

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Most Violated CIP Standards Webinar Series: CIP - 007

December 8 and December 9, 2010

Kevin Gronberg & Chris Hickman

Kevin.gronberg@nerc.net

202-942-8602

to ensure
the reliability of the
bulk power system

The NERC Board of Trustees Compliance Committee (BOTCC) has encouraged NERC and the Regions (via the Regional Compliance Implementation Group, RCIG) to conduct assessments that analyze the most frequently violated standards. The primary purpose of these analyses is to provide information on compliance including reasons for violations and to identification of process enhancements and lessons learned to assist Registered Entities in improving compliance.

Two Approaches moving forward

- Compliance Analysis Report
 - www.nerc.com/page.php?cid=3|329

- Webinars to share this information broadly in a training/workshop format that enables additional questions and information gathering

Webinar Series Schedule - 2010

- November 17th – CIP 004 1:30 EST
- November 18th – CIP 003 1:30 EST
- December 8th – CIP 007 12:00 EST
- December 8th – CIP 004 2:30 EST
- December 9th – CIP 003 12:00 EST
- December 9th – CIP 007 2:30 EST

- Training/Workshop designed to provide a summary of the issues causing the most violations with CIP 007
 - NERC Overview
 - Summary Overview of CIP's
 - Compliance versus Security
 - Overview of CIP 007
 - Summary & Discussion of CIP 007 Violations
 - Collection of questions for potential FAQ summary
- Not designed to be a mitigation workshop

- NERC is an international, independent, self-regulatory, not-for-profit organization, whose mission is to ensure the reliability of the bulk power system in North America.
- Designated the Electric Reliability Organization (ERO) per section 215 of the Energy Act as modified by the Energy Policy Act of '05.
- **Bulk Power System Oversight:**
NERC oversees reliability for a bulk power system that:
 - Provides electricity to 334 million people
 - Has a total electricity demand of 830 gigawatts (830,000 megawatts)
 - Has 211,000 miles or 340,000 km of high-voltage transmission line (230,000 volts and greater)
 - Represents more than \$1 trillion (US) worth of assets.

Critical Infrastructure Standards Scope

- Cyber

- Hardware
- Software



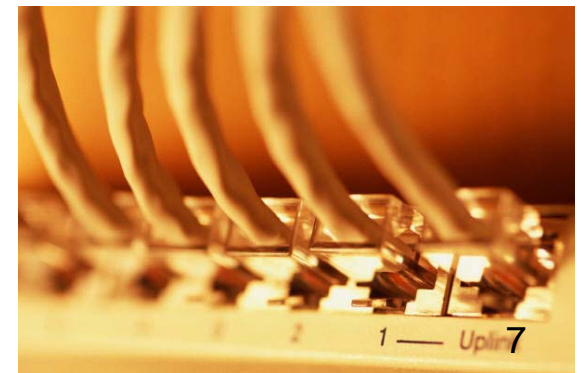
- Physical

- Cyber Equipment
- Control centers



- Communications

- Very Limited



- The Standards:
 - Provide a cyber security framework for the identification and protection of Critical Cyber Assets to support the reliable operation of the Bulk Electric System (BES).
 - Recognize the **differing roles** of the approximately 1800 registered entities in the operation of the BES the criticality and vulnerability of the assets needed to manage BES reliability, and the risks to which they are exposed.
 - Recognize that business functions and operational assets are **increasingly networked** together in order to effectively manage and maintaining a reliable BES. This results in increased risks to these Cyber Assets.

The Standards

- CIP 002 Critical Cyber Asset Identification
- CIP 003 Security Management Controls
- CIP 004 Personnel & Training
- CIP 005 Electronic Security Perimeter
- CIP 006 Physical Security for Critical Cyber Assets
- CIP 007 Systems Security Management
- CIP 008 Incident Reporting and Response Planning
- CIP 009 Recovery Plans for Critical Cyber Assets

