



USAID
FROM THE AMERICAN PEOPLE



**SCHWEITZER
ENGINEERING
LABORATORIES**



Supply Chain Security

Tim Watkins

tim_watkins@selinc.com



Security

must be a
foundations of an
organizations'
DNA

SEL Principles of Operation



Making Electric Power Safer, More Reliable, and More Economical

Securing Your Supply Chain

An essential component of a complete cybersecurity program

Securing Your Supply Chain

Best Practices From SEL



Developing supply chain cybersecurity risk management plans

Supply chain risk management is an essential component of a complete cybersecurity program. The interconnection and complexity of supply chains makes it more important than ever to systematically assess risks, but this is a difficult challenge. At SEL, we have made security, including supply chain security, a top priority for over 30 years, and we believe that managing supply chain risks is fundamental to ensuring the quality of our products. We hope that sharing our knowledge and best practices in this area will accelerate your cybersecurity and NERC CIP-013 compliance efforts. This document outlines the processes SEL follows to ensure a safe and dependable supply chain for the products we deliver to customers around the world.



Quality = Security

- Industry presence
- Customer trust
- Warranty
- Reliability indicators
- Return and repairs
- Technical Support
- Quality Assurance



<https://selinc.com/support/warranty/>

© SEL 2020



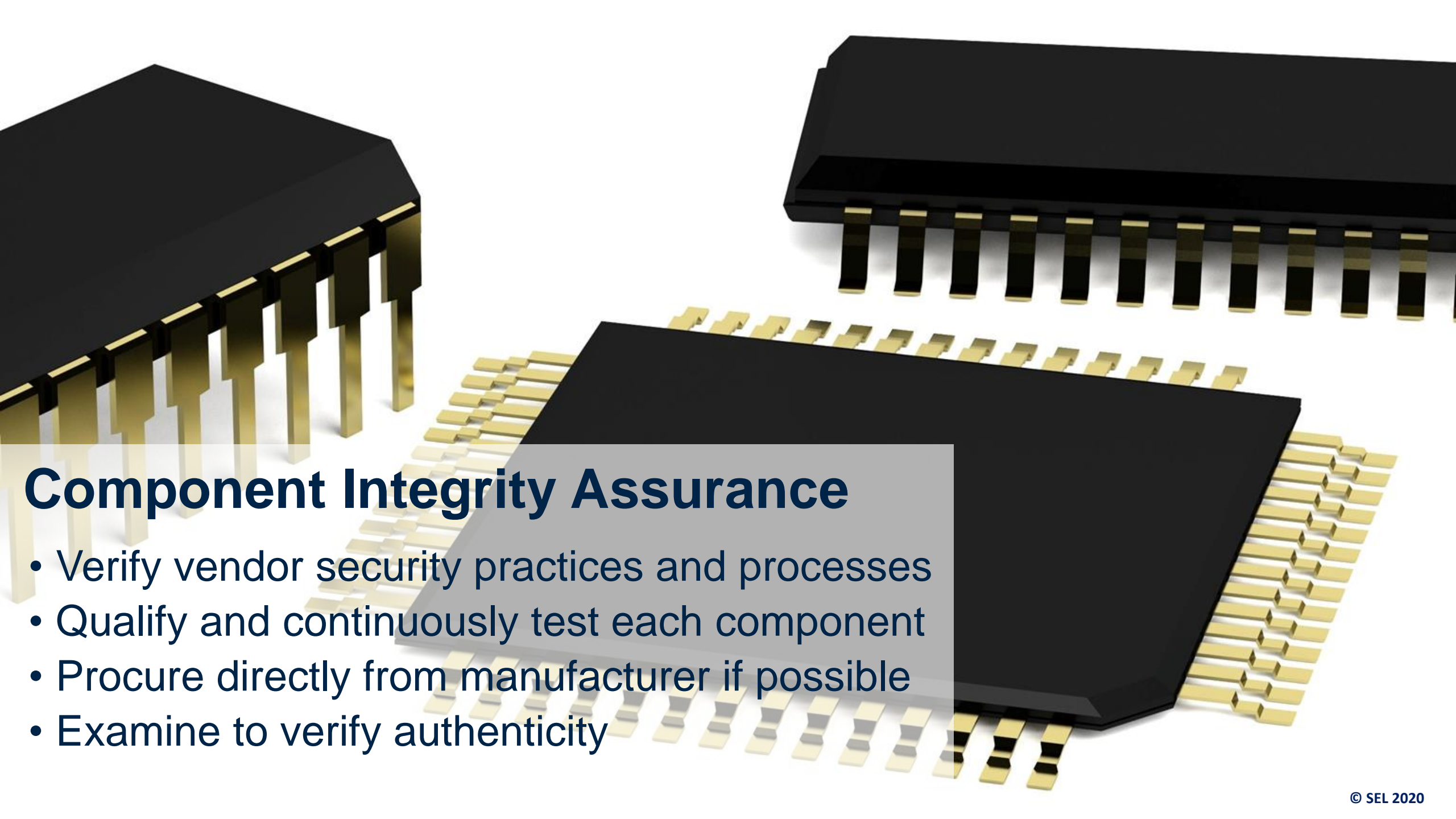
Nurture Trusted Supplier Partnerships

- Holistic approach to supplier evaluation
- Trust but verify
- Pursue redundancy whenever possible
- Cultivate lasting supplier relationships

