

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Electric Reliability Organization (ERO) Compliance Analysis Report Reliability Standard CIP-001 — Sabotage Reporting

Version 1.1

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

Table of Contents

ERO Compliance Analysis Reports.....	2
Summary of Practical Information and Suggestions	3
Analysis of CIP-001 Violations	4
Background.....	4
Analysis	4
Regional Entity Analysis	12
Summary Information and Discussion:	12
Key Reasons for Noncompliance and Suggested Process Enhancements.....	12
Common Violation Descriptions	13
Conclusion	17
Contact Information	18
Priority of Future ERO Compliance Analysis Reports	19

ERO Compliance Analysis Reports

The ERO, comprised of NERC and Regional Entities, compliance staffs are collaborating on the analysis of the top 10 violated standards, and publicly providing these reports to facilitate compliance by providing information and guidance on the most violated standards. This is the fourth report and demonstrates an integrated report, whereas the first three were essentially two part reports, the high level NERC analysis and the Regional level analysis. An additional formatting change is the highlighting of the summary and suggestions up front.

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, “Suggested Enhancements,” are included for informational purposes only.¹

1. Entities should prepare one document that contains all requirements of CIP-001-1 and ensure that all employees have access to the document and are made aware of its contents. This accessibility and availability may pose challenges for operating personnel who are routinely in the field. These challenges need to be recognized and addressed on an ongoing basis as part of a responsible entity’s sustaining compliance with the standard. Entities should clearly indicate the appropriate communications strategy in their Sabotage Reporting plan and ensure its employees are trained to act accordingly.
2. A Violation Risk Factor of “Medium” has been adopted for each CIP-001-1 requirement. Compliance trend monitoring for requirements R1-R4 is expected to continue. Violation of CIP-001-1 requirements are not considered to be of a purely administrative (VRF = Lower) consequence to the bulk electric system, in contrast to the vast number of self-assessed, reported BES impact of “minimal” found within documentation of numerous sustained self-reported violations.
3. Interpretation of CIP-001-1a was recently approved by the NERC BOT and should be found to be helpful compliance information for responsible entities efforts regarding requirement R3 (see the link provided for this interpretation):
[http://www.nerc.com/docs/standards/sar/Project2009-09 Interpretation Covanta CIP-001-1 2009July6.pdf](http://www.nerc.com/docs/standards/sar/Project2009-09%20Interpretation%20Covanta%20CIP-001-1%202009July6.pdf)
4. Responsible Entity’s operating personnel CIP-001-1 sabotage awareness and recognition obligations, may be able to be successfully performed and documented in conjunction with other BES-specific compliance activities (*i.e.* CIP-004/ CIP-008 personnel and cyber security incident response training).
5. Responsible entity compliance with requirements of CIP-001-1 is continuous. Phone numbers and contact information for local FBI officials as well as reporting procedures appropriate to circumstances may change over time. Responsible entities may consider the value of documenting reviews and validation of such procedures on a regular basis to support continuous compliance and awareness among operating personnel.
6. Current documentation of an entity’s established sabotage reporting procedures (recognition and notification) is an important reliability element and should be readily available to all appropriate operating personnel.

¹ For specific NERC guidance, see the latest CIP RSAW. NERC provided the Regions guidance in October 2009 regarding Requirement R4 via the RSAW_CIP-001-1_2010_v1, located at <http://www.nerc.com/page.php?cid=3|22>.

Analysis of CIP-001 Violations

Background

Since the beginning of the mandatory and enforceable standards on June 18, 2007, CIP-001-1 has been one of the top two most violated standards by registered entities. This standard plays a critical role in asset security, ensuring that disturbances or unusual occurrences suspected or determined by sabotage are reported to appropriate systems, governmental agencies, and regulatory bodies. Given the critical nature of these violations, NERC and the Regional Entities have performed an initial analysis of active and closed violations of this reliability standard to define trends. As of November 4, 2009, there were 341 active and closed violations of CIP-001-1, with an additional 49 violations that have been dismissed by the Regional Entities. This report focuses on the 341 active and closed violations of this standard, which currently has four requirements.

NERC focused on developing the following metrics of CIP-001-1

1. Identifying how many violations were reported for each Region for the time period of June 18, 2007 to the present.
2. The prevailing method of discovery by the Regional Entity for each violation.
3. An analysis of violations by the date of violation to determine if violations were clustered around certain months or years.
4. A trending analysis of how many violations were submitted by month to determine if violations submission levels have reached a steady state, or if they are increasing or decreasing.
5. Key reasons for noncompliance cited by the Regional Entities, classified by a bucket structure that will be further described later in this paper.
6. An analysis of those buckets to determine if the violations contained within still pose a threat to the bulk electric system.

All requirements of this standard currently have Violation Risk Factors of “medium.”

