



---

# **Documenting Compliance with CIP Standards**

**Janis Cline**  
**CIP Engineer II**

# Scope

- All registered entities are subject to audit of compliance with all reliability standards
- NERC delegated authority to regional entities to monitor and enforce compliance
- Goal is to improve reliability through effective and efficient enforcement of reliability standards
- Processes that may be used to monitor compliance include compliance audits, self-certifications, spot-checks, periodic data submittals, self-reporting and exception reporting

# CIP Standards Schedule

- Critical Infrastructure Protection (CIP) Standards:
  - Version 2 (04/10)
  - Version 3 (10/10)
- Implementation Plan
  - Implementation Schedule for Responsible Entities
  - Compliance Schedule (NERC Functional Model)
    - **Compliant (C):** entity meets full intent of the requirements, beginning to maintain “data”
    - **Auditably Compliant (AC):** entity meets the full intent of the requirement and can demonstrate compliance to an auditor

# Authority

**The authority to request and collect evidence of compliance is provided by the Federal Power Act 18 CFR 39.2 (d):**

***“Each user, owner or operator of the Bulk-Power System within the United States (other than Alaska and Hawaii) shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization and each applicable Regional Entity. The Electric Reliability Organization and each Regional Entity shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act.”***

- **FERC's Order 672 provides (in paragraph 114):**

“The Commission agrees with commenter's that, to fulfill its obligations under this Final Rule, the ERO or a Regional Entity will need access to certain data from users, owners and operators of the Bulk-Power System. Further, the Commission will need access to such information as is necessary to fulfill its oversight and enforcement roles under the statute.”

- **Section 3.0 of the Compliance Monitoring and Enforcement Program (CMEP):**

“The compliance program requires timely data from registered entities to effectively monitor compliance with reliability standards. If data, information, or other reports to determine compliance requested from a registered entity are not received by the required date, the Compliance Enforcement Authority may execute the steps described in Attachment 1, Process for Non-submittal of Requested Data. Registered entities may be assessed the most severe violation if the requested information or data is not provided.”

# Confidentiality

- Except as provided in the NERC Rules of Procedure, a receiving entity shall keep in confidence and not copy, disclose, or distribute any confidential information or any part thereof without the permission of the submitting entity, except as otherwise legally required.
- As required per FERC Order 706, Texas RE must secure and protect CIP data at all stages:
  - Requests
  - Delivery
  - Retention
  - Access

# Confidentiality – Data Submittal

- The submitting entity shall mark as confidential any information submitted to Texas RE or NERC that it reasonably believes contains confidential information in accordance with ROP Section 1500.
- Texas RE will retain CIP data as required by NERC ROP.
- If a submitting entity concludes that information for which it had sought confidential treatment no longer qualifies for that treatment, the submitting entity shall promptly notify NERC or the relevant regional entity.

# Confidentiality – Data Submittal

- **Identification of Confidential Information**
  - Category or categories as defined in Section 1501
    - Confidential Business and Market Information
    - Critical Energy Infrastructure Information (CEII)
    - Personnel information that identifies or could be used to identify a specific individual, or reveals personnel, financial, medical, or other personal information
    - Work papers, including records produced for or created in the course of an evaluation or audit
    - Investigative Files
    - Cyber Security Incident Information

# Compliance Monitoring and Enforcement

- Compliance Audit – an independent assessment of compliance by an entity with various laws or regulatory requirements
- NERC Compliance Monitoring and Enforcement Program (CMEP) conforms to the Generally Accepted Government Auditing Standards (GAGAS)
- CIP Auditing, Self-Certification, Self-Reporting, and Enforcement are new processes and are subject to change

# Texas RE CMEP Audit Process

- Texas RE CIP Auditing Tools: NERC CMEP, GAGAS, RSAWs, Standards
- Texas RE will not tell you how to become compliant with a standard:
  - Entities may contact Texas RE to ask questions.
  - Texas RE may guide you to the correct source.
- Texas RE will not provide an interpretation of a standard:
  - All requests for interpretations should be submitted to NERC.

# Texas RE CMEP Audit Process

- **60 days prior to audit**
  - Audit packets go out to entity requesting completed Reliability Standards Auditors Worksheets (RSAWs) and supporting documentation
  - Entity has 30 days to submit
- **30 days prior to audit**
  - Texas RE audit team reviews submitted information and prepares follow-up questions
- **Audit**
  - Evidence is corroborated and omissions addressed
  - Evidence needed for follow-up verification by Texas RE Enforcement is retained

# Evidence of Compliance

- The entity must demonstrate compliance
  - Evidence demonstrate policy in practice.
  - The entity must supply answers or documentation to prove compliance.
- If an entity has a contractual agreement with another company, the entity is responsible for demonstrating compliance with the NERC standard.
  - If a contractor violates a NERC Standard that is assigned to the entity, Texas RE will issue a violation to the entity assigned to that function.