“Version 1” of the standards effective through 3/31/10

“Version 2” of the standards effective 4/1/10 through 9/30/10

“Version 3” of the standards now in effect

Function Scattered within the Standards

NERC CIP CYBER SECURITY STANDARDS Eight Standards / 41 Requirements

<i>CIP-002</i>	<i>CIP-003</i>	<i>CIP-004</i>	<i>CIP-005</i>	<i>CIP-006</i>	<i>CIP-007</i>	<i>CIP-008</i>	<i>CIP-009</i>
CRITICAL CYBER ASSETS	SECURITY MANAGEMENT CONTROLS	PERSONNEL AND TRAINING	ELECTRONIC SECURITY	PHYSICAL SECURITY	SYSTEMS SECURITY MANAGEMENT	INCIDENT REPORTING & RESPONSE PLANNING	RECOVERY PLANS FOR CCA
<ol style="list-style-type: none"> 1. CRITICAL ASSETS 2. CRITICAL CYBER ASSETS 3. ANNUAL REVIEW 4. ANNUAL APPROVAL 	<ol style="list-style-type: none"> 1. CYBER SECURITY POLICY 2. LEADERSHIP 3. EXCEPTIONS 4. INFORMATION PROTECTION 5. <u>ACCESS CONTROL</u> 6. CHANGE CONTROL 	<ol style="list-style-type: none"> 1. AWARENESS 2. TRAINING 3. PERSONNEL RISK ASSESSMENT 4. <u>ACCESS</u> 	<ol style="list-style-type: none"> 1. ELECTRONIC SECURITY PERIMETER 2. <u>ELECTRONIC ACCESS CONTROLS</u> 3. <u>MONITORING ELECTRONIC ACCESS</u> 4. CYBER VULNERABILITY ASSESSMENT 5. DOCUMENTATION 	<ol style="list-style-type: none"> 1. PLAN 2. <u>PHYSICAL ACCESS CONTROLS</u> 3. <u>MONITORING PHYSICAL ACCESS</u> 4. <u>LOGGING PHYSICAL ACCESS</u> 5. ACCESS LOG RETENTION 6. MAINTENANCE & TESTING 	<ol style="list-style-type: none"> 1. TEST PROCEDURES 2. PORTS & SERVICES 3. SECURITY PATCH MANAGEMENT 4. MALICIOUS SOFTWARE PREVENTION 5. <u>ACCOUNT MANAGEMENT</u> 6. SECURITY STATUS MONITORING 7. DISPOSAL OR REDEPLOYMENT 8. CYBER VULNERABILITY ASSESSMENT 9. DOCUMENTATION 	<ol style="list-style-type: none"> 1. CYBER SECURITY INCIDENT RESPONSE PLAN 2. DOCUMENTATION 	<ol style="list-style-type: none"> 1. RECOVERY PLANS 2. EXERCISES 3. CHANGE CONTROL 4. BACKUP & RESTORE 5. TESTING BACKUP MEDIA

Security & Reliability vs. Compliance

- Goal is to increase Security & Reliability and Compliance is a natural outcome of process
- Lessons learned to date indicate need for expedited process for NERC guidance and potentially an auditor certification program
- New expedited process = Compliance Application Notice (CAN)
 - EX: Application Whitelisting adopted in Version 4 draft CIP language but potential compliance issue until Version 4 is released. (Security & Reliability is the goal and the best solutions should be utilized.)

Most Violated Standards

- CIP 002 Critical Cyber Asset Identification
- **CIP 003 Security Management Controls**
- **CIP 004 Personnel & Training**
- CIP 005 Electronic Security Perimeter
- CIP 006 Physical Security for Critical Cyber Assets
- **CIP 007 Systems Security Management**
- CIP 008 Incident Reporting and Response Planning
- CIP 009 Recovery Plans for Critical Cyber Assets

Webinar Series Presents View of Process

As this is the first Webinar Series introducing the information from the C.A.R. process, each of the CIP's are at a different stage in the process.

- CIP 004 was analyzed, draft report published reviewed and then approved and final report issued August 31, 2009
- CIP 007 was analyzed, draft report published in October 2010 and currently in final review for issuance in early 2011
- CIP 003 has been analyzed and the draft report is being drafted for publication and review in early 2011

Three Common Misunderstandings

A piecemeal approach to any CIP Standard will typically lead to problems in compliance. Examination of the entire standard, how it interacts with the other CIPs and formulating an approach to deal with each standard with a more holistic approach provides a better outcome.

