

# Cisco NERC-CIP Reporting Architecture

Ecosystem partners are a critical and integral part of Cisco Smart Grid solutions. As an approved Cisco Developer Network (CDN) Connected Energy Partner, Cisco will provide you documentation and resources to support integration with Cisco Secure ACS, Cisco LMS and the combined Cisco Connected-Grid devices necessary to deliver a NERC-CIP reporting application.

Security Information and Event Management (SIEM) is a critical part of substation network management that addresses security monitoring and regulatory compliance issues and critical to the NERC-CIP reporting function. Through the CDN program, ecosystem partners can be certified to be interoperable with the Cisco Substation Automation solution to provide a comprehensive NERC-CIP reporting function.

This document provides a brief introduction to NERC-CIP reporting and Cisco’s architecture for integration and interoperability with partners to provide NERC-CIP reporting.

## Introduction to NERC-CIP

By definition, the North American Electric Reliability Corporation (NERC) is a nonprofit corporation designed to “ensure that the bulk electric system in North America is reliable, adequate and secure.” As the federally designated Electric Reliability Organization (ERO) in North America, NERC maintains comprehensive reliability standards that define requirements for planning and operating the collective bulk power system. Among these are the Critical Infrastructure Protection (CIP) Cyber Security Standards, which are intended to ensure the protection of the Critical Cyber Assets that control or affect the reliability of North America’s bulk electric systems.

In 2006, the Federal Energy Regulatory Commission (FERC) approved the Security and Reliability Standards proposed by NERC, making the CIP Cyber Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system. After going into effect in June 2006, initial compliance auditing began in June 2007.

There are currently eight standards (see Figure 1 NERC-CIP Security Standards) and 41 published requirements in CIP supporting reliable operation of the bulk electric system transmission automation security. Just as with all standards, continuous evolution is imperative and NERC-CIP is no exception. Details of new standards and requirements can be found at the following URL: <http://www.nerc.com/>.

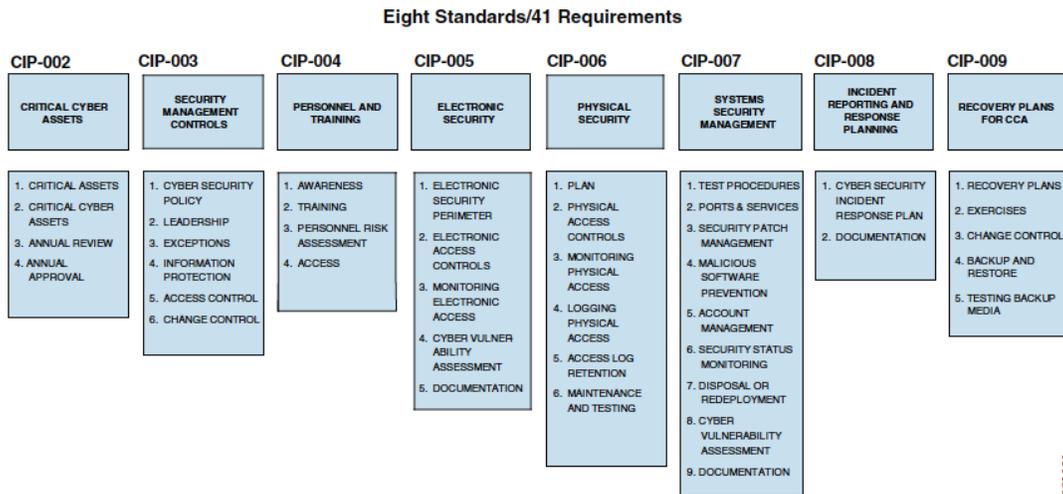


Figure 1 NERC-CIP Security Standards

## Cisco NERC-CIP Reporting Architecture

The SIEM function typically consists of Security Event Management (SEM) and Security Information Management (SIM). SEM improves security incident response capabilities by processing near real-time data from security appliances, network devices and systems to provide real-time event management for security operations. SEM helps substation security operations personnel be more effective in responding to external and internal threats. Complementary to SEM, SIM provides reporting and analysis of security event data to support security policy compliance management, internal threat management and regulatory compliance initiatives. The NERC-CIP reporting is provided by SIM.

Security Information Management (SIM) typically consists of a system where log data is analyzed for compliance reporting and privileged user and resource access. Log data sources include host system and security logs, database activity and audit logs, directories, identity and access management (IAM) systems, application logs, and transaction logs. Partner NERC-CIP reporting tools must integrate with a SEM system seamlessly and follow the Cisco NERC-CIP reporting architecture depicted below.

