
Common Violations

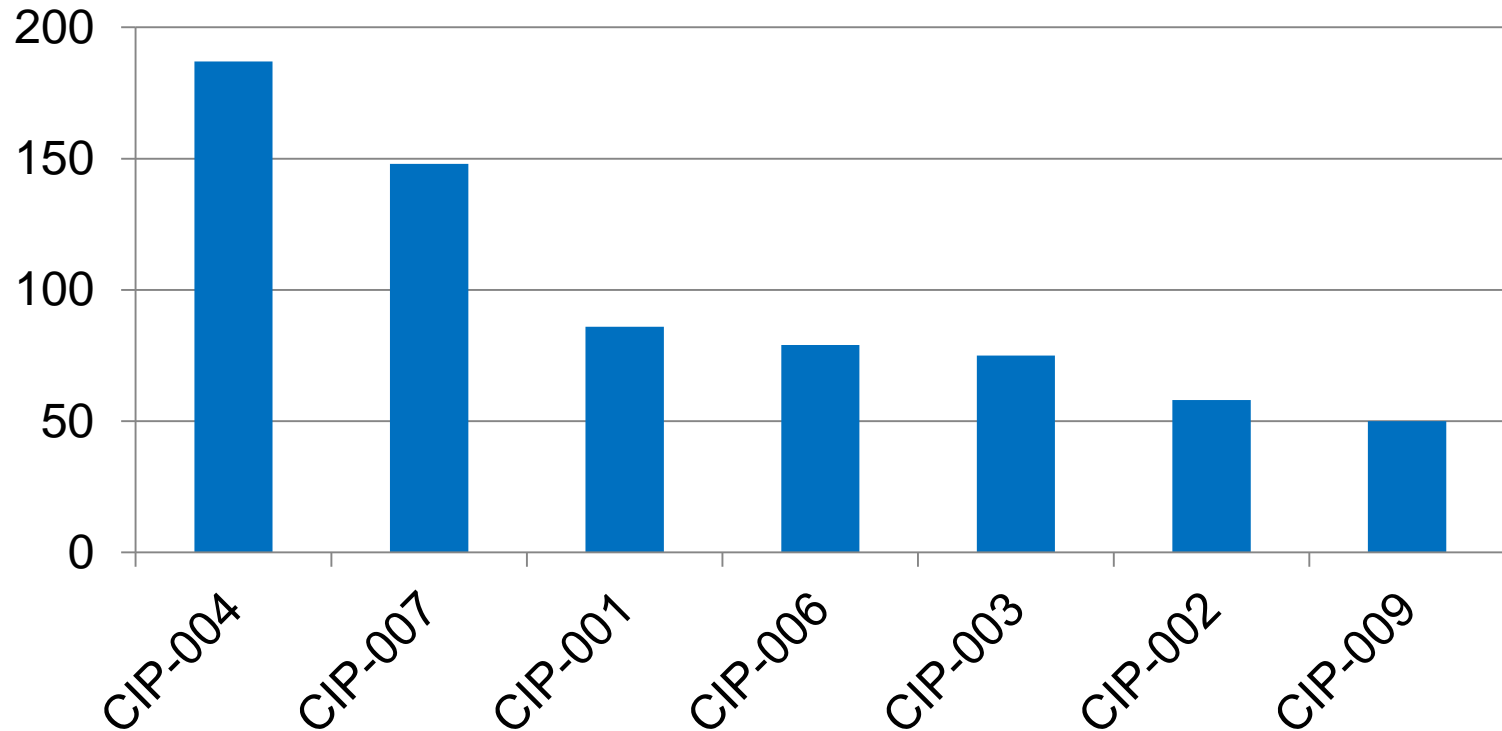
Kevin Bunch
CIP Engineer II

Overview

- **Violations from past year**
- **Common Reasons for Non-Compliance**
 - CIP-004
 - CIP-007
 - CIP-001
 - CIP-006
 - CIP-003
 - CIP-009

Most Commonly Violated CIP Standards 8-1-09 through 7-31-10

Number of Violations (All Regions)



www.nerc.com

CIP-004 Common Reasons for Non-Compliance

- **Training**
 - Not offered or completed by personnel with CCA access
 - Does not include all required items
- **Risk Assessment**
 - PRA not performed or incomplete for personnel with access to CCAs
- **Access**
 - Personnel granted access without proper clearance
- **Documentation**
 - Lack of records to demonstrate compliance

CIP-007 Common Reasons for Non-Compliance

- **Cyber Vulnerability Assessment**
 - Identify vulnerability assessment process
 - Action plans to mitigate vulnerabilities
 - Execution status of action plan
- **Account Management**
 - Identify personnel with access to shared accounts
- **Documentation**
 - Lack of records to demonstrate compliance

CIP-001 Common Reasons for Non-Compliance

- **Sabotage Reporting Deficiency**
 - Missing procedures for reporting events of sabotage
- **Communication Deficiency**
 - Procedures to communicate information regarding sabotage events to appropriate parties
- **Contacts**
 - Missing communication contacts to report sabotage events with local FBI
- **Documentation**
 - Lack of records to demonstrate compliance

CIP-006 Common Reasons for Non-Compliance

- **Physical Security Plan**
 - Visitor pass management
 - Response to loss
 - Inappropriate use of physical access
- **Documentation**
 - Lack of records to demonstrate compliance

CIP-003 Common Reasons for Non-Compliance

- **Cyber Security Policy**
 - Does not include all required items
 - Not accessible / Unaware of the policy's location
- **Information Protection Program**
 - Does not include all required items
 - Implementation of action plan to remediate deficiencies
- **Documentation**
 - Lack of records to demonstrate compliance

CIP-009 Common Reasons for Non-Compliance

- **Backup and Restore**
 - Recovery plans to include processes and procedures
- **Testing**
 - At least annually test backup media
- **Recovery Plans**
 - Actions in response to events
 - Roles and responsibilities
- **Documentation**
 - Lack of records to demonstrate compliance

Questions?

Please visit us at:
www.texasre.org



You may also submit questions to information@texasre.org

References

- <http://www.nerc.com/files/July%20Public%20Statistics%20Complete.pdf>
- http://www.nerc.com/files/CIP-004_Combined_FINAL.pdf
- http://www.nerc.com/files/20100512_ERO%20CIP-001%20Analysis%20draft%201.1_clean_final.pdf