Without documentation the policy can not be confirmed, nor can it be replicated with absolute fidelity. Documentation protects the entity when it comes to an audit but it also enables all elements of the entity to ensure they are following the same policies and processes.

The CIP's recognize that You are the expert on Your systems and therefore are in the best position to define the overall strategy to best protect these systems.

Since the beginning of the Critical Infrastructure Protection mandatory and enforceable standards on May 6, 2009, CIP-007 has quickly moved into one of the most violated reliability standards by Registered Entities. This standard is intended to ensure methods, processes and procedures for securing systems determined to be Critical Cyber Assets, as well as other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

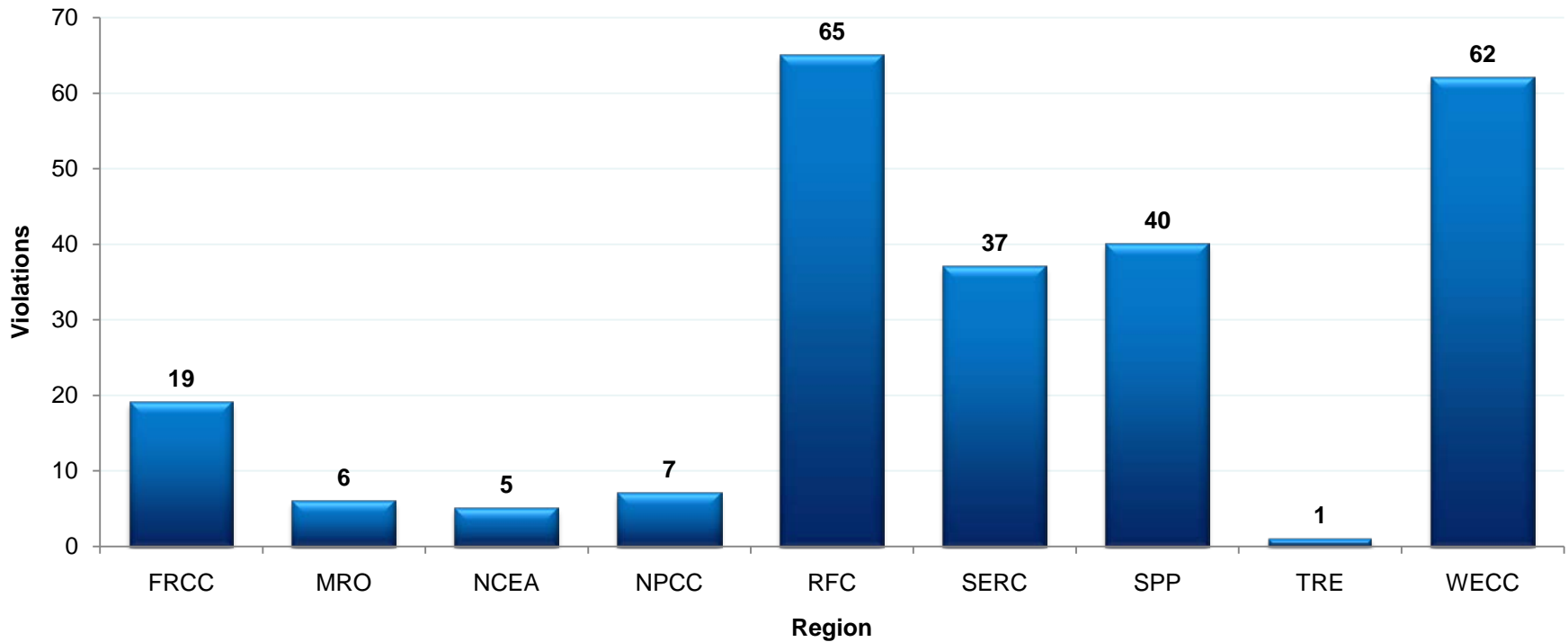
CIP-007 is in revision level 3 (FERC-approved) and has nine (9) top-level requirements and thirty-four (34) sub-level requirements.

