SUTHERLAND

CLIENT INFORMATION

February 8, 2011

Five Lessons Learned from the Reliability Compliance Front

With the recent reports on the Stuxnet computer worm and the threat it may pose to the nation's electric power grid, the impact of WikiLeaks on our national security, and increasing regulatory focus on the development of "smart grid" infrastructure and policies, cybersecurity continues to receive an unprecedented level of attention. The energy industry is particularly affected because of the potential impacts on both cybersecurity and the physical reliability of the power grid. At TechAmerica's Cybersecurity Forum last week in Florida on "Understanding, Managing and Mitigating Risk Across the Enterprise," Dan Frank, a partner in Sutherland's Energy Regulatory and Compliance Practice, spoke on cybersecurity matters on a panel specifically addressing the energy industry. In his prepared remarks, he identified "Five Lessons Learned from the Reliability Compliance Front" to provide guidance to organizations grappling with cybersecurity compliance issues, in both the energy sector and other affected industries.

All five lessons fall under one overarching theme: the importance of developing a strong, robust compliance program that will help organizations understand, manage and mitigate the risks that they face. There are two principal reasons for having a strong compliance program. First, regulators expect it. In many instances, a formal, written compliance program is not necessarily required by applicable laws and regulations. But if an organization is investigated or audited, the regulator invariably will ask for the organization's compliance program. Not having one is an immediate strike against the organization.

Second, having a formal documented compliance policy is a sound business practice. A solid compliance program will help the organization avoid violations in the first instance, thus directly reducing the risk of penalties and civil liability. Additionally, should a violation occur – and in today's complex regulatory environments, violations almost certainly will occur – a good compliance program will help mitigate the adverse consequences of the violation, from reducing regulatory penalties to helping contain and reduce potential civil liability.

For these reasons, it is imperative for every organization to develop and implement a strong compliance program. The following five lessons are intended to help in developing such a compliance program.

- Senior Management Commitment. Compliance must be top-down, and starts with the "C-suite." Without visible management commitment to full compliance, the organization will have difficulty overcoming the inertia that all too frequently stalls the best-laid plans for compliance – that is, until a massive monetary penalty is levied against the organization. A visible commitment to compliance by management will help steer the organization toward taking the steps needed to avoid penalties.
- Sufficient Resources. The organization must devote sufficient resources to compliance. Importantly, the organization must recognize that compliance is not a part-time job. All too often compliance is viewed as a temporary "extra" or "add on" job duty that can be pushed aside once the regulator completes the audit or investigation. But that is no longer an acceptable approach to compliance. One suggestion for overcoming this problem is to include compliance within job descriptions (*e.g.*, an employee's duties include being "responsible for compliance with applicable regulations"), followed by a commitment of the resources necessary for employees to fulfill their compliance duties.

This communication is for general informational purposes only and is not intended to constitute legal advice or a recommended course of action in any given situation. This communication is not intended to be, and should not be, relied upon by the recipient in making decisions of a legal nature with respect to the issues discussed herein. The recipient is encouraged to consult independent counsel before making any decisions or taking any action concerning the matters in this communication. This communication does not create an attorney-client relationship between Sutherland and the recipient.

- Training. Once it is clear that employees have a compliance responsibility, they must be given the tools to achieve compliance. One tool is training. The organization must devote sufficient resources to training, including identifying the relevant people who need to be trained (including outside vendors and contractors) and the relevant topics, timing and materials for the training.
- Compliance Officer. Each organization should designate a “point person” to be the chief compliance officer. But this responsibility must be more than simply “in name only.” The compliance officer must have both the authority and the clout to get things done. The compliance officer also must be independent and have access to senior management, or there is a risk that important compliance decisions will be overruled by the business line, to the detriment of the overall organization.
- Documentation. Finally, it is not enough for the organization to be compliant with the applicable laws and regulations. It must be able to demonstrate that compliance to the regulators and others to whom the organization may have exposure. Thus, the organization should develop and implement a rigorous documentation program.

Other Issues Addressed by the Cybersecurity and Energy Panel

Other issues addressed by the cybersecurity and energy panel at the TechAmerica Cybersecurity Forum included the status of existing cybersecurity laws and regulations affecting the energy industry, the need for additional clarity in those regulations, the need for resolution of jurisdictional conflicts and ambiguity among federal agencies addressing cybersecurity in the energy industry, the impact of Stuxnet on the status of cybersecurity legislation and regulation, the potential for a repeat of Stuxnet or a modified version of Stuxnet on the U.S. electric power grid, the status of enforcement of the NERC Reliability Standards and current level of penalties, and the status of federal “smart grid” initiatives.

For more information on the program, click here.

■ ■ ■

If you have any questions about this Client Information, please feel free to contact the attorneys listed below or the Sutherland attorney with whom you regularly work.

Daniel E. Frank	202.383.0838	daniel.frank@sutherland.com
Jennifer J. Kubicek	202.383.0822	jj.kubicek@sutherland.com

This article is for informational purposes and is not intended to constitute legal advice.