ALERT
FEBRUARY 20, 2013

Energy, Environmental and Utilities Group
News Concerning
Recent Developments in Energy and Environmental Law

COZEN O'CONNOR

Utilities Sector To Be a Focus of Executive Order Directing Development of Critical Infrastructure Cybersecurity Framework

Michael Klein • 202.912.4822 • *mklein@cozen.com*
Ahren Scott Tryon • 202.912.4827 • *atryon@cozen.com*
Joshua L. Belcher • 202.912.4826 • *jbelcher@cozen.com*

Little more than a week after reports of cyber attacks targeted at the Department of Energy, *The New York Times* and *The Wall Street Journal*, President Obama declared in his State of the Union address that these forms of attacks on the nation's critical infrastructure are rapidly growing and present "real threats to our security and our economy." Analyses from the Department of Homeland Security (DHS) underscore the administration's growing unease with the vulnerability of critical infrastructure networks. Reported cyber attacks on utility sector control systems rose more than 50 percent in 2012, with the energy and water sectors representing the greatest number of reported attacks among industrial control system networks.[1] With an upward trend in cyber attacks across critical infrastructure sectors, both government-owned and private sector utilities have anticipated the President's announcement that his administration will spearhead new defensive efforts through an Executive Order titled "Improving Critical Infrastructure Cybersecurity" (the EO).

Through the EO, signed on February 12, 2013, the President called on the executive branch to take immediate action to better communicate potential cyber threats to the private sector through increased information sharing and to develop a flexible framework for identifying and reducing the risk of cyber attacks on critical U.S. infrastructure. The administration plans to move rapidly, having already released a draft summary of a Request for Information that is to be published in the Federal Register,[2] and has started to develop workshops with the goal of getting a draft voluntary framework together in well under a year.

The EO directs DHS and the Department of Commerce's National Institute of Standards and Technology (NIST) to take the lead in developing key aspects of the initiative, but requires extensive coordination with other government agencies and the private sector. Although the private sector's involvement is voluntary, the administration has made clear in subsequent briefings that industry involvement will be the crucial component in the development of the cybersecurity framework. Utilities sector participation will be particularly important due to the unique threats faced by utilities, which not only have to deal with the threats and liabilities associated with thefts of customer data but also with an ever-expanding list of potential vulnerabilities in supervisory control and data acquisition (SCADA) system legacy hardware and software.

Cybersecurity Information Sharing

With respect to information sharing, the EO directs the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence to take coordinated action to ensure that reports on cyber threats can be rapidly disseminated to U.S. private sector entities. Unclassified reports of cyber threats would be provided to specifically targeted entities; more detailed reports, to include classified information, would be made available to certain "critical infrastructure entities."

[1] See the Department of Homeland Security's "ICS-CERT Monitor Alert" for October/November/December 2012, available at http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf.

[2] The draft summary of the Request For Information is available at http://www.nist.gov/itl/upload/rfi_02_12_13.pdf.

To further enhance information sharing, DHS and the Department of Defense are required to expand the Defense Industrial Base (DIB) Enhanced Cybersecurity Services program, an existing voluntary information sharing program providing classified cyber threat and technical information to DIB sector companies and service providers. This program would be opened to all the commercial critical infrastructure sectors (e.g., communications, transportation, power and other utilities).

Identification of High Priority Critical Infrastructure

Under the EO, "critical infrastructure" is defined to include those systems and assets, whether physical or virtual, the incapacity or destruction of which would have a debilitating impact on security, national economic security, and/or national public health or safety. However, the order requires DHS to specifically identify high risk infrastructure requiring special consideration. Where a cybersecurity incident to critical infrastructure could reasonably result in *catastrophic* regional or national effects on public health or safety, economic security, or national security, the owners and operators of that infrastructure will be confidentially notified of that determination. Security clearance processing for these entities will be prioritized and they will receive particular attention in the development and implementation of the cybersecurity framework, discussed below. Energy and water utilities traditionally are included within the realm of critical infrastructure and certain of these utility systems should be expected to fall into the "high risk" category. Utilities should assess whether they have personnel with existing clearances or may need to obtain a clearance to ensure access to priority classified information.

