NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Electricity Information Sharing and Analysis Center Code of Conduct

## 1.0 Purpose

### 1.1

The purpose of this Code of Conduct is to outline the parameters within which the Electricity Information Sharing and Analysis Center (E-ISAC) may share Protected Information, as that term is defined herein, outside of the E-ISAC and across the ERO Enterprise. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity industry. The E-ISAC gathers and analyzes physical and cyber security data; shares security information and mitigation strategies with its stakeholders; and coordinates incident management. Analyzing security threats and incident information, and providing situational assessments help maintain and enhance bulk power system (BPS) reliability.

### 1.2

The North American Electric Reliability Corporation (NERC) operates the E-ISAC. The NERC Board of Trustees (Board) has long recognized the importance of promoting robust information sharing between the E-ISAC and electric sector participants. In February 2012, the NERC Board of Trustees adopted its "*Policy on the Role of the [E-ISAC] vis-à-vis NERC's Compliance Monitoring and Enforcement Program*" (Policy).[1] The Policy addresses concerns that electric sector participants may be reticent to share information with the E-ISAC due to NERC's responsibility to monitor compliance with and enforce mandatory Reliability Standards as the certified Electric Reliability Organization (ERO) under Section 215 of the Federal Power Act. The purpose of the Board Policy was to establish a clear separation between the E-ISAC and the ERO Enterprise's Compliance Monitoring and Enforcement Program (CMEP). In the Policy, NERC outlines the following general principles:

#### 1.2.1

E-ISAC personnel shall not, directly or indirectly, report or convey information about possible violations they may encounter or learn about in the course of their E-ISAC activities to the compliance monitoring and enforcement program or to personnel assigned to that program; and

#### 1.2.2

Compliance monitoring and enforcement personnel shall not, directly or indirectly, obtain or seek to obtain information about possible violations of Reliability Standards from E-ISAC personnel.

#### 1.2.3

The E-ISAC and E-ISAC Personnel shall have no responsibilities for CMEP activities.

### 1.3

This Code of Conduct furthers the principles of the Policy and outlines the parameters within which E-ISAC personnel can share Protected Information outside of the E-ISAC.

[1] *Available at*: http://www.esisac.com/Public%20Library/Documents/E-ISACFirewallPolicy.pdf.

## 2.0 Scope and Applicability

This Code of Conduct applies to all personnel of the organizations comprising the ERO Enterprise, and covers all E-ISAC Information, as that term is defined herein.

## 3.0 Definitions

### 3.1 Bulk Power System Awareness (BPSA) Department

One of the two departments that make up the Reliability Risk Management (RRM) group, which in cooperation with the Reliability Assessments and Performance Analysis group carries out the ERO's statutory responsibility to perform assessments of the reliability and adequacy of the BPS.

### 3.2 BPSA Department Personnel

NERC employees and contractors in the BPSA Department.

### 3.3 CMEP

The ERO Enterprise Compliance Monitoring and Enforcement Program, the purpose of which is to monitor, enforce, and ensure compliance with the ERO's mandatory Reliability Standards. The CMEP is administered by NERC's Compliance Assurance and the Compliance Enforcement departments and the equivalent departments of the Regional Entities.

### 3.4 CMEP Personnel

All personnel of the organizations comprising the ERO Enterprise who are engaged in compliance monitoring and enforcement duties and related CMEP processes, including activities conducted pursuant to Appendix 4c of the NERC Rules of Procedure. CMEP Personnel include employees and contractors of NERC's Compliance Enforcement and Compliance Assurance departments and the compliance and enforcement personnel of the Regional Entities.

### 3.5 E-ISAC Information

Any information that E-ISAC Personnel learn about in the course of their E-ISAC activities that supports the E-ISAC's mission of rapidly disseminating cyber and physical threat and vulnerability information, and mitigation strategies to industry.

### 3.6 E-ISAC Personnel

The NERC officer responsible for the E-ISAC as well as all NERC employees and contractors who report to that officer.

### 3.7 ERO Enterprise

NERC and the Regional Entities.

### 3.8 Oversight Team

This team is comprised of the NERC President and CEO, the NERC officer responsible for BPSA, the NERC officer responsible for the E-ISAC, the NERC officer responsible for Compliance Assurance, the NERC General Counsel and an executive from each Regional Entity appointed by the Regional Entity. The Oversight Team monitors implementation of this Code of Conduct.

