

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Most Violated CIP Standards Webinar Series: CIP - 003

November 18 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
- Please begin submitting questions now or as you think of them

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 003
 - NERC Overview
 - Summary Overview of CIP's
 - Compliance versus Security
 - Overview of CIP 003
 - Summary & Discussion of CIP 003 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



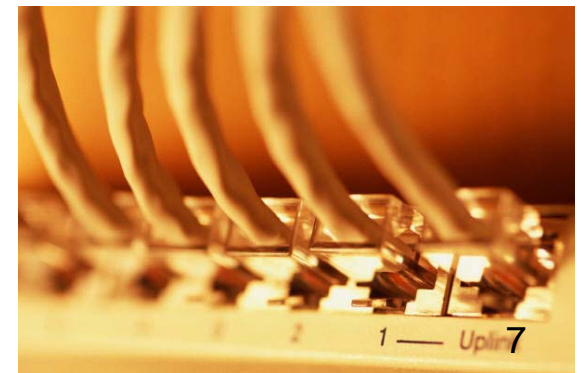
- Physical

- 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

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009
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 ASSETS2. CRITICAL CYBER ASSETS3. ANNUAL REVIEW4. ANNUAL APPROVAL	<ol style="list-style-type: none">1. CYBER SECURITY POLICY2. LEADERSHIP3. EXCEPTIONS4. INFORMATION PROTECTION5. <u>ACCESS CONTROL</u>6. CHANGE CONTROL	<ol style="list-style-type: none">1. AWARENESS2. TRAINING3. PERSONNEL RISK ASSESSMENT4. <u>ACCESS</u>	<ol style="list-style-type: none">1. ELECTRONIC SECURITY PERIMETER2. <u>ELECTRONIC ACCESS CONTROLS</u>3. <u>MONITORING ELECTRONIC ACCESS</u>4. CYBER VULNERABILITY ASSESSMENT5. DOCUMENTATION	<ol style="list-style-type: none">1. PLAN2. <u>PHYSICAL ACCESS CONTROLS</u>3. <u>MONITORING PHYSICAL ACCESS</u>4. <u>LOGGING PHYSICAL ACCESS</u>5. ACCESS LOG RETENTION6. MAINTENANCE & TESTING	<ol style="list-style-type: none">1. TEST PROCEDURES2. PORTS & SERVICES3. SECURITY PATCH MANAGEMENT4. MALICIOUS SOFTWARE PREVENTION5. <u>ACCOUNT MANAGEMENT</u>6. SECURITY STATUS MONITORING7. DISPOSAL OR REDEPLOYMENT8. CYBER VULNERABILITY ASSESSMENT9. DOCUMENTATION	<ol style="list-style-type: none">1. CYBER SECURITY INCIDENT RESPONSE PLAN2. DOCUMENTATION	<ol style="list-style-type: none">1. RECOVERY PLANS2. EXERCISES3. CHANGE CONTROL4. BACKUP & RESTORE5. 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 CIP draft 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.

CIP 003 Overview

- Cyber Security — Security Management Controls
- Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
- 6 Requirements
 - The entity shall have a cyber security policy
 - The entity shall identify a responsible senior manager for the policy
 - The entity shall document any exceptions to the policy
 - The entity shall protect information about critical cyber assets
 - The entity shall manage access to those critical cyber assets
 - The entity shall establish and document a change control process

Purpose of CIP-003

- The purpose of CIP-003 is really the purpose of all of the CIP standards to have Responsible Entities create minimum security management controls to protect their critical cyber assets.
 - Note: CIP-003 does not go into detail as to what the cyber security policy must contain, other than it should cover the requirements of CIP-002 through CIP-009. The details are left to the entity who is more familiar with its networks and systems.