Continuous Supply Chain Assessment

- Analyze business and threat intelligence
- Assess suppliers based on risk
- Scrutinize shipping services
- Multiple vertices





Component Integrity Assurance

- Verify vendor security practices and processes
- Qualify and continuously test each component
- Procure directly from manufacturer if possible
- Examine to verify authenticity

Firmware Tools | Schweitzer Engir x +

selinc.com/products/firmware/?hashProduct=SEL-T400L

SEL SCHWEITZER
ENGINEERING
LABORATORIES

check the authenticity and integrity of firmware by digital signature verification. If a mismatch occurs, the SEL device will reject the firmware file and abort the firmware upgrade process.

SEL provides firmware hashes as an additional security measure to ensure the integrity of SEL firmware files. This page helps ensure that the firmware received from the factory is complete and unaltered prior to being loaded onto the SEL device.

Use this page to verify that the firmware file in your possession with the hash value provided on this website by selecting the product from the drop down below.

If a product or firmware version is not listed, or the firmware file in your possession does not match the hash value from this tool, or you need firmware hash values for other file types, please contact SEL Technical Support.

Firmware Hashes for


SEL-T400L

Revision	Type	Hash
R103-V0	zds	SHA-1 COPY b42986288e8de9a50a10f743c1f202fc3f06d8fa
		SHA-256 COPY 848d6a60ff20d9d52584141167281215cdcb91426dd36ec6aaf0da5a4305fa05
R102-V0	zds	SHA-1 COPY 75e104b6e146365b65c7ce57779573b8a5e58b6b
		SHA-256 COPY 505e8eaa158fdc6c8f9c6ae55d0250158f5faed356403d1c99481ca47f942d7d

© SEL 2020

Verification of Software Integrity and Authenticity

- Protection products continuously verify software integrity and disable themselves if corruption is detected
- Control products whitelist applications at the kernel level
- FW/SW is digitally signed
- FW/SW can be authenticated by reference hash values published on SEL website

A woman with brown hair tied back, wearing safety glasses and a blue lab coat, is shown in profile, focused on inspecting a green printed circuit board (PCB). She is wearing white gloves. The background is a blurred industrial setting with shelves and equipment.

Monitor for Quality and Security Vulnerabilities

- Determine Root Cause
- Component level product tracking
- Service Bulletins
- Security Vulnerabilities

