Cisco Connected Grid Security Readiness Assessment Services for NERC CIP

NERC CIP: North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards are intended to protect and improve the reliability of the bulk power system. These standards apply to the users, owners, and operators of the bulk power system and are mandatory in the United States as approved by the U.S. Federal Energy Regulatory Commission (FERC). NERC is authorized by FERC to impose penalties for violations of the reliability standards.

Today's utilities face the significant challenge of providing critical infrastructure security for the bulk electric power system, in compliance with the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards. NERC CIP regulates the requirements for monitoring and securing access to critical cyberassets across the grid and mitigating potential threats.

Cisco helps utilities conform to industry standards, regulations, and best practices through its Connected Grid Security Services for NERC CIP. This service includes a readiness assessment plan to help electric utilities prepare for compliance by identifying and remediating gaps in their ability to meet regulatory requirements.

The Future Evolution of NERC CIP

Compliance readiness is becoming even more complex as NERC CIP evolves toward a systemwide approach to reliability assurance. Under the direction of the Federal Energy Regulatory Commission (FERC), NERC is accelerating development and adoption of revised standards to expand the requirements and coverage of critical electrical and cyber assets. CIP Version 4 is currently under FERC review. It includes "bright-line" critieria for critical asset identification, shifting the focus more toward reliability functions and measures to assure pervasive security throughout the utility environment. At the same time, Version 5 is being developed to include a number of tactical as well as holistic changes.

NERC CIP and the Communication Network

The communications fabric plays a central role in operations risk and NERC CIP compliance management. Network security controls enable the necessary monitoring and reporting of critical assets and business processes. If network security controls are not properly designed and implemented, the availability, integrity, and confidentiality of information and business-critical processes can be compromised. Securing utility networks for ongoing compliance helps utilities avoid potential penalties, increases consumer confidence, and speeds adoption of smart grid technologies.

However, compliance with NERC CIP standards requires comprehensive cybersecurity solutions, including segmentation, authentication, authorization, monitoring, and logging, as well as physical security solutions, such as access control and video surveillance, deployed using a purpose-built end-to-end network architecture. Cisco is closely following the development and evolution of NERC CIP and is working with industry leaders to develop intellectual capital and methodologies to help utilities assess compliance readiness.

Connected Grid Security Readiness Assessment Service

The Cisco® Connected Grid Security Readiness Assessment Service for NERC CIP provides the following benefits:

- NERC CIP technical readiness gap identification
- Physical security design and remediation plan
- Information security planning, design, and strategy
- Remediation and mitigation planning for compliance gaps
- Strategic planning, assessment, and design of security infrastructure
- Performance tuning and ongoing optimization of security infrastructure