This assessment will examine the implementation of the standard, determine the possible reasons for violations, and identify suggested process enhancements to improve compliance. While current summarized evidence sustains the 10 most-violated ranking, there is anecdotal and statistical evidence suggesting a downward trend in violations. Testing this trend may be valuable and prudent through some selected spot check efforts, performed in conjunction with ongoing CIP spot check schedules.

We would like to acknowledge the work of the CIP Compliance Working Group (CCWG) in the assisting with the preparation of this assessment.

Analysis

The initial NERC overarching analysis reviewed 341 violations of CIP-001-1 and identified the specific requirement(s) violated by registered entities using the following table, with common

violation descriptions. It further analyzes accumulated violations. Most interesting for further review and discussion are four selected graphs, re-ordered, and in two cases, **graphically enhanced** in order to present a case for plausible, actionable trends for consideration by Regional Entities.

1. Violations grouping by Requirement ²
2. Violations by Registration Function ³
3. Violations by date of violation with Compilers’ superimposed trend line ⁴
4. Violations by Submission Date with Compilers’ superimposed trend line ⁵
5. Violations by Classification ⁶

Examining approximate trend lines from NERC violation statistics leads to several conclusions and suggestions:

- a. Conclusion: Evidence presented suggests CIP-001 violations are on a decreasing trend toward exit from the top 10 “most violated” status through the end of calendar year 2009.
- b. Conclusion: Bulk electric system risk due to persistent noncompliance with CIP-001-1 requirements has decreased significantly.
- c. Suggestion: Selected Spot Checking of CIP-001 compliance of LSE, GOP registered entity functions amidst scheduled CIP Spot Checks for these registered functions may be useful given somewhat high concentration of violations among those registered functions.

The first analysis of CIP-001-1 is to show how violations were reported to NERC on a requirement level basis. Table 1 below represents the results of this analysis.

Table 1

CIP-001-1	Violations	Percentage
R1 – Make Personnel Aware of Sabotage Events	93	27%
R2 – Communication of Events to Relevant Parties	86	25%
R3 – Sabotage Response Guidelines	75	22%
R4 – Appropriate Contacts with Federal Agencies	87	26%
Totals	341	100%

The analysis shows that active and closed violations of this standard are almost equally distributed across all requirements. A more visual representation of this analysis is shown in Figure 1.

