

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## Electric Reliability Organization (ERO) Compliance Analysis Report

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

December 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](http://www.nerc.com)

## Table of Contents

---

ERO Compliance Analysis Reports.....	2
Summary of Practical Information and Suggestions.....	3
Analysis of CIP-006 Violations .....	4
Regional Entity Analysis of CIP-006.....	10
Recommendations to Revise the CIP-006 Reliability Standard.....	13
Analysis of CIP-007 Violations .....	14
Regional Entity Analysis of CIP-007.....	18
Recommendations to Revise the CIP-007 Reliability Standard.....	22
Conclusion .....	23

## ERO Compliance Analysis Reports

---

The ERO is comprised of NERC and Regional Entities. Their compliance staffs are collaborating on analysis of the Top 10 Violated Standards. This is the seventh report wherein NERC and the Regional Entity compliance staffs have publicly provided information and guidance on the most violated standards in order to facilitate compliance. This document further serves as a formal mechanism to provide feedback to the standards developers.

The next compliance analysis report for the ERO is expected to be submitted in the first quarter of 2011 to the NERC Board of Trustees Compliance Committee, and will cover EOP-005.

## Summary of Practical Information and Suggestions

---

This summary is intended to capture the analysis detailed below, by providing some essential elements of the requirements, and by offering some suggestions for consideration. It is not a complete list of all possible elements or actions. Evaluation or undertaking such actions or suggestions does not guarantee compliance and does not replace the NERC Reliability Standards language.

The industry is deserving of credit for the high percentages of self reports and self certifications for CIP-006 and CIP-007 violations. This is indicative of the complexity and newness of integrating the security requirements.

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

### **CIP-006**

- Responsible Entities should have a regular maintenance and testing plan as part of their larger Physical Security Program.
- Responsible Entities should perform a gap analysis and or regular testing of their physical security and access controls at access points to their Physical Security Perimeters.
- Responsible Entities should verify personnel with unescorted physical access have access to the necessary access methods such as key cards.
- Responsible Entities should ensure and reinforce through their annual Cyber Security Training the concepts of escorted and unescorted physical access to critical assets.

### **CIP-007**

- Responsible Entities shall have a test plan, follow their test plan, and document the results of their test plan.
- Responsible Entities should work with all vendors of systems and applications of applicable cyber assets in their infrastructure to determine required ports and services. Most if not all vendors will have some form of documentation detailing this information.
- Responsible Entities should consider leveraging a corporate level Patch Management Program if one does not exist for their Real-time systems area. Typically, the corporate level program will be established and include the necessary tracking, evaluating, testing, and installation of applicable cyber security patches required for all Cyber Assets within the Electronic Security Perimeter(s).
- Responsible Entities should baseline cyber asset logging service capabilities in a test, development, and or pre-production environment prior to moving a cyber asset to production.

## Analysis of CIP-006 Violations

---

### **Background**

Since the beginning of the Critical Infrastructure Protection mandatory and enforceable standards on May 6, 2009, CIP-006 has quickly moved into the top ten most violated reliability standards committed by registered entities. This standard is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Given the nature of these violations, NERC has performed an initial analysis of active and closed violations of this reliability standard to define prevailing trends. As of September 30, 2010, there are 103 violations of CIP-006 that are closed or active, with another five dismissed at the Regional Entity level.

CIP-006 is in revision level 3 (FERC-approved as of 10/1/2010) and has eight (8) top-level requirements and fifteen (15) sub-level requirements. For the purpose of consistency, all CIP-006 violations will be in the form of CIP-006-2. In the Revision History section the mapping of Requirements and sub-requirements will be shown for CIP-006-1, CIP-006-2, and CIP-006-3.

## Revision History

Of the 103 violations of CIP-006, 89 were violations when CIP-006-1 was enforceable, while 14 were violations when CIP-006-2 was enforceable. This is important to know because the Requirements changed from each version. Sub-requirements were rolled up into the Requirements, while two new Requirements were added with regard to the protection of physical and electronic access controls. For the ease of the reader, below is a mapping of each Requirement and sub-requirement for CIP-006-1, CIP-006-2 and CIP-006-3.

Three new additions for CIP-006-2 included:

- R2: Protection of Physical Access Control Systems
- R2.1: Be protected from unauthorized physical access
- R3: Protection of Electronic Access Control Systems

The sub-requirements for R2, R3, and R4 for CIP-006-1 have been rolled up into the high level requirement of R4, R5, and R6 respectively in the current enforceable CIP-006-2.

