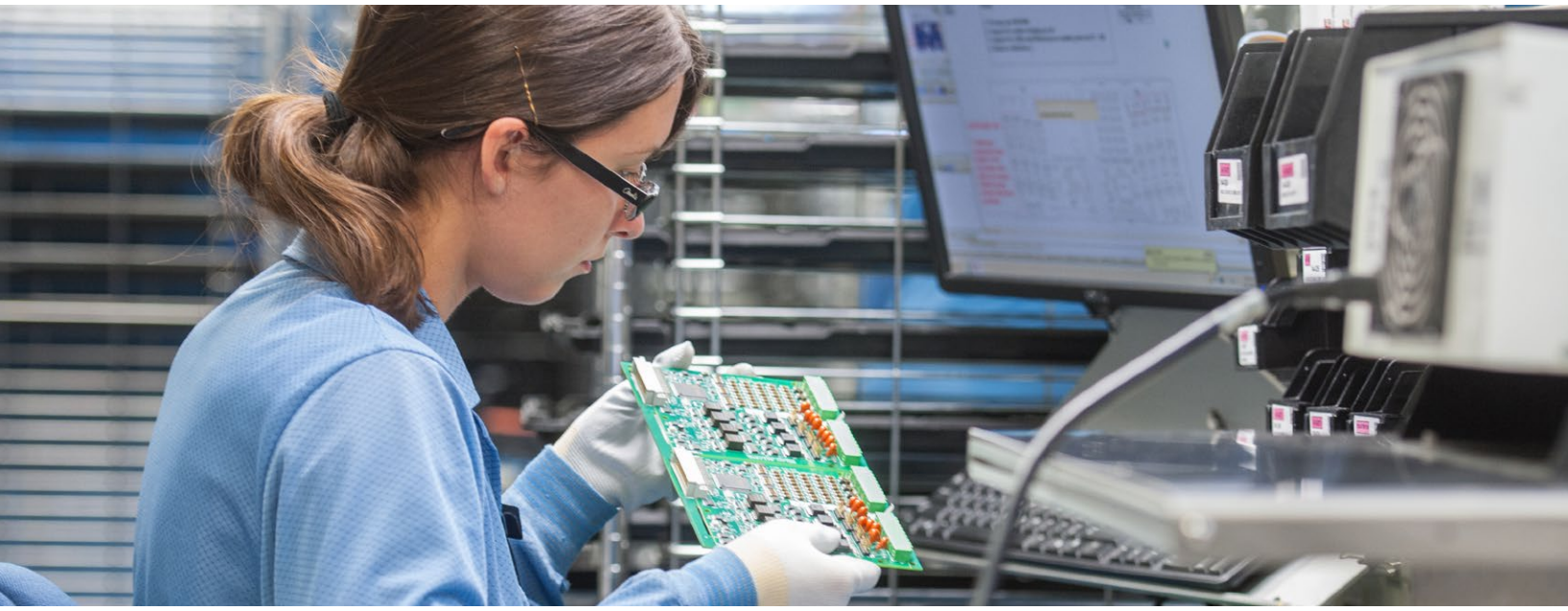
Securing Your Supply Chain

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.

SEL

NERC CIP-013-1, "Cyber Security—Supply Chain Risk Management"

Purpose

"To mitigate cybersecurity risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems."

Enforcement Date

July 1, 2020

Summarized Requirements

- Assessment of risk from vendor products or services (R1.1)
- Notification of vendor-identified incidents (R1.2.1)
- Coordination of response to incidents (R1.2.2)
- Notification by vendor when remote/onsite access not needed (R1.2.3)
- Disclosure by vendors of known vulnerabilities (R1.2.4)
- Verification of software integrity and authenticity (R1.2.5)
- Coordination of controls for remote access (R1.2.6)

How SEL Ensures a Secure and Dependable Supply Chain

SEL's supply chain is global and complex. We take a comprehensive five-part approach to evaluating the risks to our supply chain.

Part 1: Build Trusted Supply Networks

Supplier Rating System

At SEL, we employ a supplier rating system that evaluates every supplier based on price, quality, features, innovation, delivery, and service. To arrive at this rating, we assess the following supplier risks:

- Manufacturing locations
- Material lead times
- Financial health
- Replenishment methodologies
- Technology type
- On-time delivery performance

Annual Supplier Conference

Every year, we host a conference for vendors who supply us with component parts, equipment, and services. During this event, more than 200 companies come to our headquarters in Pullman, Washington, where we share our technical needs and strategic objectives for the coming year and identify ways of partnering to ensure a continuous supply of quality parts.

Onsite Audits

We build relationships with our suppliers as we conduct ongoing onsite audits to verify that their quality and security processes meet our requirements.

Organizational Approach to Supplier Selection and Monitoring

At SEL, supply chain risk management relies on cross-functional collaboration. The process begins with the selection of vendors, which is a team effort between our product development, quality, and purchasing groups. Similarly, different teams weigh in on component selection, ongoing monitoring of vendors and parts, and onsite vendor audits. This approach makes risk management everyone's responsibility.

Privacy

We do not share our bills of materials (BOMs). We provide forecasts by part number, unrelated to the product. To avoid disclosing product and part information from other vendors, we never send out design schematics.

Our Suppliers' Suppliers

It's not enough to know our first-tier suppliers. We ask our suppliers to identify their first-tier suppliers along with key risks, mitigation strategies, and replenishment methodologies.

Preference for Domestic Suppliers

To the greatest extent possible, we source materials from the United States.

