THE
NATIONAL LAW REVIEW

FERC to NERC: Develop Cyber Control Supply Chain Risk Management Standard By J. Daniel Skees and Serge Agbre

Morgan Lewis

Article By
J. Daniel Skees
Serge Agbre
Morgan, Lewis & Bockius LLP
Power & Pipes

- Environmental, Energy & Resources
- All Federal

Friday, July 29, 2016

On July 21, FERC directed NERC to develop a new or modified "forward-looking, objective-driven" Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services ("cyber controls") associated with BES operations. FERC required the standard to address

- software integrity and authenticity;
- vendor remote access;
- information system planning; and
- vendor risk management and procurement controls.

FERC is concerned that a "gap" exists in the CIP Reliability Standards, which has been highlighted by recent events where malware campaigns have targeted supply chain vendors in BES cyber control systems.

FERC expressed concern that vulnerable systems may be attacked either through hardware or software components of a cyber-control system or a third-party service provider may be attacked who has access to sensitive IT infrastructure or that holds or maintains sensitive data.