Revisions from CIP-006-2 to CIP-006-3 include:

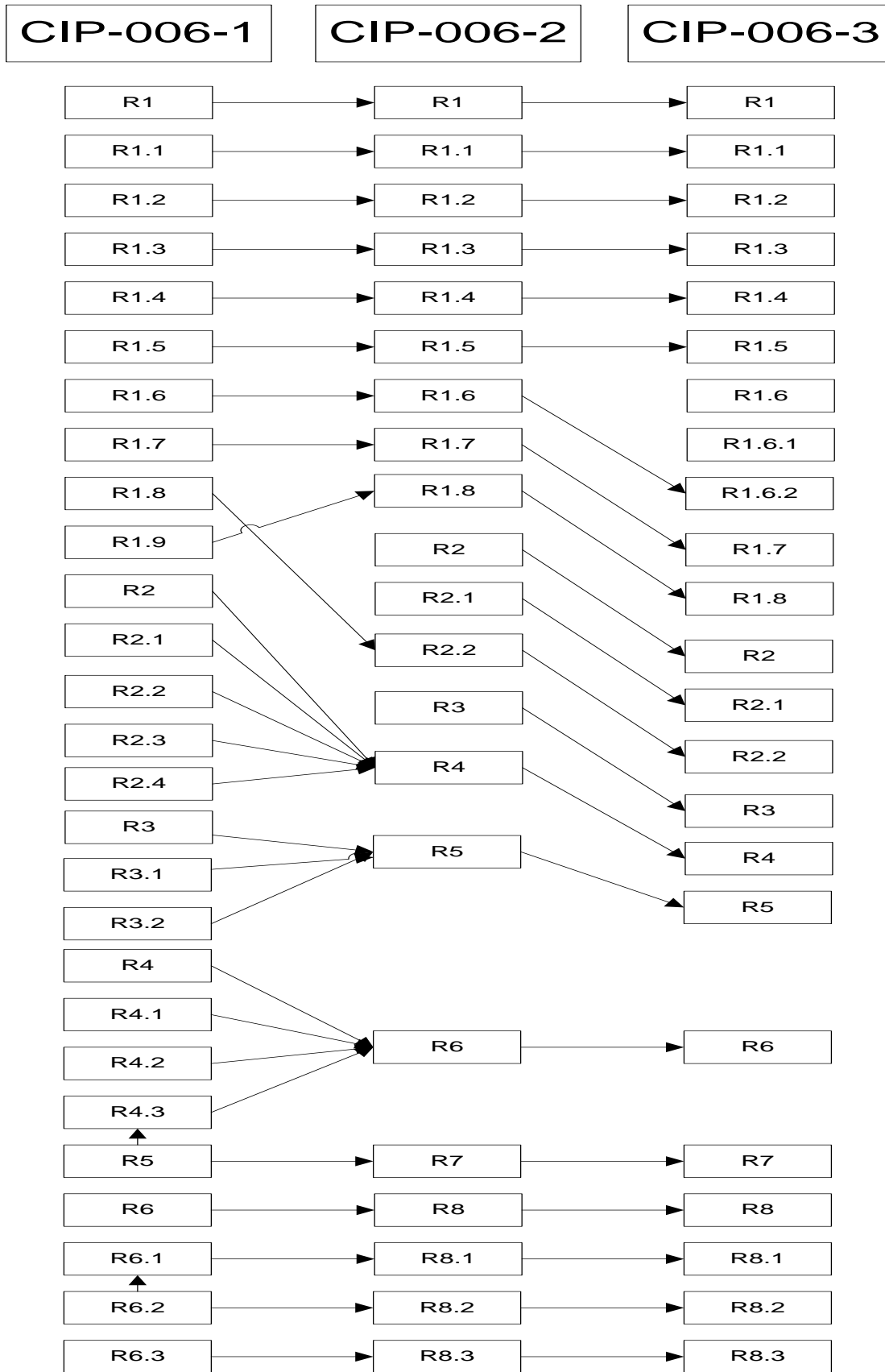
- Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009.
- In Requirement R7, the term “Responsible Entity” was capitalized.

Revision 1 was enforceable from 7/1/2009 to 3/31/2010 for Table 1 and 2 entities, and from 1/1/2010 to 3/31/2010 for Table 3 entities.

Revision 2 was enforceable from 4/1/2010 to 9/30/2010 for all entities.

Revision 3 is enforceable effective 10/1/2010.

The changes for all versions are shown below.



## Analysis of CIP-006

NERC focuses on developing the following metrics for both CIP-006 and CIP-007:

1. Violations by requirement give a high-level view of the violations and their severity, while violations by sub-requirement give insight into more specific information.
2. Violations by Region show how the violations are distributed throughout the ERO Regions.
3. The prevailing method of discovery by the Regional Entity for each violation.
4. The date of violation will show if there are particular months, quarters, or years of interest to see if there are noticeable trends.
5. Key reasons for noncompliance cited by the Regional Entities.

