
Margaret H. Claybour


Robert G. Scott, Jr.

Federal Cybersecurity Framework Calls for Increased Vigilance

The energy industry, already familiar with the latest iteration of the North American Electric Reliability Corp. (NERC) Critical Infrastructure Protection (CIP) reliability standards, should take note: Meeting those standards may not be enough to satisfy evolving cybersecurity threats and the need to protect cyber assets as well as personal data. As cyber crime continues to make headlines, the energy industry may turn to the first version of the National Institute for Standards and Technologies (NIST) Framework for Improving Critical Infrastructure Cybersecurity, in addition to sector specific standards, to mitigate cybersecurity risks to critical infrastructure. Plaintiffs' attorneys and government enforcement agencies may, in turn, use the framework as a possible de facto legal standard of care for cybersecurity—even for entities already subject to the NERC standards or the Department of Energy's Electricity Subsector Cybersecurity Risk Management Process. In addition to operational cybersecurity and risk management, the framework also highlights the need to evaluate and manage risks to the security of personal data.

Criminals and terrorists are constantly scanning systems looking for back doors or unmonitored assets. Seeking to shore up the defense of critical infrastructure, in early 2013, President Obama directed NIST to create the cybersecurity framework. In doing so, the administration identified energy systems as "uniquely critical" infrastructure that enables all other critical infrastructure systems to function. The president's designation of energy systems as "uniquely critical" infrastructure did not recognize any distinction between bulk power system facilities, already subject to NERC oversight and CIP standards for cybersecurity, and other energy facilities that have no such oversight or mandatory standards for cybersecurity. Indeed, NERC's submission in the NIST process developing the framework recognized both the lack of an end-to-end cybersecurity protocol for the energy industry and the "siloed" approach across industries that has resulted in variable guidelines, standards, and regulations. The framework, according to NIST's introduction, provides a "common language to address and manage cybersecurity risk," while allowing organizations flexibility in how they implement the practices.

The framework is not intended to supplant CIP standards, which are focused on the impact on the bulk power system. The detailed framework provides three sets of risk evaluation and management tools that can be more broadly applied to cyber assets and personal data. One tool provides a high-level strategic view of an organization's existing and target activities for addressing risks. Another allows an organization to grade its current level of risk and examine the cost-effectiveness of risk reduction in light of business objectives. The third tool helps define strategic areas for improvement, taking into account specific risks, and the costs of mitigation measures.

Unlike NERC, NIST has no enforcement authority. The framework is voluntary. However, as the administration's efforts to identify and implement incentives to promote adoption of the framework have stalled, Congress could step in to mandate compliance. Several pending bills would give the Department of Homeland Security (DHS) expanded authority over the cyber-readiness of critical infrastructure and other private entities. Another bill would impose certain limits on liability and provide important defenses to utilities that use DHS-approved cyber-defense technology. Although each bill currently would maintain the voluntary nature of the framework, the legislative process leaves plenty of room to add mandates.

The NIST framework is not limited to the security of critical assets—it also includes standards for organizations to address the privacy and civil liberties of consumers. These standards cover functions such as taking inventory of personal data; privacy training; transparency; notice to individuals whose personal information is collected, used, and maintained; and data minimization practices. These provisions of the framework highlight the need for power companies to have not only robust cyber defenses, but also appropriate policies and standards to protect personal data, such as customer power usage data collected via the smart grid, from cyber theft and other inappropriate use or disclosure.

Every energy company collects and maintains a substantial amount of personal information from employees, including the background check information sometimes required by the NERC CIP standards themselves. Companies with retail customers collect names, addresses, email addresses, phone numbers and financial information, including credit card data. Various standards exist for the collection, use, sharing, protection, and destruction of all of that data. For example, the stringent PCI Data Security Standards govern the protection of credit card data. Recent California laws and regulations limit disclosure to third parties of any specific consumer's energy consumption data. And the Federal Trade Commission has demonstrated through at least 50 settlements of data security practices that it will apply its Section 5 enforcement authority to any company that it believes failed to adhere to "reasonable" standards for data protection, regardless of whether another federal agency ostensibly has primary jurisdiction.

In this environment, compliance with NERC cybersecurity standards may not suffice to protect energy companies from the myriad risks presented by cyber crime and other data breach incidents. Companies must affirmatively consider specific risks to their business assets and consumer data, define their tolerance for those risks, and build or improve risk-based programs to address areas for improvement that are cost-effective in light of the risks. Energy companies that systematically consider cybersecurity and the protection of personal data in this way will responsibly manage their risks, protect their organizational reputations, and prepare for increased government scrutiny. ■

*—**Margaret H. Claybour** is a senior associate in Davis Wright Tremaine's Energy practice group. **Robert G. Scott, Jr.** is a partner with Davis Wright Tremaine's Communications practice. Both work out of the firm's Washington, D.C., office.*