CIP-007 Violations Summary

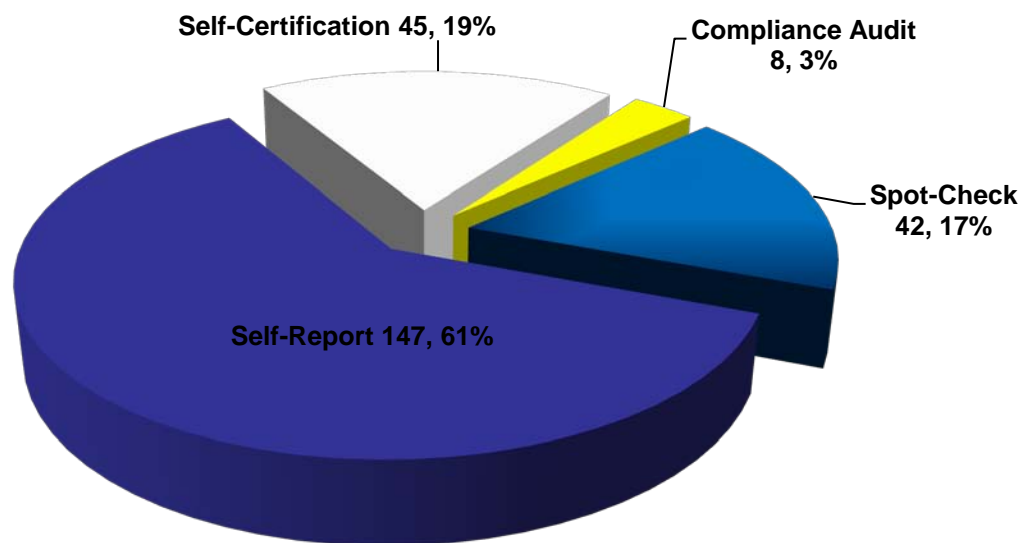
- 242 CIP-007 Violations*
- 12 Dismissed at Regional Entity Level
- Key Statistics
 - By Region
 - By Method of Discovery
 - By Requirement
 - By Date of Violation