² Ibid, Figure 1, Page 4

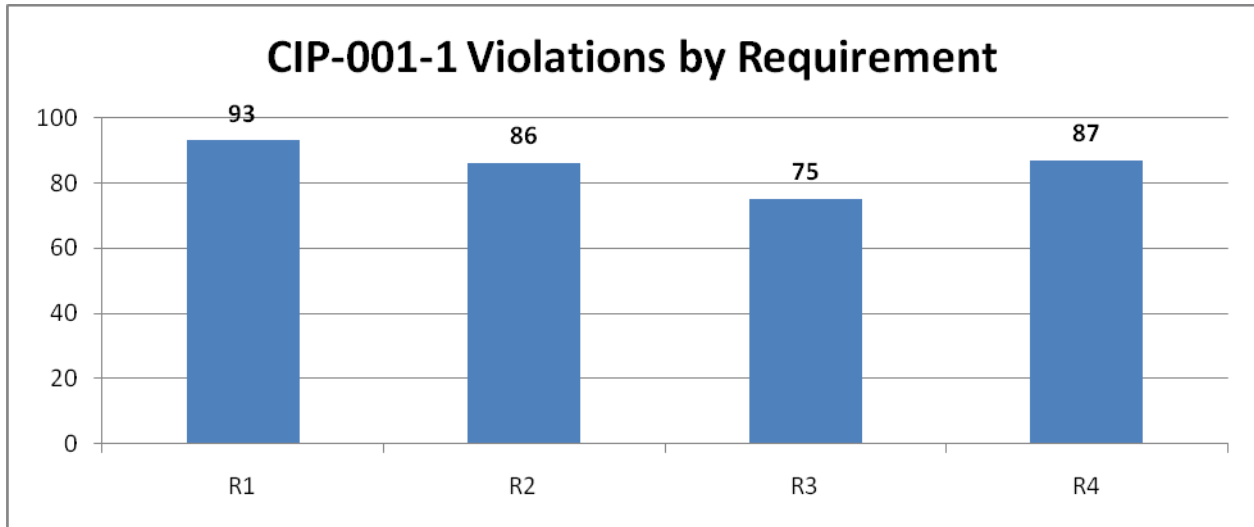
³ Ibid, Figure 3, Page 5

⁴ Ibid, Figure 5, Page 7

⁵ Ibid, Figure 6, Page 8

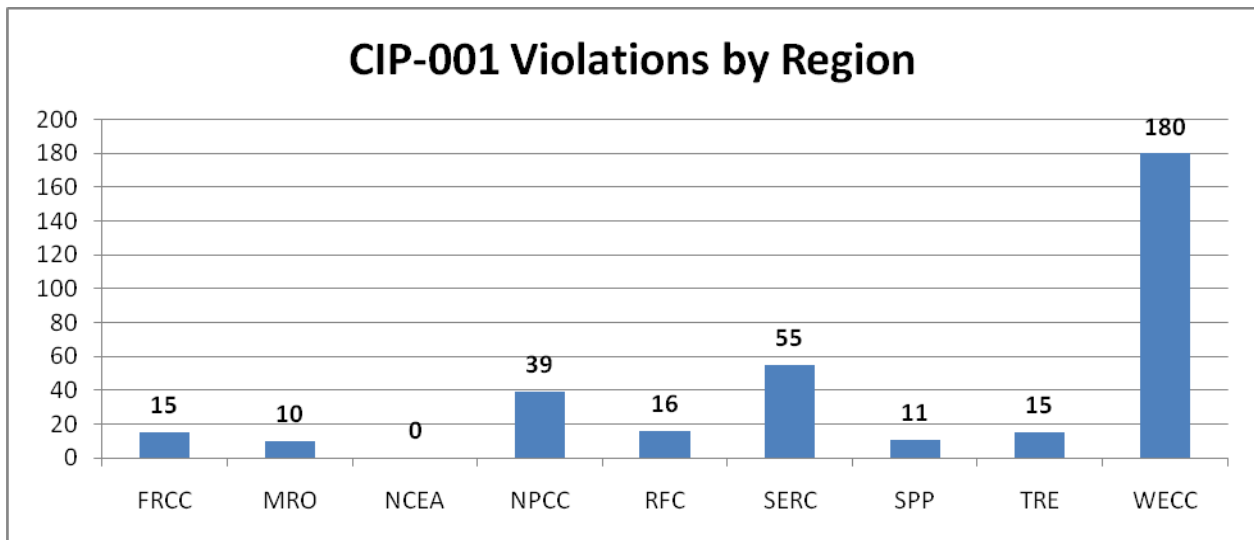
⁶ Ibid, Figure 7, Page 9

Figure 1



The second analysis focused on identifying CIP-001-1 violations that were spread across the Regional Entities. Figure 2 below illustrates the results of this process:

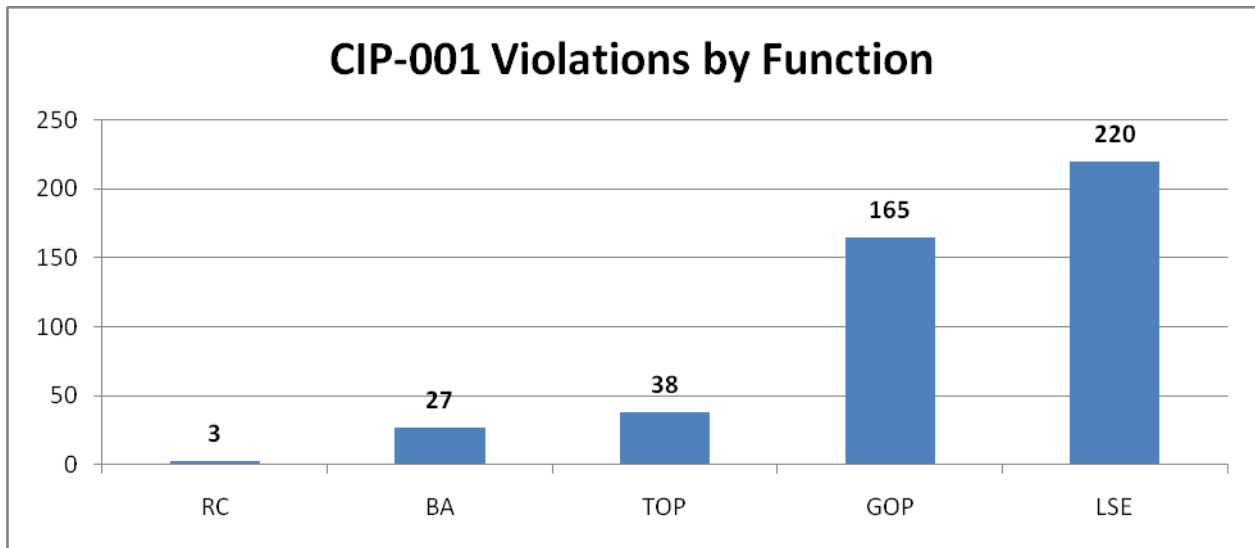
Figure 2



As of October 29, 2009, the WECC Region continues to cover the largest geographic footprint of all the Regional Entities. In its footprint, WECC monitors the largest number of registered entities (471 out of 1,865 total entities). However, the results of this analysis show that nearly 53% of the violations reported to NERC occurred in the WECC Region, while the WECC Region only monitors approximately 25% of the total registered entities. The results of more extensive analysis of violations in the WECC Region reveal that approximately 58% violations were discovered through self-reports, with the second most frequent method of discovery being self-certifications.