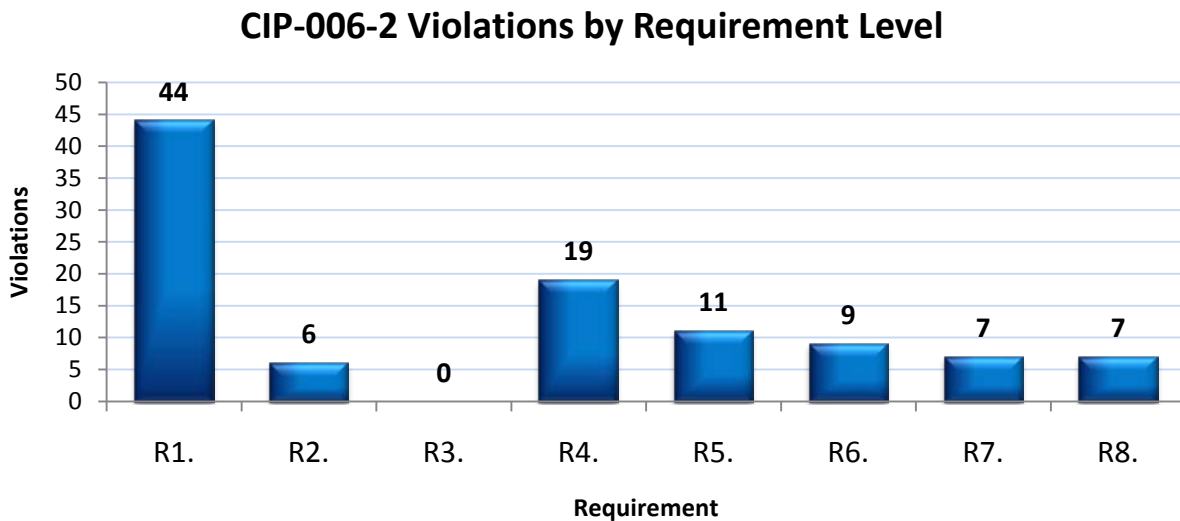
The first way to view the 103 violations of CIP-006-2 is by requirement and sub-requirement level. Table 1 below shows how the 103 violations have been submitted to NERC accordingly. From the mapping table above all violations are in the form of CIP-006-2 for consistency purposes.

**Table 1**

<b>CIP-006-2 Violations by Requirement</b>	<b>Violations</b>	<b>Percentage</b>
R1 – Physical Security Plan	44	43%
R2 – Protection of Physical Access Control System	6	6%
R3 – Protection of Electronic Access Control Systems	0	0%
R4 – Physical Access Controls	19	18%
R5 – Monitoring Physical Access	11	11%
R6 – Logging Physical Access	9	8%
R7 – Access Log Retention	7	7%
R8 – Maintenance and Testing	7	7%
<b>Totals</b>	<b>103</b>	<b>100%</b>

A visual representation of the CIP-006-2 by requirement level is shown below.

**Figure 1**



Requirement R1 contains eight sub-level requirements for CIP-006-2, and it is understandable that most of the violations fall under this requirement.

Figure 2 below shows the CIP-006-2 violations by Region.

**Figure 2**

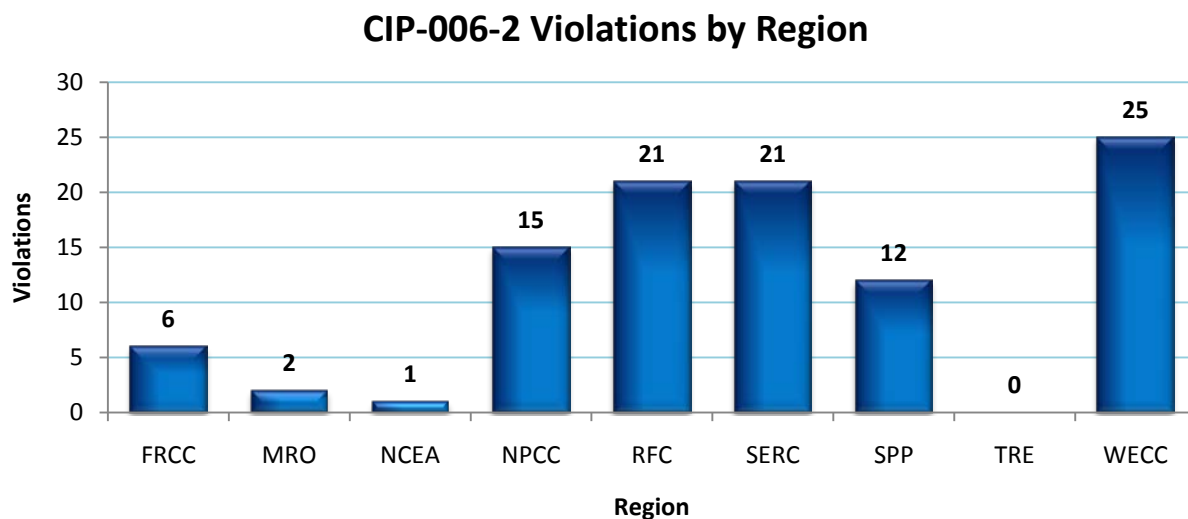
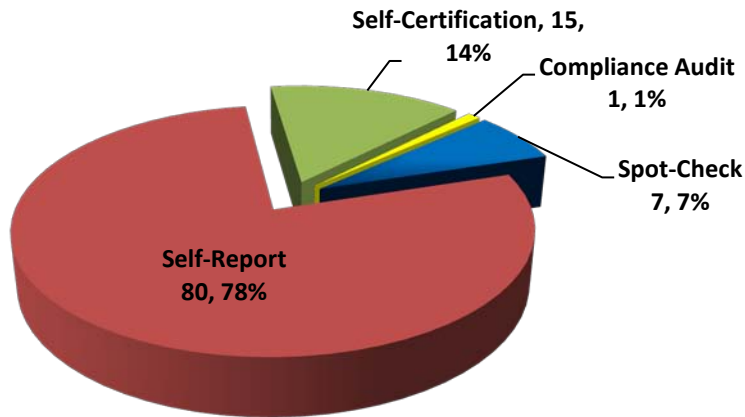