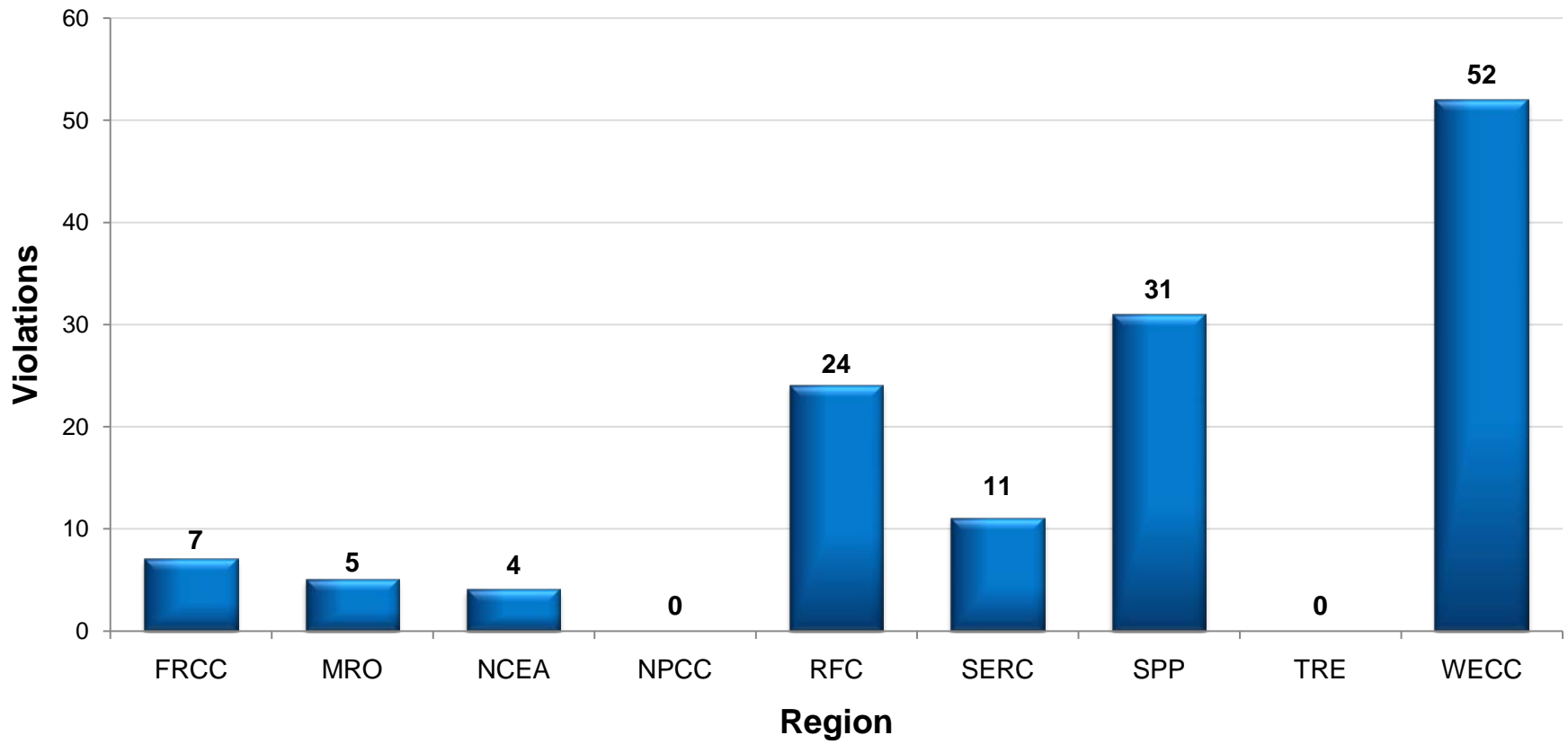
CIP-003 Violations Summary

- 125 CIP-003 Violations
- 9 Dismissed at Regional Entity Level
- Key Statistics
 - By Region
 - By Method of Discovery
 - By Requirement
 - By Date of Violation