*As of September 30, 2010

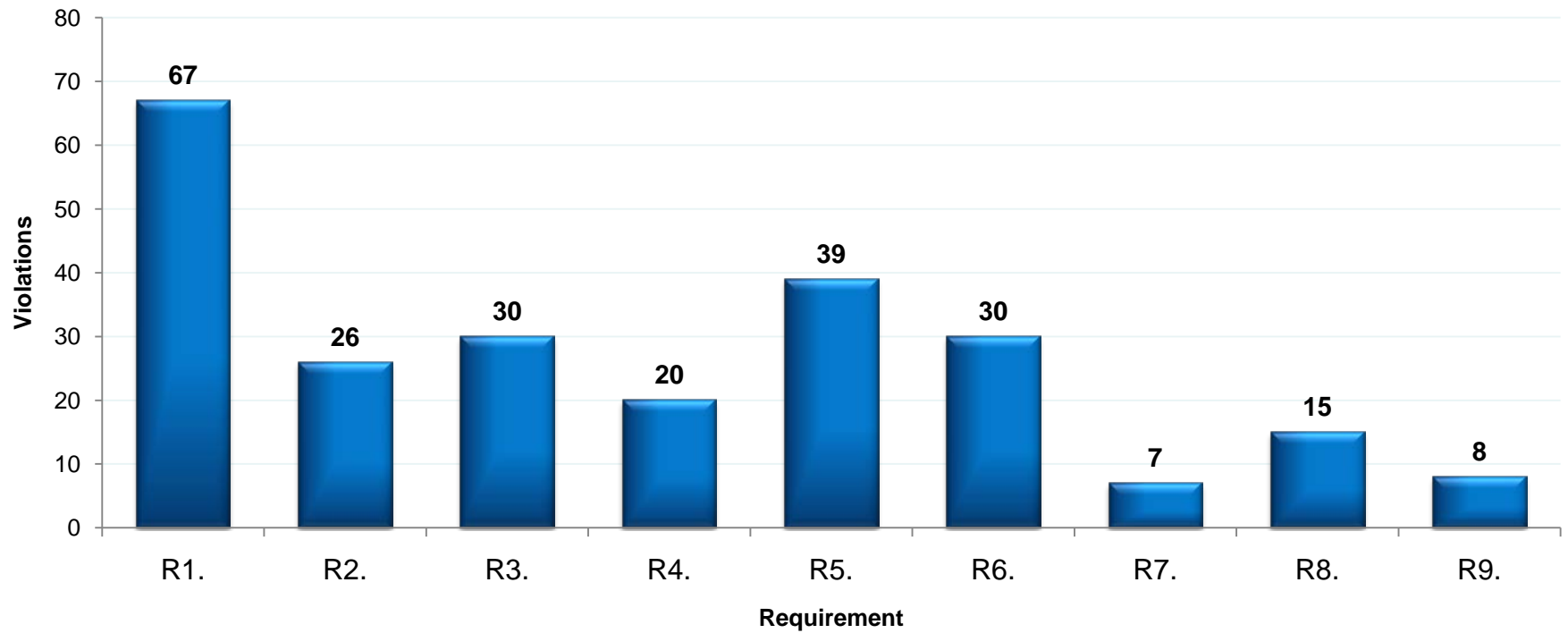
CIP-007 Violations by Region



CIP-007 Violations by Method



CIP-007 Violations by Requirement Level



C.A.R. for CIP 007(& 006) - On the way

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Electric Reliability Organization (ERO)
Compliance Analysis Report

Reliability Standard CIP-006 — Physical
Security of Critical Cyber Assets
Reliability Standard CIP-007 — Systems
Security Management

October 2010

to ensure
the reliability of the
bulk power system

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

Expected Date:

- Early 2011

Report will detail:

- Conclusions
- Examples
- Recommendations

Preliminary/Draft Observations

It is clear that requirements 1 (test procedures) and 5 (Account management) are the most violated.

It is important to note that Req. 1 applies to all cyber assets inside the electric security perimeter not just the critical ones as the potential for improperly tested equipment can impact others within the ESP. The implications for networked equipment goes beyond just the critical and all assets within the ESP.

Managing employees' logical access to cyber assets within the ESP is critically important yet can be difficult to handle with different employees handling different responsibilities on the same system. Entities need to fully understand the full implications of employees' access within the ESP and carefully manage that in the context of their business operations.

1. The entity failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within an ESP did not adversely affect existing cyber security controls.

R1. The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, and other third-party software or firmware.

Common Violation Descriptions cont.

2. Entity failed to fully establish and document a procedure to ensure only the ports and services required for normal and emergency operations are enabled.

***R2.** The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.*

3. Entity failed to document the assessment of security patches and upgrade availability within thirty calendar days of availability of the patches or updates.

***R3.** The Responsible Entity, either separately or as a component of the documented configuration management process, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security patches for all Cyber Assets within the Electronic Security Perimeter(s).*

4. Registered Entity failed to document and implement a process for the update of anti-virus and malware prevention tools (including “signatures”) and TFEs were not submitted.

***R4.** The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).*

5. The Windows and EMS/SCADA passwords were not changed and the account was not otherwise secured following the retirement of a dispatcher.

***R5.** The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authorization of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.*

6. The entity had cyber assets located within the ESP that were not configured to send log information to a centralized location for review.

R6. The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

7. The entity failed to destroy or erase data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7. The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

8. The entity failed to perform a cyber vulnerability assessment of all Cyber Assets at least annually.

R8. The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum: a document identifying the process; a review that only ports and services required for operation of Cyber Assets within the ESP are enabled; a review of controls for default accounts; and document of the results of the assessment.

Additional Resources

- Compliance Application Notices <http://www.nerc.com/page.php?cid=3|22|354>
- Compliance resources: <http://www.nerc.com/page.php?cid=3|22> includes RSAWs, Quarterly reports and Public Notices
- Compliance analysis reports: <http://www.nerc.com/page.php?cid=3|329>
- Reliability Standards: <http://www.nerc.com/page.php?cid=2|20>
- Standards under development: [http://www.nerc.com/filez/standards/Reliability Standards Under Development.html](http://www.nerc.com/filez/standards/Reliability_Standards_Under_Development.html)
- NERC Alerts: <http://www.nerc.com/page.php?cid=5|63>

