Separation Protocol Applicable to E-ISAC and NERC

The North American Electric Reliability Corporation ("**NERC**") and the Electricity Information Sharing and Analysis Center ("**E-ISAC**"), as an internal division of NERC, have established this Separation Protocol to facilitate information sharing with E-ISAC and to delineate the policy regarding information sharing and functional separation between E-ISAC and NERC personnel and actions. Capitalized terms used herein but not defined shall have the meanings given to them in the E-ISAC Code of Conduct effective May 16, 2015.

1. E-ISAC's primary function of information sharing and analysis related to security-related threats, vulnerabilities and incidents are to be separated from NERC's broader functions of compliance monitoring and enforcement consistent with (a) this Separation Protocol; (b) the Policy on the Role of the [E-ISAC] vis-à-vis NERC's Compliance Monitoring and Enforcement Program" approved by the NERC Board of Trustees on March 8, 2013, as amended from time to time; (c) the [E-ISAC] Code of Conduct; and (d) any further applicable policies implemented by NERC or E-ISAC (collectively, the "**E-ISAC Policies**").

2. Information and communications related to situational assessments and security-related threats, vulnerabilities and incidents within the electricity subsector (collectively with all Protected Information, as defined in the E-ISAC Code of Conduct, and Confidential Information, as defined in Section 1500 of the NERC Rules of Procedure, including any related member information or details, the "**Prohibited Information**") shall not, directly or indirectly, be shared with any NERC personnel other than E-ISAC Personnel except in strict adherence with the E-ISAC Policies.

3. E-ISAC Personnel shall not, directly or indirectly through a conduit, report or convey information about possible violations they may encounter or learn about in the course of their E-ISAC activities, including without limitation any Prohibited Information, to any NERC personnel, including, without limitation, CMEP Personnel. CMEP Personnel shall not, directly or indirectly, obtain or seek to obtain Prohibited Information, directly or indirectly through a conduit. Any contractor, consultant, agent or other third party who may receive Prohibited Information from E-ISAC will be familiar with and subject to the E-ISAC Policies and shall report any violations or suspected violations in accordance with their terms.

4. With respect to employees conducting E-ISAC functions, the following processes will be put in place:
   - Physical separation of work space -- The work space of E-ISAC Personnel will be physically separated from the work space of CMEP Personnel.
   - Restricted physical access to Prohibited Information – Except as otherwise provided in the E-ISAC Policies, Prohibited Information will be physically protected from non-E-ISAC Personnel

by locked files, password protected computers, and removing such information from view when it is not being used.

- Restricted electronic access to Prohibited Information – Except as otherwise provided in the E-ISAC Policies, Prohibited Information will be electronically protected from non-E-ISAC Personnel by restricted access to any server or shared drive that includes such information. Access to these servers and shared drives by E-ISAC Personnel will require pre-approval under an authorization process administered by the CSO.

5. E-ISAC and NERC may use shared support services in a manner consistent with the E-ISAC Policies including those provisions related to protection of Prohibited Information and indirect information sharing through conduits. All personnel providing such shared services are to be familiar with and subject to the E-ISAC Policies and shall report any violations or suspected violations in accordance with their terms. Personnel providing shared services (such as management, external affairs, information technology, legal and human resources personnel, among others, to the extent they provide services to E-ISAC Personnel and non-E-ISAC Personnel) shall take all reasonable precautions to prevent disclosure of Prohibited Information to non-E-ISAC Personnel including:
   - Maintaining separate files for Prohibited Information to prevent its commingling with general NERC information.
   - Diligently protecting Prohibited Information from being released to non-E-ISAC personnel, directly or indirectly through a conduit (including in shared meetings or facilities).
   - Sharing Prohibited Information only with E-ISAC Personnel with a business need to know such information.
   - Including clear disclaimers on documentation or correspondence related to or containing Prohibited Information that such information is not to be shared with non-E-ISAC Personnel.
   - Reviewing all documentation shared with non-E-ISAC Personnel to verify that it is free of Prohibited Information prior to distribution.

6. This Separation Protocol will be reviewed for effectiveness and to determine if any changes are necessary no less than annually in the same manner as the E-ISAC Code of Conduct.

Effective: February 1, 2016