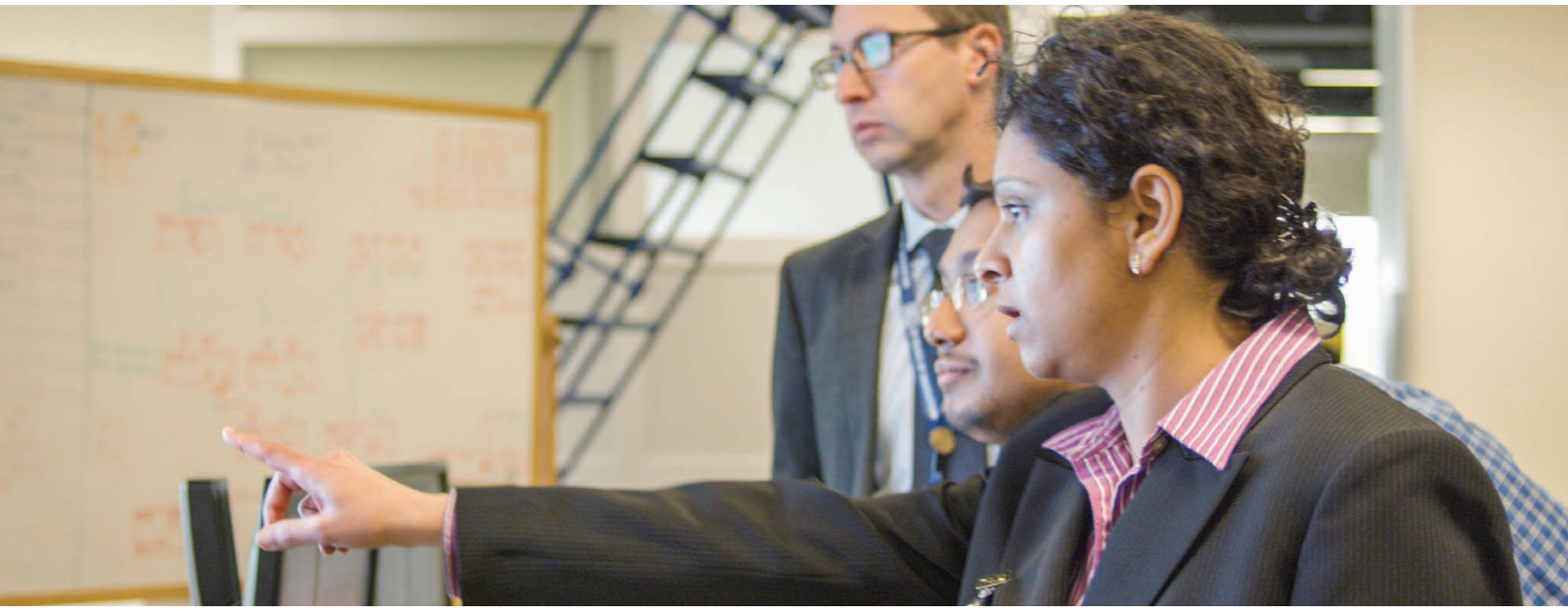
Security, Compliance, and Networking Assessment Service



SEL experts provide a thorough analysis of your substation cybersecurity

- See a holistic picture of your substation security.
- Understand vulnerabilities to address for NERC CIP compliance.
- Receive recommendations for modifying existing systems and processes to align with industry best practices.

Security threats are more common today than ever before. With increased focus on security and new regulations, many companies find themselves asking:

How much security is needed?

Which assets do I protect?

What social engineering and physical security risks do I have?

How does my company compare to my peers'?

SEL Engineering Services has experienced and accredited professionals with a deep understanding of electric utility substations and power system applications. They are are uniquely qualified to evaluate your systems and processes from a cybersecurity standpoint.

Assessments

Each year, new security breaches and threats pose additional risks to the operation of the power grid and industrial processes. SEL can help you stay secure and ahead of regulations with a flexible and low-cost onsite assessment. Our security experts review your system and provide a custom report with recommendations based on your needs. You can choose a general cyber assessment, a custom networking or security assessment, or both.

General Cyber Assessment

A general cyber assessment provides a snapshot of your cybersecurity posture using the most important security facets. Our experts focus on best practices for cybersecurity and cyber-asset management as well as the ability to detect and respond to cybersecurity events, recover from cybersecurity incidents, and restore normal operation. We include comparative analyses to peers in your industry and a NERC CIP compliance overview.

Custom Assessment

A custom cyber assessment offers more detail with a specific focus. For example, a custom cyber assessment might include system audits, compliance reviews (including NERC CIP), system scans, or a review of any of the following:

- Cyber and physical security program—The security of people, property, and policies, including policies/procedures, social engineering, risk awareness, and compliance.
- Cyber and physical vulnerability— Patching, updates, good practices, gates, guards, and surveillance.
- Network security—Firewalls, intrusion detection systems (IDSs)/intrusion prevention systems (IPSs), perimeters, and entry points.
- Information technology (IT), operational technology (OT), and network considerations—Design, efficiency, resilience, and components.

These assessments provide a high-level review of your organization's cybersecurity, physical security, IT, OT, or network posture and act as a baseline for improving security. The assessment provides insight for management, including identifying weak spots and whether best practices are being followed. It also includes recommendations for modifying existing practices. The assessment lets you know where you are now so you have something to measure your system improvement against.