Figure 3 below shows the CIP-006-2 violations by method of discovery. It is important to note that 78% of the violations have been self-reported, while 14% have been through a self-

certification, leaving only 8% of the violations discovered through a compliance audit or spot check.

**Figure 3**

**CIP-006-2 Violations by Method of Discovery**

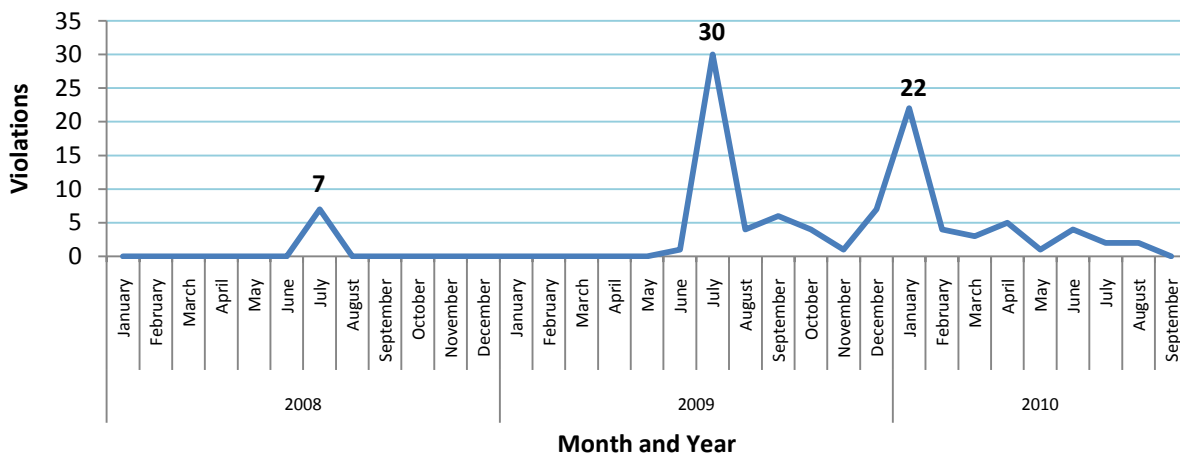


The result of the method of discovery analysis shows that a significant percentage of violations are being self-reported. Registered entities are encouraged to self-report their violations as soon as they are found.

Figure 4 below shows when the violations occurred.

**Figure 4**

**CIP-006 Violations by Date Occurred**



The three months that stand out are July 2008, July 2009, and January 2010. This tracks the “C” date for table 1, 2, and 3 entities which supports the large number of self reports.

## Regional Entity Analysis of CIP-006

---

### Summary Info and Discussion

Violations of the NERC Reliability Standard CIP-006 are for the most part scattered, with Requirement R1 being the requirement most violated.

### Key Reasons for Noncompliance

The following information is organized by requirement. For each, typical facts surrounding violations are notes and suggestions for improvements are offered, based on the experience to date, of Regional compliance staff.

After reviewing the results of the information gathered, the following key reasons were identified by the Regional Entities as the primary reasons that registered entities were found to be noncompliant with CIP-006.

### Common Violation Descriptions for Frequently Violated Requirements

#### 1. Entity reported instances where unauthorized individuals had unescorted access to critical assets.

*R1. The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address all of the sub-requirements when dealing with physical security plans.*

### Suggested Enhancements

- Responsible Entities should ensure and reinforce through their annual Cyber Security Training the concepts of escorted and unescorted physical access to critical assets. This training should reinforce that physical security is the first line of defense in protecting critical assets, critical cyber assets and personnel.
- Responsible Entities should perform a gap analysis and or regular testing of their physical security and access controls at access points to their Physical Security Perimeters. As an example, the Responsible Entity could work with their Corporate Security group to perform regular “physical penetration attempts” to determine the effectiveness of their physical security and access control procedures and mechanisms.
- The proliferation of keys is “key” to many of these violations. Also, past practice of guards and other key-holding staff implies cyber security training is not well understood and/or enforced by management.

#### 2. The entity did not afford protective measures for all Cyber Assets used in access control and monitoring of the PSP as required by CIP-006-2, R2.2.

**R2.** *Cyber assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access points such as electronic lock control mechanisms and badge readers, shall be protected from unauthorized access and be afforded protective measures specified in other CIP standards.*

**Suggested Enhancements**

- Responsible Entities should ensure that all Critical Cyber Assets and Cyber Assets are clearly defined through the annual application of their Risk-Based Assessment Methodology.