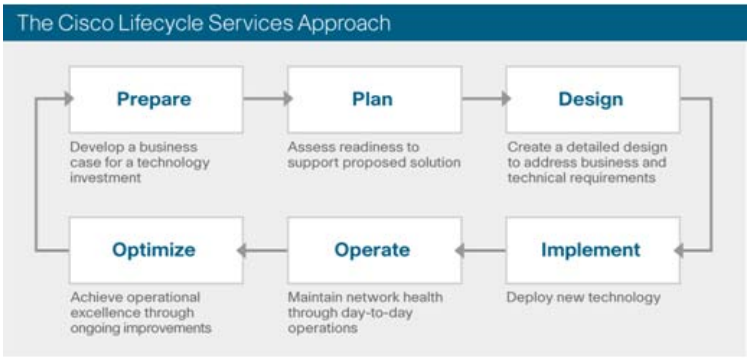
Service Activities and Deliverables

Activities	Deliverables
Cisco Security Readiness Assessment for NERC/CIP Service • Assess current policies, processes, and security requirements • Work with stakeholders to verify the accuracy of the identified critical cyberassets; identify and assess management and policy controls • Review policies, procedures, and practices for employee hiring, training, and access management • Assess personnel awareness of the standards and training • Review current state of compliance program, including organizational and operating structure • Assess the critical asset network for type and placement of electronic security perimeter(s) and identify gaps with NERC CIP requirements; evaluate entry and exit points into the electronic security perimeter • Conduct communication reviews of onsite technologies (PLCs, HMIs, RTUs) to assess their capabilities (availability, security, and so on) in meeting the requirements • Evaluate practices for remote access architectures as well as network and system management practices • Review the current physical access security plans, controls, and procedures • Review the current level of logging, asset monitoring, incident response, and log retention policies • Review business continuity plans as well as backup and restore procedures for critical cyberassets • Review compliance program's roadmap and ability to scale to newer versions of the standard	**Readiness Assessment Report** • The readiness assessment report details gaps in the utility environment for compliance with NERC/CIP requirements • Recommendations for addressing findings through mitigation planning • Recommendations for readiness in transition and migration to future versions of NERC/CIP
Cisco Security Architecture Assessment Service • Review security business goals, objectives, and requirements • Review security architecture and design documentation, including physical and logical designs, network topology diagrams, device configurations, and blueprints with the Cisco Security Control Framework as reference • Evaluate whether the existing security infrastructure conforms to each of the recommended controls as described in the Cisco Security Control Framework is present in the security infrastructure • Evaluate effectiveness of controls implemented in the security infrastructure based on the Cisco Security Control Framework to define its designated security function • Evaluate the security architecture for scalability, performance, and manageability; identify vulnerabilities in the security infrastructure • Provide a metrics-based report that highlights the critical assets and risks and identifies security gaps • Provide an executive presentation of findings and prioritized recommendations	**Security architecture assessment report** • The security architecture assessment report outlining the architectural gaps and detailing the security architecture roadmap and end state • Indicating the overall effectiveness of the security infrastructure
Cisco Remediation Assessment Service • Identify business-critical networks and assets to qualify risk and prioritize recommendations and remediation efforts • Identify and confirm the presence of security vulnerabilities in the IT infrastructure through expertise, tools, and data from Cisco Security Intelligence Operations, a cloud-based solution that synthesizes and analyzes threat information • Simulate typical malicious activities in a test environment to confirm the presence of vulnerabilities and the level of unauthorized access they can expose • Provide an assessment report containing: ◦ Detailed analysis of simulated attacks to identify critical vulnerabilities ◦ Comparison of assessment results with recommended industry best practices and operational requirements ◦ Recommended prioritization of vulnerabilities based on risk to the organization ◦ Recommended actions to remediate vulnerabilities and improve the organization's security posture • Evaluate end devices, communication flows, and protocols and technologies for vulnerabilities • Evaluate auditing and logging functionalities in end devices • Deliver executive presentation of findings and recommendations	**Security Remediation Report** • A formal report and executive presentation detailing prioritized and actionable recommendations based on the identified and confirmed vulnerabilities affecting critical assets and data

Why Cisco Services?

Cisco Services provides a team of experts and partners with the mission of helping utilities to plan, build, and run future-state grid security architectures, including physical security, network security, and other advanced capabilities. Its unique Cisco Lifecycle approach defines the requisite activities at each phase of the utility lifecycle to help ensure service excellence. Offerings include defining security requirements, developing forward-looking architectures, coordinating the deployment and integration of security solutions, and delivering ongoing optimization and managed services. Cisco Services provides:

- Industry-leading security expertise in designing and deploying large-scale, mission-critical networks for two decades for some of the largest IP-based deployments in the world
- Expertise specific to electric utilities, their communications, and security requirements



Availability and Ordering Information

Cisco Connected Grid Security Services are available globally. Service delivery details may vary by region.

For More Information

Cisco has created NERC CIP-validated architectures as part of the Cisco Connected Grid Solution. For more information about Cisco and NERC CIP, including architectural services for the smart grid, visit http://cisco.com/go/smartgrid or contact your local account representative.

Cisco services. smarter together

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C78-677407-00 06/11