### 3.9 Protected Information

A subset of E-ISAC Information that is voluntarily reported to assist the E-ISAC in its analysis and identification of emerging threats and that is not otherwise reported to any other NERC department. Protected Information is generally provided to the E-ISAC as "***Attributed Protected Information,***" which is Protected Information that contains the identity of the entity reporting the information and/or the identities of other entities and/or information about specific locations of assets that may be subject to threats or vulnerabilities as set forth in the Protected Information submitted to the E-ISAC. ***"Unattributed Protected Information***" is ***Protected Information*** that that does not contain the identity of entities or specific locations of assets, either because such information was not submitted to the E-ISAC or because the E-ISAC has removed such information. Protected Information may be submitted by entities concerning facilities both within and outside of the BPS as well as by entities that are not NERC registered entities.

Information that is reported to any other NERC department or to the government is not Protected Information for the purposes of this E-ISAC Code of Conduct. However, all NERC employees, including E-ISAC personnel, are nonetheless governed by this Code of Conduct at all times. Information that is not Protected Information under this Code of Conduct is subject to any applicable confidentiality policies that apply to such information and to all NERC employees.

The following information is specifically identified as not constituting Protected Information for purposes of this Code of Conduct:

(i) Information mandated by NERC Reliability Standards or other applicable governmental authority's laws, rules, regulations, or orders;

(ii) Information required by Department of Energy Form OE-417, NERC EOP-004 reports, and Federal Energy Regulatory Commission Order Nos. 693, 706, and 761;

(iii) Information voluntarily provided to NERC through the Event Analysis (EA) program;

(iv) Information that is discovered or reported pursuant to a compliance monitoring method (whether self-identified or externally identified) set forth in the CMEP; or

(v) Information that is otherwise publicly available or simultaneously reported

### 3.10 Regional Entity

An entity having enforcement authority pursuant to 18 C.F.R. § 39.8.

### 3.11 Regional Entity Administrator

The employee of a Regional Entity responsible for overseeing the Regional Entity's participation in E-ISAC activities and managing Regional Entity Designated Personnel.

### 3.12 Regional Entity Designated Personnel

Regional Entity employees designated and approved by the Regional Entity Administrator for their Regional Entity to have access to E-ISAC applications, including the E-ISAC Portal.

### 3.13 NERC Senior Management

For purposes of this Code of Conduct, NERC Senior Management includes NERC's President and CEO, the NERC officer responsible for BPSA, the NERC officer responsible for the E-ISAC, and the NERC General Counsel.

## 4.0 Department Responsibilities and Functions

### 4.1 BPSA Department

Works with Regional Entities and registered entities to monitor and assess present conditions on the BPS using various software tools and applications and enabling human analysis. This department communicates and coordinates with Regional Entities and registered entities to share information with them regarding various types of threats and conditions (terrestrial and space weather, cross-sector interdependencies, significant non-BPS events, etc.) that could negatively impact the reliability of the BPS and ultimately the ability to serve load. The BPSA Department also administers the NERC Alert program for development and distribution of important reliability- and security-related notifications. Additionally, when significant BPS disturbances occur, the BPSA Department facilitates the coordination of communications between Regional Entities, registered entities and applicable governmental authorities. This department does not execute or support any compliance or enforcement department responsibilities.

### 4.2 Compliance Enforcement Department

Oversees enforcement processes, applies penalties or sanctions or mitigation activities to prevent recurrence of remediated issues or confirmed violations. It also monitors the Regional Entity enforcement processes, collects and analyzes compliance enforcement and violation data, and files notices of penalty.

### 4.3 Compliance Assurance Department

Develops baseline monitoring requirements, overseeing Regional Entities' delegated compliance functions, holds education programs on industry compliance, and trains auditors.

### 4.4 E-ISAC

Gathers information from electricity industry participants about security-related events, disturbances, and off-normal occurrences within the electricity subsector and shares that information with industry and government partners. The E-ISAC regularly receives classified and non-classified information on potential threats to the electricity subsector. Using this information, the E-ISAC develops alerts and notifications for distribution to registered entities. It uses a secure Portal to receive voluntary reports from both NERC registered entities and other sector participants who are not NERC registered entities. E-ISAC does not execute or support any compliance or enforcement department responsibilities.

