Bond Case Briefs

Municipal Finance Law Since 1971

Infrastructure Investment and Jobs Act: Cybersecurity Impacts on the Energy Sector.

The November 15 signing of the Biden administration's bipartisan $1 trillion Infrastructure Investment and Jobs Act offers a prime opportunity to review the legislation, which brings a significant reinvestment in America's energy infrastructure and an opportunity for many in the energy sector. Unsurprisingly, following the Solarwinds Orion compromise and the ransomware attack on the Colonial Pipeline, cybersecurity features centrally in the act's provisions.

Service providers hoping to benefit from the act's substantial funding must be keenly aware of the cybersecurity requirements it implements, as they offer both potential opportunities for the prepared and potential pitfalls for the unwary. Although it would be impossible to analyze the full impact of the cybersecurity provisions here, we hope to highlight key aspects that warrant your further attention.

Cybersecurity Plans

One of the key cybersecurity provisions of the Infrastructure Investment and Jobs Act is its imposition of cybersecurity requirements as a potential precondition to receive federal funds. These requirements include submission of a cybersecurity plan demonstrating that the applicant has a mature cybersecurity program and a plan for maintaining cybersecurity throughout the life of the project. The plan will require detailed descriptions of how cybersecurity will be maintained, how ongoing risk evaluations will be conducted, how vulnerabilities or compromises will be reported and how Department of Energy cybersecurity programs will be leveraged.

These requirements create an urgent need for utilities, contractors and suppliers to ensure that they have robust cybersecurity mechanisms in place. The best way to do this is through regular risk assessments identifying gaps in technical, administrative and physical security. These assessments should be overseen by outside counsel so that potential security gaps and liabilities can be identified and rectified in a privileged manner before it becomes necessary to demonstrate that cybersecurity maturity to potential clients or funders.

Application of Cybersecurity Standards

The act further cements the centrality of two key cybersecurity models, the DOE's Cybersecurity Capability Maturity Model and the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity. Both models provide a procedural framework for evaluating an organization's cybersecurity, conducting risk assessments and targeting future improvements. The act, however, makes these previously voluntary standards the default and requires documentation of any deviations, establishing their central role in discussions of cybersecurity going forward.

Continued Reporting

Perhaps the most significant change that we anticipate is the focus on continued evaluation and

patching of cybersecurity risks. The cybersecurity plans potentially required under the act require ongoing evaluation and threat reporting, and the act provides a route to compliance by establishing a “voluntary” reporting program, encompassing:

1. Product testing,
2. A vulnerability reporting process,
3. Technical assistance to close vulnerabilities,
4. Biennial reviews of tested products and analysis of how they respond to and mitigate threats, and
5. Development of procurement guidance.

These ongoing requirements create an extended service obligation for vendors and contractors, which we anticipate may be filled by the original manufacturers and suppliers of equipment, by operations and maintenance contractors or by other third-party vendors. We also anticipate that, with increased and extended cybersecurity scrutiny, suppliers and contractors will face increased litigation risks as more vulnerabilities are identified and required to be corrected. Such reporting processes will also expose suppliers to potential compromise of intellectual property or the potential harm of inaccurate threat assessments.

Funding Opportunity

Although the Infrastructure Investment and Jobs Act imposes significant additional obligations on the energy industry, it also provides significant opportunities for growth through rate-based cybersecurity incentives, $250 million in grants and technical assistance for rural and municipal utilities and $250 million in grants for enhanced power grid security.

This funding creates massive opportunities for those with the cybersecurity infrastructure in place to satisfy the act’s requirements. We also note, however, concern that the added requirements connected to this funding may disadvantage smaller businesses, including women- and minority-owned business enterprises, that have not yet developed cybersecurity maturity, potentially forcing partnerships with more mature actors or reliance on external cybersecurity resources.

Key Takeaways

Cybersecurity requirements are not new to the energy sector, but the act significantly expands their application, creating both risks and opportunities for the energy industry. We encourage industry participants to begin thinking proactively about the act’s impacts, how best to position themselves to take part in government-funded projects subject to those requirements and what risks might lurk within these provisions.

Duane Morris LLP – Owen Newman and Chris J. Chasin

November 16 2021