



**Innovation and
Regulation –
Cybersecurity and
Supply Chain Risk
Management**

Joel deJesus
Dinsmore & Shohl LLP
Washington, DC
joel.dejesus@dinsmore.com

For the ACEC Environment & Energy
Committee, Summer Meeting
August 25, 2016

“In today’s rule, FERC directed NERC to develop a forward-looking, objective-based Critical Infrastructure Protection (CIP) Reliability Standard that requires each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.”



- How did we get here?

NERC and its CIP Standards

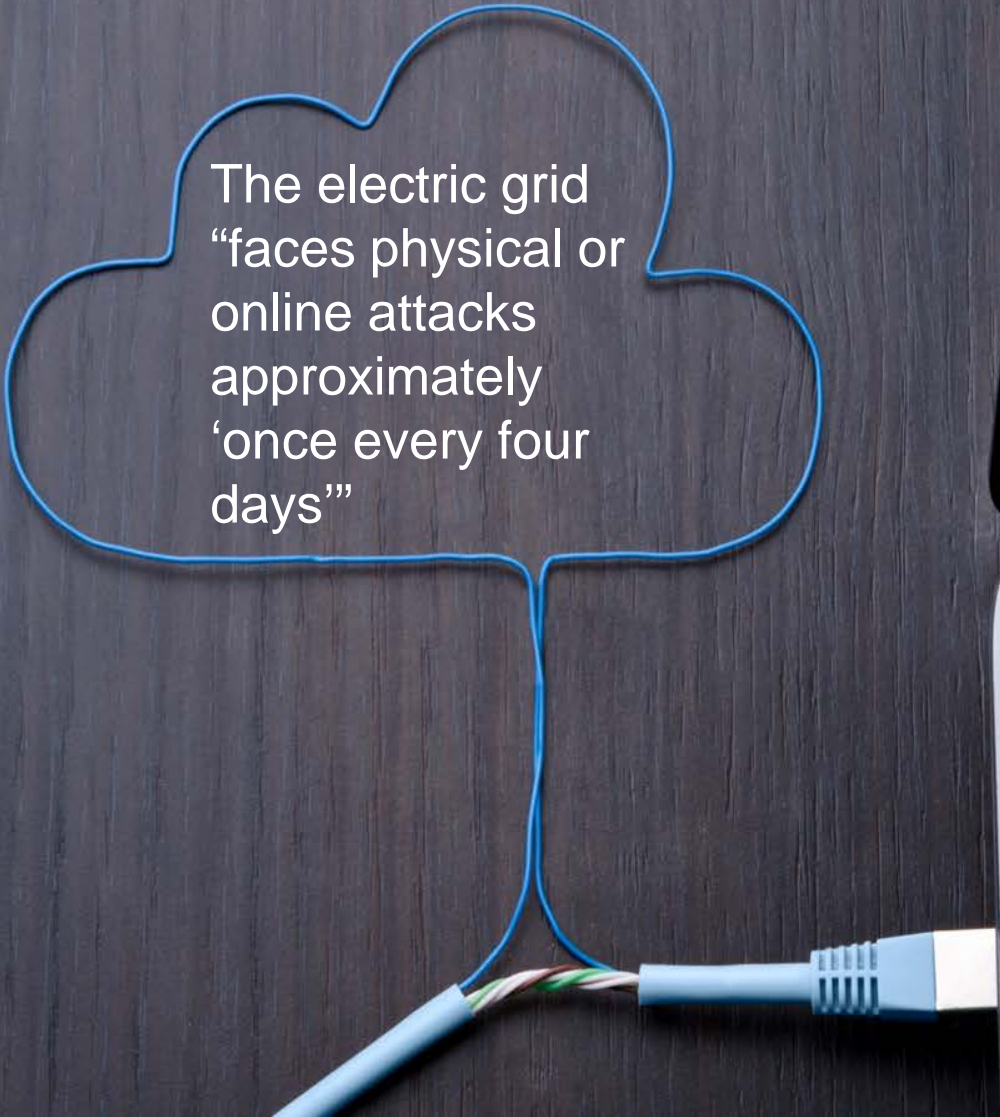
- What happened?

FERC's recent interest in Supply Chain Risk Management

- What lies ahead?