## 5.0 Separation of Functions

### 5.1

E-ISAC Personnel, Regional Entity Administrators, and Regional Entity Designated Personnel must not execute or support any CMEP functions or responsibilities.

**5.2**
CMEP Personnel of the organizations comprising the ERO Enterprise must not execute or support any E-ISAC functions or responsibilities and cannot have access to the E-ISAC Portal or other applications. Regional Entity CMEP Personnel cannot serve as Regional Entity Administrators nor be designated as Regional Entity Designated Personnel, and they cannot have access to the E-ISAC Portal or other applications.

# 6.0 Information Sharing

## 6.1 General Restrictions

### 6.1.1
Any personnel of the organizations comprising the ERO Enterprise who receive Protected Information shall not, directly or indirectly through a conduit, report or convey such information to any personnel of the organizations comprising the ERO Enterprise that is not E-ISAC Personnel, a Regional Entity Administrator, or Regional Entity Designated Personnel, except as permitted herein.

### 6.1.2
CMEP Personnel shall not, directly or indirectly through a conduit, obtain or seek to obtain Protected Information.

## 6.2 Unattributed and Attributed Protected Information

### 6.2.1
BPSA Department Personnel provide situational awareness of any potential threats to BPS reliability, and do not execute or support any CMEP responsibilities.

### 6.2.2
For the purpose of maintaining situational awareness of issues that affect the reliability of the BPS, the NERC officer responsible for the E-ISAC, or their designee, may share Unattributed Protected Information with BPSA Department Personnel.

### 6.2.3
The sharing of Attributed Protected Information is restricted to (i) E-ISAC Personnel, (ii) NERC's President and CEO; (iii) NERC's General Counsel, for the sole purpose of providing legal advice to NERC; (iv) those persons and entities for which the submitting entity has provided permission prior to any such sharing; and (v) those persons and entities authorized to receive such attributed Protected Information pursuant to policies approved by the Electricity Subsector Coordinating Council. For the avoidance of doubt, in no event shall any personnel of the organizations comprising the ERO Enterprise share Attributed Protected Information with either CMEP Personnel or individuals outside of the E-ISAC except as authorized herein or as required by law upon the advice of the NERC General Counsel and, where applicable, the appropriate Regional Entity General Counsel.

#### 6.2.4
E-ISAC Personnel may share aggregated Unattributed Protected Information with: (1) E-ISAC Members; (2) governmental partners; (3) cross-sector and other partners; and (4) personnel of the organizations comprising the ERO Enterprise for the limited purposes of: (i) enhancing situational awareness and understanding of actual or potential cyber or physical security incidents that are causing or have the potential to cause reliability events on the BPS; and (ii) developing and communicating mitigation strategies for potential or actual cyber or physical security incidents. The sharing of Unattributed Protected Information is subject to any additional conditions set forth by NERC Senior Management.

## 7.0 Access Restrictions

### 7.1 General Requirements
As a general matter, all Protected Information shall be maintained by the E-ISAC and the Regional Entities in a manner that does not permit physical or electronic access by any personnel of the organizations comprising the ERO Enterprise who are not E-ISAC Personnel, Regional Entity Designated Personnel, or Regional Entity Administrators. Personnel of the organizations comprising the ERO Enterprise who are not E-ISAC Personnel, Regional Entity Designated Personnel, or Regional Entity Administrators shall not have or seek access to any Protected Information without coordination with the NERC officer responsible for the E-ISAC, or their designee, pursuant to this Code of Conduct.

### 7.2 E-ISAC Physical Access Restrictions

#### 7.1.1
Access to the E-ISAC operations room shall require keycard access.

#### 7.1.2
Only E-ISAC Personnel know the combination to the E-ISAC operations room safe in which E-ISAC Personnel store keys to cabinets containing sensitive documents.

#### 7.1.3
The office of the NERC officer responsible for the E-ISAC shall require key access and is otherwise locked and only accessible by E-ISAC Personnel.

