Supply Chain Security

What can be expected from CIP-013-1?

September 14, 2017

Bill Johnson - TDI Technologies
Leonard Chamberlin - Archer Security Group

First things first…

- Thank you for attending our webinar.
- Q&A will be at the end. So send your questions in throughout the webinar and we will queue them up for the presenters!
- How?

How to Ask Questions

1. Click on the Questions and Answers icon to submit a question to all panelists
2. Type your question in the box and click Send
3. Click on the Chat to send comment to "All Panelists" or "Everyone"
4. Type your comment, question, or URL and hit <Enter>
5. Raise Hand to get Host's attention

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Introductions

Presenters

Bill Johnson

President & CEO

TDi Technologies

www.tditechnologies.com

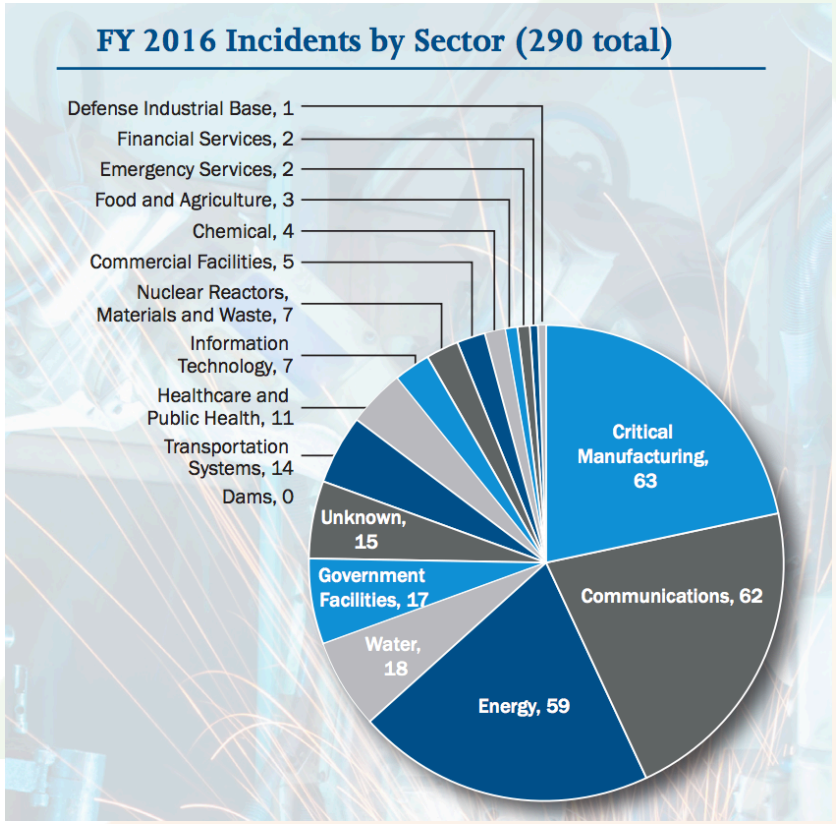
Leonard Chamberlin

Senior Security Consultant

Archer Security Group

www.archersecuritygroup.com

Supply Chain Attacks



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

FERC Order 829

- Issued July 21, 2016
- Ordered NERC to address perceived gap in the CIP standards re: supply chain.
  - Software integrity and authenticity
  - Vendor remote access
  - Information system planning
  - Vendor risk management and procurement controls
- LaFleur dissented

156 FERC ¶ 61,050
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM15-14-002; Order No. 829]

Revised Critical Infrastructure Protection Reliability Standards

(Issued July 21, 2016)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) directs the North American Electric Reliability Corporation to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The new or modified Reliability Standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System.