# General Guidelines

- Audit Criteria – measurable, complete and relevant to objectives
- Control Procedures - used to ensure key activity type is controlled, monitored and documented
- Acceptable Documentation:
  - Policies
  - Procedures/Processes
  - Screenshots
  - Logs
  - Correspondence

# General Guidelines

## When Submitting Documentation:

- Labeling
  - Dates
  - Classification
  - Lists
- Redacting
  - Usability
- Relevancy
  - Support Action
- Record
  - Demonstrate Action

Can the document be understood without further explanation?

# General Guidelines

---

- Address all Elements of the Standards
  - Policies, procedures and plans
- Treat as a Single Group of Standards
  - Interrelated
- Use Consistent Language in Documentation
- Align Supporting Documentation with Policy/Processes/Procedures
- Do Not Assume Texas RE has any Information Besides the Information Provided

*Documentation, Documentation, Documentation.*

# Pre-Audit Evidence Review

- **CIP 002:**
  - Risk Based Assessment Methodology (RBAM)
  - Evidence that all required BES assets were evaluated by the RBAM for inclusion on the Critical Asset List
  - Critical Asset List derived through application of the RBAM
  - Evidence to support approval and review of lists (for applicable timeframe)

# Pre-Audit Evidence Review

- **CIP 003:**
  - Cyber Security Policy and all referenced policies and procedures
  - Evidence for annual review and approval of the policy
  - Appointment of Senior Manager
  - Appointments of delegations of responsibilities, if applicable
  - Exception Handling

# Pre-Audit Evidence Review

- **CIP 004:**

- Cyber Security Awareness Program
- Cyber Security Training Program
- Cyber Security Training Materials
- Cyber Security Training Schedule (for applicable timeframe)
- Personnel Risk Assessment Program
- List of Personnel with Access to CCAs
- Evidence to Support Access Control

# Pre-Audit Evidence Review

- **CIP 005:**
  - Description or Documentation for:
    - ESP(s) and CCA/non-CCA within ESP(s)
    - ESP Access Points
    - Ports and Services
    - Monitoring and Logging Access
    - Assessment

# Pre-Audit Evidence Review

- **CIP 006:**
  - Physical Security Plan
  - Evidence Supporting Annual Review and Update (for appropriate timeframe)
  - Description or Documentation of:
    - PSP(s)
    - PSP(s) Access Points
    - Access Control
    - Logging

# Pre-Audit Evidence Review

- **CIP 007:**
  - Test Procedures
    - Example
    - Form (if applicable)
    - Results
  - Logs (review, maintenance)
  - Description or Documentation for:
    - Ports and Services
    - Patch Management
    - CVAs
    - Disposal or Redeployment

# Pre-Audit Evidence Review

- **CIP 008:**
  - Cyber Security Incident Response Plan
  - Procedures for classifying events
  - Roles and Responsibilities, incident handling procedures and communication plans
  - Process for reporting incidents (ES-ISAC)
  - Evidence to support annual review and update of plan

# Pre-Audit Evidence Review

- **CIP 009:**
  - Critical Cyber Asset Recovery Plans
  - Conditions that activate CCA Recovery Plan
  - Recovery Actions
  - Evidence to support annual review and update to plan

# Audit Evidence Review

- **Additional evidence will be requested for on-site review.**
  - CIP related and protected data to be available on-site:
    - Critical Cyber Asset list, policy exceptions, details of personnel with access (including transfers and terminations), quarterly access reviews, cyber security controls (test plans and procedures), reportable incidents, and recovery plan exercises.
  - Samples of training, PRA, and cyber security controls testing.
  - Additional evidence deemed necessary to support determination of compliance.

# In Summary

- **Does the document reflect:**
  - Type of activity, action (testing)?
  - Include appropriate references?
  - Document control processes?
- **Is the document:**
  - Labeled correctly?
  - Relevant to the standard?
  - Dated and signed (if applicable)?
  - Updated correctly?
  - Easily located?

*Documentation, Documentation, Documentation.*

# Useful Links

- **NERC CMEP:**

[http://www.nerc.com/files/2010\\_NERC\\_CMEP\\_Implementation\\_Plan\\_093009.pdf](http://www.nerc.com/files/2010_NERC_CMEP_Implementation_Plan_093009.pdf)

- **Standards:**

<http://www.nerc.com/page.php?cid=2|20>

- **Implementation Plan:**

[http://www.nerc.com/fileUploads/File/Standards/Revised\\_Implementation\\_Plan\\_CIP-002-009.pdf](http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf)

- **GAGAS:**

<http://www.gao.gov/govaud/ybk01.htm>

- **Texas RE:**

<http://www.texasre.org>



# Questions?

Please visit us at:  
[www.texasre.org](http://www.texasre.org)



You may also submit questions to [information@texasre.org](mailto:information@texasre.org)