Another interesting way to view the CIP-001-1 violations is by the functional registration of the registered entity. Standard CIP-001-1 currently applies to Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities. The results of this analysis are presented below in Figure 3, and since most entities are registered by the Regional Entities and NERC under multiple functions, the following graph will sum to more than 341 violations that this report is covering.

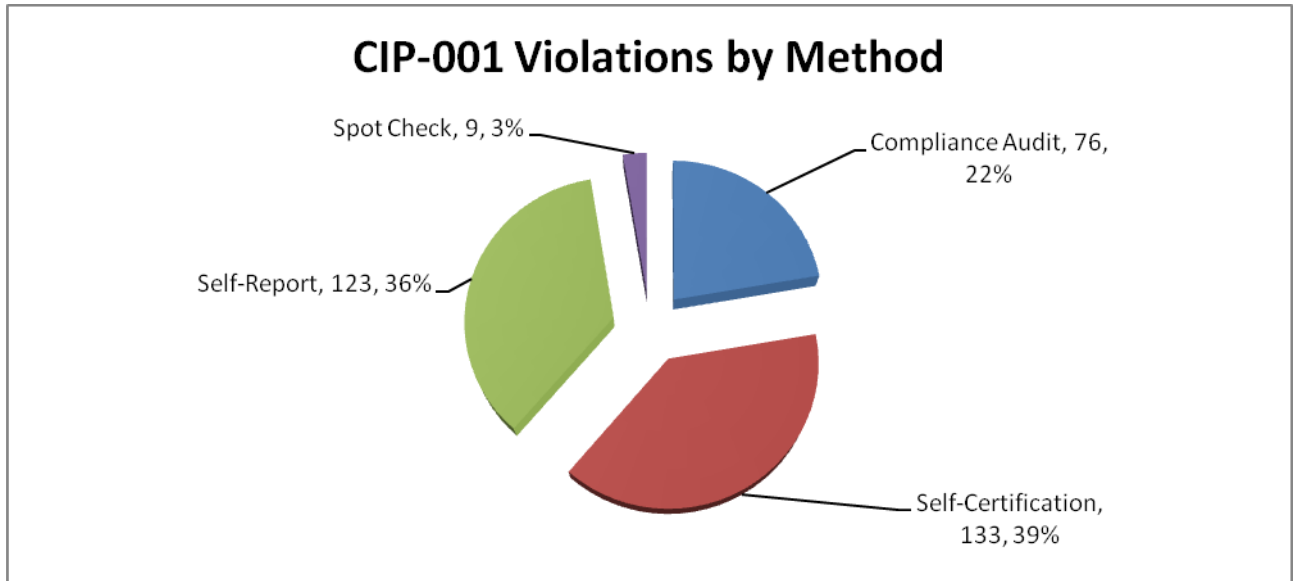
Figure 3



The registered function data that the Regional Entities reported to NERC was mostly accurate. Regional Entities have been directed by NERC to specify only which registered functions of an entity and the standard have been violated.

The next analysis focused on determining the most frequent method of discovery for violations of CIP-001-1 that were reported to NERC from the Regional Entities. The results of this analysis are shown below in Figure 4.

Figure 4



The interesting data point for the method of discovery analysis is that the primary methods of discovery for violations of CIP-001-1 were self-certifications and not self-reports. Previous analyses of PRC-005-1, CIP-004-1, and VAR-002 had all shown self-reports being the most frequent method of discovery for violations of these reliability standards. Self-certifications had the leading number of violations reported to NERC for requirements 1, 3, and 4 of CIP-001-1, with requirement 2 only missing the top spot by one violation submission. The WECC Region accounted for approximately 41% of self-certification violations (55 out of 133), with SERC accounting for the second most self-certification violations at nearly 22% (29 out of 133).

The fifth analysis focused on determining the clustering effects of violations when analyzed by the date the violation occurred. Figure 5 below, shows that a significant number of violations have a violation date clustered around June 2007. This is not an unexpected result with the initial wave of self-reported violations, since audits, self-certifications, and spot checks would identify potential violations that have not been self-reported and subsequently corrected or mitigated.