Broader implications





The electric grid
“faces physical or
online attacks
approximately
‘once every four
days’”

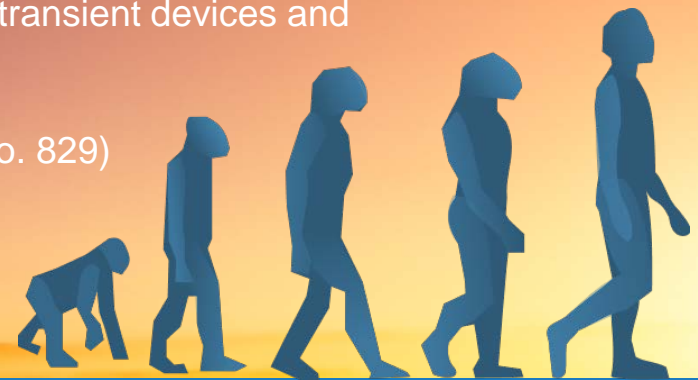
CIP Reliability Standards - Cybersecurity

- CIP-002 –Asset Identification/Categorization
- CIP-003 – Security Management Controls
- CIP-004 – Personnel & Training
- CIP-005 – Electronic Security Perimeters
- CIP-006 – Physical Security
- CIP-007 – Systems Security Management
- CIP-008 – Incident Reporting and Response Planning
- CIP-009 – Recovery Plans
- CIP-010 – Configuration Change Management
- CIP-011 - Information Protection



CIP Standards Evolution – 7 Versions in 10 years?

- 2003 – **Urgent Action 1200** – Voluntary pre-ERO cybersecurity standards
- 2008 – **Version 1** – First set of mandatory CIP standards approved (Order No. 706)
- 2009 – **Version 2** – Eliminated “reasonable business judgment” and “acceptance of risk” criteria; added rigor in critical cyber asset identification
- 2010 – **Version 3** –Addressing FERC directives to clarify standards and implementation plans
- 2012 – **Version 4** – Added “bright line” criteria for identifying critical cyber assets (Order No. 761)
- 2013 – **Version 5** – Shifted from critical cyber assets to BES Cyber Systems; added configuration change management (Order No. 791)
- 2016 – **“Revisions to Version 5”** – Eliminated “identify, assess, and correct” language; enhanced security controls for Low Impact assets; addressed transient devices and nonprogrammable components of communications networks
- 2017 – **Supply chain risk management standard?** (Order No. 829)



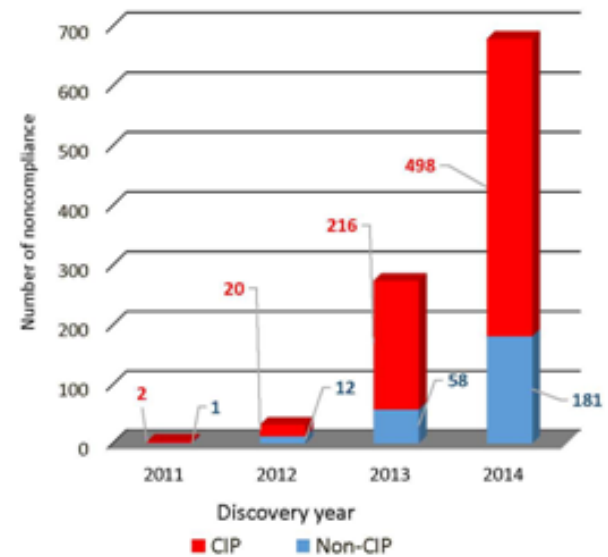
Enforcement of CIP Standards



Source: NERC Compliance Monitoring and Enforcement Program Quarterly Update, Q3 2015

Noncompliance in ERO Enterprise inventory by discovery year

* Excludes violations that are held by appeal, a regulator, or a court



Source: NERC, Key Compliance Enforcement Metrics and Trends, February 11, 2015

“Separately, we are concerned that changes in the bulk electric system cyber threat landscape, identified through recent malware campaigns targeting supply chain vendors, have highlighted a gap in the protections under the CIP Reliability Standards. These malware campaigns represent a new type of threat to the reliability of the bulk electric system where malicious code can infect the software of industrial control systems used by responsible entities.”

Revised Critical Infrastructure Protection Reliability Standards, 80 Fed. Reg. 43,354 (July 22, 2015), 152 FERC ¶ 61,054 (2015)

NOPR – Identified Risks

- Such supply chains are complex, globally distributed and interconnected systems that have geographically diverse routes and consist of multiple tiers of outsourcing.
- Supply chain risks may include the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices.



