August, 2020

NATIONAL ELECTRICAL COORDINATOR PUBLISHES CYBER SECURITY STANDARD FOR THE ELECTRICAL SECTOR

The National Electricity Coordinator ("CEN") is Chile's grid operator in charge of coordinating the operation of all the facilities of the National Electricity System. One of its roles is to preserve the security of the service in the electricity system, and it has drafted the Cybersecurity Standard for the Electricity Sector ("Cybersecurity Standard") in accordance with the instructions of the Superintendency of Electricity and Fuels ("SEC").

The Cybersecurity Standard sets forth the minimum cybersecurity requirements and measures that must be complied within the national electrical industry to prevent and/or mitigate potential cyberthreats that endanger the security and continuity of the electrical energy service.

The cybersecurity standard chosen by CEN to be adopted by the electrical industry at a national level is the CIP (Critical Infrastructure Protection) Standard of NERC (North American Electric Reliability Corporation) or NERC-CIP which, according to CEN, includes fundamental aspects for information security and critical technological and operating infrastructures of electrical systems

The requirements established in the Cybersecurity Standard are applicable to both the CEN and the Coordinated Companies ("Responsible Entities"), notwithstanding that the specific applicability of this standard is associated with the existence of facilities or assets that qualify within any of the impact rating categories established in this standard (high, medium, or low).

Thus, the Responsible Entities shall have an obligation to implement the requirements under the Cybersecurity Standard within the time periods indicated therein, which include white-running periods ranging from three (3) to twenty-four (24) months.

The Responsible Entities shall monitor and report annually to the SEC the level of compliance with the control measures for each requirement within the first quarter of each year in a format defined by the SEC.

The Responsible Entities shall also have the obligation to notify the CEN and SEC of reportable cybersecurity incidents within one hour from the incident being detected, through the CIP Officer that each entity shall have.

If you have any questions regarding the matters discussed in this news alert, please contact the following attorneys or call your regular Carey contact.

Carey y Cía. Ltda.
Isidora Goyenechea 2800, 43rd Floor.
Las Condes, Santiago, Chile.
www.carey.cl

Lastly, Responsible Parties must maintain records of evidence and control measures for a period of at least 3 years, which may be extended as required by the SEC if there is an ongoing investigation because of an audit. In addition, the SEC may instruct compliance audits and/or certifications by third parties specializing in cybersecurity matters to verify compliance with the standard.

The Cybersecurity Standard is a lengthy and complex document that we recommend reviewing in detail with your IT and legal teams. We look forward to assisting you in reviewing and understanding this document to help you determine the operational impact of the new obligations that are generated.