SUTHERLAND

LEGAL ALERT

February 13, 2013

New Regulation Under Cybersecurity Executive Order

President Obama yesterday issued an Executive Order to address the growing cyber threat to the Nation's "critical infrastructure," a term broadly defined to potentially cover natural gas and oil pipelines, storage sites and refineries as well as electric generation, transmission and distribution facilities. The Executive Order has been widely rumored for months, particularly given the congressional impasse on cybersecurity legislation and numerous reports of cyber attacks of varying severity affecting public and private enterprises nationwide. Citing "national and economic security," the executive branch finally took matters into its own hands with the Executive Order. The energy industry should pay attention, both for regulatory compliance purposes and also as a matter of sound business practice, in the face of the increasing security threat posed by cyber attacks.

The Executive Order

The Executive Order applies to "critical infrastructure," defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." This expansive and vague definition could include a range of natural gas, oil, and power systems and assets.

Developed by national security officials in conjunction with the Department of Homeland Security (DHS) and other federal agencies, the Executive Order:

- Promotes the sharing of "cyber threat information" with private sector entities, and directs DHS, the Attorney General and the Director of National Intelligence to adopt procedures for the "timely" and "rapid" dissemination of unclassified cyber threat reports to the entities specifically targeted by those threats;

- Expands the Enhanced Cybersecurity Services program to provide for the sharing of classified cyber threat and technical information with eligible critical infrastructure companies and commercial service providers offering critical infrastructure security services;

- Directs federal agencies to ensure that privacy and civil liberties protections are incorporated into activities outlined in the Executive Order;

- Requires DHS to establish a "consultative process" to coordinate improvements to critical infrastructure cybersecurity, including seeking the advice of other federal agencies as well as owners and operators of critical infrastructure;

- Directs the National Institute of Standards and Technology (NIST) to coordinate with other federal agencies and owners and operators of critical infrastructure to develop a "prioritized, flexible, repeatable, performance-based, and cost-effective" "Cybersecurity Framework" to identify, assess and reduce cyber risks to critical infrastructure, including the use of "voluntary consensus standards and industry best practices," technology-neutral guidance on commercial products and services that address cyber risks, the development of performance goals for the Framework, and guidance for measuring entities' performance in implementing the Framework;

- Directs DHS to establish a "voluntary program" for owners and operators of critical infrastructure to adopt the Framework and incentivize them to participate in the program;

- Requires DHS to use a "risk-based approach" and "consistent, objective criteria" to identify critical infrastructure where "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security," annually update the list of such infrastructure, and confidentially notify owners and operators of such identified critical infrastructure;

- Directs federal agencies with existing cybersecurity regulatory authority to adopt "prioritized, risk-based, efficient, and coordinated" actions addressing cyber risks to critical infrastructure, consistent with the Framework and subject to each agency's regulatory authority, and to identify "ineffective, conflicting, or excessively burdensome" cybersecurity requirements applicable to critical infrastructure; and

- Encourages independent federal agencies, such as the Federal Energy Regulatory Commission (FERC), to work with DHS through the consultative process to prioritize cybersecurity regulatory actions to mitigate cyber risks to critical infrastructure, consistent with each agency's existing authority.

The Executive Order does not grant any liability protections to industry participants for sharing cyber threat or vulnerability information, nor does it otherwise address the liability of program participants.

In addition to the Executive Order, the White House also issued a Presidential Policy Directive (PPD-21) that establishes a national policy on critical infrastructure security focused on (i) improving collaboration among federal agencies, (ii) improving information exchange among agencies, and (iii) improving risk management, mitigation and restoration efforts. The directive relies on DHS to lead the initiative with input from sector-specific agencies, such as the Department of Energy, as well as "partnerships" with owners and operators of critical infrastructure and state and local governments. Importantly, the energy industry is identified as "uniquely critical."

What This Means for the Energy Industry

Portions of the Executive Order may come as welcome news to the energy industry. For example, the Executive Order seeks to expand the sharing of cyber threat information with the private sector. This information sharing should help energy companies identify, respond to and mitigate cyber risks.

But at the same time, the Executive Order raises several areas of potential concern for energy industry participants:

- Expanded scope of facilities subject to federal oversight. The Executive Order broadly defines the term "critical infrastructure" to cover facilities that could have a "debilitating impact on national security, the economy, or public health or safety." This language may include facilities not traditionally regulated at the federal level, such as intrastate pipelines and electric distribution facilities. Owners and operators of facilities at all levels should consider whether their assets may be identified as critical infrastructure under the Executive Order.

- Ambiguity in status of IT products and services. The Executive Order directs DHS to exclude commercially available information technology (IT) products and services from the scope of critical infrastructure at greatest risk. But it is not clear if such products and services themselves nonetheless may constitute critical infrastructure otherwise subject to the Executive Order.

- Risk of expanded federal regulatory oversight. DHS will identify high risk critical infrastructure and confidentially notify owners and operators of the identified critical infrastructure. Beyond receiving this notification, it is unclear to what extent these owners and operators will need to comply with "voluntary" guidelines developed through the Executive Order's consultative processes.

- Potential for duplicative or inconsistent regulation. The Executive Order aims to increase collaboration among federal agencies and the private sector, but collaboration does not necessarily result in consistency. And while the Executive Order directs agencies to identify "ineffective, conflicting, or excessively burdensome" cybersecurity requirements, agencies have two years to identify such requirements and are directed only to make *recommendations* for further actions to minimize or eliminate such requirements. There is no guarantee those recommendations will be enacted, and in the meantime, regulated companies may face unduly burdensome and confusing requirements, potentially from multiple agencies.

- Unfamiliar agency in charge. DHS, the lead federal agency under the Executive Order, as well as the NIST, may be unfamiliar to many in the energy industry. The new rulemakings, processes and procedures prescribed by the Executive Order will require regulated companies to invest time and resources to bring their legal and compliance departments up to speed on these agencies.

- No liability protection. A major stumbling block to cybersecurity legislation has been the absence of liability protection for those who voluntarily share cyber threat and vulnerability information. Similarly, the Executive Order does not provide any liability protection for those who participate in the information sharing and other programs authorized by the Executive Order, such as the Framework. In the absence of additional legislative authority, the President cannot issue directives providing such protection. But the lack of protection may prove problematic and may discourage program participation.

In sum, the Executive Order is likely to result in a host of new cybersecurity regulations applicable to critical infrastructure, including natural gas and oil pipelines, storage and other facilities. The electricity sector also may see an expansion of cybersecurity regulation of electric generation, transmission and distribution facilities. Although Congress has not enacted any new legislation in this area, the Executive Order still carries the force of law. Energy industry participants should engage in and monitor the expected new rulemakings and other processes outlined in the Executive Order.

■ ■ ■

If you have any questions about this Legal Alert, 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
Paul F. Forshay	202.383.0708	paul.forshay@sutherland.com
David L. Wochner	202.383.0381	david.wochner@sutherland.com
Alison C. Graab	202.383.0861	alison.graab@sutherland.com
Meghan R. Gruebner	202.383.0933	meghan.gruebner@sutherland.com
Jennifer J.K. Herbert	202.383.0822	jj.herbert@sutherland.com
Alexandra D. Konieczny	212.389.5072	alexandra.konieczny@sutherland.com
Sandra E. Safro	202.383.0246	sandra.safro@sutherland.com
Mark Thibodeaux	713.470.6104	mark.thibodeaux@sutherland.com