



#### **PRACTICE CONTACTS**

Michael D. Farber

Partner

[mfarber@vnf.com](mailto:mfarber@vnf.com)

202-298-1803

Gwendolyn Keyes Fleming

Partner

[gffleming@vnf.com](mailto:gffleming@vnf.com)

202-298-1928

Terese (T.C.) Richmond

Partner

[ter@vnf.com](mailto:ter@vnf.com)

206.623.9372

Malcolm C. McLellan

Partner

[mcm@vnf.com](mailto:mcm@vnf.com)

206.829.1814

## **ENERGY CYBERSECURITY**

Cybersecurity, proprietary data, and information protection have long existed within the risk management portfolio of government, private and public organizations, especially in the energy and environmental space. There is increasing recognition that threats exist not only to traditional information technology (IT), but operational technology (OT) as well. As the number of incidents increase and the vulnerability of critical infrastructure becomes more apparent, these risks have rapidly risen to become a top priority for various sectors.

State and local governments across the country are examining ways to protect their citizens and strengthen their resilience against physical, natural and cyber threats. Institutional and industrial control systems that are connected to networks face exacerbated risks because of the increased reliance on the networked devices necessary to operate these systems and the severe health, safety, environmental, and regulatory consequences of a cyber-attack. These at-risk systems include 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.

Van Ness Feldman has the experience and capabilities to assist operators of these facilities in addressing the multifaceted cyber threats impacting their assets. Our decades of experience with all aspects of energy and natural resources project development and operation, along with our work as former government officials, allow us to offer the following types of cybersecurity services:

### **RISK ASSESSMENT & MITIGATION**

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

### **INCIDENT PLANNING & RESPONSE**

Our team can assist clients in coordinating with enforcement authorities and provide appropriate notifications in the event of a security breach. 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.

### **INTERNAL INVESTIGATIONS**

In the event that a cyber-incident does occur, Van Ness Feldman attorneys can assist with or conduct interviews of client personnel and review relevant documents and data to determine whether failures and/or misconduct occurred, and report any findings.

### **LITIGATION**

Our talented team of litigators can respond quickly and effectively if a cyber-attack or incident results in an enforcement action or litigation. We have served as lead counsel in numerous complex proceedings in federal and state courts (both trial and appellate) and in administrative proceedings before federal, state, and local agencies.

## 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 experience includes working with clients to ensure regulatory compliance with various electric power industry reliability standards, including the Critical Infrastructure Protection (CIP) standards enforced by the North American Electric Reliability Corporation (NERC).

## GOVERNMENT RELATIONS & ADVOCACY

The lawyers and public policy professionals who comprise Van Ness Feldman's bipartisan government relations team have served as legal counsel and policy advisers to members of Congress and Congressional committees, White House staff, and presidential appointees to federal agencies in both Democratic and Republican administrations.

Our professionals have significant experience assisting clients with advocacy before Congress and the executive branch with regard to the development and implementation of cybersecurity-related legislation. Through our experiences and relationships, we are able to effectively coordinate funding and other legislative efforts for our clients.

Our team has significant executive branch experience and strong relationships with those agencies who have oversight of systems at risk by cyber-attack, including:

- Bureau of Ocean Energy Management
- Bureau of Safety and Environmental Enforcement
- Department of Homeland Security
- Department of Justice
- Environmental Protection Agency
- Federal Energy Regulatory Commission
- National Oceanic and Atmospheric Administration
- National Transportation Safety Board
- North American Electric Reliability Corporation
- Nuclear Regulatory Commission
- Occupational Safety and Health Administration
- Pipeline and Hazardous Materials Safety Administration
- U.S. Chemical Safety Board
- United State Coast Guard