Legal & Regulatory Conference

IN PARTNERSHIP WITH

GRIDLIANCE

MANAGING SUPPLY CHAIN CYBER RISK
BEST PRACTICES FOR SMALL ENTITIES

Cindy Bogorad
Latif Nurani

APPA Legal & Regulatory Conference

October 9, 2018

cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

SPIEGEL & MCDIARMID

Cyber Threats Are Real

- “The warning lights are blinking red again. Today, the digital infrastructure that serves this country is literally under attack.”
  - Dan Coats (Director of National Intelligence), July 13, 2018
- Russian attempts to compromise industrial control systems
- Connecticut September 2018 report finds utilities “faced a larger number and greater sophistication of penetration attempts” during past year

Supply Chain Cyber Risks

- Supply chains for industrial control systems hardware, software, and operational support have become global
- Global supply chain creates opportunities for adversaries to directly or indirectly compromise grid reliability
  - E.g., injection of malware into a product prior to delivery to customer – not a hypothetical risk!

Supply Chain Reliability Standard

- July 2016: FERC directs NERC to develop a supply chain cyber risk management standard
- August 2017: NERC BOT approves standard, requests studies and industry input
- January 2018: FERC proposes to approve NERC's proposed standards, with directives

NERC Board August 2017 Resolution

- NERC, in collaboration with industry, to further study supply chain risks, including low impact assets
- Request NATF/NAGF to develop white papers on best and leading supply chain management practices
- Request APPA/NRECA to develop similar white papers, focusing on smaller entities

Context: Scope of CIP Standards

- NERC Critical Infrastructure Protection (CIP) standards protect BES Cyber Systems and associated cyber assets
- BES Cyber Systems: Programmable devices that, if compromised, would adversely impact reliable operation of the BES within 15 minutes

Context: Associated Cyber Assets Protect BES Cyber Systems

- PACS: Physical access control system (e.g., keycard)
- EACMS: Electronic access control or monitoring systems (e.g., firewalls)
- PCA: Protected Cyber Asset not part of the BES Cyber System but connected within the Electronic Security Perimeter

Context: NERC's Risk-Based Approach

Starting with CIPv5, BES Cyber Systems are classified into low, medium, and high impact

High Impact	Medium Impact	Low Impact
E.g.: • BA Control Centers	E.g.: • Generator > 1500 MW • Transmission > 500 kV	• BES Cyber Systems not high or medium • More diverse set of systems

Context: NERC's Risk-Based Approach

Lower Impact

Higher Impact

More Flexibility

More Rigorous Requirements

Context: CIP-003 for Low Impact

- Implemented documented cyber security plan:
  - Cyber Security Awareness
  - Physical Security Controls *
  - Electronic Access Controls *
  - Incident Response
  - Transient Devices *

* New requirements enforceable in 2020

Proposed Supply Chain Standard Does Not Apply to Low Impact

- Applies only to medium and high impact
- NERC Board's resolution anticipated questions about low impact
- FERC NOPR proposes not to expand scope to low impact, pending requested studies

OVERVIEW OF APPA/NRECA WHITE PAPER

SPIEGEL & MCDIARMID

APPA/NRECA White Paper

- Submitted to NERC Board and FERC in April 2018
- Identifies supply chain cyber risk management practices for small registered entities with low-impact BES Cyber Systems
- Shows what some small entities are already doing; intended as useful resource of practical steps that others can take

APPA/NRECA Survey of Best Practices

- Retained U.S. Resilience Project to interview nine APPA/NRECA members
- Sampled companies ranged in size and types of assets—including larger members that will be subject to the Supply Chain Standards
- Mix of Munis, JAAs, Distribution Coops, G&Ts

High-Level Findings

- High awareness of supply chain cyber risks
- Smaller registered entities can—and do—implement several supply chain management practices, commensurate with risk
- Relative magnitude of risk varied from entity to entity, based on impact to BES and to entity's own operations