Figure 5

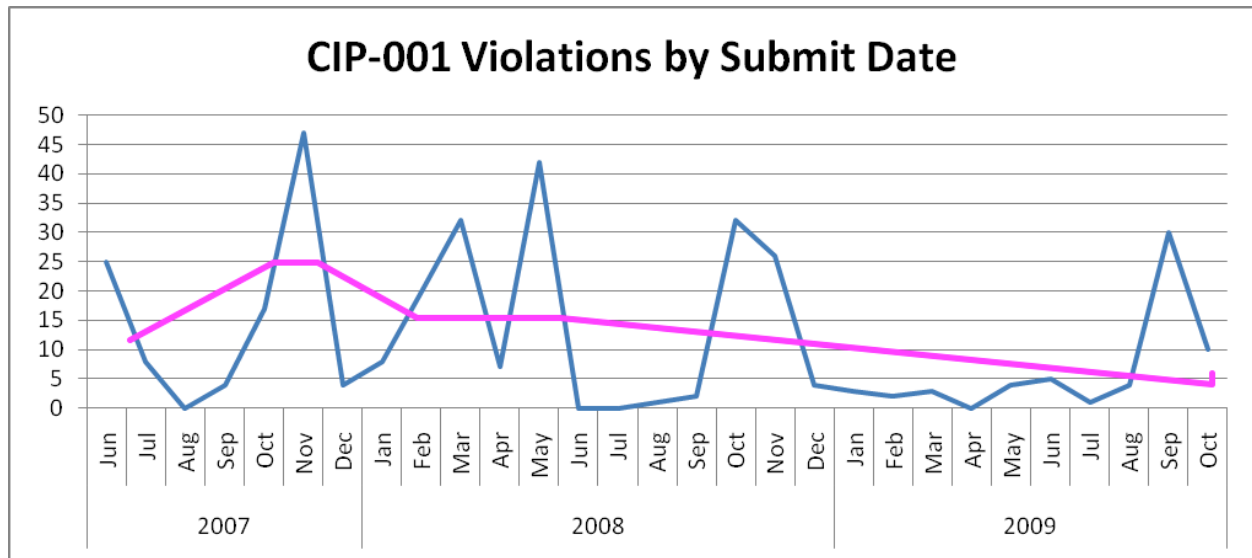


The results of this analysis show that violations were primarily clustered around June 2007, but two months required more extensive analysis: April 2008 and December 2007. In April 2008, 20 violations began occurring according to data submitted by the Regional Entities, with these violations being discovered through compliance audits in the WECC and NPCC Regions. The 18 violations that reportedly began to occur in December 2007 had varying methods of discovery. Nine of the December 2007 violations were discovered through self-certifications, eight violations were self-reports, and one violation was discovered through a spot check. These 18 violations for December 2007 came from FRCC, SPP, TRE, and the WECC Regions.

While there is some clustering of violations by the Date of Violation analysis, there is no discernable pattern when viewing the violations by their submission date to NERC, as Figure 6 below indicates.

With the addition of the trend line (pink), the clear indication is a rather constant slope decrease after initial “hockey stick” spike. The low overall violations as a function of time through February 2009, suggests that CIP-001-1 is moving out of the top 10 most violated status.

Figure 6



The analysis of submission trends (blue line) reveals that there are two peak months of violation submissions that warrant further investigation: November 2007 and May 2008. November 2007, which saw the submission of 47 violations to NERC, were due in large part to self-certifications (33 out of 47 violations, 70%) in MRO, NPCC, RFC, and SERC Regions, but violations were also discovered via Compliance audits (10 out of 47 violations, 21%) and self-reports (4 out of 47 violations, 9%). May 2008 saw the submission of 42 violations to NERC, which was due in large part to Compliance audits in the WECC and NPCC Regions (25 out of 42 violations, 60%), with the other source of discoveries due to self-reports (17 out of 42 violations, 40%).

Examination of the submission trend of the last six months (May 1, 2009 through October 30, 2009) indicates one large spike of violations warranting further analysis: September 2009. The 30 violations that were submitted in September 2009 were discovered in many different ways: 21 came from self-certifications, 5 from self-reports, 3 from spot checks, and one was discovered through a Compliance audit in the WECC Region. All of the violations that were submitted in September 2009 had a Date of Violation of June 18, 2007, which indicates that they were undiscovered for a period of over 800 days. Breaking these violations down by Region: 23 violations came from WECC, four were in SPP, two were in RFC, and one was in FRCC.

Figure 5 and Figure 6 vary from each other because Regional Entities are required to identify the actual occurrence of a violation, and such date may not be the date the violation was discovered. While Regional Entities may have only recently found or discovered a violation, the violation could have existed in the BES for a significant period of time before discovery. This is the reason why Figure 5 and Figure 6 show different amounts of violations found and reported for each month.

The general statistical trend (pink line) shows a decrease in number of overall violations over time. This trend is supportive of other trends showing decreasing noncompliance.

