CIP Data Submittal Guidance

Compliance Audits & Spot Checks

805 LAS CIMAS PARKWAY, SUITE 200
AUSTIN, TEXAS 78746
(512) 583-4900

Purpose:

The intent of this document is to assist registered entities in understanding the engagement process for NERC CIP Cyber Security Standards (CIP Standards) and understand the necessary documentation to validate compliance. It is important to note that all Requirements and component Parts of the CIP Standards not listed within this document must be documented and implemented, although only Requirements and component Parts that are within the scope of the engagement are required for validation of compliance.

The initial submission may not be the only documentation that will be requested. Other documents that may be requested are those showing reasonable confidence of compliance with CIP Standards, such as samples of specific CIP Standards. NOTE: For CIP-014, documentation is to be retained at the registered entity site and not transmitted to Texas RE.

Documentation:

The registered entity must provide documentation of policies, processes, and procedures that are aligned with the CIP Standards. Further, the registered entity must provide detailed documentation of the implementation of those policies, processes, and procedures that verifies their completeness and accuracy. The documentation must contain sufficient information which:

- Enables an auditor to determine the completeness of the work, who performed the work, and the date such work was completed; and
- Enables an auditor to understand the nature, timing, extent, and results of the procedures performed, evidence documented, and conclusions reached.

The documented evidence must be complete, accurate, valid, reliable, and appropriately marked with its data security classification. Reliability Standards Audit Worksheet (RSAW) documentation must clearly reference the appropriate parts of the evidence (e.g., name of document, page number and paragraph).

Risk-Based Compliance Monitoring and Enforcement Program (Risk-Based CMEP):

Risk-Based CMEP originated from the Risk Assurance Initiative (RAI) and was approved by FERC on February 19, 2015. Risk-Based CMEP is a program in which Compliance Enforcement Authorities (CEA) create an audit scope tailored to a specific entity or registration and focused on areas of significant risk to the Bulk Electric System (BES). Risk-based engagements may not contain an engagement scope that includes all of the CIP Standards. The guidance below is for all the CIP Standards although not all Standards may be included in a given risk-based engagement.

Guidance for CIP-002-5.1a through CIP-014-2 Evidence Submission:

All guidance below is for the period in scope of the engagement and for the applicable BES Cyber Systems for the Standards and Requirements. The guidance below captures what is needed at a high level. Please review each Requirement and Part for discrete information. In a given engagement, not every CIP Standard may be in scope and the timeframe of the audit period may vary.

CIP-002-5.1a

R1: Provide documented evidence of the implemented process that:

- identifies high impact BES Cyber Systems (BCS);
- identifies medium impact BCS; and
- identifies each asset that contains a low impact BCS.

R2: Provide documented evidence the identifications in R1 were reviewed at least every 15 calendar months and that the CIP Senior Manager or delegate approved those identifications.

CIP-003-6

R1: Provide documented evidence of one or more cyber security policies.

R2: If applicable, provide one or more documented cyber security plans for low impact BCS.

R3: Provide documented evidence that a CIP Senior Manager has been identified and that changes to the CIP Senior Manager were documented within 30 calendar days of the change.

R4: If applicable, provide documentation that demonstrates the implementation of the process to delegate authority.

CIP-004-6

R1: Provide documented evidence that shows the implementation of the process to provide at least quarterly security awareness training.

R2: Provide documented evidence that shows security training was provided, evidence which demonstrates the training was provided prior to granting electronic and physical access, and was completed at least every 15 calendar months.

R3: Provide documented evidence that shows the implementation of a process to confirm identity, a process to perform a seven year criminal history records check, a process to evaluate criminal history records checks, a process that criminal history records checks are applied to contractors or service vendors, and the process that validates every person with physical or electronic access had a personal risk assessment within the last seven years.

CIP-005-5

R1: Provide documented evidence that shows the implementation of the process in which all applicable Cyber Assets connected with a routable protocol reside within an Electronic Security Perimeter (ESP), that all External Routable Connectivity goes through an Electronic Access Point which requires inbound and outbound access permissions (with rationale), that dial-up access requires authentication, and that there are one or more methods of detecting known or suspected malicious communications.

R2: If Interactive Remote Access is used, provide documented evidence that shows the use of an Intermediate System, that all Interactive Remote Access uses encryption ending at the

Intermediate System, and that multi-factor authentication is required for Intermediate Remote Access.

