SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

Information for SEL Customers About Data Security When Returning Devices to SEL for Service

Customers have expressed concerns about compliance with NERC CIP information security rules when returning products to SEL for technical support, including repair, information recovery, or analysis of undesired operation or failures. SEL cybersecurity professionals reviewed the NERC CIP standards, drafts, and other guidance documents, and were unable to find any direct wording that addresses concerns about leaving data in SEL devices for recovery and analysis after an event.

The NERC CIP standards require an information handling and protection program for all information dealing with critical cyber assets. SEL recommends that customers' security programs make provisions for direct factory technical support from device manufacturers to enable manufacturers to provide accurate and thorough analysis and improve reliability.

The NERC CIP standards also require that responsible entities erase all data if a product is undergoing disposal. SEL does not consider product returns for technical support as disposal, because SEL repairs returned products and sends them back to customers.

The data stored in the SEL product are essential for testing and analysis. Fault analysis helps to improve the reliability and safety of the grid. This analysis helps customers understand the root cause of an unintended operation or failure, including identifying potential malicious intent. For SEL to arrive at root cause and to most accurately determine the cause of an event, the data in the device must accompany the product return.

When a device is repaired, before it is returned to the customer, its data can be destroyed (replaced with factory defaults), or the original data can be retained in accordance with instructions from the customer. In some cases, the SEL Product Hospital may choose to replace customer equipment. In this situation, SEL provides two methods for product disposal that align with the NERC CIP requirements. SEL will either send the customer the original non-operating equipment along with a replacement, or SEL will destroy the equipment, provide proof of destruction of the device and its data or memory devices in the Service Activity Report, and send a replacement.

Recommendations on Information Handling for SEL Products

- ✓ In your information handling and protection program, include procedures for returning products to their manufacturer for diagnosis and repair with settings and diagnostic data intact.
- ✓ Set device accounts to new strong passwords before sending the device to the SEL Product Hospital.
- ✓ Avoid settings data that identify the location to members of the public. Data configured by customers into devices are most useful to an attacker who steals or gains access to that information if the location of the device's installation can be determined. For this reason, settings and notes stored on SEL products should refer to the device or its location in an esoteric form (meaningful only within your organization), and not plainly identify the location of the device. For example, use a device designator (e.g., RT5Z35S22R9) as opposed to a text description ("sunshine substation, bay 9").

Contact Information

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 USA
Telephone: +1.509.332.1890
Fax: +1.509.332.7990
Internet: www.selinc.com
Email: security@selinc.com