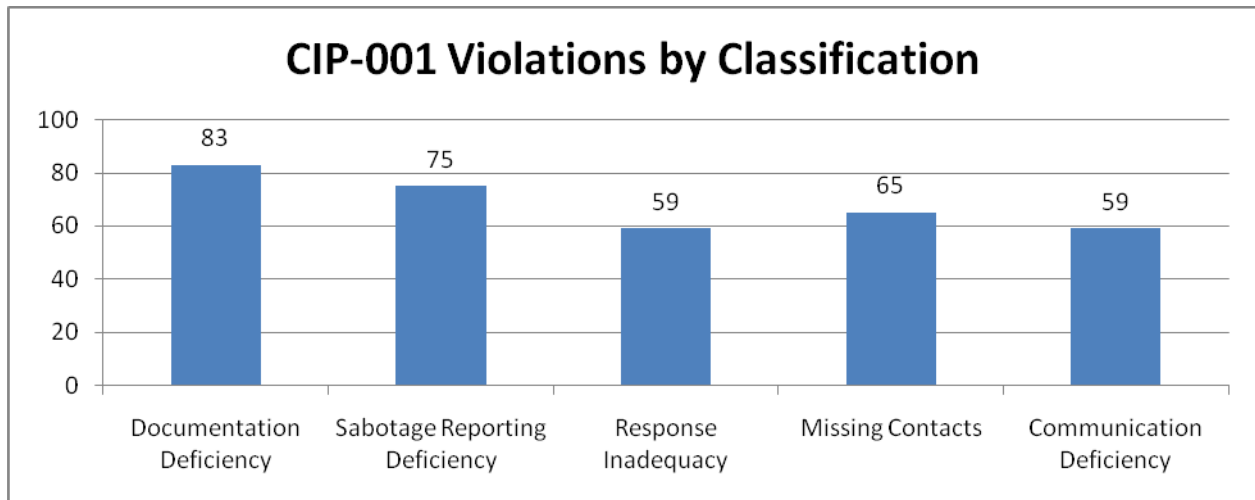
Noncompliance Analysis

There are many forms of noncompliance by registered entities, from documentation issues to performance-related issues. NERC classified the 341 violations of CIP-001-1 by five different types of classification buckets which are further described below. Violations were classified by the information provided by the Regional Entities violation workbook submissions, focusing specifically on the violation description and potential impact determinations. The classifications are:

1. *Sabotage Reporting Deficiency* – Procedures were missing for reporting events of sabotage on entity facilities – usually a violation of requirement 1.
2. *Communication Deficiency* – Lack of procedures to communicate information regarding sabotage events to the appropriate parties – usually a violation of requirement 2.
3. *Response Inadequacy* – Entity lacks sabotage response guidelines, including specific personnel to contact for reporting disturbances – usually a violation of requirement 3.
4. *Missing Contacts* – Communications contacts to report sabotage events with local FBI or RCMP officials are missing – usually a violation of requirement 4.
5. *Documentation Deficiency* – Entity has Sabotage reporting procedures and guidelines, but does not have the documentation to verify compliance.

Figure 7 represents the results of this basic classification structure.

Figure 7



The results demonstrate that violations are well distributed across all categories of this analysis. Documentation deficiencies at registered entities are the most frequent trend across all violation categories. Further examining the data behind documentation-related deficiencies shows that nearly 54% of the total violations occurred in the WECC Region. The Region with the next highest documentation deficiencies was the SERC Region, with approximately 12% of the total. The discovery method of these documentation deficiency violations was varied, from 42 violations being discovered through self-reports, 30 through self-certifications, and 11 through Compliance audits. The WECC Region once again had the largest number of self-reports, accounting for 37 out of 42 violations, or approximately 88%.

The second highest classification, Sabotage Reporting deficiencies, incorporated violations from all eight Regional Entities. The primary method of discovery for violations of this classification were through self-certifications (25 violations), closely followed by self-reports (24 violations) and Compliance audits (24 violations). The remaining two violations were attributable to spot check violations performed in RFC and TRE Regional Entities. Violations of this classification were primarily clustered in the WECC Region, where 52% of the violations occurred (39 out of 75), with SERC (16%) and NPCC (13%) also having significant percentages of violations.

The third highest classification, Missing Contacts, is comprised of violations from seven of the eight Regional Entities (the MRO being the only exclusion). Approximately 55% of the violations were discovered in the WECC Region and violations of this classification were discovered through a variety of methods, with the leading method being self-certifications (28 out of 65, 43%) followed closely by self-reports (20 out of 65, 31%). Compliance audits (15 out of 65, 23%) and spot checks (2 out of 65, 3%) round out the methods of discovery for this classification.

The overall trend when performing an analysis on violations of CIP-001-1 was the tendency of the Regional Entities to submit violations on all four requirements of the standard for the same registered entity. However, a significant number of violations of this standard were classified to be of a “Minimal” or “Low” impact by the Regional Entities to the BES, thus somewhat diminishing the current ranking of this standard as one of the top two most frequently violated reliability standards.

