Van Ness Feldman LLP
vnf.com

CYBERSECURITY & EMERGING TECHNOLOGIES

PRACTICE CONTACTS

Michael D. Farber
Partner
mfarber@vnf.com
202.298.1803

Technology continues to transform the way businesses conduct all aspects of their operations—from maximizing efficiencies to improving how organizations gather, analyze, and share information to facilitating connections to a broader network of stakeholders. The benefits of this progress create the need to protect systems from unwanted disruptions through cyber-attacks and to navigate the outdated regulatory provisions that did not contemplate new levels of innovation. Van Ness Feldman's Cybersecurity and Emerging Technologies Team recognizes these unique challenges and provides counsel to a diverse range of clients concerned with how to find flexibility in rigid legal constructs as well as to organizations looking to mitigate the cyber-related vulnerabilities that threaten critical infrastructure. Our client base includes oil and gas pipelines; LNG facilities; offshore oil and gas rigs/platforms; electricity generation, transmission, and distribution assets; hydropower and municipal water facilities; nuclear reactors and chemical plants; and medical, research and academic institutions. Our team combines decades of experience providing regulatory compliance, risk mitigation, incident response, and advocacy representation to the energy and environmental sectors and is highly-regarded for assisting clients with their compliance planning and policy development goals.

CYBERSECURITY

With an increased prevalence of threats to physical, natural, and cyber systems, both public and private sector entities must strengthen their defense and resilience against at-risk systems—particularly given an increased reliance on networks necessary to operate these systems and the severe health, safety, environmental, and regulatory consequences arising from cyber-attacks to these types of assets. Recognizing that businesses are at varying levels of cyber maturity and that each industry has its own regulations, guidelines and expectations, our team provides customized services to meet clients' needs and obligations to keep critical infrastructure secure and bolster national security.

GOVERNMENT RELATIONS & ADVOCACY

Through our experiences and relationships, we are able to effectively coordinate funding and other legislative efforts for our clients. Team members have significant experience assisting clients with advocacy regarding the development and implementation of cybersecurity-related legislation. Our team also has noteworthy executive branch experience with agencies that have oversight of systems at risk of cyber-attacks.

REGULATORY COMPLIANCE & MONITORING

Our professionals make it a priority to stay ahead of new legislation, regulations, and other cyber developments in order to keep our clients well-versed and in compliance with requirements as they arise. Our team is able to provide keen insights to help clients implement the best practices outlined in the National Institute of Standards and Technology (NIST) Framework, and the Pipeline Security Guidelines proffered by the Transportation Security Administration (TSA) and various electric power industry reliability standards, including the Critical Infrastructure Protection (CIP) standards enforced by the North American Electric Reliability Corporation (NERC). We can also survey the relevant rules and regulations in any industry for businesses looking to determine whether their new approach to operations triggers any compliance concerns.

Van Ness Feldman LLP
vnf.com

RISK MITIGATION & INCIDENT RESPONSE

Employing our unique understanding of the regulatory framework governing these industries, our attorneys—with the help of cyber risk professionals—can conduct compliance audits to evaluate general operational system vulnerabilities and offer potential solutions, including system improvements and employee training to mitigate risks.

In the event that a cyber-incident does occur, our team is able to conduct internal investigations, help in coordinating with enforcement authorities, and provide appropriate notifications in the event of a security breach. In addition, for clients that have avoided incidents to date, we can offer advice on response planning, including partnering with technical experts to conduct “table top“ exercises that yield lessons learned from a simulated incident.