other regulators in the region working with energy sector stakeholders and their respective governments to establish legislation and coordination on cybersecurity?
Our approach was to first adopt the Energy Law Amendments, wherein the ERC gained a legal basis to enforce secondary legislation, and after that to publish the Cybersecurity Rules. However, this legal process was quite long. Our advice to other regulators that decide to establish legislation first is that they should start drafting cyber documents and any amendments to laws as soon as possible.

We also encourage other regulators to start approving more investment from stakeholders in cybersecurity. As an example, we would like to point out that the ERC has approved investments for the regulatory period 2021-2023 for the transmission system operator for the purchase and installation of anti-virus and anti-spam security, an analysis of data with log management, and the purchase of redundant security devices and cybersecurity software and security equipment.

Working Together to Protect the Energy Sector

Cybersecurity regulations, like any piece of legislation, take time to draft, review, and adopt. However, in the face of the increased digitalization of the electric grid, it is of utmost importance for regulators around the world to work with their utilities and other governmental institutions to develop a set of regulatory mechanisms that protect critical infrastructure and keep electricity flowing into homes and businesses alike. USAID and NARUC welcome North Macedonia's legislative developments and commend the ERC and all stakeholders involved for their diligence and collaboration. Through the Europe and Eurasia Cybersecurity Initiative, USAID and NARUC will continue to support regulators in the region as they mitigate the challenges associated with promoting cybersecurity legislation and coordination and work to ensure the energy security of their countries.

This story is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of NARUC and do not necessarily reflect the views of USAID or the United States Government.

Photo Caption: Macedonian training participants discussing ISO27001 within the cyber bylaws, Photo Credit: NARUC

---

[1] "Critical Infrastructure Digitalization and Resilience." USAID. https://www.usaid.gov/north-macedonia/fact-sheets/mar-31-2023-critical-infrastructure-digitalization-and-resilience

[2] Joshi, Akshay and Spencer Feingold. "Europe is bolstering energy sector resilience. But cyber risk remains a major vulnerability." World Economic Forum. October 2022. https://www.weforum.org/agenda/2022/10/europe-is-energy-sector-resilience-cyber-risk/

[3] James, Luke. "Energy sector: More cyberattacks in 2022 than ever before." Power & Beyond. March 2023. https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a010c7a7e7d3/

[4] "Renewable Energy Law and Regulation in North Macedonia." CMS Legal. https://cms.law/en/int/expert-guides/cms-expert-guide-to-renewable-energy/north-macedonia

[5] "Bylaw." Vocabulary.com, Inc. https://www.vocabulary.com/dictionary/bylaw