ISO 27002-2013

Canadian CSE Top 10

NIST CSF 1.2

CIS

IEC 62443

***Before Regulation there
needs to be Standards***

NERC CIPv7

HIPAA

**NIST RMF and
800-53r5**

***Before Standards there
needs to be **Innovation*****

PCI DSS 3.2

Australian Top 35

DHS CDM Program

Victorian PDSF v1.0

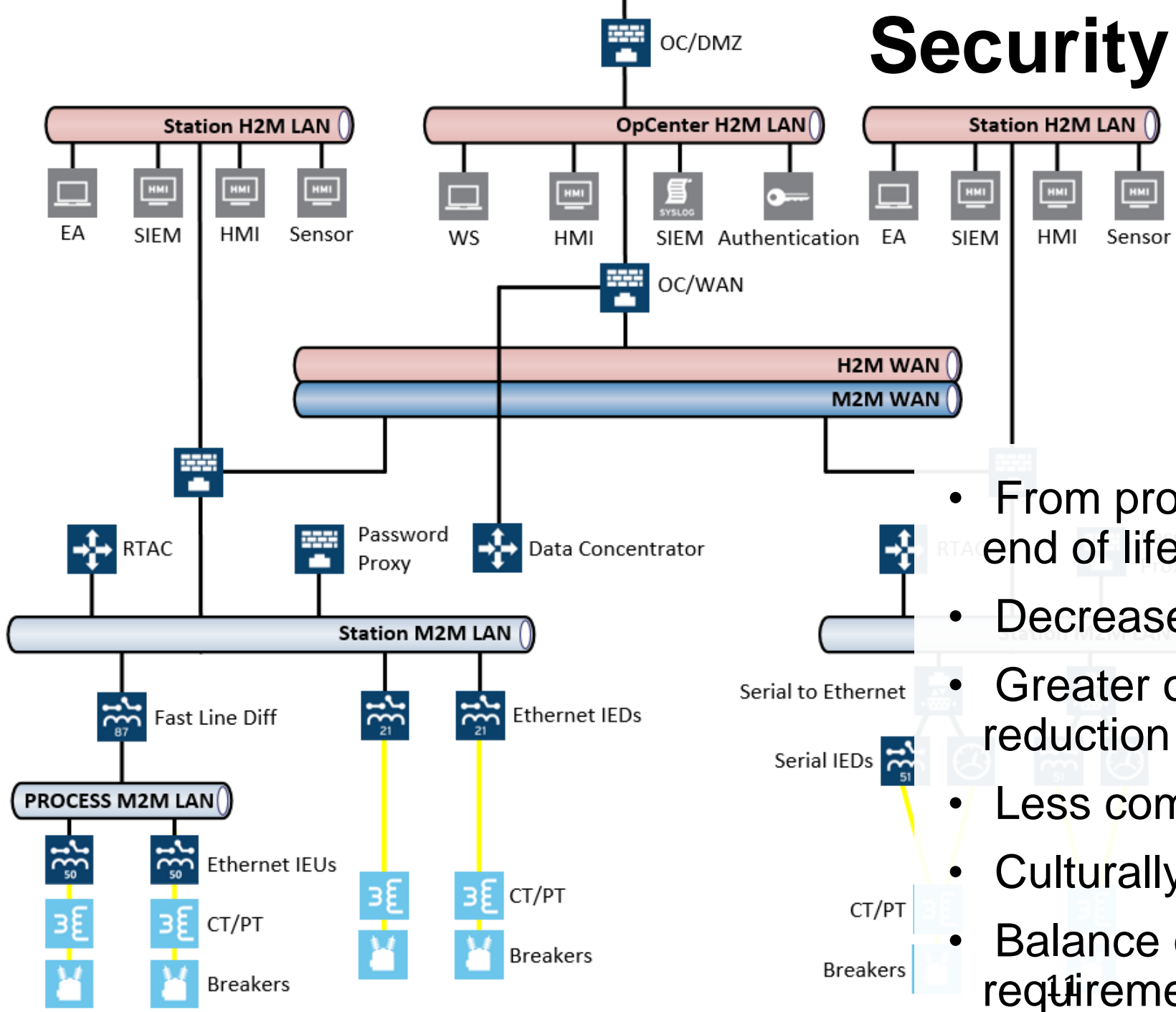
COBIT 5

NSA MNT

GCHQ 10 Steps

Security by Design

L4.5 - Perimeter	OC/DMZ
L4 - SCADA	H2M
L3.5	WAN/OC
L3 - Access	ECS WAN
L2.5	H2M/M2M SS ESP
L2 - Automation	Station M2M
L1 - Protection	
L0 - Sensors and Actuators	Process M2M



- From project conception to end of lifecycle
- Decreased lifetime cost
- Greater overall risk reduction
- Less complex
- Culturally accepted
- Balance operational requirements with risk

Contracting Language

- Typically see
 - “sibre” in Appendix Z
 - Multiple frameworks
 - No security control overlay
- Customer needs to select security controls during the design process
- Balance between:
Cost vs Usability vs Security
- Secure by Design but with “options” to “dial” cyber



Guide to the Distributed Energy Resources Cybersecurity Framework

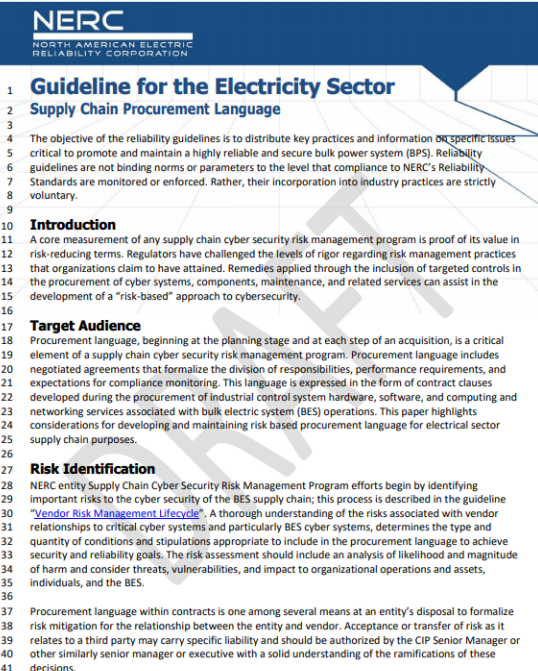
Charisa Powell, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC
This report is available at no cost from the National Renewable Energy
Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-6R00-75044
December 2019



Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities

May 2019

Michael Mylrea, JA Rotondo, Sri Nikhil Gupta Gouriseti

Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

Version 2.0

May 2020



Tim Watkins

+1 509 592 3546

tim_watkins@selinc.com

LinkedIn - <https://www.linkedin.com/in/tim-watkins-4707869/>