How new cybersecurity rules bedevil electric industry

By Joel deJesus
USA Today
July 18, 2013

(Editor's note: In this guest post, Joel deJesus, a partner at the law firm Schiff Hardin, outlines how new security rules breed uncertainty for the electric industry.)

Cybersecurity is currently at the forefront of the electric industry's collective mind. The problem is that the rules of the road seem to be constantly changing.

Now as the National Institute of Standards and Technology (NIST) is contemplating a new cybersecurity framework for all critical infrastructure industries, including the electric industry, the question remains for the electric industry: how is this supposed to work?

Cybersecurity in the electric industry has been regulated by the North American Electric Reliability Corporation for a long time. NERC administers what's known as the Critical Infrastructure Protection (CIP) Reliability Standards. CIP requires implementation of specific cybersecurity protections, and subject industry to penalties for noncompliance.

The first mandatory CIP standards were proposed in 2006, and FERC is now considering Version 5. Moreover, apart from the formal standards revisions, NERC's reading and application of the CIP standards has evolved in the past several years. Audit findings from three years ago are now being revisited in recent audits.

Regulators are also trying out new ways of preserving cybersecurity. NERC and FERC -- the Federal Energy Regulatory Commission -- are supplementing their role as enforcement agencies and taking on more voluntary outreach activities, including the sharing of cyberthreat information.

It may be hard for NERC and FERC to marry their roles as enforcers of CIP standards and as partners with industry in information sharing.

Executive Order 13636 appears to be a blend of the standard setting and information sharing approaches, requiring NIST to develop a "cybersecurity framework" for all critical infrastructure industries.

Although framework would be voluntary, the Executive Order calls on federal agencies to adopt incentives for industry compliance. The nature of these incentives and how the NIST framework will interact with the existing NERC CIP standards remains to be seen.
The Executive Order also embraces the voluntary information sharing concept by enlisting private sector experts into Federal service as cybersecurity advisors, and by directing federal agencies to produce unclassified cybersecurity reports in a timelier manner.

Change may be an inherent part of the cybersecurity landscape, but as regulators attempt to improve cybersecurity standards and to take new approaches to safeguarding cybersecurity, they should consider the pace of such changes and the industry’s need for certainty to make necessary investments in critical infrastructure and critical infrastructure protection.

Reproduced with Permission of USA Today.

© 2013 Schiff Hardin LLP
This publication has been prepared for the general information of clients and friends of the firm. It is not intended to provide legal advice with respect to any specific matter. Under rules applicable to the professional conduct of attorneys in various jurisdictions, it may be considered attorney advertising material. Prior results do not guarantee a similar outcome.

For more information visit our Web site at www.schiffhardin.com.