

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Most Violated CIP Standards Webinar Series: CIP - 004

November 17 and December 8, 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 004
 - NERC Overview
 - Summary Overview of CIP's
 - Compliance versus Security
 - Overview of CIP 004
 - Summary & Discussion of CIP 004 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



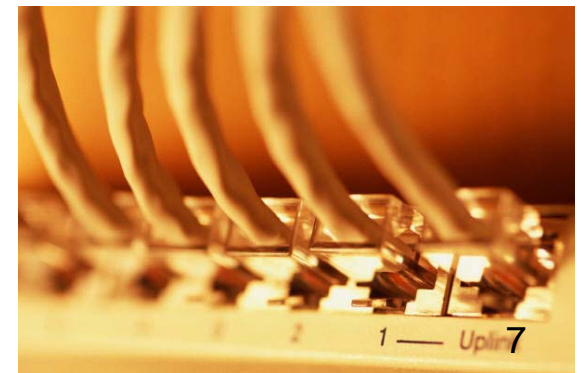
- Physical

- 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.

*CIP-004-1 is a key cyber security standard and has recently become an enforceable standard. CIP-004-1 became effective on July 1, 2008 for Registered Entities under urgent Action Directive 1200 and on July 1, 2009 for other entities and has become one of the reliability standards reported to be most frequently violated.

*C.A.R. published August 31, 2010. Remaining portion of presentation based on this C.A.R.

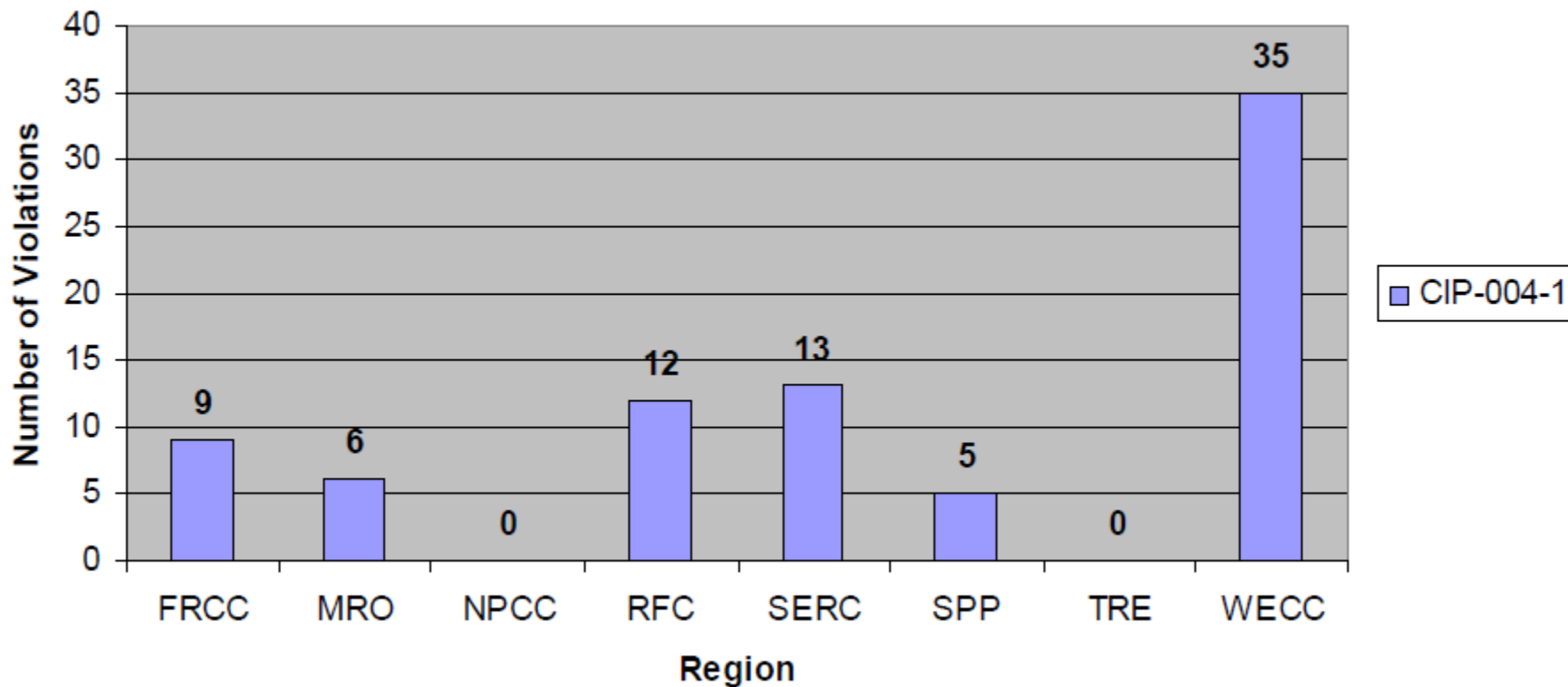
CIP-004 Violations Summary

- 80 CIP-004 Violations*
- 13 Dismissed at Regional Entity Level*
- Key Statistics
 - By Region
 - By Method of Discovery
 - By Requirement
 - By Date of Violation