## Cisco NERC-CIP Reporting

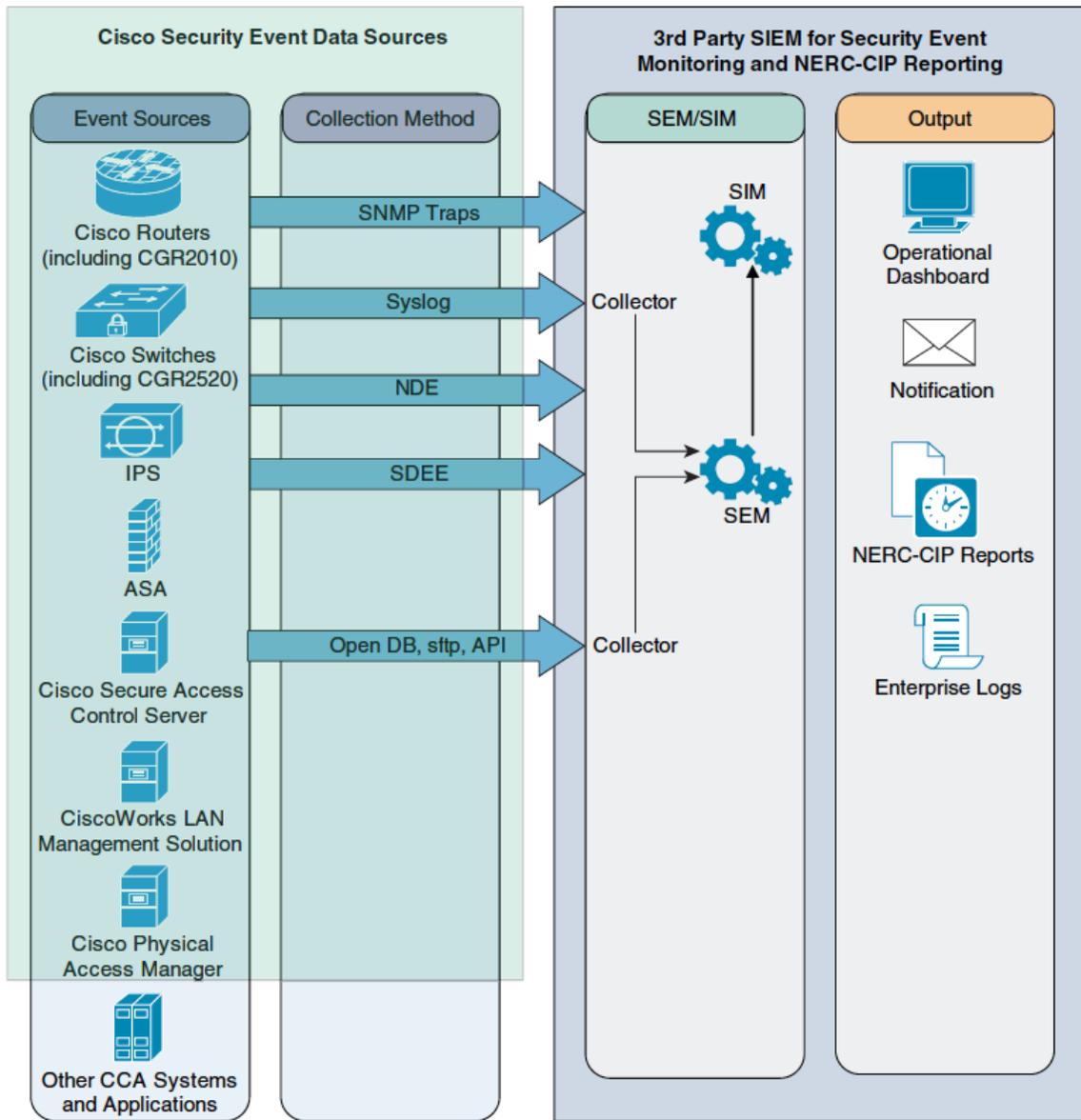


Figure 2 Cisco NERC-CIP Reporting Architecture

NERC-CIP reports are required for Critical Cyber Assets. Partner compliance reporting tools will be used to generate NERC-CIP reports for substation compliance audit.

The NERC-CIP partners reporting tools must:

- Collect CIP required data and be able to provide complete CIP required reports.
- Integrate with a Security Event Management (SEM) system seamlessly, or provide the SEM function.
- Be able to backup/restore.
- Provide the ‘canned’ (or predefined) CIP report templates that are common to most of the utility customers.
- Support the identification of Critical Cyber Asset (CCA)

## Cisco NERC-CIP Reporting Architecture

Cisco Secure ACS will typically be deployed to provide RADIUS/TACACS+ services managing user/device access to the substation network, authorizing the services those users/devices are allowed to invoke, and accounting for usage of it.

Cisco Management for Smart Grid Substation Automation provides FCAPS management of Cisco's Connected-Grid routers and switches, for Smart Grid primary substation automation in utility networks. This includes support for NERC-CIP reporting delivered through integration with partner products so utility customers may achieve regulatory compliance.

Ecosystem partners who complete integration will deliver a set of NERC-CIP reports that represent the latest published industry standards and support for Cisco Connected-Grid devices and management data.

By the definitions of CIP standards, critical assets of bulk electric systems include the following:

- Utility Facilities and backup Utility Facilities
- Transmission substations
- Generation resources
- Systems critical to system restoration
- Systems to automatic load shedding of 300MW or more
- Special Protection System
- Any additional assets that support the reliable operation

CCAs are the entities essential to the operation of the critical asset. The CCAs use a routable protocol within a utility facility or communicate outside the electronic security perimeter. Examples of critical cyber assets include the following:

- Monitoring and control systems at master site and remote site
- Automatic generation control
- Real-time power system modeling
- Real-time inter-utility data exchange

Partner NERC-CIP reporting application support must be able to do the following:

- Collect cyber security related events via SNMP traps, syslog, NDE (routing devices only), SDEE (routing devices only), and process these networking events and archive the relevant data per CIP requirements.
- Change logs including those changes made by the network management tool – CiscoWorks LMS 4.0. The required change logs include the device configuration changes and device image updates.
- User identity management. This includes user identity administration (e.g. Add/delete a user) by Cisco Secure ACS 5.1 and collecting user access logs such as ACS RADIUS user access and TACACS+ user access logs.
- Cisco Physical Access Manager (CPAM).