**3. Violations for this Requirement R3 have not occurred.**

**R3.** *Cyber assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.*

**Suggested Enhancements**

- Responsible Entities should clearly define their Physical Security Perimeters and regularly review Critical Cyber Assets (CCAs) and Cyber Assets (CAs) that reside within. These reviews should be performed against their known active list(s) of CCAs and CAs.
- Have an individual owner of Physical Security Perimeter documentation ensuring that detailed lists and or drawings are accurate and up-to-date.

**4. Employee used a key instead of a card key to access a Physical Security Perimeter.**

**R4.** *The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: card key, special locks, security personnel, or other authentication devices.*

This occurred six times, and the type of employees violating this Requirement was different. A communication employee, as well as security guards and a generation company employee, used a key instead of a card key.

**Suggested Enhancements**

- Responsible Entities should reinforce proper application of operational and procedural controls used to access Physical Security Perimeters. This could be accomplished through the annual Cyber Security Training.
- Responsible Entities should verify personnel with unescorted physical access have access to the necessary access methods such as key cards.

**5. Entity self-reported one instance where an individual entered a Physical Security Perimeter without logging the individual's access, documentation of logging missing, and the personnel did not follow procedures for applying specific access control.**

**R6.** *Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeters(s) using one of more of the following logging methods or their equivalent: computerized logging, video recording, or manual logging.*

**Suggested Enhancements**

- Responsible Entities should reinforce proper application of technical and procedural controls used to access Physical Security Perimeters. This could be accomplished through the annual Cyber Security Training.
- Responsible Entities should perform a gap analysis and or regular testing of their physical security and access controls at access points to their Physical Security Perimeters. As an example, the Responsible Entity could work with their Corporate Security group to perform regular “physical penetration attempts” to determine the effectiveness of logging access attempts whether authorized and unauthorized, of their technical or manual logging methods.

**6. Entity failed to implement a maintenance and testing program for all physical security systems.**

**R8.** *The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirement R4, R5, and R6 function properly. The program must include, at a minimum: testing and maintenance on all mechanisms on cycle of three years or less, retention of these records, and retention of outage records for at least one calendar year.*

**Suggested Enhancements**

- Responsible Entities should have a regular maintenance and testing plan as part of their larger Physical Security Program. When resources are tight, the Entities could leverage internal employees, plans and procedures already in place from their Information Technology or Corporate Security groups to assist with implementation of a regularly scheduled maintenance and testing of physical security mechanisms. When internal resources and or programs are not available Responsible Entities should consider including regular (cycle of three years or less) maintenance and testing of physical security mechanisms within vendor contracts. This would leverage the expertise of the integrators whom most likely implemented the mechanisms for the Entity.
- See the comment under R1 regarding documentation of site visits to verify proper security and function of security mechanisms.

## Recommendations to Revise the CIP-006 Reliability Standard

---

Based on the experience gained from monitoring and enforcing this standard, the following recommendations will be provided to the NERC Standards Department to consider revisions to make the standard more clear and understandable. This would assist entities in complying with the standard and Regions in applying the standard.

### **1. Recommendations for Requirement R1:**

- a. Change CIP-006 R1.8 to read: “Update the physical security plan as needed and perform an annual review that includes a date and signoff”.
- b. Provide more guidance on acceptable “alternative measures” when a completely enclosed six-wall border cannot be established per CIP-006 R1.1.
- c. Maintenance of the plan is the weakest aspect of this requirement. Suggestion would be to include verbiage that would require documentation of site visits to verify plan is maintained and assets continue to be protected.

## Analysis of CIP-007 Violations

---

### **Background**

Since the beginning of the Critical Infrastructure Protection mandatory and enforceable standards on May 6, 2009, CIP-007 has quickly become the second most violated reliability standard. 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). Given the nature of these violations, NERC has performed an initial analysis of active and closed violations of this reliability standard to define prevailing trends. As of September 30, 2010, there are 242 violations of CIP-007 that are closed or active, with another 12 dismissed at the Regional Entity level.

CIP-007 is in revision level 3 (FERC-approved) and has nine (9) top-level requirements and thirty-four (34) sub-level requirements. For the purpose of consistency, all CIP-007 violations will be in the form of CIP-007-2. When changing from version 1 to version 2 for CIP-007, there were no significant changes to the Requirements or sub-requirements, so a mapping history is not pertinent here.

