CIP-014 Evidence Review and Data Handling Process

The authority to request and collect evidence of compliance is provided by the Code of Federal Regulations (18 CFR § 39.2) which states:

"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."

It is incumbent upon registered entities to mark any document as confidential where appropriate prior to disclosing such information to Texas Reliability Entity, Inc. (Texas RE). In addition to marking documents prior to producing them in response to a pre-engagement questionnaire or request for information, the registered entity should be prepared to mark documents as necessary that are requested during the on-site engagement. Pursuant to the provisions of Section 1500 of the NERC Rules of Procedure, Texas RE will take appropriate and reasonable steps to protect the confidentiality of all reviewed evidence. Please take note that NERC and FERC staff may ultimately receive access to any information disclosed to Texas RE either by their participation in the engagement team or in subsequent review of the engagement record.

Texas RE recognizes the sensitivity of certain information reviewed or collected during the course of any Critical Infrastructure Protection (CIP) engagement and the desire by some registered entities to retain control over the information in order to minimize risk exposure. To accommodate the needs of both Texas RE and registered entities, the following protocols are defined for engagements containing CIP-014 requirements:

1. Data reviewed while the engagement team is on-site shall be delivered as agreed to by the registered entity and the engagement team. (Note: Texas RE recommends no specific location or Facility be represented in the evidence file names.)

2. Upon review of the CIP-014 on-site evidence, the engagement team will verify the evidence including document names (and file names).

3. The engagement team will review the CIP-014 evidence with the identified subject matter expert(s) (SMEs).

4. Following completion of the on-site phase of the engagement and before departing the site, the engagement and registered entity team members will place and confirm all audit record evidence in a secure method provided by the registered entity. The secure method could be encryption, physical access controls, etc. in media such as Tyvek envelopes, CD-R, DVD-R, writable USB devices, and/or other media mutually agreeable to registered entity personnel and Texas RE. The CIP-014 documentation shall remain accessible to

Texas RE. The CIP-014 documentation shall be retained by the registered entity for the full regulatory retention period determined through the utilization of a compliance monitoring process as supported by the Rules of Procedure and supporting ERO processes (NOTE: This is, at the minimum, a three year period as indicated in the Data Retention section of the Standard. There is a Rules of Procedure proposed change that may extend that to five years) This documentation must be made available during the full regulatory retention period upon reasonable notice following completion of the engagement.

5. The registered entity shall not dispose of the engagement records without the express written consent of Texas RE.

6. The engagement team will retain brief notes and listing of evidence file names in RSAWs to support CMEP activities.

7. RSAWs shall be completed in such a manner that no CIP-014 critical data is revealed (e.g., locations, actions, inactions, etc.). RSAWs shall be simply a listing of evidence reviewed, brief notes, and disposition determined. No highly specific details shall be retained by Texas RE staff.

8. Non-public reporting shall consist of a listing of evidence reviewed, brief notes, and disposition determined. As with any CIP engagement, all references to CIP will be removed for the public report.

Further, evidence in the ERO Enterprise's possession as a result of CMEP activities performed for other Reliability Standards, such as the cybersecurity-related Critical Infrastructure Protection (CIP) Reliability Standards and Transmission Planning (TPL) Reliability Standards, is not subject to the site restrictions of CIP-014 and may be used to assess the adequacy of CIP-014 evidence.

If you have any questions regarding this guidance please reach out to compliance@texasre.org.