*As of November 15, 2010

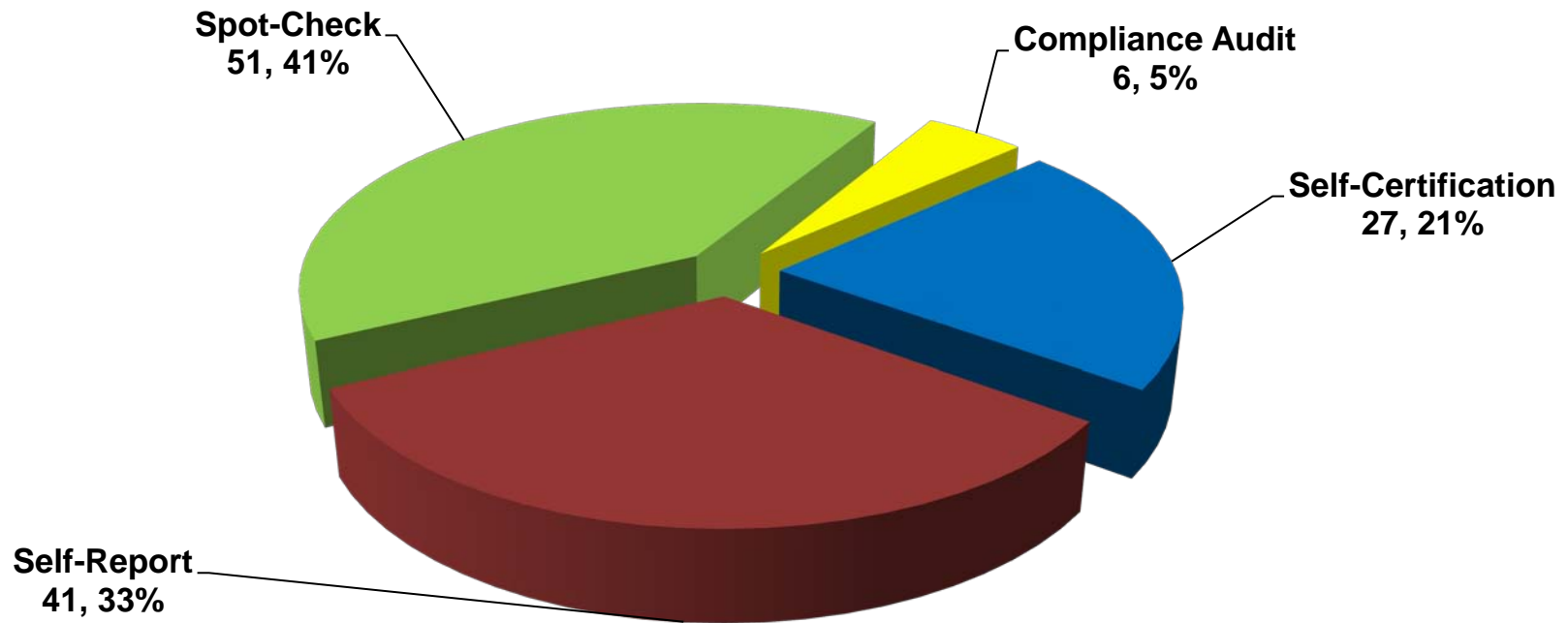
CIP-003 Violations Region

CIP-003 Violations by Region thru 11/15/2010



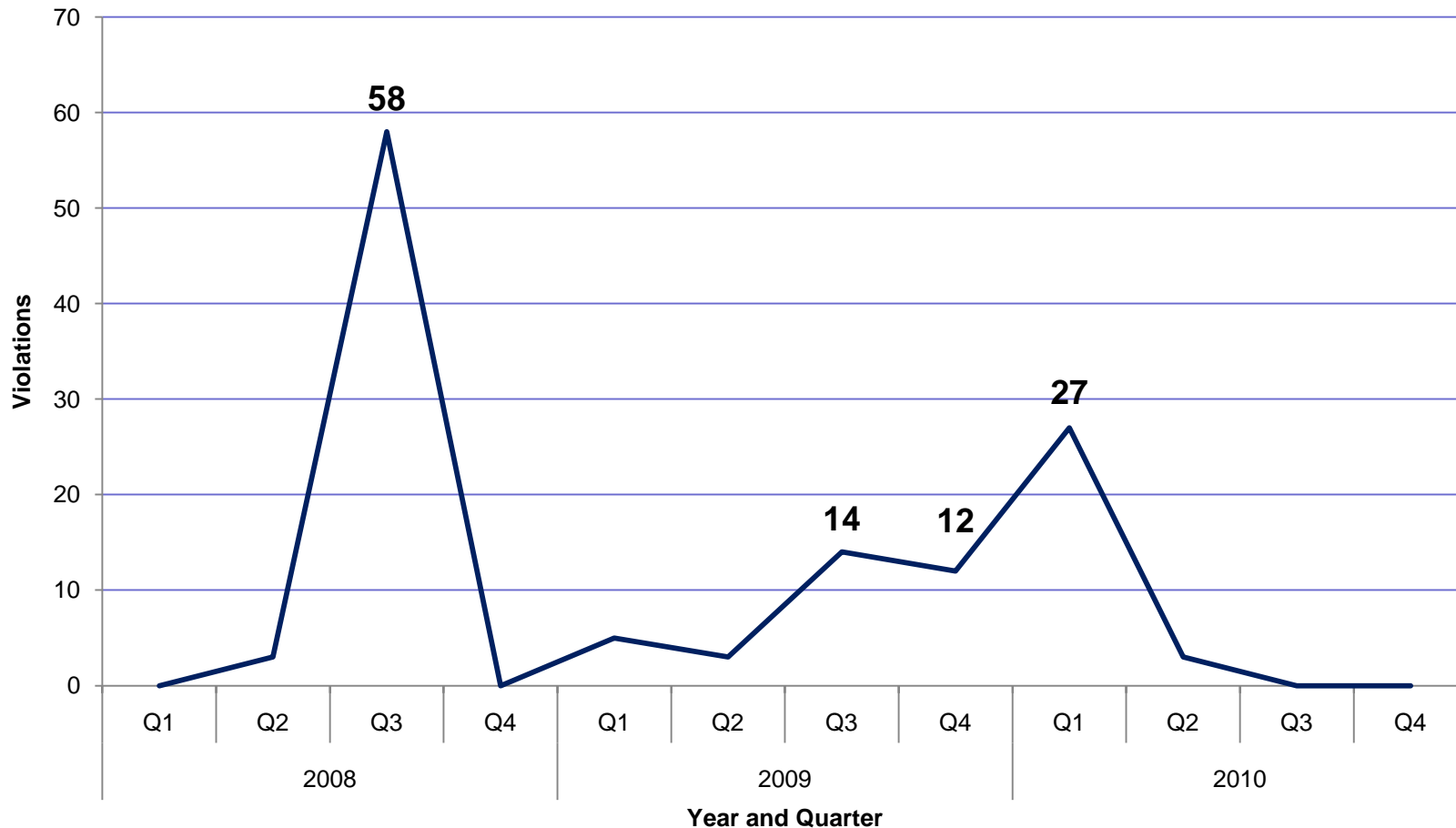
CIP-003 Violations Method of Discovery

CIP-003 Violations by Method of Discovery thru 11/15/2010



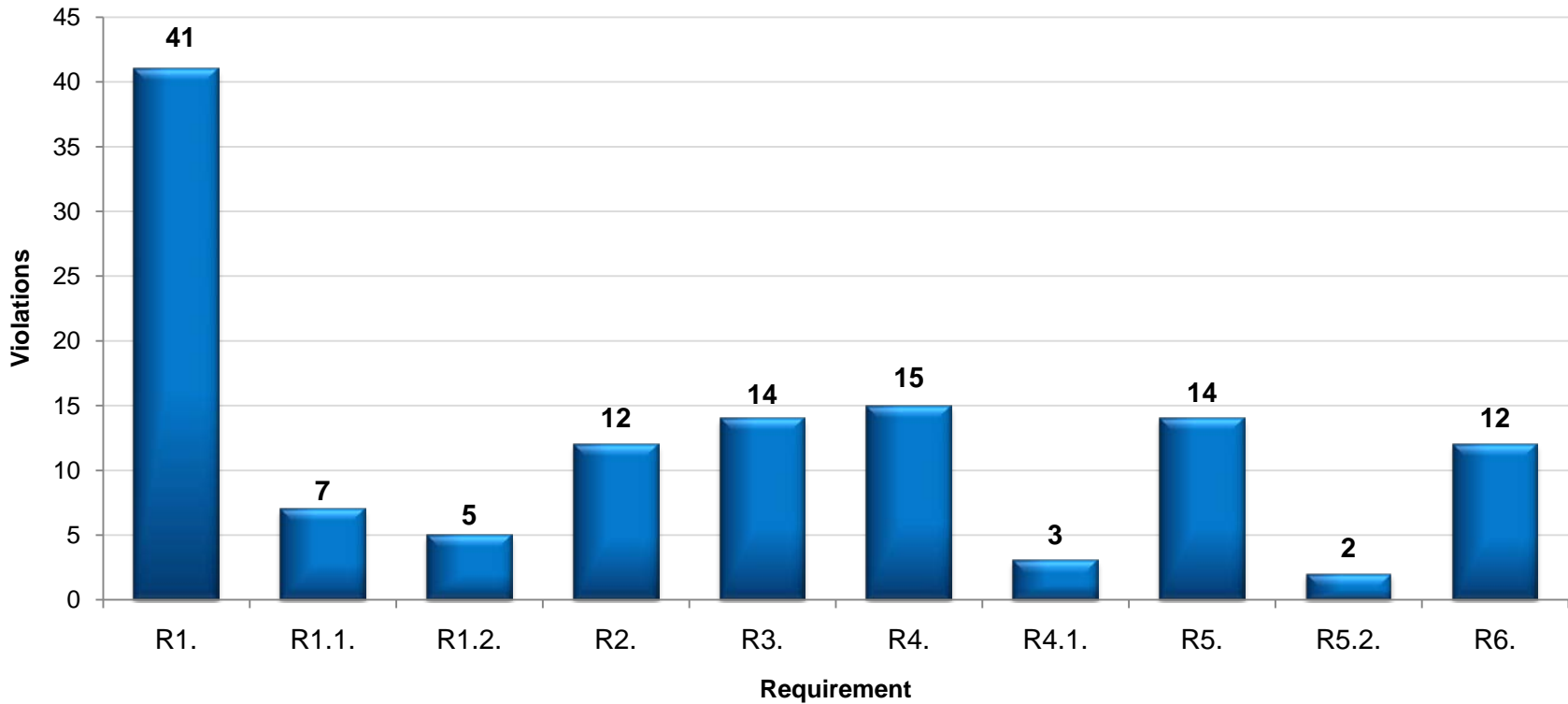
Violations by Date of Submission

CIP-003 Violations by Date of Occurrence



CIP-003 Violations Requirement

CIP-003 Violations by Requirement thru 11/15/2010



C.A.R. for CIP 003 on the way

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Compliance Analysis Report

to ensure
the reliability of the
bulk power system

111-190 Widge Blvd., Princeton, NJ 08540
609-412-9000 | 609-412-9500 Fax
www.nerc.com

Expected Date:

- Early 2011

Report will detail:

- Conclusions
- Examples
- Recommendations

One Preliminary Observation

A piecemeal approach to this (or any other 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.

Preliminary Observations continued

- The heart of CIP-003 is documentation. Each requirement, except R.2, mentions the need for documentation.
 - 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.

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>