Regional Entity Analysis

In addition to the Regional Entity contributions identified throughout the document, the following specific items warrant further discussion, and a summary of practical compliance information and suggestions is provided at the end of this assessment.

Looking at graphs 1 (CIP-001-1 Violations by Requirement, see page 5) and 2 (CIP-001-1 Violations by Registered Function, see page 7) the following perspective is provided from the Regional Entity staffs.

Summary information and Discussion:

Total violations reported by Function: 453 (vs. 341 by Requirement)

Approximate distribution: Skewed (85% are violations attributed to GOP, LSE functions)

Discussion and Observations:

- a. LSE, GOP function violations are likely different registered entities.
- b. GOP, LSE functions shown may indicate candidacy for CIP-001-1 spot checks.

Key Reasons for Noncompliance and Suggested Process Enhancements

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

Common Violation Descriptions

CIP-001	Violations	Percentage
R1 Sabotage events and Sabotage recognition awareness	93	27%
<i>R1 Violation Description: “Does Not have a Sabotage Reporting Plan”</i>		
R2 Communication of Sabotage events	86	25%
<i>R2 Violation Description: “Document does not contain procedures for notifying appropriate parties within the Interconnection”</i>		
R3 Sabotage response guidelines	75	22%
<i>R3 Violation Description: “Entity did not provide its operating personnel with Sabotage response guidelines, including personnel to contact for reporting disturbances due to Sabotage events”</i>		
R4 Communications contacts with Federal Agencies	87	26%
<i>R4 Violation Description: “Entity did not establish communication contacts with the local Federal Bureau of Investigation (FBI) or the JTTF.”</i>		
Totals	341	100%

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the interconnection.

Violation Examples:

- a. An entity’s Sabotage Reporting procedures for the recognition of or making its operating personnel aware of sabotage events focused only on the entity’s facilities affecting the BES and not on all of the entity’s facilities as required by the requirement.
- b. An entity did not have a specific written procedure for its operating personnel for reporting sabotage events.

Suggested Enhancements:⁷

- a. An entity should ensure that its sabotage reporting procedures, as described in the requirement, addresses all of its facilities, not just those affecting the BES. Examples

⁷This and all future “Suggested Enhancements” in this document are part of this report for informational purposes only. Evaluation or undertaking such actions or suggestions does not guarantee compliance and does not replace the NERC Reliability Standards language.

include the entity’s Control Center, office areas, and the field. Also, to further address awareness, an entity can expand its sabotage awareness training scope and content.

- b. Develop and adopt a written procedure for recognition and awareness of sabotage events. Coordinate procedure, recognition, and awareness activities with adjacent Generator Operators, Transmission Operators, and Balance Authorities.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

Violation Examples:

- a. An entity’s Sabotage Reporting procedure did not have instructions for the communication of information concerning sabotage events to the appropriate parties in the Interconnection.
- b. An entity had a Sabotage Reporting procedure, but it did not identify the appropriate parties in the Interconnection.

Suggested Enhancements:

- a. An entity should ensure that its Sabotage Reporting procedure includes instructions to communicate information concerning sabotage events to the appropriate parties in the Interconnection.
- b. An entity’s Sabotage Reporting procedure should clearly identify the appropriate parties in the Interconnection that should receive communications of information concerning sabotage events.

Lessons Learned – R2:

Requirement R2 has presented some compliance and auditing challenges. These challenges are due in part to uncertainty over what “appropriate parties in the Interconnection” is intended to include. The recent NERC BOT-Approved Interpretation CIP-001-1a should improve reliability through clearer entity compliance efforts and compliance monitoring enforcement efforts:

The drafting team interprets the phrase “appropriate parties in the Interconnection” to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. For example, reporting responsibilities result from NERC Standards IRO-001 Reliability Coordination — Responsibilities and Authorities, COM-002-2 Communication and Coordination, and TOP-001 Reliability Responsibilities and Authorities, among others. Obligations to report could also result from agreements, processes, or procedures with

other parties, such as may be found in operating agreements and Interconnection agreements. The drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

Violation Examples:

- a. An entity did not provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.
- b. An entity did not train its operating personnel on reporting disturbances due to sabotage events.

Suggested Enhancement:

An entity should provide a sabotage response guideline for its operating personnel. The guidelines should include valid personnel contact information (*i.e.* names, phone numbers, location, availability) with notification instructions for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

Violation Examples:

- a. An entity's evidence did not confirm that it had a list of correct and working contact information with the FBI or RCMP officials, or that its reporting procedures had been developed as appropriate to their circumstances.⁸
- b. A U.S. entity did not have FBI telephone contact information in its sabotage reporting procedures.

