USAID
FROM THE AMERICAN PEOPLE

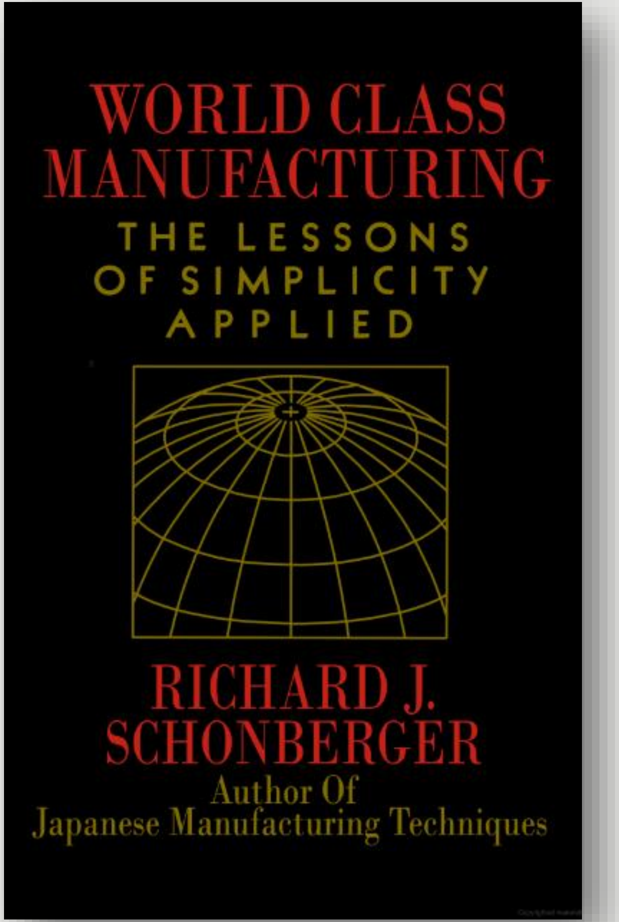
USEA
United States Energy Association

Leveraging Procurement for Cybersecurity Resilience

Cybersecurity and Digitalization: Supply Chain Risks in the Electricity Sector

Frank Harrill

April 25, 2024



WORLD CLASS MANUFACTURING

THE LESSONS OF SIMPLICITY APPLIED

RICHARD J. SCHONBERGER

Author Of
Japanese Manufacturing Techniques

“Contractual requirements should be tough so as to drive the supplier into the mode of continual and rapid improvement.”
(page 157)

PROCUREMENT LANGUAGE IS AN ADMINISTRATIVE CONTROL

- It is not an effective stand-alone control
- It must be part of a comprehensive supply chain risk control strategy
- It must be understandable to all parties
- It should be as simple as possible… but no simpler
- It should create a flow-down obligation to downstream suppliers

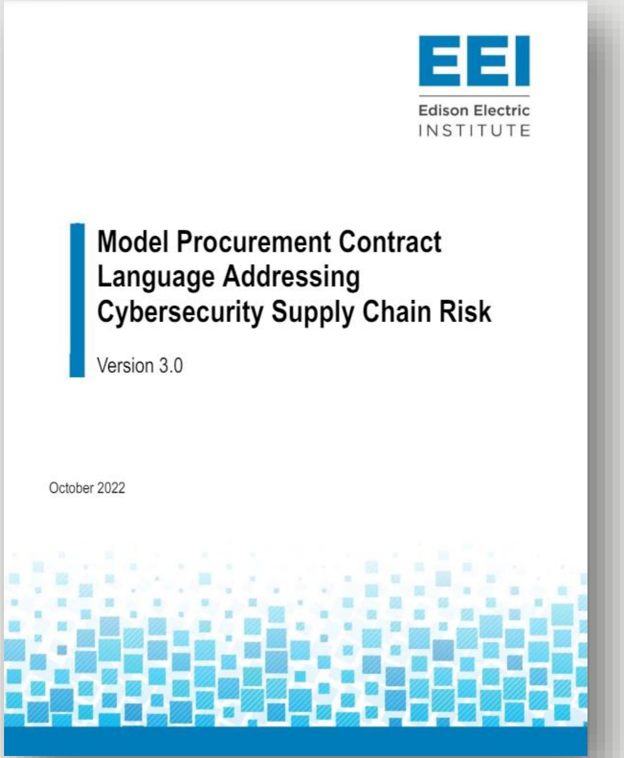
NURTURE TRUSTED SUPPLIER PARTNERSHIPS

- Treat suppliers as true business partners
- Trust but verify
- Establish redundancy whenever possible
- Cultivate lasting supplier relationships

CONTINUOUS ASSESSMENT

- Assess suppliers based on risk.
- Visit and review compliance whenever possible.
- Ensure continuity and incident response plans are in place.
- Examine external risk surfaces of suppliers.
  - https://securityscorecard.com/security-rating/domain name of supplier
  - https://webscan.upguard.com/

MODEL PROCUREMENT LANGUAGE



EEI
Edison Electric
INSTITUTE

Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

Version 3.0

October 2022

- Joint effort by the Edison Electric Institute
- Available at: https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf

IMPORTANT CONSIDERATIONS

- Requests to obtain sensitive supplier documents increase risk without enhancing security.
  - Instead, rely on independently audited third-party certifications or visual inspections.