### 7.2 E-ISAC Electronic Access Restrictions

#### 7.2.1
Only E-ISAC Personnel and designated information technology personnel have unrestricted access to the E-ISAC Portal and other E-ISAC applications.

#### 7.2.2
E-ISAC Members and partners, Regional Entity Administrators, and Regional Entity Designated Personnel have varied, but restricted access to E-ISAC Portal, which enables them to post information and view information posted by others, depending on the manner in which the information is posted on the Portal.

#### 7.2.3
All systems and applications housed in the E-ISAC shall be secured using user identification and password protection controls assigned only to E-ISAC Personnel and designated information technology personnel.

### 7.3 Regional Entity Access Restrictions

#### 7.3.1 Physical Access Restrictions
Access to areas in which a Regional Entity stores E-ISAC Information shall require key access or shall be otherwise locked and only accessible to the Regional Entity Administrator or Regional Entity Designated Personnel.

#### 7.3.2 Electronic Access Restrictions
All Regional Entity systems and applications housing E-ISAC Information shall be secured using user identification and password protection controls assigned only to the Regional Entity Administrator and Regional Entity Designated Personnel.

## 8.0 Code of Conduct Oversight Team

### 8.1
The Oversight Team will oversee implementation of this Code of Conduct.

### 8.2
The NERC officer responsible for the E-ISAC and the NERC officer responsible for the BPSA Department shall meet periodically with the Oversight Team to assess whether the BPSA Department is receiving useful information from the E-ISAC and whether any changes to the Code of Conduct are warranted.

## 9.0 Training and Certification

### 9.1
Every year, all personnel of organizations comprising the ERO Enterprise must undergo Code of Conduct training and complete a written certification demonstrating that they have read and understood the provisions of this Code of Conduct as well as any changes that have been made since the last effective policy.

## 10.0 Enforcement

### 10.1
Any questions regarding interpretation or clarification of this Code of Conduct should be directed to the NERC General Counsel and the General Counsel of the appropriate Regional Entity, as applicable.

### 10.2
The NERC General Counsel shall investigate any claims of breach of this Code of Conduct. For any claims of breach involving Regional Entity personnel, the NERC General Counsel shall work with the applicable Regional Entity General Counsel.

### 10.3
Personnel of the organizations comprising the ERO Enterprise who wish to report a potential violation of this Code of Conduct should contact the NERC General Counsel and their Regional Entity General Counsel, as applicable. In accordance with the "Policy on Reporting Complaints Regarding Accounting and Code of Conduct Matters," the organizations comprising the ERO Enterprise prohibit retaliation against employees who submit Code of Conduct complaints in good faith.

### 10.4
Personnel of organizations comprising the ERO Enterprise must immediately notify the NERC General Counsel and their Regional Entity General Counsel, if applicable, upon learning of a violation of this Code of Conduct.

### 10.5
Any personnel of organizations comprising the ERO Enterprise who is found to have violated this Code of Conduct and/or failed to report such a violation may be subject to disciplinary measure up to and including termination.

## 11.0 Records and Records Retention

### 11.1
The following records related to compliance with this Code of Conduct must be retained by NERC in compliance with NERC's Data and Record Retention Policy:

#### 11.1.1
The annual, written certifications completed by all NERC employees demonstrating that these personnel have read and understood the provisions of this Code of Conduct as well as any changes that have been made since the last effective policy.

#### 11.1.2
The electronic log, maintained by the NERC officer responsible for the E-ISAC or their designee, of all Attributed Protected Information that is shared outside of the E-ISAC.

### 11.2
The following records related to compliance with this Code of Conduct must be retained by each Regional Entity in compliance with a Regional Entity's Data and Record Retention Policy:

#### 11.2.1
The annual, written certifications completed by all of the Regional Entity's employees demonstrating that these personnel have read and understood the provisions of this Code of Conduct as well as any changes that have been made since the last effective policy.

**11.2.2**

The list of Regional Entity Designated Personnel maintained and updated by each Regional Entity Administrator annually.

## Version History

| Version | Date | Action |
|---|---|---|
| **1.0** | May 16, 2014 | Adopted |
| **1.1** | March 11, 2015 | Revised |
| **1.2** | September 2, 2020 | Revised |
| **2.0** | July 17, 2023 | Revised to apply across ERO Enterprise |