*As of July 21, 2009

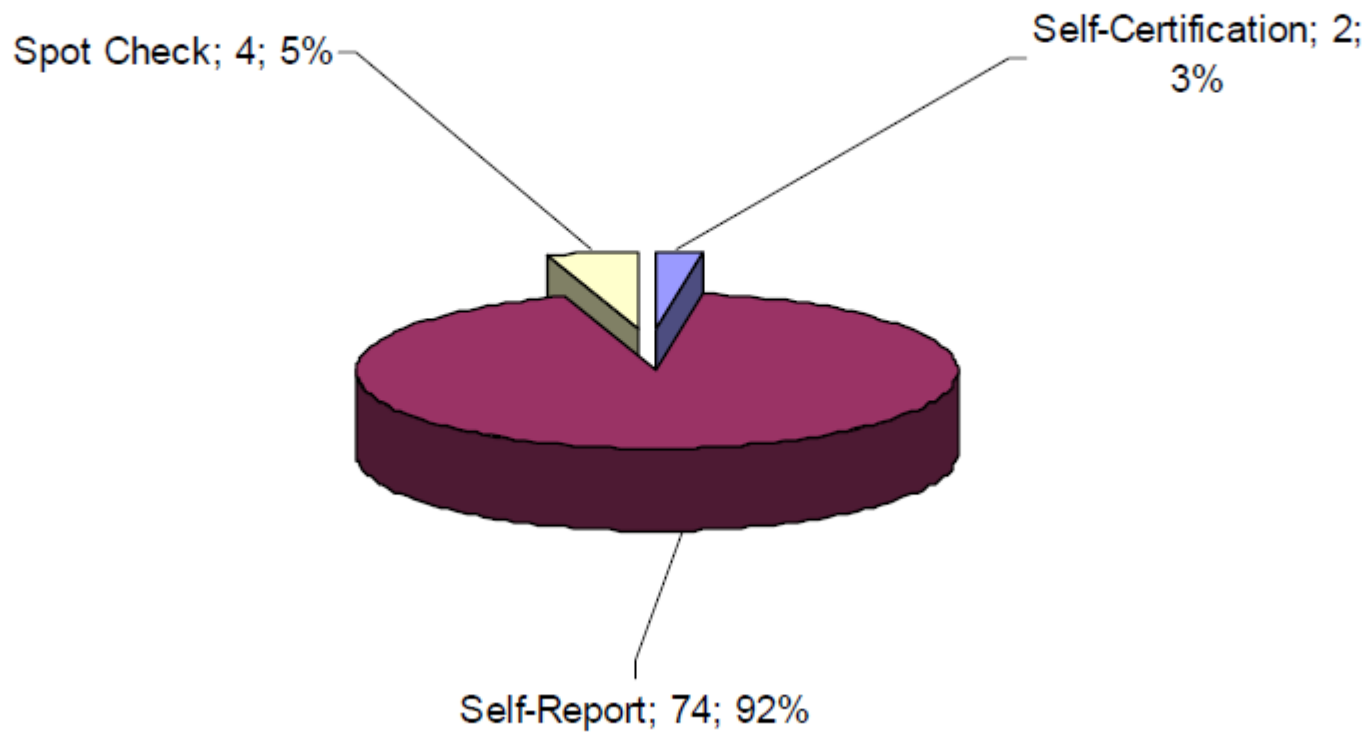
Violations by Region

CIP-004-1 Violations by Region



Violations by Discovery Method

CIP-004-1 Violations by Discovery Method



Violations by Requirement

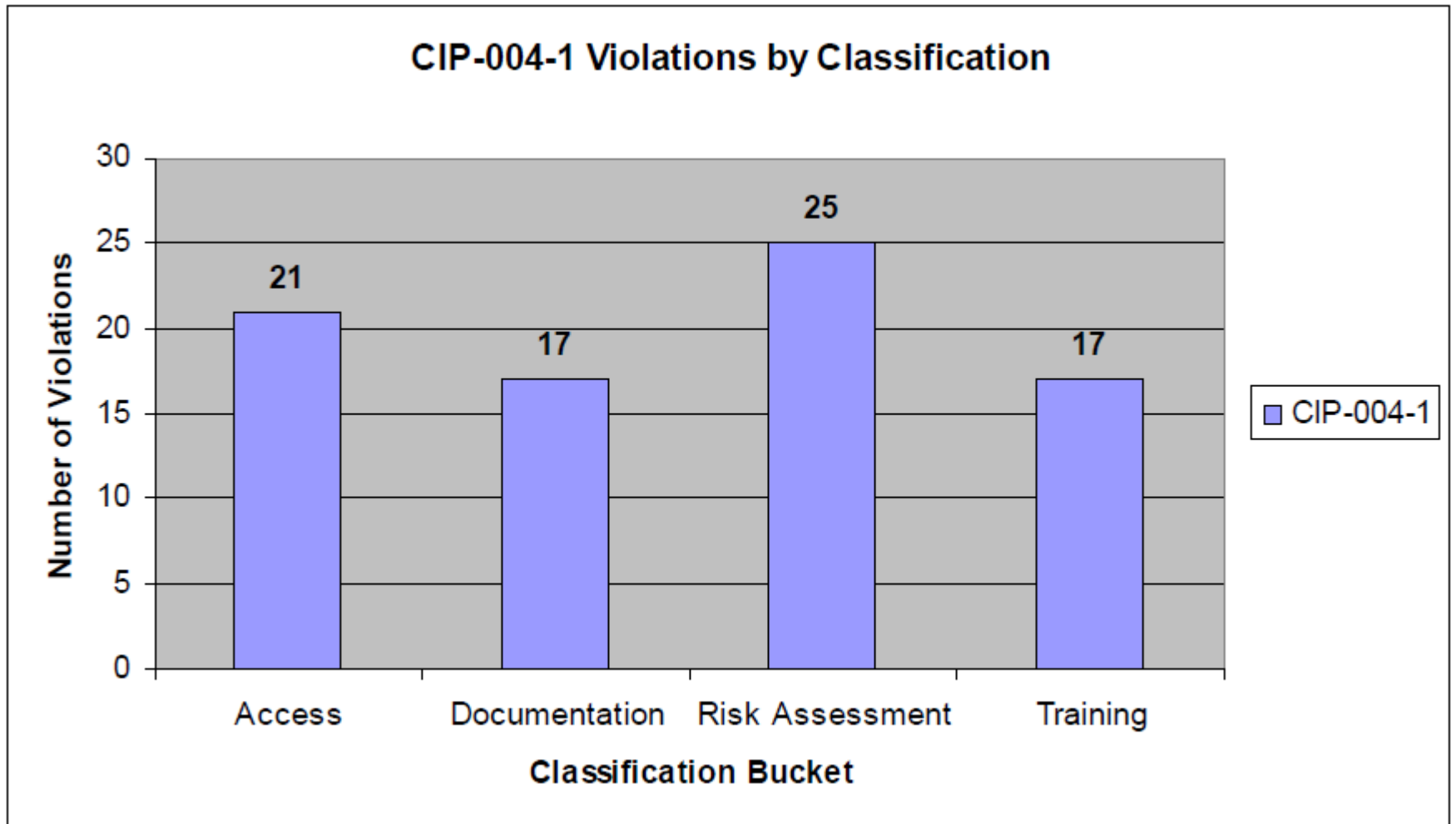
CIP-004-1 by Requirement	Number of Violations
Requirement 1 – Awareness (All Sub levels)	0
Requirement 2 – Training (All Sub levels)	23
Requirement 3 – Risk Assessment (All Sub levels)	29
Requirement 4 – Access (All Sub levels)	28
Grand Total	80

Classification of Violations

There are many reasons identified for non-compliance by Registered Entities, from documentation to performance-related issues. NERC classified the 80 violations of CIP-004-1 by four different types of violations given the information provided in the Violation Description and the Potential Impact fields of the Regional workbook submissions to NERC. The classification buckets are:

1. *Documentation - a lack of records to demonstrate compliance with the standard;*
2. *Access - employees or contractors granted access to critical cyber assets without proper clearance or escorted access;*
3. *Training - training was not offered or completed on time by employees or contractors ;*
4. *Risk Assessment - employees or contractors with access to critical cyber assets did not complete or had an incomplete background check*

Violations by Classification



When CIP-004-1 is applied in conjunction with the other cyber security standards of CIP-002-1 through CIP-009-1, it provides an effective component of defense-in-depth for Critical Cyber Assets. As this Analysis of CIP-004-1 Violations is still in the process of being phased in, a complete picture of cyber security gaps in Registered Entities can not be determined without more data. While CIP-004-1 has multiple sub requirements for each top level requirement, it appears to NERC that Regions are reporting violations without enough granularities to more clearly understand the nature of the violation at the sub requirement level, skewing any effective data analysis in the short term. As CIP-004-1 becomes compliant for all registered functions over the next year and half, more violations will be detected and discovered and a more accurate picture of cyber security will develop. But until that time, NERC is only left to conduct its analysis based on the data available, and right now it is an incomplete picture.