DATES: This rule will become effective **[INSERT DATE 60 days after publication in the FEDERAL REGISTER].**

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

CIP-013-1

- R1 – Supply Chain Risk Management Plan for H/M BCS that includes:
  - R1.1 – Process used in planning / procurement of BCS to identify and assess cybersecurity risks to the BES from vendor products/services resulting from:
    - Procuring and installing vendor equipment and software
    - Transitions from one vendor to another

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Supplier Perspective on R1

- NIST 800-61 Supply Chain Risk Management Practices for Federal Government
- SANS Procurement Language
- NERC Supply Chain Risk Management Plans
- Vendor disclosure of supply chain to utility in contracts

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

CIP-013-1

- R1.2 – Process that addresses the following, as applicable:
  - 1.2.1 – Notification by the vendor of vendor-identified incidents related to the products or services provided;
  - 1.2.2 – Coordination of responses to vendor-identified incidents related to the products or services provided;
  - 1.2.3 – Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
  - 1.2.4 – Disclosure by vendors of known vulnerabilities;
  - 1.2.5 – Verification of SW integrity and authenticity of all SW and patches from the vendor for use in BCS; and
  - 1.2.6 – Coordination of controls for:
    - Vendor-initiated IRA, and
    - System-to-system remote access w/ a vendor.

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Supplier Perspective on R1.2

- 1.2.1 - Vendor proactive customer notification should be required in reasonable timeframe.
  - In some cases even if solution is unknown or incomplete.
  - State Timeframe and set customer expectation.
  - Solicit customer input.

- 1.2.2 – Vendor plan identified in contracts and have accountability
  - Fines for failure.
  - Holdback for failure

- 1.2.3 – Vendor access should always be controlled by customer
  - Require two person Authentication/Approval
  - Oversight of Vendor Actions and Access.

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Supplier Perspective on R1.2 (part 2)

- 1.2.4 – Known vulnerabilities with corrections should come out with new versions in change documentation associated with each new version.
- 1.2.5 – Image Hash and signatures available on vendor website – clearly available to customer.
  - Some applications could even hash its image and validate the hash at runtime against the vendor site or against a vendor certificate associated/included with the product version/license.
- 1.2.6 - Coordination of any outsider access is critical.
  - Including authentication, authorization, logs
  - Audits of access and interacting assets
  - Configuration audits: before and after any access to determine changes made, if any.

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

CIP-013-1

- R2 – Implement the Supply Chain Risk Management Plan specified in R1

- NOTE – implementation of R1 does not require renegotiation or abrogation of existing contracts (incl. amendments). Additionally, these are out of scope:
  - Terms/conditions of procurement contract
  - Vendor performance & adherence to contract

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Supplier Perspective on R2

- Implementing plan is harder than developing or acquiring plan.
  - Often impacting business processes beyond procurement.
- Contract renegotiation not necessary.
  - How to measure success?
  - What if the vendor is uncooperative but has a 10 year contract?
- How to manage vendor/customer communication, notifications, patch updates and product certifications, compliance and verification?

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

CIP-013-1

- R3 – CIP Senior Manager review & approval of the R1 plan every 15 months.

- Rationale for R3 suggests that the plans are kept "up-to-date and address current and emerging supply chain-related concerns and vulnerabilities."

- Examples of sources:
  - NERC or E-ISAC
  - ICS-CERT
  - CCIRC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Supplier Perspective on R3

- Annual meeting and discussion with suppliers.
  - Have supplier show progress and measurement of their supply chain.
  - Update and improve plan with the CIP Senior Manager review.

- Define which emerging threats were reviewed and considered.
  - Include threats no longer considered critical and removed.
  - Include how they are measured or not and what risk or challenges still exist.
  - This impacts business continuity plan as well.

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

NERC BOT Approved – Now What?

- CIP-013-1 goes to FERC for final approval
  - Must be filed by September 2017
- 3 scenarios:
  - Approve outright
  - Approve w/ changes ordered
  - Remand

- If approved, likely effective the first day of the first calendar quarter that is twelve (12) months after the effective date of approval by FERC

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Supplier Perspective

- Challenges include coordination and partnership with customer/supplier.
  - Trust is key here.
  - Where supplier can expose their weaknesses from a cyber perspective is a fine balance.
  - Work with Customer, not in the closet.
- Measurement, reporting and incremental refinement of non-binding agreements can work.
- Consider deeper implementation of 800-161 controls and measurements.
- Don’t try to eat the whole elephant at once, you will get a headache, never mind it doesn’t taste good.

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Q&A

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

Thank you very much!

Bill Johnson, President and CIO
TDI Technologies, Inc.
bill.johnson@tditechnologies.com

Leonard M. Chamberlin III, CISSP, CISA, PSP
Archer Security Group
leonard.chamberlin@archerenergysolutions.com

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions