SUTHERLAND

# LEGAL ALERT

September 21, 2012

## FERC Launches New Cybersecurity Office

The Federal Energy Regulatory Commission (FERC) is creating a new office to address cyber and physical security risks to FERC-jurisdictional facilities, such as electric generation and transmission facilities, oil and gas pipelines, and LNG terminals. The new Office of Energy Infrastructure Security (OEIS) will rely on FERC's existing statutory authority in providing "leadership, expertise and assistance" to identify and mitigate such risks. While electric utilities will be familiar with FERC's efforts to address cybersecurity risks, such oversight will be new to companies in the oil and gas sectors.

### The Office of Energy Infrastructure Security

According to a FERC press release, OEIS will focus on "identifying, communicating and mitigating potential cyber and physical security threats and vulnerabilities to FERC-jurisdictional facilities." OEIS's activities will include:

- Developing "recommendations";
- Providing "assistance, expertise and advice" to regulated entities, Congress and other federal and state agencies;
- Participating in conferences, workshops, classified briefings, and other "interagency and intelligence-related coordination and collaboration efforts" with government agencies and industry; and
- Conducting "outreach" with the private sector.

FERC-jurisdictional facilities include electric generation and transmission facilities that are owned or operated by electric utilities and regional transmission organizations (RTOs), hydroelectric facilities, interstate oil and gas pipelines, gas storage facilities, and import/export terminals for liquefied natural gas (LNG). Users, owners and operators of the "bulk power system" are already subject to FERC oversight through FERC's authority over the electric reliability standards developed and enforced by the North American Electric Reliability Corporation (NERC), including critical infrastructure protection (CIP) requirements.

FERC tapped the director of FERC's existing Office of Electric Reliability (OER) to head the new OEIS. With an electricity-minded individual at the helm, OEIS may, at least in its infancy, look to OER efforts in the electricity space as guiding principles in developing oversight in the oil and gas sectors as well as expanding oversight in the electricity sector.

### What This Means For You

Companies in the electric utility sector likely will find themselves on familiar turf with the new office because they are already subject to FERC oversight through the CIP reliability standards. Companies in the oil, gas and LNG sectors, however, likely will be subject to new oversight, expanding beyond FERC's previously limited Critical Energy Infrastructure Information (CEII) designation requirements. Although OEIS's functions appear to be limited to developing recommendations for industry (as opposed to requirements), all sectors subject to the new office's oversight should remain vigilant to guard against the development of new requirements, at least in the absence of new legislation conferring additional statutory authority on FERC.

FERC's creation of OEIS is significant for two other reasons. First, FERC's action is consistent with the draft executive order reportedly being developed by the White House on the coordination of efforts to protect critical infrastructure against cyber threats. The draft executive order would direct federal agencies like FERC to adopt measures to coordinate with their regulated industries to identify and mitigate cybersecurity risks. FERC's establishment of OEIS would thus seem to implement aspects of the draft executive order, even though it has not yet been issued.

Second, FERC officials have urged Congress to grant FERC expanded authority to address cyber threats. The FERC officials have asserted that FERC lacks the authority that it deems necessary to effectively combat cybersecurity threats to critical infrastructure. FERC's creation of the new OEIS is a step FERC can take within its "existing statutory authority" while continuing to make its case that it needs additional authority.

In sum, the new OEIS holds the promise of bringing effective coordination to public-private efforts to combat cyber threats to critical infrastructure. But it also may represent an expansion of agency action for which there is inadequate legislative authorization. The energy industry should approach the new OEIS with guarded optimism.

■ ■ ■

*If you have any questions about this Legal Alert, please feel free to contact any of 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 |
| Meghan R. Gruebner | 202.383.0933 | meghan.gruebner@sutherland.com |
| Alexandra D. Konieczny | 212.389.5072 | alexandra.konieczny@sutherland.com |
| Jennifer J. Kubicek | 202.383.0822 | jj.kubicek@sutherland.com |
| Sandra E. Safro | 202.383.0246 | sandra.safro@sutherland.com |
| Mark Thibodeaux | 713.470.6104 | mark.thibodeaux@sutherland.com |
| David L. Wochner | 202.383.0381 | david.wochner@sutherland.com |