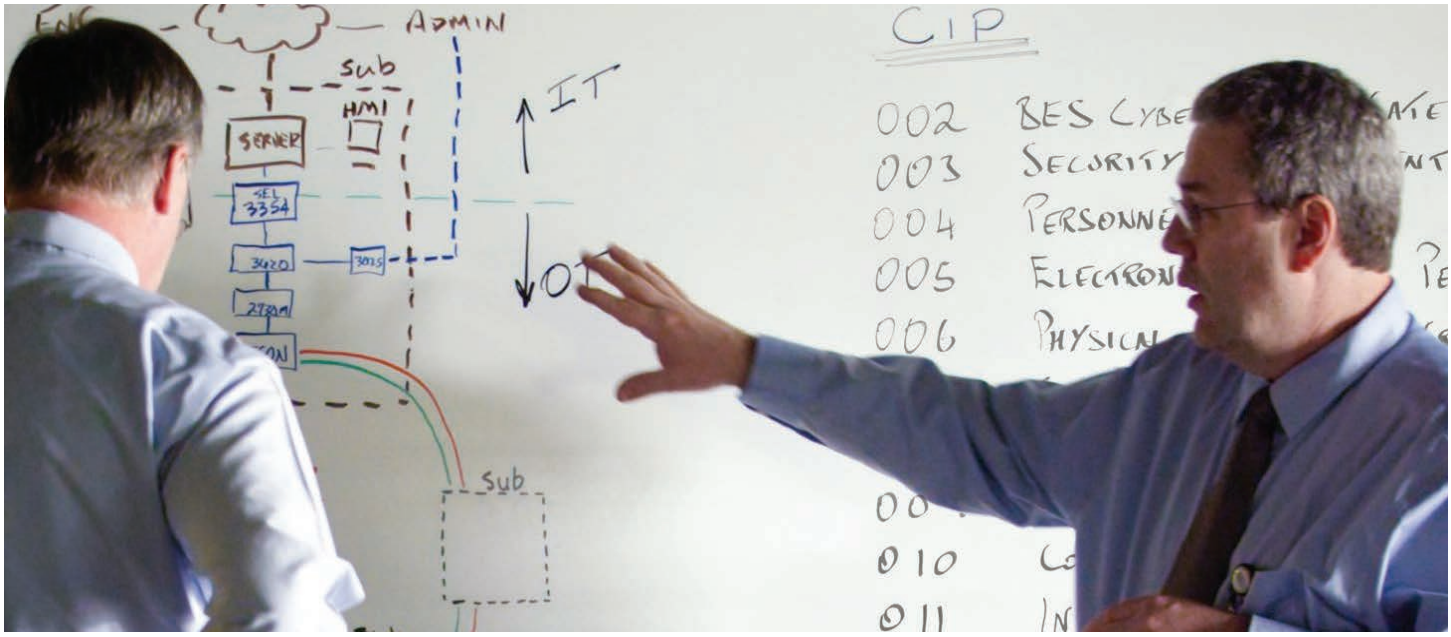
Typical Timeline

Each assessment is a tailored plan, specific to your system, that we develop to fit your deadlines. The timeline ensures that you get the most out of your assessment and that you understand your role in the process.

Order Placement	We set up a 1-hour teleconference to review the objectives, responsibilities, and schedule and to identify your participants. This is also where we finalize the scope definition for custom assessments.
14 Days Prior	We send you a pre-assessment questionnaire containing initial security questions (due in 7 days). The assessment logistics and schedule are finalized.
7 Days Prior	We review the upcoming logistics and discuss open items from the completed questionnaire with you.
Day 1	On the first day, there is a full-day meeting for you and the Engineering Services security team to complete the discovery process, discussion, and review. Our security experts will also gather additional system information.
Day 2	Morning—SEL security experts create a presentation. Afternoon—We present and discuss the assessment findings, answer questions, and provide any recommendations.
Follow-Up	SEL security experts are available to answer questions and discuss next steps (if any).

Assessment Deliverables

The assessment includes two deliverables: a copy of the presentation and a report. The report contains an executive summary, details of data gathered based on the current state, a peer ranking, and recommended enhancements. This report provides actionable insights to improve your company's cybersecurity posture.



Accredited Engineers With Proven Expertise

Because cybersecurity is constantly evolving, a thorough knowledge of the threat landscape, including emerging and advanced persistent threats, is necessary. Many regulatory requirements require an audit by a certified third party since earning credentials requires demonstrating a combination of experience and knowledge across a range of material. SEL Engineering Services has industry-experienced engineers with GIAC Security Essentials (GSEC), Certified Information Systems Security Professional (CISSP), and Project Management Professional (PMP) certifications. These engineers deliver a thorough assessment of your current cybersecurity state and recommend actions to create a more secure operation.

Next Steps

Security is a continuing process, not a single event. Contact Engineering Services Security Services at **ES.Security.Services@selinc.com** to discuss your compliance and security challenges.

CISSP is a registered mark of the International Information Systems Security Certification Consortium in the United States and other countries.

SEL SCHWEITZER ENGINEERING LABORATORIES

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

PF00600 • 20181030