Appendix A3: Northeast Power Coordinating Council (NPCC) 2019 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the NPCC as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

- NPCC will continue to offer formal O&P Internal Control Evaluations to all entities on the 2019 audit schedule.
- NPCC will also offer to perform CIP Internal Control Evaluations on entities that have already had their initial CIP Version 5 audit.
- NPCC will refresh existing IRA's and use the 2019 ERO and NPCC Implementation Plans to develop Compliance Oversight Plans (COPs) for its 2019 monitoring engagements.

Other Regional Key Initiatives & Activities

- In 2019, NPCC will continue with a cyber-security and physical security outreach program for volunteering entities.

Regional Risk Assessment Process and Results

NPCC considers the Risk Elements identified in the ERO CMEP Implementation Plan and the Risk Factors identified in the ERO Guide for Compliance Monitoring to identify important reliability risks within NPCC's footprint. If NPCC concludes that any of the ERO Risk Elements are not relevant reliability risks within NPCC's footprint, NPCC will provide documented rationale.

NPCC determines whether any additional regional risks specific to the NPCC footprint, but sufficiently different from the risks identified in the ERO Implementation Plan, should be added as Regional Risk Elements into the NPCC Implementation Plan. Input into Regional Risk Element determination can take the form of Enforcement trends, audit team observances, ERO or Regional events, issues raised by NERC or stakeholder groups, etc. Often, additional regional risks specific to the NPCC footprint may be categorized within a NERC identified Risk Element and would not likely require an additional Regional Risk Element.
In the event NPCC identifies an additional Regional Risk Element that is not included in the ERO CMEP Implementation Plan, NPCC will provide justification and documentation regarding the additional Regional Risk Element.

In the development of the standards and requirements that appear in this regional plan, NPCC considered the 2019 ERO Risk Factors and other tangible Bulk Electric System (BES) attributes such as entity functional registration, transmission assets, Remedial Action Schemes, black start plans and facilities, generation assets, role of Under Frequency Load Shedding (UFLS) , Enforcement trends, historical events, etc.

NPCC did not expand the requirements under ERO Risk Elements.

NPCC identified three Regional Risk Elements for 2019.

Regional Risk Elements and Areas of Focus

The table below contains NPCC Regional risk elements, for focus during 2019, based on the NPCC's Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of a registered entity's compliance oversight plan (COP).

Table A3.2: Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Improper BES Cyber System Classification	In order to verify proper classification of BES Cyber Systems, and ensure appropriate protections are applied, NPCC will review select entities for compliance to CIP-002-5.1.	CIP-002-5.1, R1, R2
Improper UFLS Settings	Although rarely used, UFLS schemes owned by the TO and DP are an extremely important aspect in limiting the extent of major disturbances. This is especially true in NPCC which has transmission corridors that are of the radial nature. As such, NPCC has a regional UFLS standard and will focus on the design and implementation of UFLS programs which are key in order to prevent a total system blackout like those that occurred in 1965, 1977, and 2003. In addition, the proper underfrequency settings at the GO directly correlate to the success of the UFLS program.	PRC-006-NPCC-1 R4 (TO, DP) R7 (TO, DP) R13 (GO)
Failure to Report Generator Capabilities	Accurate generator capabilities are necessary for the planning and operation of a reliable bulk electric system. This Standard is the leading non-compliance issue in the NPCC footprint on 2018. While the violations were not deemed to be highly impactful individually, the high number of non-compliance issues is a concern.	MOD-025-2, R1, R2

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2019 implementation year.

Compliance Audits

The NPCC Compliance Monitoring Plan includes the 2019 Compliance Audit Plan that lists all planned audits for registered entities during the 2019 implementation year. The 2019 Compliance Audit Plan, located on NPCC's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2019 Compliance Audit Plan for NPCC is located here: Audit Schedules. Throughout the implementation year, NPCC may make updates to the 2019 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

NPCC conducts spot checks based on a registered entity's COP, or at RE discretion at any time. NPCC may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. NPCC will follow the process outlined in Appendix 4C of the NERC ROP to initiate and conduct a Spot Check.

Self-Certifications

NPCC determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. NPCC will follow the NERC ROP for notifying registered entities of any Self-Certifications, ensuring advanced notice according to the NERC ROP.

NPCC will conduct Self-Certifications for Entities that have Low Impact BES Cyber Systems to ensure that the entity has completed its assessment of cyber assets properly. As shown in the table below, NPCC will perform Self-Certifications on a quarterly basis in 2019, with a 45-day advance notice given to the entity. The entity will receive the notice of the requirement covered by the Self-Certification and will be instructed to submit their compliance documentation into the NPCC compliance portal. Only a subset of the entities registered for the function that applies to the chosen requirement will receive the Self-Certification notification in the particular quarter.

Table A3.2: Self-Certification Schedule

Quarter 1			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	January 22	March 8
Quarter 2			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	April 15	May 30
Quarter 3			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	July 15	August 29
Quarter 4			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	October 15	November 29

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. NPCC follows the ERO Enterprise 2019 Periodic Data Submittal posted here: Periodic Data Submittals.

Compliance Outreach

Table A3.3: Compliance Outreach Activities

Outreach Activity	Anticipated Date
Spring and Fall Workshops – NPCC holds semi-annual workshops as a primary mechanism for outreach to registered entities.	May 2019 November 2019
Introduction to NPCC for Beginners – NPCC provides an introductory class for those new to CMEP activities prior to the May and November workshops.	May 2019 November 2019

Table A3.3: Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
Physical Security Information Exchange Sessions - The sessions take place at the May and November workshops and address NPCC Awareness Programs, Security Strategies, and subjects such as CIP-014 implementation, and evolving physical threats to the electric industry.	May 2019 November 2019
CIP and O&P Internal Controls Evaluation (ICE) Outreach Session – The sessions will take place at the May and November workshops to provide awareness and promote participation in the program. It will provide NPCC's purpose, approach and implementation of the voluntary ICE process, including expectations, tools, education/examples, best practices, deliverables, and feedback into Risk-Based CMEP.	May 2019 November 2019
Cyber Security Outreach for Non-Nuclear Generators – This will provide guidance to non-nuclear sites on all facets of their on-site cyber security.	Throughout 2019
Physical Security Outreach for Non-Nuclear Generators – This will provide guidance to non-nuclear sites on all facets of their on-site physical security.	Throughout 2019
Individual Meetings with Registered Entities – NPCC will meet with registered entities for specific CMEP related issues if requested and warranted.	
CDAA – NPCC will issue announcements via CDAA (the NPCC Compliance Portal) informing registered entities of CMEP aspects.	
Webinars – NPCC will conduct CMEP related webinars as needed. NPCC conducts pre-ICE webinars for all participants.	
FAQs – NPCC will post FAQs on an as needed basis.	
Compliance Guidance Statements – NPCC may issue Compliance Guidance Statements to offer clarification on the compliance approach associated with the NERC Rules of Procedure, NERC Reliability Standards, or NPCC Regional Reliability Standards.	
Registered Entity Surveys – NPCC will issue surveys to registered entities on an as needed basis. Such surveys have included acquiring registration data, BES element data, workshop content preferences, etc.	
Website – The NPCC website provides information in the areas of Standards, Registration, Compliance Monitoring, and Compliance Enforcement.	