SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: 509.332.1890 • Fax: 509.332.7990
www.selinc.com • info@selinc.com

The SEL Process for Personnel Risk Assessments

Response to NERC CIP-004 R3

Introduction

SEL believes hiring appropriately qualified, responsible employees is critical to the success of our organization. SEL also believes that direct factory support is a powerful tool that continually improves the operational reliability of the power system. SEL's mission is to provide products and services that make electric power safer, more reliable, and more economical. A key component of SEL's ability to deliver its mission is our personnel: *we take hiring highly qualified employees very seriously*.

NERC CIP compliance requires a level of personnel background screening on all who have access to the critical components that make up our power systems. This document provides the assurance that SEL performs the appropriate level of assessments on employees with potential to have authorized cyber or authorized unescorted physical access to critical cyber assets allowing SEL to provide close support and partnership with the electric power industry in all aspects of the power systems.

SEL Process

1. Each candidate must go through a robust interviewing process to evaluate the candidate's technical proficiency, work ethic, and fit with SEL's mission, culture, and principles.
2. For each new hire, we carefully check references and complete a thorough background check using a professional firm.
3. We require an extensive post-offer drug screen before an employee can begin work with SEL in the United States. We also conduct random drug testing of our United States employees and in cases of safety incidents or suspicion.
4. SEL repeats background checks for applicable employees before completion of seven years of service.

Summary

A good security program begins and ends with the people that make up the organization. Personnel background checks are one of the safeguards that ensure SEL protects its people and that we provide a safe working environment where they will accomplish their jobs. The program also provides protections for our customers and their proprietary information. Performing background checks on employees, as well as third-party contractors with access to the most critical technical components in an organization's operations establishes a high level of trustworthiness. SEL believes our processes exceed current regulatory requirements.

SEL provides our customers with high-quality products and services that are reliable and secure. SEL believes direct technical support from our subject matter experts is the best way to ensure the highest level of reliability for SEL products.

Please contact SEL with any questions or requests for assistance on this topic. You may contact us through any of the following:

- Call or email: SEL Field Engineer
- Call or email: SEL Regional Sales and Service Director
- Email: security@selinc.com
- Call: +1-509-332-1890

To identify the SEL support staff for your region, please visit the Contact Us page on the SEL website, www.selinc.com.

Specific Regulatory Requirements

The following information assists SEL customers in documenting compliance to specific regulatory requirements. The information is current as of the date of this document, but SEL suggests customers reference regulatory requirements directly.

NERC Reliability Standard CIP-004, Requirement 3, requires responsible bulk electric system entities to define methods, processes, and procedures for performing personnel background checks on any employees or third-party contractors with unescorted physical or cyber access to critical cyber assets.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

> *R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.*
>
> *R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.*
>
> *R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.*[1]

[1] North American Electric Reliability Corporation. CIP-004. Available at http://www.nerc.com/files/CIP-004-1.pdf. Accessed July 27, 2009.