



# NERC CIP Compliance

## Automated NERC CIP reporting solution

Electric utilities that contribute to the bulk electric system (BES) must assure cybersecurity for their control systems cyber assets by complying with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards. Electric utilities subject to NERC CIP audits must continually adhere to the requirements and protect their cyber assets appropriately or face steep fines.

### Unique Challenges

The NERC CIP audit process presents a unique set of challenges for electric utilities including:

- ▶ Collecting information from multi-vendor control system environments
- ▶ Producing necessary reports and documentation for auditors
- ▶ Collecting and archiving all compliance related data
- ▶ Continually assuring information collection is accurate and systems remain compliant
- ▶ Managing labor intensive processes with minimal resources



Save time, money  
and labor when  
fulfilling NERC CIP  
audit requirements.

## THE CURRENT REGULATORY ENVIRONMENT

Although responsible entities are currently required to comply with Version 3 of the NERC CIP standards, Version 5 has been approved and will come into effect April 1st, 2016, superseding Version 4.

NERC CIP version 5 standards bring a number of changes from previous versions including a risk-based criteria, and two new CIP standards: CIP- 010-1 Configuration Change Management & Vulnerability Assessments, and CIP-011-1: Information Protection.

## EASING THE COMPLIANCE BURDEN

Leidos' Industrial Defender Solutions are helping electric utilities large and small all over North America automate their NERC CIP reporting. Industrial Defender ASM™ is the only product exclusively built for industrial control systems that provides a single, unified view into your heterogeneous and geographically dispersed asset base.

Industrial Defender ASM is a turnkey solution for NERC CIP compliance that automatically collects and normalizes data from your control system assets, including those hard-to-reach industrial endpoints such

as RTUs, IEDs, and PLCs. Thanks to this automated data collection and the builtin NERC CIP reporting package, you can easily provide auditors with required reports reducing the manual effort associated with compliance by 80%.

"Faster, better audit results."

- NERC COMPLIANCE MANAGER, TOP 5 IOU

## INDUSTRIAL DEFENDER ASM ENABLES ELECTRIC UTILITIES TO:

- ▶ Automate NERC CIP compliance through automated data collection
- ▶ and reporting, reducing the complexity and workload of laborious, error-prone manual tasks
- ▶ Maintain system performance and reliability standards using configuration monitoring and exception notification features
- ▶ Ensure NERC CIP compliance with Industrial Defender ASM, the only technology purpose-built for control system security, compliance, and change management
- ▶ Future proof yourself against NERC CIP v5 requirements with change management functionality
- ▶ Build a sustainable compliance program leveraging Industrial Defender Solutions and deep domain expertise

"80% Reduction in our compliance documentation preparation"

- IT MANAGER, TOP 3 US UTILITY

Asset	User ID	Time
ASA55-JR-L2	root	10/11/2013 6:26:29 AM
ASA-L1	root	10/7/2013 12:47:54 PM
ASA-L1	root	10/8/2013 2:38:30 PM
ASA-L1-SCADA-FW	NOUSER	10/10/2013 4:15:36 AM
ASA-L1-SCADA-FW	root	10/10/2013 4:15:35 AM
108-pm-desktop	Administrator	10/7/2013 9:01:22 AM
108-pm-desktop	Administrator	10/7/2013 9:01:25 AM
108-pm-desktop	Administrator	10/7/2013 10:52:58 AM
108-pm-desktop	venkat	10/7/2013 9:03:00 AM
108-pm-desktop	venkat	10/7/2013 9:03:00 AM
108-pm-desktop	venkat	10/7/2013 10:05:03 AM
108-pm-desktop	venkat	10/7/2013 9:01:30 AM
108-pm-desktop	vpothamsetty	10/7/2013 9:04:49 AM
108-pm-desktop	vpothamsetty	10/7/2013 9:05:02 AM

Sample Reports