NOPR – Proposed Directive

- NERC to develop a new or modified Reliability Standard to provide security controls for supply chain management for Industrial control system hardware, software, and computing and networking services associated with bulk electric systems
- But
 - Respect section 215 jurisdiction and not directly impose obligations on vendors
 - Forward-looking and not dictate abrogation or re-negotiation of contracts with vendors
 - Set goals while allowing flexibility
 - Allow exceptions
 - Be specific enough to be enforceable – not just “have a plan”

Comments

- **NERC** – Supports FERC’s attention to supply chain management, but asks for 2 years to develop a standard to allow for stakeholder outreach and understanding existing practices for dealing with supply chain risks
- **Trade Associations** - Oppose directive for mandatory supply chain requirements because supply chain risks have not lead to any events or disturbances and the existing CIP standards already address a broad range of supply chain risks
- **ACEC Letter to Norman Bay** – Voluntary implementation of DOE procurement language has been constructive, but would be problematic if made mandatory.

Technical Conference – January 28, 2016

- FERC staff – “Supply Chain Security Efforts by Other Federal Agencies”
 - OMB, DoD, DOE, NIST, Comptroller of the Currency
- Panels on
 - Need for Reliability Standard
 - Scope and implementation of Reliability Standard
 - Existing practices and collaborative efforts.

<http://ferc.gov/EventCalendar/EventDetails.aspx?ID=8137&CalType=&CalendarID=116&Date=01/28/2016&View=Listview>

Order No. 829

- On July 21, 2016, FERC directed NERC to develop a standard within one year
- Four security objectives
 - Software integrity and authenticity
 - Vendor remote access
 - Information system planning
 - Vendor risk management and procurement controls
- Periodic assessment, taking into account guidance from NERC, DHS, etc.



Order No. 829

Most commenters opposed the directive, but...

The directive is beyond FERC's jurisdiction under FPA § 215

Registered Entities have minimal control over vendors

The Reliability Standard should only address responsible entities and not vendors

A mandatory standard will inhibit innovation

Voluntary guidelines would be more effective

A mandatory standard will inhibit needed contractual flexibility

The directive only specifies 4 objectives. NERC has flexibility in how to achieve them

Existing CIP standards are adequate

No, they are not

Order No. 829

Objective #1: Software Integrity and Authenticity

- Verify identity of software publisher
- Verify integrity of software and patches prior to installation
- Avoid “Watering Hole” Attack

Order No. 829

Objective #2: Vendor Remote Access

- Logging and controlling all third-party initiated remote access sessions
- User initiated and machine-to-machine remote access
- Theft of credentials and remote persistent connections were central to Ukraine Attack

Order No. 829

Objective #3: Information System Planning

- Include security considerations as part of IS planning
- Document role of CIP Senior Manager
- ICS-CERT
 - BlackEnergy Malware alert – “minimize network exposure for all control system devices/subsystems”
 - Ukraine incident – strategic technology refreshes

Order No. 829

Objective #4: Vendor Risk Management and Procurement Controls

- Verification of security concepts in future contracts for ICS hardware, software and computing and networking services
 - Security event notification processes
 - Personnel termination
 - Vulnerability disclosures (authentication bypass/hardcoded passwords)
 - Coordinated incident response

Project 2016-03

NERC is soliciting nominations for the standards drafting team through August 18, 2016, and will pick the team in September



Potential SDT members should have

- Significant experience with the global supply system related to communications and control hardware, software, and services
- Expertise with controls to mitigate the introduction of cybersecurity risks in the supply chain
- An understanding of the CIP Standards. Compliance, legal, regulatory, facilitation, and technical writing skills are desired.
- Previous drafting team experience or other experience with development of standards is beneficial, but not required.



Order No. 829 - What is Really Required?

Software Integrity and Authenticity	➔	CIP-007 R2 CIP-004 R3	+	Secure transmittal of patches Validate patch integrity
Vendor Remote Access	➔	CIP-005 R2	+	Machine-to-machine session logging Monitor/terminate unsafe sessions
Information System Planning	➔	CIP-010	+	Procurement controls
Vendor Risk Management & Procurement Controls	➔	Include security concepts in future contracts		

Supply Chain Risk Management

- What is Really at Stake?

ICS-ALERT-14-176-02A – ICS focused malware campaign

- Software installers were infected with Havex Trojan
- 3 known ICS vendors
- Indicators of compromise to critical infrastructure owners and operators



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Supply Chain Risk Management

- What is Really at Stake?