## Analysis of CIP-007

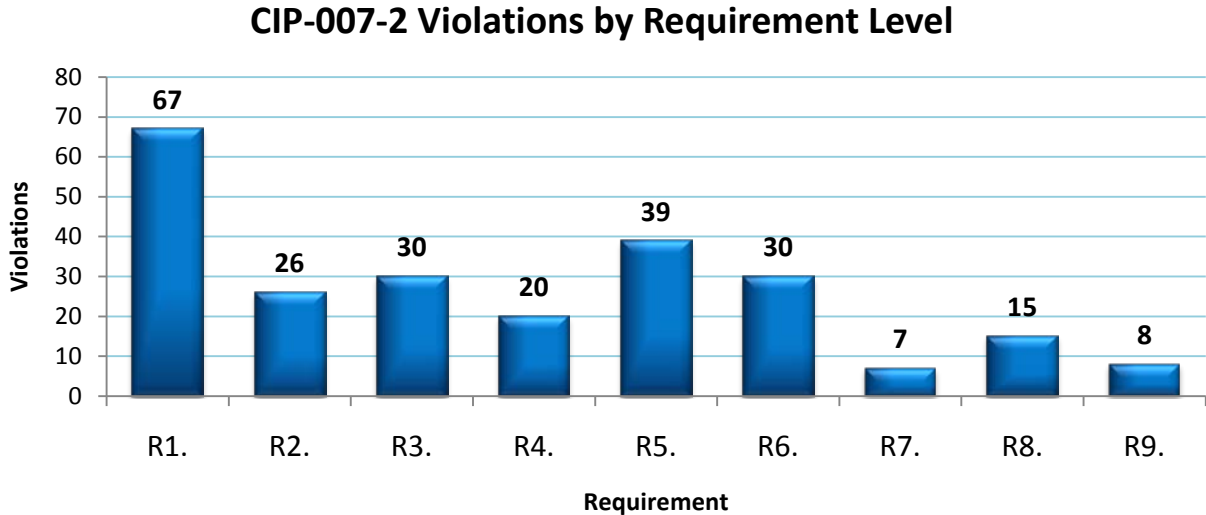
Unlike the CIP-006 family of standards the revisions from CIP-007-1 and CIP-007-2 are similar and contain no substantive differences.

**Table 2**

<b>CIP-007-2 Requirements</b>	<b>Violations</b>	<b>Percentage</b>
R1 – Test Procedures	67	28%
R2 – Ports and Services	26	11%
R3 – Security Patch Management	30	13%
R4 – Malicious Software Prevention	20	8%
R5 – Account Management	39	16%
R6 – Security Status Monitoring	30	12%
R7 – Disposal or Redeployment	7	3%
R8 – Cyber Vulnerability	15	6%
R9 – Documentation Review and Maintenance	8	3%
<b>Totals</b>	<b>242</b>	<b>100%</b>

Figure 5 below shows a visual representation of the violations by Requirement level. Besides R7 and R9, all Requirements are in the double digits for violations.

**Figure 5**



It is important to provide analysis by each Requirement due to the high number of violations for each Requirement. To gain more insight into this reliability standard, we will now analyze the violations by sub-requirement.

Figure 6 below shows the CIP-007-2 violations by Region.

**Figure 6**

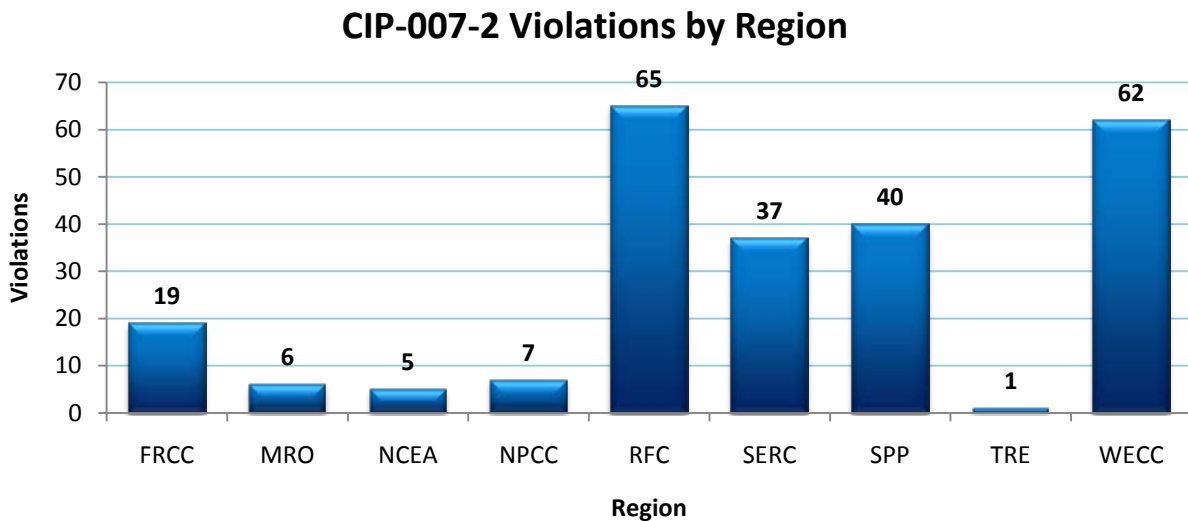
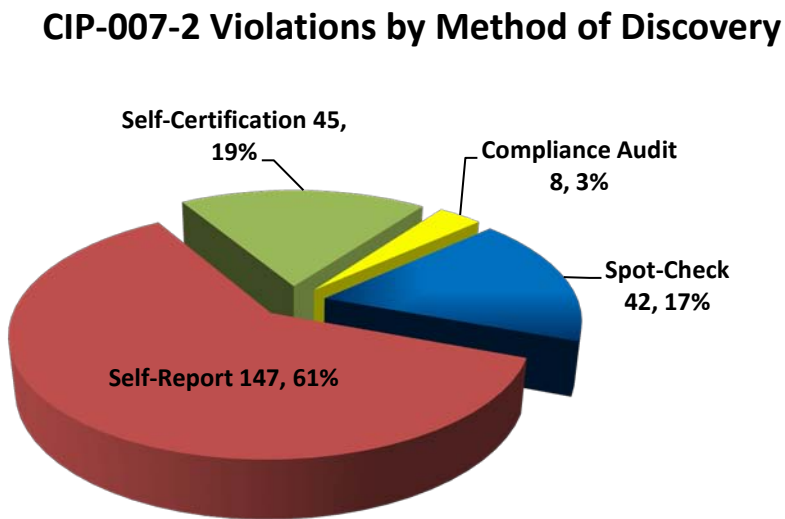