Cybersecurity Framework

The most significant aspect of the EO is the development of a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework), to be led by NIST. As explained in the EO and the administration's subsequent briefings, the initial phase of this effort will be to establish performance goals in the face of a hypothetical threat. Later phases will include crafting sector-specific baseline standards, methodologies, procedures and processes necessary to meet those goals. The framework that emerges from these efforts is to be "technology neutral," allowing for a competitive market in products and services and giving companies flexibility in the design and implementation of cybersecurity strategies. For utilities, an effective framework will need to do more than focus on SCADA software vulnerabilities, but will have to lead to thoughtful consideration of potential threats from both internal and external exploits of software, operating systems, legacy hardware and other physical assets unique to each utility.

Under the EO, the framework must incorporate voluntary consensus standards and industry best practices to the fullest extent possible. DHS is required to engage a broad coalition of interests, including critical infrastructure owners and operators and the sector-specific government agencies that already have been coordinating with their assigned sectors on various security issues (i.e., Department of Energy for the energy sector; Environmental Protection Agency for the water sector). A significant portion of the Cybersecurity Framework development is expected to be achieved at the sector-specific agency level. The director for NIST has emphasized that industry is expected to become heavily involved in the process and to take ownership of the Cybersecurity Framework development.

Next Steps

The EO sets forth a highly ambitious timeframe for implementation, requiring several agencies take action within the next three to five months to assess current cybersecurity programs and the scope of their relative implementation authority and to begin to open the channels of communication required to increase transparency on the identification and assessment of cyber threats.

In only 240 days, DHS is required to publish a preliminary version of the Cybersecurity Framework, to be finalized within a year. While optimistically ambitious, this abbreviated timeframe calls into question the feasibility of reaching the level of consensus required to construct a draft voluntary Cybersecurity Framework under the EO, especially in an environment in which the current responses of critical infrastructure owners and operators to potential cybersecurity threats are so varied. Nonetheless, early participants in the process may be the best situated to receive incentives for implementing cybersecurity measures, as the EO directs agencies to work on identifying potential incentives to encourage adoption of the Cybersecurity Framework. Notably, the EO also directs agencies to assess their regulatory authority to implement cybersecurity requirements, so regulated entities should consider the significance that their input on a voluntary framework may have on future efforts to mandate cybersecurity measures. While the administration is working within its executive branch powers to reach a voluntary framework, multiple officials at the administration's briefing on the EO noted the EO was but a "down payment" on future legislation.

In the near future, NIST will formally issue its Request For Information in the Federal Register, soliciting input from stakeholders and the public. NIST is expected to hold workshops beginning in April. Significant and diverse participation of water, gas and electric utilities (both privately and publicly owned) and pipeline operators will be a necessity for the process to achieve a meaningful and effective "technology neutral" framework that is workable across the utilities sector.

As noted above, each utility employs a combination of physical assets, SCADA and other hardware and software culminating in a set of strengths and vulnerabilities that is specific to that utility. Utilities with a presence across multiple states will want to ensure that standards under the framework allow for company-wide adoption and are consistent with the requirements of multiple regulators (including those of state public utility commissions with existing cybersecurity program mandates). Further, utilities operated by governments and authorities may have unique operational, budgetary and regulatory considerations that affect their assessment and implementation of cybersecurity initiatives. Thus, individual utilities should at a minimum monitor the process and participate where necessary to ensure the framework, which may inform later regulatory or legislative efforts, adequately accounts for their needs and allows for the development of effective cybersecurity strategies for their unique systems. Moreover, participating at an early stage in the development of the draft Cybersecurity Framework may help utilities ensure awareness of best practices that in turn can combat susceptibility to cyber attacks, reduce potential civil or regulatory liability, and increase insurability.

To discuss any questions you may have regarding this Alert, or how it may apply to your particular circumstances, please contact a member of Cozen O'Connor's Energy, Environmental & Public Utilities Practice.

Comments in the Cozen O'Connor Alert are not intended to provide legal advice. The analysis, conclusions, and/or views expressed herein do not necessarily represent the position of the law firm of Cozen O'Connor or any of its employees, or the opinion of any current or former client of Cozen O'Connor. Readers should not act or rely on information in the Alert without seeking specific legal advice from Cozen O'Connor on matters which concern them.