ICS-ALERT-14-281-01E – Ongoing malware campaign compromising ICS

- Ongoing since 2011
- Variant of BlackEnergy malware (BE3)
- Various vendors have been targeted (GE Cimplicity, Advantech/Broadwin WebAccess and Seimens WinCC)
- 2016 Update: BE3 was present in Ukraine Attack



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Supply Chain Risk Management

- What is Really at Stake?

E-ISAC, Analysis of the Cyber Attack on Ukrainian Power Grid (March 18, 2016)

- Spear Phishing/Theft of credentials
- Used VPNs from business network to enter ICS network
- “[T]he cyber attacks in Ukraine are the first publicly acknowledged incidents to result in power outages”
- Mitigation – Procurement/licensing of trusted hardware/software; network monitoring; strategic technology refresh



Beyond the Electric Industry - Water

“Utilities should develop standard design and implementation requirements that define the testing required by software vendors and system integrators, as well as doing their own testing of the integrity of results.”

- Manually initiated access
- Service Level Agreements



American Water Works Association Cybersecurity Guidance & Tool. <http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx> (implementation of NIST Cybersecurity Framework and EO 13636)

Beyond the Electric Industry – Oil and Gas Pipelines

“Establish and document standards for cyber security controls for use in evaluating systems and services for acquisition. Encourage vendors to follow software development standards for trustworthy software throughout the development lifecycle.”

“Incorporate security into cyber system design and operation, whether designing a new system or modifying an existing system. Secure design and operation of SCADA control system architecture is critical for the creation of a sustainable and reliable system.”



Transportation
Security
Administration

TSA, *Pipeline Security Guidelines* (April 2011)

<https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf>

Beyond the Electric Industry - Banks



- Exercise appropriate due diligence in selecting its service providers;
- Contract to implement appropriate measures designed to meet the objectives of the Security Guidelines
 - Protect against unauthorized access to customer information
 - Proper disposal of customer information
- Monitor service providers based on risk assessment

Federal Reserve Board, *Interagency Guidelines establishing Information Security Standards*, <https://www.federalreserve.gov/bankinfo/interagencyguidelines.htm#vii> (promulgated under Section 501(b) of Gramm-Leach-Bliley Act, 15 U.S.C. § 6801)

Beyond Electric Industry – Payment Cards

“Do not use vendor-supplied defaults for system passwords and other security parameters” PCI DSS Requirement 2

“Track and monitor all access to network resources and cardholder data” PCI DSS Requirement 10

“Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the entity’s security requirements, including PCI DSS.” PCI DSS Best Practice 6



PCI Security Standards Council, *PCI Data Security Standard*, Version 3.2 (April 2016)

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1471019303191

Beyond Electric Industry - Retail



"Like Target, we are a victim of a sophisticated cyber attack operation," said Ross Fazio, president of Fazio Mechanical Services, in a statement. "We are fully cooperating with the Secret Service and Target to identify the possible cause of the breach."



"HVAC vendor eyed as entry point for Target breach" *CNN Money* (February 7, 2014)
<http://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html>

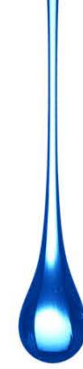
Beyond the Electric Industry – Consumer Goods



“While supply chain risk management may be a relatively new concept for many organizations, it has been a board-driven initiative at P&G since 2000.”

“For P&G, the business continuity efforts are seen as ‘insurance’ for the business. The program enables them to protect their critical assets and systems in a cost effective way.”

NIST, US Resilience Project, *Best Practices in Cyber Supply Chain Risk Management*,
Procter & Gamble Excellence in Supply Chain Risk Management
http://www.nist.gov/itl/csd/upload/NIST_USRP-P-G-Cyber-SCRM-Case-Study.pdf



Take Aways

It's not just FERC... Not just the electric industry

The dynamics of contracting and providing for ICS hardware, software and services are likely to change.



- Additional validation steps
- Tighter controls on access, even for maintenance
- Security is part of the design

Pay attention to NERC Project 2016-03

Postscript on Innovation

Security is part of the design

Asset management automation

Isolation of ICS from untrusted networks,
including the Internet

Standardization of procurement and contracting
could be a good thing





Joel deJesus

Washington, DC

joel.dejesus@dinsmore.com

Let's *Accomplish* more.SM Together.