Figure 7 below shows the CIP-007-2 violations by method of discovery.

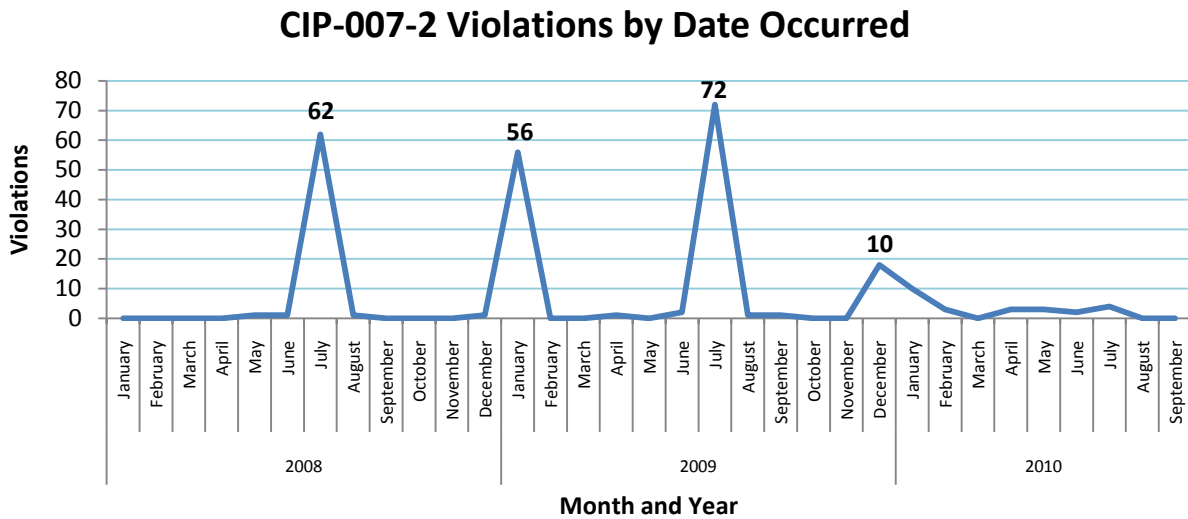
**Figure 7**



It is important to note that 80% of the CIP-007-2 violations were reported through self-certifications and self-reports, while only 20% were reported through compliance audits and spot-checks.

Figure 8 below shows when the violations occurred.

**Figure 8**



The months with high counts of violations are July 2008, January 2009, July 2009, and December 2009. Coinciding with CIP-006-2, July of both 2008 and 2009 has high counts of violations for both CIP-006-2 and CIP-007-2. As mentioned in the CIP-006 analysis, the above mentioned dates track the “C” dates for table 1, 2 and 3 entities which supports the large number of self reports.

## Regional Entity Analysis of CIP-007

### Summary Info and Discussion

Violations of the NERC Reliability Standard CIP-007-2 are for the most part scattered, with Requirement R1 being the requirement most violated.

### Key Reasons for Noncompliance

The following information is organized by requirement. For each, typical facts surrounding violations are notes and suggestions for improvements are offered, based on the experience to date, of Regional compliance staff.

After reviewing the results of the information gathered, the following key reasons were identified by the Regional Entities as the primary reasons that registered entities were found to be noncompliant with CIP-007-2.

### Common Violation Descriptions for Frequently Violated Requirements

#### 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-007-2, 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.*

### Suggested Enhancements

- Responsible Entities should be reminded that test procedures should be maintained for ALL cyber assets or at least categories of cyber assets within their defined ESPs and not just their mission critical cyber assets such as their EMS system.
- Responsible Entities should be reminded that R1.3 requires them to maintain documentation of test results. Responsible Entities should ensure that they have a test plan, follow their test plan, and document the results of their test plan.
- One common mistake in compliance with R1 is that the Requirement may have an entity concentrate on testing the functionality of changes. That is not what this Requirement says. The testing required is to ensure there is no adverse impact on cyber security controls. Furthermore, there have been instances where the tools (both software and database) used for implementing a change were not tested themselves to ensure that they wouldn't adversely affect the systems.

