MAYER | BROWN

April 16, 2019

Cybersecurity & Data Privacy

Strategic Thinking and Practical Legal Advice

One Size Does Not Fit All: EU Commission Recommendations on Cybersecurity in the Energy Sector

As new technologies develop, the smart grid and smart devices become increasingly interconnected and exposed to security incidents. As in other jurisdictions, in the European Union ("EU") the critical nature of energy infrastructure (and the vital nature of energy supply) demands the attention of EU cybersecurity policies and initiatives.

On April 3, 2019, the EU Commission issued its recommendations on cybersecurity in the energy sector (the "EU Commission Recommendations"). The EU Commission Recommendations highlight actions that EU member states and relevant stakeholders present in the EU, such as network operators and technology suppliers, should take to enhance preparedness for potential cyberattacks considering the very specific nature of the energy sector, namely: (i) real-time requirements, (ii) the risk of cascading effects, and (iii) the combination of legacy systems with new technologies. Energy companies may decide voluntarily to comply with the EU Commission Recommendations.

This Legal Update gives a refresher on the EU cybersecurity framework for the energy sector and provides a summary of the EU Commission Recommendations, including next steps that energy network operators should consider.

The EU Cybersecurity Framework for the Energy Sector

The EU cybersecurity landscape is evolving, with different pieces of legislation that have, or will have, an impact on the energy sector. The EU Commission Recommendations build on other EU legislation in the area.

- Last year, the Directive on Network Security Infrastructure (the "NIS Directive") entered into force. The NIS Directive seeks to achieve a high common level of security for networks and information systems by imposing security standards and incident notification requirements on operators of essential services in specific sectors—including the energy sector. The NIS Directive required implementation at the national level by May 9, 2018. Many EU member states were late in the implementation process and in the identification of the operators of essential services at the national level.
- Last month, the EU institutions (i.e., the European Parliament, the Council and the EU Commission) reached an agreement on the Cybersecurity Act (the "Act"). The Act creates EU cybersecurity certification schemes for information communications technology ("ICT") products (the hardware

and software elements of network and information systems); services (the services involved in transmitting, storing, retrieving or processing information via network and information systems); and processes (the sets of activities performed to design, develop, deliver and maintain ICT products and services). This new framework should, amongst others, give companies operating in the energy sector an opportunity to certify their products, services or processes.

- The EU Commission also proposed sector-specific legislation under the "Clean Energy for All Europeans" package that, if adopted, has cybersecurity aspects:
  - A new Regulation on Risk Preparedness of the Electricity Sector requires EU member states to develop national risk preparedness plans that take into account cybersecurity and guarantee the stability of their systems against potential threats.
  - A proposal to review the Electricity Regulation provides for the adoption of technical rules for electricity and tasks the EU Commission with developing a network code on cybersecurity for the electricity sector to increase its resilience.
  - Finally, under the Gas Security of Supply Regulation, EU member states are required to take into account cybersecurity as part of their regional and national risk assessments.

The EU Commission Recommendations

The EU Commission Recommendations highlight the main challenges that energy service providers face and identify necessary steps to enhance cybersecurity preparedness. These are summarized below.

REAL-TIME REQUIREMENTS OF ENERGY INFRASTRUCTURE COMPONENTS

The EU Commission recognizes the challenges of implementing cybersecurity measures for those elements of energy systems that work under "real-time" conditions, meaning that they react to commands within milliseconds (e.g., circuit breakers).

According to the EU Commission, to appropriately face this challenge, energy network operators should:

- Take real-time constraints into account in developing security for assets, with attention paid to asset classification;
- Implement the most recent security standards for new installations and consider complementary physical security measures where cybersecurity mechanisms would not be able to ensure the right level of protection;
- Apply international standards on cybersecurity as soon as products are commercially available;
- Do not rely on a one-size-fits-all approach for the security of their products but, rather, split the overall systems into logical zones and apply appropriate measures to each of them; and
- Consider relying on privately owned networks for tele-protection schemes to guarantee the quality of service level required for real-time constraints.

CASCADING EFFECTS

The EU Commission Recommendations highlight how, due to the interconnection of the electricity grids and the gas pipeline in the EU, a cyberattack in a part of an energy system may have effects in other parts of that system. To mitigate far-reaching cascading effects, energy network operators should:

- When developing and introducing new devices, especially in regard to Internet of Things ("IoT") devices used in industrial settings, ensure they maintain a high level of cybersecurity that is appropriate to the site's criticality;

- Take into account cyber-physical effects when establishing and periodically reviewing business continuity plans; and
- Establish design criteria and architecture for a resilient grid, for instance by collaborating with other relevant operators and technology suppliers and trying to identify critical nodes.

LEGACY AND STATE-OF-THE-ART TECHNOLOGY

The EU Commission explains how, in today's energy system, two different types of technologies coexist: "an older technology with a lifespan of 30 to 60 years, designed before cybersecurity considerations, and modern equipment, reflecting state-of-the-art digitalization and smart devices."

In this regard, the EU Commission encourages energy network operators to:

- Assess the risks of connecting legacy and IoT equipment, and be aware of the vulnerabilities of both internal and external interfaces;
- Implement appropriate security measures against malicious attacks originating from bots;
- Establish an automated monitoring and analysis capability for security-related events in both legacy and IoT environments;
- Periodically run specific cybersecurity risk analysis on all legacy installations, in particular when new technologies are connected to old ones;
- Update the software and hardware of both legacy and IoT systems to the most recent version whenever possible;
- Take cybersecurity requirements into account in procurement processes by, amongst others, ensuring that information is sought about security features or compliance with existing cybersecurity standards, and to clarify vendor liability in the event of cyber-attacks or incidents; and
- Collaborate with technology suppliers to replace legacy systems whenever beneficial for security reasons.

Next Steps

Member states are expected to take steps to follow the EU Commission Recommendations when developing national cybersecurity frameworks (e.g., through strategies, laws, or regulations). Within the next 12 months and every two years thereafter, EU member states are required to communicate to the EU Commission details about the state of the implementation through the NIS Cooperation Group (established under the NIS Directive, which is composed of representatives of member states, the European Agency for Cybersecurity ("ENISA") and the EU Commission). Using this information, the EU Commission will regularly review the EU Commission Recommendations, in consultation with EU member states and relevant stakeholders.

Companies in the energy sector present in the EU should keep the EU Commission Recommendations in mind even if they are not legally binding and stay tuned for other developments in the area, such as the work conducted by ENISA on the development of certification schemes in the energy sector and the adoption of national legislation implementing the NIS Directive.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Diletta De Cicco
+32 2 551 5945
ddecicco@mayerbrown.com

Charles-Albert Helleputte
+32 2 551 5982
chelleputte@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com