CIP-006-6

R1: Provide documented evidence that shows the implementation of the plan(s) that defines operational or procedural controls to restrict access, the use of at least one physical access control to allow authorized unescorted individuals, two or more different physical access controls to collectively allow authorized unescorted physical access into Physical Security Perimeters (PSP), monitoring physical access points, and the issuance of alerts within 15 minutes of detection, the monitoring of physical access to each Physical Access Control and Monitoring System (PACS), the issuance of alerts within 15 minutes of detection of unauthorized physical access to a PACS and logging the entry of personnel into the PSP, the retention of these logs for at least 90 days, and restricting physical access to cabling and other nonprogrammable communications components when located outside a PSP.

R2: Provide documented evidence that shows the implementation of the process that requires continuous escorted visitor access, log entry and exit of the PSP, and retention of logs for 90 days.

R3: Provide documented evidence that shows the implementation of the process that requires maintenance and testing of each PACS, which includes components, once every 24 months.

CIP-007-6

R1: Provide documented evidence that shows the implementation of the process that enables only logical network accessible ports that have been determined to be necessary and protects against the use of unnecessary physical input/output ports.

R2: Provide documented evidence that shows the implementation of the patch management process that tracks, evaluates, and installs cyber security patches (including the source of patches), reviews security patches for applicability within 35 days of release, installs the patch or creates/updates a mitigation plan, and implements the mitigation plan.

R3: Provide documented evidence that shows the implementation of the process that deploys methods to deter, detect, or prevent malicious code, mitigates detected malicious code, and the process to test and update signatures or pattern files.

R4: Provide documented evidence that shows the implementation of the process (or processes) that logs events at the BCS level or Cyber Asset level, generates alerts for security events, retains the logs for at least 90 calendar days, reviews a summary or sample of log events no more than every 15 days.

R5: Provide documented evidence that shows the implementation of one or more process(es) to: enforce authentication of interactive user access; identify and inventory all known enabled default or generic account types; identify individuals with access to shared accounts; change default passwords, per Cyber Asset capability; enforce password parameters which include password length and minimum password complexities; password changes no more than

every 15 months; and limit the number of unsuccessful logins or generate alerts after a threshold of unsuccessful authentication attempts.

CIP-008-5

R1: Provide documented evidence that shows the implementation of the process that identifies, classifies, and responds to Cyber Security incidents, determination of a reportable incident, roles and responsibilities of response groups, and incident handling procedures.

R2: Provide documented evidence that shows the implementation of the process that tests the response plans at least once every 15 months, document deviations from the plan when conducting the test, and retain records of reportable incidents.

R3: Provide documented evidence that shows the implementation of the process to update the response plan within 90 days of the incident or test; and within 60 days after a change to roles or responsibilities, and includes documentation of any lessons learned as well as communication to the individuals involved.

CIP-009-6

R1: Provide documented evidence that shows the process that describes the conditions for activating the recovery plan(s), roles and responsibilities, description of the backup and storage of information required to recover critical information, the process to verify successful completion of backup processes, and the process to preserve incident data.

R2: Provide documented evidence that shows the implementation of the process that tests the recovery plan(s) at least every 15 months, tests a sample of the information used to recover BCS functionality at least every 15 months, and tests the recovery plan(s) at least every 36 months.

R3: Provide documented evidence that shows the implementation of the process which shows that no later than 90 days after a test or actual recovery, and no later than 60 days after a change in roles/responsibilities, documentation occurred for lessons learned, updating the plan(s), and notification of the updates.

CIP-010-2

R1: Provide documented evidence which shows the implementation of the process that develops a baseline configuration, makes changes to the baseline, evaluates the changes, updates the baseline, and tests changes.

R2: Provide documented evidence that shows the implementation of the process that monitors for changes to the baseline configuration.

R3: Provide documented evidence that shows the implementation of the cyber vulnerability assessment (CVA) process.

R4: Provide documented evidence that shows the implementation of the process that includes Transient Cyber Assets and Removable Media.

CIP-011-2

R1: Provide documented evidence that shows the implementation of the process to identify and protect BCS Information.

R2: Provide documented evidence that shows the implementation of the process to prevent unauthorized retrieval of BCS Information prior to release, reuse, or disposal of Cyber Assets.

CIP-014-2

NOTE: For CIP-014, all evidence is to be retained at the registered entity site. This guidance should be used to facilitate the onsite review. Texas RE is not requesting this evidence to be transmitted. Retention of the evidence will be needed in such a manner that allows for enforcement process review (if needed) and future compliance monitoring efforts.

R1: Provide documented evidence that shows initial and subsequent risk assessments.

R2: Provide documented evidence that shows unaffiliated third party verification of the risk assessment(s) and subsequent actions based on the verification.

R3: Provide documented evidence that shows notification of operational control, if applicable.

R4: Provide documented evidence that shows an evaluation of threats and vulnerabilities.

R5: Provide documented evidence that shows a documented physical security plan.

R6: Provide documented evidence that shows unaffiliated third party verification of the physical security plan.