#### 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.*

### **Suggested Enhancements**

- Responsible Entities should consider running ports and services scans (manual or automated) as part of normally scheduled maintenance on cyber assets. This has the potential of least impact to cyber assets in a production environment.
- Responsible Entities should baseline cyber asset ports and services in a test, development, and or pre-production environment prior to moving a cyber asset to production.
- Responsible Entities should work with all vendors of systems and applications of applicable cyber assets in their infrastructure to determine required ports and services. Most if not all vendors will have some form of documentation detailing this information.
- Responsible Entities should work with the Network Services department in their organizations to perform regular Data Flow Analysis of applications used within their ESPs and necessary communication outside the ESPs to assist in further defining the required ports and services needed for normal and emergency operations. This could be done in lieu of or complementing manual analysis of cyber assets and or system and network scans.
- Responsible Entities should note the most common problem with R2 is the failure to demonstrate only those ports and services required for operation are those that are enabled. The Responsible Entity needs to demonstrate that a port of service is required for operation.

### **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).*

### **Suggested Enhancements**

- Responsible Entities should consider leveraging a corporate level Patch Management Program if one does not exist for their Real-time systems area. Typically, the corporate level program will be established and include the necessary tracking, evaluating, testing, and installing applicable cyber security patches required for all Cyber Assets within the Electronic Security Perimeter(s).
- Responsible Entities should understand the scope of their patch management programs.

### **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).*

**Suggested Enhancements**

- Responsible Entities should consider leveraging a corporate level program for updating Antivirus and Malware if one does not exist for their Real-time systems area. Typically, the corporate level program has systems in place for the automatic and or scheduled updating of tested antivirus and malware signatures to computing resources.

**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.*

**Suggested Enhancements**

- Reinforce CIP procedures with Real-time systems support and supervisory personnel. Failure to follow procedures for password changes in this scenario creates operational, security and regulatory compliance risk for the Responsible Entity.

**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.*

**Suggested Enhancements**

- Responsible Entities should baseline cyber asset logging service capabilities in a test, development, QA and or pre-production environment prior to moving a cyber asset to production. This will ensure that when moved to production the cyber asset is properly configured to send automated events to centralized logging servers and or generate event logs for manual review.

**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-005-2.*

#### **Suggested Enhancements**

- Implement and or leverage a corporate level data and media destruction program. If one does not exist, contract with a third-party for disposal and destruction services.
- If not sure how to implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) consider the following guideline:
  - NIST Special Publication 800-88; Guidelines for Media Sanitization.

#### **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.*

#### **Suggested Enhancements**

- The Responsible Entity should consider leveraging a corporate level “Risk and or Vulnerability Assessment” program if one does not exist for the Real-time systems area. Typically, the corporate level program has a regularly scheduled vulnerability assessment plan implemented by the Information Security group or a third-party. These groups will have the expertise to run automated tools or perform manual system reviews to determine a system state in regards to existing vulnerabilities, ports and services and default accounts. A plan should be scoped with the Real-time systems area to perform the annual vulnerability assessments so as not to impact the production systems, including tests of the proposed plans and tools used in a development or pre-production environment.

## Recommendations to Revise the CIP-007 Reliability Standard

---

Based on the experience gained from monitoring and enforcing this standard, the following recommendations will be provided to the NERC Standards Department to consider revisions to make the standard more clear and understandable. This would assist entities in complying with the standard and Regions in applying the standard.

**1. Recommendations for Requirement R1:**

- a. Add to CIP-007 R1.4: "Sign-off is required to verify that individuals that initiate a change or test a change do not also migrate it to production without proper approval".

**2. Recommendations for Requirement R3:**

- a. Establish acceptable timeframes for the implementation of Security Patches where compensating measures have not been asserted. This will help further define and provide accountability in the Responsible Entities Security Patch Management Programs.

## Conclusion

---

With CIP-007 the most violated FERC enforceable standard of the past 12 months and CIP-006 the sixth most violated FERC enforceable standard, there is a pressure for the industry to react to CIP violations and learn ways to decrease the frequency of these violations.

Compliance to the CIP standards is a must to maintaining reliability of the bulk power system. Over the past 12 months, eight of the top 10 most violated FERC enforceable standards are in the CIP family.

As the CMEP matures and the industry becomes more familiar about compliance of CIP standards, CIP-006 and CIP-007 will improve as long as the registered entities, NERC, and the Regional Entities all are proactive in working together for a more clear understanding of the CIP standards.

### Contact Information

Mike Moon  
Director of Compliance Operations  
609-452-8060  
[Michael.Moon@nerc.net](mailto:Michael.Moon@nerc.net)

Ryan Stewart  
Engineer of Organization Registration,  
Certification, and Compliance Monitoring  
609-751-7808  
[Ryan.Stewart@nerc.net](mailto:Ryan.Stewart@nerc.net)