⁸ For specific NERC guidance, see the latest CIP RSAW. NERC provided the Regions guidance in October 2009 regarding Requirement R4 via the RSAW_CIP-001-1_2010_v1, located at <http://www.nerc.com/page.php?cid=3|22>

Suggested Enhancements:

- a. United States entities should be able to demonstrate they have correct and working contact information for their local respective officials and that their reporting procedures appropriately reflect the required internal reporting procedures according to its circumstances.
- b. A U.S. entity should have valid contact information for local FBI officials unless the local FBI officials indicate otherwise. In such a case, the entity should maintain documentation of this instruction as part of sustaining its compliance, and should be alert to any FBI-initiated changes of preferred process or procedure.

Lessons Learned – R4:

During the course of audits, at least one Regional Entity found a situation where a responsible entity produced written documentation indicating local FBI officials preferred the entity report instances of suspected sabotage to a regional Information Analysis Center rather than the local FBI field office.

As Canadian entities work to develop a compliance approach to CIP-001-1, at least one Regional Entity is finding there may need to be some specific NERC-issued guidance developed in conjunction with RCMP officials regarding establishment of CIP-001-1 contacts and sabotage reporting procedures appropriate to their circumstances.

Conclusion

Standard CIP-001-1 is the first ordered and adopted Critical Infrastructure Protection standard. Awareness, recognition, and reporting incidents or events of suspected sabotage are important BES reliability activities. The purpose of CIP-001-1 is that disturbances or unusual occurrences, suspected or determined to be caused by sabotage, would be reported to the appropriate systems, governmental agencies, and regulatory bodies. The recognition of sabotage as distinguished from other criminal acts such as spurious vandalism and or metal theft is an important aspect of responsible entities' awareness and recognition roles. Prompt recognition and appropriate reporting of sabotage can aid local law enforcement and the FBI or RCMP in maintaining appropriate situation awareness and in appropriately distinguishing criminal actors of ordinary vandalism from criminal actors intended to cause local or widespread disruption and damage to BES operators or beneficiaries.

Registered entities have made significant progress in achieving compliance with this standard, as violation submissions by the Regional Entities fell off significantly in the early portion of 2009; but this standard was still ranked as one of the top two violated reliability standards at the end of October 2009. Registered entities and Regional Entities must remain vigilant in enforcing compliance with this standard to maintain the reliable operation of the bulk electric system within the United States, Canada, and Mexico.

Contact Information

Michael A. DeLaura
NERC, Manager of Compliance Reporting,
Tracking, and Analysis
609-452-8060
mike.delaura@nerc.net

Eric Rollison
Engineer of Compliance Reporting, Tracking,
and Analysis
609-452-8060
eric.rollison@nerc.net

Barry Pagel
FRCC, Manager of Compliance
813-289-5644
bpagel@frcc.com

Marisa Sifontes
SERC, Interim Director of Compliance and
Legal Counsel
704-357-7372
msifontes@serc1.org

Wayne Van Osdol
MRO, Vice President of Compliance
651-855-1760
ww.vanosdol@midwestreliability.org

Ron Ciesiel
SPP, Executive Director, Compliance
501-614-3265
rciesiel@spp.org

Stan Kopman
NPCC, Assistant Vice President of
Compliance
212-840-1070
skopman@npcc.org

Mark Henry
TRE, Manager, Compliance Review &
Verification
512-225-7041
mark.henry@texasre.org

Ray Palmieri
RFC, Vice President and Director, Compliance
330-456-2488
ray.palmieri@rfirst.org

Connie White
WECC, Vice President of Compliance
801-582-0353
cwhite@wecc.biz

Mike Moon
NERC, Director of Compliance Operations
609-452-8060
michael.moon@nerc.net

Priority of Future ERO Compliance Analysis Reports

	NERC Analysis	RCIG Input Analysis	ERO Combined report to BOTCC	Posted to NERC Web site
CIP-001	Complete	Complete	May 12	May 13
VAR-002	Complete	June BOTCC		
PER-002	Complete	June BOTCC		
FAC-003	Initiated			
PRC-004	Next in Queue			
EOP-005	2 nd in Queue			

Completed reports are posted on the NERC Web site at:
<http://www.nerc.com/page.php?cid=3|329>

Document Version History

Version	Date	Reviewers	Revision Description
Draft v1.0	December 2009	NERC staff and Regions	Initial Draft of Collaborated Creation
Draft v1.1	April 30, 2010	NERC staff	<ol style="list-style-type: none"> 1. Modified Requirement 4 violation language in line with NERC Compliance Guidance included in October 2009 CIP RSAW; 2. Included footnote on NERC Compliance Guidance for Requirement R4; 3. Modified disclaimer language to emphasize use of material in line with formal guidance; 4. Modified page 4 reference to state that CIP-001 had four requirements, not four primary level requirements and no requirements.
v1.1	May 12, 2010	NERC staff	Posted