Examples/Suggestions from RCIG

RCIG – The Regional Compliance Implementation Group has provided examples and suggestions for each of these requirements in the Compliance Analysis Report.

More Examples in C.A.R.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Compliance Analysis Report
Reliability Standard CIP-004
Personnel and Training

to ensure
the reliability of the
bulk power system

August 31, 2009

111-190 Widge Blvd., Princeton, NJ 08540
609-412-9000 | 609-412-7500 Fax
www.nerc.com

www.nerc.com/page.php?cid=3|329

Common Violation Descriptions

R 2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

Example: Due to a late identification of one or more critical assets and associated Critical Cyber Assets, the entity did not have a documented cyber security training program by the time the entity was required to be fully compliant with the CIP Standard requirement.

Entity's training program documentation was not up to date

Example: The entity's training program was compliant with the CIP Standards requirements; however, the training policy and procedure were not up to date.

Suggested Enhancement: Need to ensure that the documentation of the program is reviewed and updated along with program changes and developments.

Common Violations Descriptions cont.

R.2.1 This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

Example 1: The entity granted temporary access for a period less than 90 days. The entity believed that since access was revoked before the 90 day training window expired, there was no longer a need to conduct the required training.

Example 2: The entity's access management policy required verification of the required cyber security training before granting access even though Version 1 allows training up to 90 days following access. However, the implementation procedures failed to include the verification step. As a result, personnel were found to have been granted access without having undergone the required training.

Example 3: In preparation for compliance with the requirement, the entity bulk uploaded a large number of employees into the access management and tracking system. Due to an administrative oversight, a small number of those employees did not receive the required training.

Example 4: Entity failed to apply training to its existing employees upon implementation of the program once the requirement reached the compliant stage.

Common Violations Descriptions cont.

R.2.1 cont.

Contractor/vendor support personnel not trained

- **Example:** The entity determined that contractors with authorized unescorted physical access had not completed the required cyber security training.

Suggested Enhancement: Ensure the access management program requires all personnel who are granted either authorized electronic or unescorted physical access to receive the training specified by the requirement. The personnel must include all personnel with such access, such as janitorial staff and maintenance personnel with unescorted physical access and vendor support staff who provide remote support of the Critical Cyber Assets or other cyber assets within the Electronic Security Perimeter.

Req 2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

Incomplete documentation

Example 1: The entity did not have records confirming that all required employees have completed the annual cyber security training.

Example 2: Entity lacked accurate training records demonstrating all employees, contractor, and vendor support staff had completed the annual cyber security training.

Suggested Enhancement: If training is conducted in a formal classroom setting, ensure all trainees have signed the dated class attendance roster. If training is computer-based, investigate utilizing technology that will automatically track progress and report completion of the training, preferably with a reporting database that can be queried. If static training materials, such as a PowerPoint presentation with or without voiceover, are distributed electronically or in hardcopy form, include a certification page that the trainee signs, dates, and returns. In all cases, follow up with scheduled trainees to ensure the training is completed within the required time frame and immediately revoke access at the end of the annual training window for any employee, contractor, or vendor support personnel who fail to complete the training.

R 3.2 The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

Seven year update not completed

Example 1: Entity discovered a number of personnel who had retained access without having updated their personnel risk assessment within the past seven years.

Example 2: Entity did not update the personnel risk assessment within seven years for a number of contractors.

Suggested Enhancement: Review records for existing employees, contractors, and vendor support staff to ensure the personnel risk assessment has been completed within the past seven years. Establish a suspense file to trigger a seven-year recheck in sufficient time to complete the assessment before the seven year expiration is reached. Federal agencies should consult with the Office of Personnel Management to determine if regulations permit a seven year criminal check and retain documentation of the determination.

After a thorough review of violation descriptions and potential impact statements submitted to NERC via the Regional Entities, the following recommendations can be made:

1. Entities need to ensure and verify that all employees with access to Critical Cyber Assets, including contractors and service vendors, have had the appropriate training within 90 days of authorization (V1), or prior to access (V2 & V3)
2. Entities need to ensure and verify that risk assessments on employees, contractors and service vendors with access to Critical Cyber Assets are not only completed within given time frames, but that the assessments focus on appropriate pieces of information
3. Entities need to ensure that appropriate changes are made to access lists upon the termination or transfer of employees from or to areas that contain Critical Cyber Assets, and that the access lists are frequently updated to contain contractors or service vendors.

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>

