Energy Regulator Entity of Albania

Julinda Hoxhalli

Legal developments on Cyber security

- Law No.2 / 2017, "On Cyber Security "
- National Cybersecurity Strategy and its Action Plan 2020-2025 (DCM No1084, dated 24.12.2020).
- DCM No. 553, dated 15.07.2020, "On approval of the list of critical information infrastructures and list of important information infrastructures "
- National Authority for Electronic Certification and Cyber Security –bylows
  - Methodology for identification and classification of Critical Infrastructures and Important Information Infrastructures
  - Regulation on the Categories of Cyber Incidents and the format & elements of the report (Order No.62, dated 10.09.2018).
  - Regulation on the content and method of documenting security measures (Order No. 22, dated 26.04.2018), etc.

Regulation on cyber security of critical infrastructures in the power sector

- Regulation on cyber security of critical infrastructures in the power sector was approved by the ERE Board with the decision No. 126, Dated 30.07.2020
  - The adoption of this regulation was preceded by a consultation process with the Ministry of Infrastructure and Energy, Competition Authority, DSO, TSO, KESH, and the Electricity Community Secretariat.
  - The draft Regulation was also sent to the "National Authority for Electronic Certification and Cyber Security" for comments and suggestions.
  - Comments and opinions of stakeholders and consultants are taken into account and are reflected in the Regulation by making the necessary adaptation to the laws and bylaws in power.
- The regulation consists of 11 Articles which set out General rules and basic principles, as well as three Annexes:
  - ✓ Annex 1 Self Assessment Report on Critical Infrastructure Protection and Risk Management
  - ✓ Annex 2 The form of reporting a security incident and/or violation of integrity
  - ✓ Annex 3 Self-assessment report of the Operator on the Security Incident impact

Obligations of Critical Infrastructures Operators

- The operator for critical infrastructures on power sector shall take appropriate, proportional, cost effective, technical and organizational measures to guarantee network security, to properly manage, address, and handle appropriately the risks submitted for the networks and information security.
- The Critical Information Infrastructure Operator shall submit its self-assessment to ERE based on the "Regulation on the content and method of documenting security measures (Approved by Order No. 22, dated 26.04.2018 of the NAECCS) and in accordance with Annex no.1 of the regulation
  - After submitting the self-assessment report, the operator must propose their action plans to the competent authorities.
  - Identifies needs and reviews investment plans, which should take into account the need to reduce the risks identified.
- In conformity with the provisions of article 6 the Critical Information Infrastructure Operator shall report periodically once in every six months within January and July for the previous six months, in accordance with Annex 1 of this regulation.
- The operators shall submit to ERE, the reports on each unplanned intervention, violation or incident in the scope of the security, availability and integrity of their electronic communication networks, as well as any intervention, damage that considerably impacts the networks operation and/or their service status in accordance with Annex no.2 and Annex no.3

ERE Actions regarding Cyber Regulation

- After the submission of self-assessment, when appropriate, ERE may enter into discussions and request additional information on the reported issues to realize the respective assessments.
- ERE may require that the self assessment reports prepared by the Critical Information Infrastructure Operator to be audited.
- ERE, may case-by-case, require review of the actions plan from the Critical Information Infrastructure Operator in order to assist them in prioritizing and planning cyber risk protection.
- After submitting the first self-assessment and improvement plan, ERE shall carry out onsite monitoring at the Critical Information Infrastructure Operator and following the monitoring results shall submit the respective recommendations.
- ERE may require detailed information from the Critical Information Infrastructure Operator to support any assessment regarding the compatibility of the licensee actions with the rules regarding the security of the critical infrastructures. If ERE concludes that the cooperation with the Critical Information Infrastructure Operator has not operated or it is clear that there are not taken the necessary measures to avoid the incidents on the critical infrastructure, ERE shall inform the operator for the identified failures. ERE may set deadlines to correct the failures evidenced by the Critical Information Infrastructure Operator.

Periodic reporting by Critical infrastructure Operator

- TSO respected the legal deadline for reporting on cyber security for the first 6 months of 2021, but the reporting format does not comply with the requirements of the regulation, making it difficult its evaluattion by ERE. TSO reports that the self-evaluation is still under process.
- OSHEE respected the legal deadline for reporting on cyber security for the first 6 months of 2021 but submitted 2 separate reports for various infrastructures. As the reporting requirements under Annex 1 and the NAECCS regulation are the same for all infrastructures, we think that the reporting template must be unique.
- KESH did not comply with the requirements of the regulation on cyber security reporting and and did not respond to the ERE request for information.

NARUC -Short Term Technical Assistance

- Our Term of Reference (TOR) have been selected by NARUC for the first round of short-term technical assistances on cybersecurity.
- These STTAs will be part of USAID/NARUC's Europe & Eurasia Cybersecurity Initiative and efforts to improve cybersecurity and resilience in our energy sector.
- NARUC intends to support ERE with regulatory assessments of utility preparedness by working towards the following deliverables:

✓Customized instructional walk-through for evaluating cyber investments using the results of a maturity model

✓Customized risk assessment template and walk-through

✓Customized schedule and plan for continuous updates of processes and incident reporting

- Through this STTA ERE will be in better position to evaluate the cyber preparedness plans submited by the utilities and will become better equipped to oversee the security and reliability of the Albanian power grid and to advance cybersecurity best practices, thus, enabling the effective monitoring of the critical infrastructure protection of the power grid.

THANK YOU!