Morgan Lewis

alert

energy lawflash

September 21, 2012

FERC Forms New Office to Focus on Cybersecurity

In the absence of new federal cybersecurity legislation, FERC uses its available authority in an effort to increase the resilience of the nation's critical electric infrastructure to cyber attacks.

On September 20, the Federal Energy Regulatory Commission (FERC or the Commission) announced the creation of a new office, the Office of Energy Infrastructure Security (OEIS), which will focus on physical and cyber risks to energy facilities subject to FERC jurisdiction.[1] Headed by the current director of the Office of Electric Reliability, Joseph McClelland, OEIS will assist the Commission in identifying security risks, communicating those risks to other federal and state agencies and regulated utilities, and developing solutions to mitigate those risks. Consistent with the existing approach taken by the Obama administration in the absence of new legislation, FERC's action draws on its existing statutory authority in an effort to increase the cyber resilience of critical infrastructure.

According to FERC Chairman Jon Wellinghoff, OEIS will concentrate on the following four areas:[2]

1. Developing recommendations to mitigate security risks to FERC-jurisdictional facilities
2. Advising Congress, other agencies, and utilities regarding these risks
3. Participating in intelligence-related collaborative efforts to address these risks alongside other agencies and utilities
4. Conducting outreach to address these threats with private-sector owners and operators of critical infrastructure

OEIS represents the Commission's response to the increased visibility of security risks to key infrastructure, including cyber attacks and electromagnetic pulse events, and is intended to provide for a more rapid and effective response to these risks by the Commission. Chairman Wellinghoff stressed that OEIS's activities will complement, not replace, the existing work performed by the Office of Electric Reliability and the North American Electric Reliability Corporation (NERC) in overseeing the enforcement and development of Reliability Standards, including Critical Infrastructure Protection (CIP) Reliability Standards.

The creation of OEIS reflects the growing focus at the federal level on the need for greater cybersecurity protections for critical infrastructure and an interest in taking any available steps in the absence of new legislation. Despite recent efforts, Congress was ultimately unable to reach a consensus on cybersecurity legislation. As a result, while efforts on comprehensive cybersecurity reform legislation are likely to continue, the Obama administration is drafting an executive order on cybersecurity. This policy is highlighted in the recently approved Democratic National Platform, which states that "going forward, the President will continue to take executive action to strengthen and update our cyber defenses."

The executive order, which is reportedly close to completion, will rely on existing federal authority to increase cyber protections for key infrastructure, including the bulk electric system, and will create a program of voluntary

1. View the FERC Press Release at http://ferc.gov/media/news-releases/2012/2012-3/09-20-12.asp.
2. View Chairman Wellinghoff's statement at http://ferc.gov/media/statements-speeches/wellinghoff/2012/09-20-12-wellinghoff.asp.

security standards developed at least partly by the federal government. The executive order is expected to create a cybersecurity council, led by the Department of Homeland Security (DHS), to determine which federal agencies should be responsible for the various critical infrastructure categories and to establish the voluntary cybersecurity standards companies will be encouraged to follow. According to reports, DHS would identify the various owners and operators of critical infrastructure who would be asked to follow the voluntary standards. The executive order is likely to direct the council to identify incentives for compliance with these voluntary standards, including liability protections, faster security clearances, and federal recognition that a company meets the voluntary standards. The draft executive order may also require the development of a process for identifying and mitigating cybersecurity risks, although it may not identify or recommend a specific approach.

Contacts

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

Washington, D.C.

John McGrane	202.739.5621	jmcgrane@morganlewis.com
Stephen M. Spina	202.739.5958	sspina@morganlewis.com
J. Daniel Skees	202.739.5834	dskees@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 24 offices across the United States, Europe, and Asia, Morgan Lewis provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. Our international team of lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—more than 1,600 legal professionals total—serves clients from locations in Almaty, Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Moscow, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.