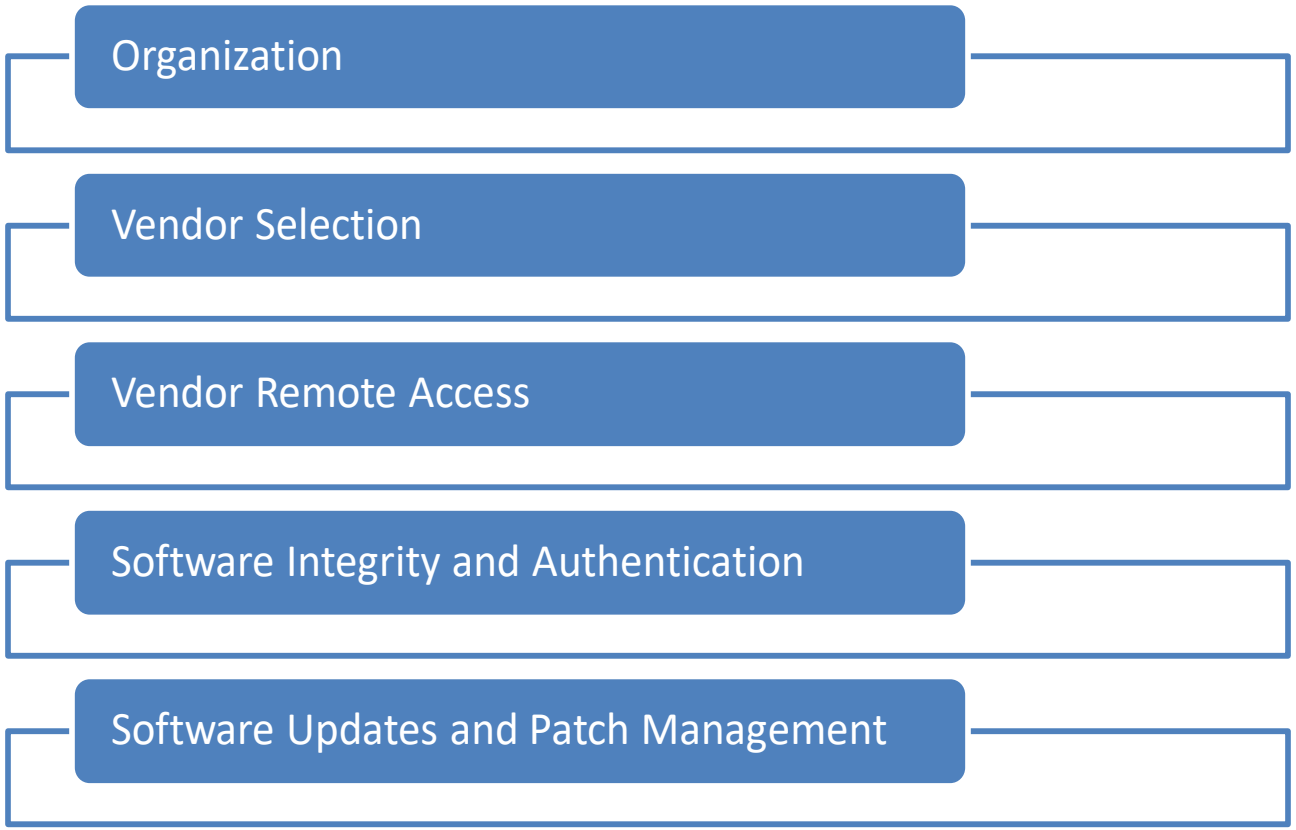
Supply Chain Cyber Risks for Small Entities

- Products infected with malicious code while still within vendor control
- Products infected during maintenance or upgrades
- Malicious actions using credentials of vendor employees with remote access to BES Cyber Systems

CATALOG OF EFFECTIVE PRACTICES

SPIEGEL & MCDIARMID

Five Categories of Practices to Mitigate Supply Chain Cyber Risk



Organization - Leadership

- Senior management leadership is necessary, regardless of the size of an organization
- Essential role in making supply chain cyber risk mitigation a priority
- Cybersecurity—particularly supply chain—is a organizational issue, not an IT issue
- Consistent theme throughout the interviews

Organization - Coordination

- Supply chain cyber risk management is complicated by the range of personnel involved
- Improving coordination and cooperation between departments mitigates supply chain risks
- Helps address organizational blind spots due to silos

Organization – Risk Assessments

- Enterprise-wide cyber risk assessments, including supply chain, help identify the most significant threats to each individual organization
- Crucial building block for all cyber protection and priority setting (not just supply chain)

Organization – Rapid Awareness and Rapid Response

- Having processes to identify unusual system activity allows utilities to respond rapidly to cyber events, including those arising from supply chain vulnerabilities
- Need to know what “normal” looks like

Vendor Selection

- Using well-known, trusted, and established vendors
- Reducing number of vendors
- Standard questionnaires for vendors
- Standard contract language
- Potential for future third-party accreditation and vendor self-certification

Vendor Remote Access

- Limit systems that can be accessed remotely
- Limit remote access to specific service requests
- Monitor vendor remote access
- Monitor remote access points

Software Integrity and Authentication

- Risk assessments should be part of decisions to upgrade systems
- Testing new software in “sandbox” environment prior to implementation

Software Updates and Patch Management

- Patch management contracts
- Confirming patch authenticity
- Testing patches in “sandbox” environment prior to implementation

RECENT DEVELOPMENTS

SPIEGEL & MCDIARMID

EPRI Supply Chain Paper to NERC Board

- Identifies 10 “industry standards”/ vendor practices
  - Includes recommendation to consider accreditation model (cites APPA whitepaper)
- Urges further modeling and assessment of “common-mode” exploits targeting multiple low-impact BES Cyber Systems
- NERC final report due Feb 2019

To Sum Up...

- Global supply chains create new cyber risks
- FERC and NERC have already taken actions, for application to medium and high impact
- Scope of requirements may expand
- There are many practical precautions that APPA members can take to mitigate supply chain cyber risk to the their systems and the BES

QUESTIONS?

CINDY BOGORAD
LATIF NURANI
202.879.4000
cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW
Suite 700
Washington, DC 20006
www.spiegelmcd.com

SPIEGEL & MCDIARMID LLP