- Ensure vulnerability disclosure timelines are reasonable and risk-based.
  - The careful balance we all must strike is described in ISO/IEC standard 30111:2019 "Premature disclosure of sensitive vulnerability information can increase the costs and risks associated with disclosure for vendors and users."

INTERNATIONAL STANDARDS COVERAGE

IEC 62443-4-1 Audited Controls

1 Development process
2 Identification of responsibilities
3 Identification of applicability
4 Security expertise
5 Process scoping
6 File integrity
7 Development environment security
8 Controls for private keys
9 Security requirements for externally provided components
10 Custom developed components from third-party
11 Assessing and addressing security-related issues
12 Process verification
13 Continuous improvement
14 Product security context
15 Threat model
16 Product security requirements
17 Product security requirements content
18 Security requirements review
19 Secure design principles
20 Defense in depth design
21 Security design review
22 Secure design best practices
23 Security implementation review
24 Secure coding standards
25 Security requirements testing
26 Threat mitigation testing
27 Vulnerability testing
28 Penetration testing
29 Independence of testers
30 Receiving notifications of security-related issues
31 Reviewing security-related issues
32 Assessing security-related issues
33 Addressing security-related issues
34 Disclosing security-related issues
35 Periodic review of security defect management practice
36 Security update qualification
37 Security update documentation
38 Dependent component or operating system security update documentation
39 Security update delivery
40 Timely delivery of security patches
41 Product defense in depth
42 Defense in depth measures expected in the environment
43 Security hardening guidelines
44 Secure disposal guidelines
45 Secure operation guidelines
46 Account management guidelines
47 Documentation review

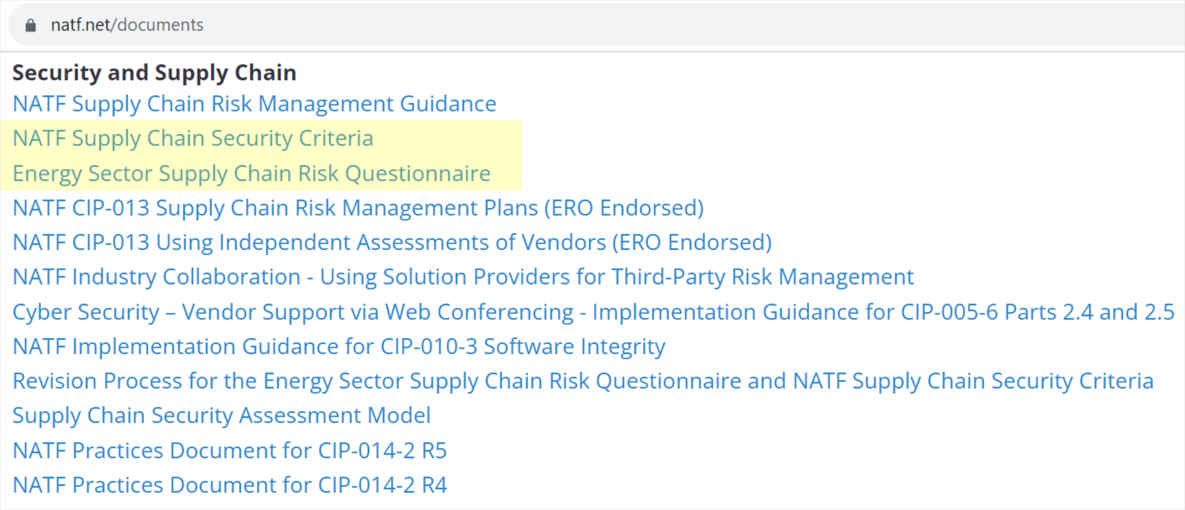
INTERNATIONAL STANDARDS COVERAGE
ISO 27001: 2022

- 93 controls, in four categories
  - Organizational Controls (37 controls)
  - People Controls (8 controls)
  - Physical Controls (14 controls)
  - Technological Controls (34 controls)
  - In addition to proper operation of the information security management system including: context of the organization, leadership, planning, support, operation, performance evaluation, and continuous improvement.

- Always review the supplier Statement of Applicability

NATF SUPPLY CHAIN QUESTIONNAIRE

- The North American Transmission Forum (NATF) with cross-industry collaboration created and curates two supply chain risk assessment instruments especially useful when certifications are unavailable:
  - The Criteria
  - The Questionnaire



natf.net/documents

Security and Supply Chain

NATF Supply Chain Risk Management Guidance

NATF Supply Chain Security Criteria

Energy Sector Supply Chain Risk Questionnaire

NATF CIP-013 Supply Chain Risk Management Plans (ERO Endorsed)

NATF CIP-013 Using Independent Assessments of Vendors (ERO Endorsed)

NATF Industry Collaboration - Using Solution Providers for Third-Party Risk Management

Cyber Security – Vendor Support via Web Conferencing - Implementation Guidance for CIP-005-6 Parts 2.4 and 2.5

NATF Implementation Guidance for CIP-010-3 Software Integrity

Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Supply Chain Security Criteria

Supply Chain Security Assessment Model

NATF Practices Document for CIP-014-2 R5

NATF Practices Document for CIP-014-2 R4

Thank You!

Frank Harrill, Schweitzer Engineering Laboratories, Inc.
frank_harrill@selinc.com

Jacob Phillips, Midcontinent Independent System Operator (MISO)
jrphillips@misoenergy.org

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association