Transportation and Shipping Supplier Qualification

To help ensure the secure delivery of our products to our customers, we apply the same supplier qualification processes to our transportation and shipping suppliers.

Part 2: Ensure Component Integrity and Availability

Component Qualification Process

To ensure the integrity of our products, we verify the performance of purchased components against supplier product specifications. Whenever possible, we procure components directly from the manufacturer or official distributors. In cases where components must be sourced from independent distributors, we use several methods to detect counterfeit products, including functional testing and microscopic, x-ray, x-ray fluorescence, and decapsulation inspections.

Continuous Testing

Throughout the manufacturing process, we constantly test our products. If variations in performance are found, we work to understand the root cause of the discrepancy.

Minimizing the Impact of Disruptions

We work with suppliers to ensure we and they keep sufficient inventory of specialty and at-risk parts. Whenever possible, we ensure that critical components can be sourced from at least two vetted suppliers.

Part 3. Verify Security of Software and Firmware

Source Code

We own every line of our source code, and we do not share source code or schematics. We develop most software internally, providing a quality control advantage along with the ability to make rapid enhancements. If we use third-party software, we acquire the source code. Access to code is only permitted for SEL R&D engineers working on these projects.

Internal Testing

We have a robust process that includes reviews by peer developers and both positive and negative testing. We also use automated tools for inspecting code in order to identify potential issues developers may have missed. All testing is performed onsite at SEL by SEL employees.

SEL Digital Signatures and Firmware Hashes

Digitally signed software allows you to be sure that software and firmware files are genuine (produced by SEL) and that they have not been altered or tampered with. Microsoft Windows users can check for and verify digital signatures for SEL software products by using Windows Explorer. SEL hardware products transparently check the integrity of firmware files during the firmware upgrade process using additional data built into the firmware. If a mismatch occurs, the SEL device will reject the firmware file and abort the firmware upgrade process. We provide firmware hashes as an additional tool to verify the integrity of SEL firmware files.

Part 4: Protect Operations and Control Access

SEL Physical Security and Cybersecurity

Our internal physical and information security infrastructure is layered and conforms to internationally recognized standards. This ensures all SEL devices and services are delivered securely and all data entrusted to SEL is protected. We also challenge ourselves to go beyond standards to increase cybersecurity. For example, we've implemented software-defined networking in our manufacturing operation to eliminate several common network security vulnerabilities.

Our Quality Management System is certified to the ISO 9001 standard, and our manufacturing processes comply with the IPC-A-610 Class 3 workmanship standard for products requiring high reliability, such as those used in life-support and aerospace systems.

All SEL employees undergo an exhaustive prehire background and criminal history review process. Access to SEL buildings and sensitive spaces within them is protected by configurable access controls, CCTV, and other monitoring systems. SEL equipment and information systems are protected from physical and environmental threats. SEL security systems are monitored and supported by our Security Operations Center, which is staffed 24/7 by SEL employees. Our teams scour an array of public and private threat and other intelligence streams to detect and analyze potential threats.

Need to Know

The SEL security culture is rooted in the concepts of least privilege, need to know, and defense in depth. We compartmentalize projects and limit access to information internally to those with a need to know.

Protection of Customer Information

We protect customer information both in our business systems and during support activities. This includes securing customer information in products sent back for repair. When we identify an incident affecting customer information, we notify customers and offer full support for incident response.

Remote Access

When remote access is necessary for technical support, we use a tracking and notification system to document and coordinate control of that access.

Part 5: Monitor for Quality and Security Vulnerabilities

Determining Root Cause

Offering a ten-year warranty provides an incentive for our customers to return products to us when they fail. We can then examine these products and find the root causes of defects, which in turn enables us to identify problems with our design process or with our suppliers and improve our product designs. We provide a ten-year warranty at no cost on all products.

Product Tracking to the Component Level

We keep a detailed record of every product we manufacture and the components built into them so we know where our products are installed and can notify customers about potential quality or security issues.

Service Bulletins

When we identify a potential issue with a product, we assemble a multidisciplinary team of product design experts to analyze the problem. If it poses a risk to customers, we inform affected customers with a service bulletin. Service bulletins include an explanation of the identified problem as well as the root cause, impact, observed defect rate, affected products by customer, corrective actions, and recommended maintenance solutions. A service bulletin allows the customer to make an informed decision on how to address the issue. We distribute service bulletins to customers both directly and through our sales force.

Security Vulnerabilities

A service bulletin that relates to a security vulnerability in affected products is classified as "Security Vulnerability." Our team develops suggested corrective steps for any product security vulnerability before disclosure and includes them in the associated service bulletin.

Industry Involvement

We participate in various government-led initiatives and standards development activities so we can be aware of the current best practices of others, contribute to industry best practices, and stay attuned to the evolving demands placed on our customers. Similarly, we contribute to and use guidance documents, such as the NIST Cybersecurity Framework, to improve our own processes and controls and help shape agreed-upon industry best practices.

SEL's Ongoing Commitment

At SEL, our quality policy is to "Understand, Create, and Simplify." This represents our relentless pursuit of understanding opportunities and challenges, creating innovative solutions, and ensuring those solutions are simple, robust, and secure. Executives at SEL include security risk management as part of their daily activities. They stay informed of emerging threats to SEL's supply chain and operations and make adjustments accordingly.

SEL SCHWEITZER ENGINEERING LABORATORIES

Making Electric Power Safer, More Reliable, and More Economical
+1.509.332.1890 | info@selinc.com | selinc.com

PF00551 • 20191209

WORLDWIDE 10 years WARRANTY