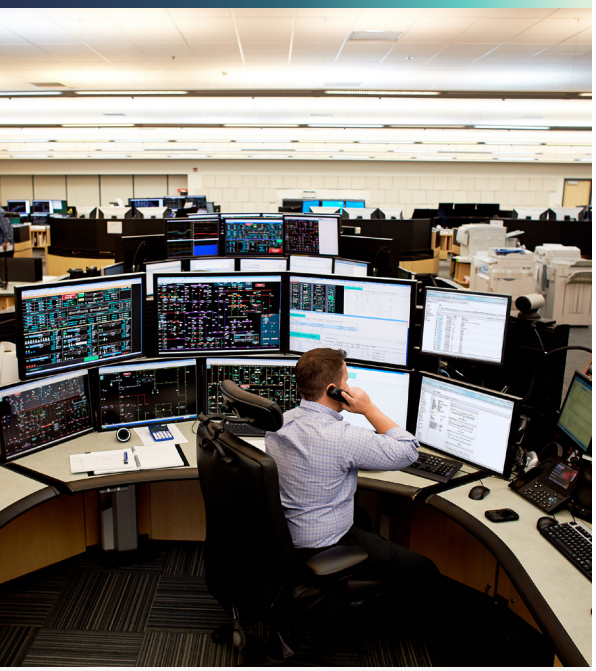
At-a-Glance



"Cybersecurity vendors are aware that utility data infrastructures and their associated OA&M require specialized architectural constructs. These environments have specific security posture visibility needs as well as industry specific status and compliance reporting requirements. For years, we've been engaged with Cisco, who has demonstrated active engagement in understanding utility customers and their unique security requirements."

Mike Prescher
Senior Security Architect,
Telecommunications
Black & Veatch

Substation Security Solution

NERC CIP Alignment

As attacks become more sophisticated and attackers more persistent, cybersecurity is critical to the reliability and resiliency of a nation's electric grid.

What if you could get complete and secure real time visibility and control at substations and control centers? Cisco Substation Security Solution enables utilities to do just that. This latest evolution of the Substation Security Solution helps enable utilities to meet the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) mandated standards to monitor, log, and diagnose systems with ease. The Cisco Validated Design solution eases the increasing burden of compliance reporting and audit response for utilities.

Overview

The NERC CIP compliance program improves reliability by enforcing compliance with NERC standards. The program ensures that accepted practices are in place so that the likelihood and severity of future system disturbances are substantially reduced, while recognizing that no standards or enforcement process can completely prevent all such disturbances from occurring.

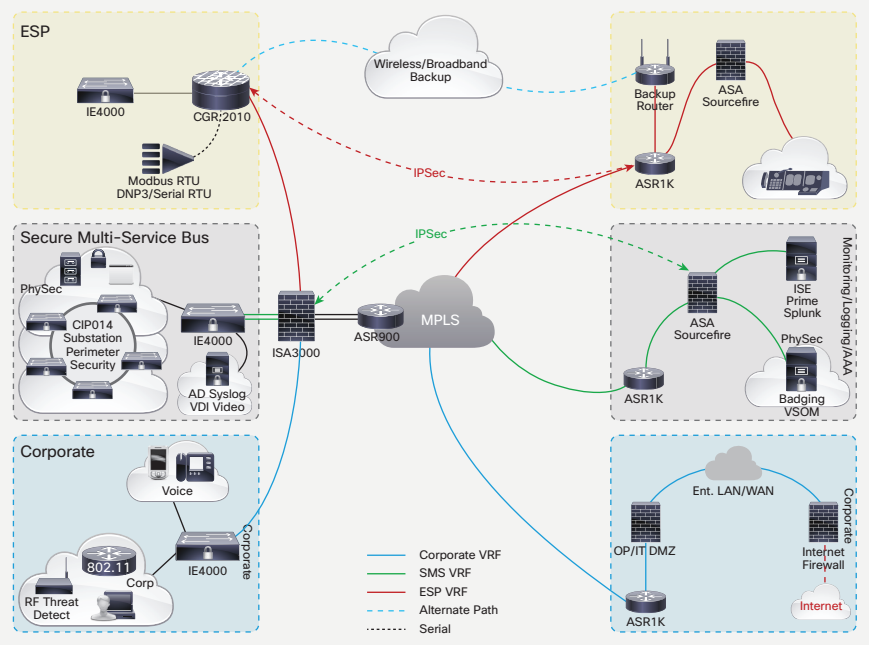
Aligning NERC Cybersecurity Mandates and Cisco Solutions

NERC CIP mandates both cybersecurity and physical security protection. Some of the most critical sections follow:

CIP #	Mandate Description	Cisco Solution	Comments
CIP-002-5	BES Cyber System Categorization	n/a	Utilities' responsibility
CIP-003-5	Security Management Controls	✓	
CIP-004-5	Personnel and Training	n/a	Utilities' responsibility
CIP-005-5	Electronic Security Perimeters	✓	
CIP-006-5	Physical Security of BES Cyber Systems	✓	
CIP-007-5	System Security Management	✓	
CIP-008-5	Incident Reporting and Response Planning	n/a	Utilities' responsibility
CIP-009-5	Recovery Plans for BES Security Systems	n/a	Utilities' responsibility
CIP-010-1	Configuration Change Management and Vulnerability Assessments	✓	
CIP-011-1	Information Protection	✓	
CIP-014-1	Physical Security	✓	

The Substation Security Solution (Figure 1) makes use of the Cisco ISA-3000 security appliance with integrated capabilities for firewall, and encryption and intrusion prevention systems (IPSs), including supervisory control and data acquisition (SCADA) signatures. It is designed to operate in harsh environments with high electromagnetic interference (EMI), meeting or exceeding the certifications for substation use. The ISA-3000 builds on decades of Cisco experience in network security.

Figure 1. Cisco Substation Security Solution



Build Smarter, Safer, More Secure Electric Grids

Benefits of the Cisco Substation Security Solution include:

- **Define and enforce** electronic security perimeter.
- **Enforce access control** of interactive user.
- **Identify and inventory** all known enabled default or other generic account types.
- **Monitor and report** incidents and help plan responses.

Cisco has deployed solutions to help meet security requirements worldwide including NERC CIP mandates at leading utilities in North America.

Next Steps

To learn more about the Cisco Substation Security Solution, contact your local Cisco representative, email us at nerc-cip@cisco.com, or visit www.cisco.com/go/smartgrid.

C45-735700-01 04/16