NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Electricity Sector Information Sharing and Analysis Center Code of Conduct

(Effective May 16, 2014; Revised March 11, 2015)

1.0 Purpose

1.1

It is the North American Electric Reliability Corporation's (NERC) policy to protect all information submitted to NERC that contains Confidential Information, as that term is defined in section 1500 of the NERC Rules of Procedure. NERC shall keep in confidence and not copy, disclose, or distribute any Confidential Information or any part thereof without the permission of the entity that submits the Confidential Information, except as otherwise legally required. NERC shall ensure that its officers, trustees, directors, employees, subcontractors and subcontractors' employees, and agents to whom Confidential Information is exposed are under obligations of confidentiality and abide by all NERC rules and processes relating to access and management of Confidential Information.

1.2

NERC, in its role as the Electric Reliability Organization (ERO) and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), gathers information and communicates situational assessments and security-related threats, vulnerabilities, incidents and indicators of compromise within the electricity subsector, with United States and Canadian government agencies, and with other Critical Infrastructure sectors. Analyzing security threats and incident information and providing situational assessments help maintain and enhance bulk power system (BPS) reliability.

1.3

The NERC Board of Trustees adopted a "Policy on the Role of the [ES-ISAC] vis-à-vis NERC's Compliance Monitoring and Enforcement Program" (Policy) on March 8, 2013.[1] In the Policy, NERC outlines two general principles:

1.3.1

ES-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 ES-ISAC activities to the compliance monitoring and enforcement program or to personnel assigned to that program; and

1.3.2

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

1.4

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

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

2.0 Definitions

2.1 Authorized Personnel
The SDRRM and the Associate Director of Bulk Power System Awareness (BPSA).

2.2 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.

2.3 BPSA Department Personnel
All employees in the BPSA Department.

2.4 CSO
The Chief Security Officer, who is responsible for evaluating the threats to, and vulnerabilities of, the BPS. Additionally, the CSO is responsible for evaluating threat intelligence information and reported cyber and physical events occurring on BPS systems.

2.5 CMEP
NERC's 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 the Compliance Assurance and the Compliance Enforcement departments. The respective responsibilities of these departments are outlined below.

2.6 CMEP Personnel
All employees of the Compliance Enforcement and Compliance Assurance departments. CMEP Personnel include the compliance and enforcement personnel of the eight Regional Entities.

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

2.8 ES-ISAC Personnel
The CSO as well as all NERC employees who report to the CSO.

2.9 Oversight Team
This team is comprised of the President and CEO, the Chief Reliability Officer (CRO), the General Counsel, and the Director of Internal Audit and Corporate Risk Management. The Oversight Team monitors implementation of this Code of Conduct.

2.10 Protected Information
A subset of ES-ISAC Information that is voluntarily reported to assist the ES-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 ES-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 ES-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 ES-ISAC or because the ES-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 ES-ISAC Code of Conduct. However, all NERC employees, including ES-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 to another NERC department.

2.11 SDRRM

The Senior Director of RRM, or person fulfilling such role.

2.12 Senior Management

For purposes of this Code of Conduct, NERC Senior Management includes the President and CEO, the CRO, and the General Counsel.

3.0 Department Responsibilities and Functions

3.1 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. BPSA also administers the NERC Alert program for development and distribution of important reliability- and security-related notifications. Additionally, when significant BPS disturbances occur, BPSA 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.

3.2 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.

3.3 Compliance Assurance Department

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

3.4 ES-ISAC

Gathers information from electricity industry participants about security-related events, disturbances, and off-normal occurrences within the electricity sub-sector and shares that information with industry and government partners. The ES-ISAC regularly receives classified and non-classified information on potential threats to the Electricity Sub-sector. Using this information, the ES-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. ES-ISAC does not execute or support any compliance or enforcement department responsibilities.

4.0 Information Sharing

4.1 General Restrictions

4.1.1

Any NERC employee who receives Protected Information shall not, directly or indirectly through a conduit, report or convey such information to any NERC personnel not part of the ES-ISAC, except as permitted herein.

4.1.2

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

4.2 Unattributed and Attributed Protected Information

4.2.1

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

4.2.2
For the purpose of maintaining situational awareness of issues that affect the reliability of the BPS, the CSO, or his designee, may share Unattributed Protected Information that the ES-ISAC receives through the portal with Authorized Personnel. Authorized Personnel may, in turn, share this Unattributed Protected Information with other BPSA Department Personnel.

4.2.3
The sharing of Attributed Protected Information is restricted to (i) ES-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 Sub-sector Coordinating Council. For the avoidance of doubt, in no event shall any NERC employee share Attributed Protected Information with either CMEP Personnel or individuals outside of NERC except as authorized herein or as required by law upon the advice of the General Counsel.

5.0 ES-ISAC Access Restrictions

5.1 General Requirements
As a general manner, all Protected Information shall be maintained by the ES-ISAC in a manner that does not permit physical or electronic access by any NERC personnel who are not ES-ISAC personnel. NERC personnel who are not ES-ISAC personnel shall not have or seek access to any Protected Information without coordination with the CSO or his designee pursuant to this Code of Conduct.

5.2 Physical Access Restrictions

5.1.1
Access to the ES-ISAC operations room shall require keycard access.

5.1.2
Only ES-ISAC Personnel know the combination to the ES-ISAC operations room safe in which ES-ISAC Personnel store keys to cabinets containing sensitive documents.

5.1.3
The CSO's office shall require key access and is otherwise locked and only accessible by ES-ISAC Personnel.

5.2 Electronic Access Restrictions

5.2.1
Only ES-ISAC Personnel have unrestricted access to the ES-ISAC portal.

5.2.2
Members of industry have varied, but restricted access to the ES-ISAC portal, which enables them to submit information to the portal.

5.2.3
All systems and applications housed in the ES-ISAC shall be secured using user identification and password protection controls assigned only to ES-ISAC Personnel.

6.0 Code of Conduct Oversight Team

6.1
The Oversight Team will oversee implementation of this Code of Conduct.

6.2
The CSO and the SDRRM shall meet periodically with the Oversight Team to assess whether the BPSA Department is receiving useful information from the ES-ISAC and whether any changes to the Code of Conduct are warranted.

7.0 Training and Certification

7.1
Every year, all NERC employees 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.

8.0 Enforcement

8.1
Any questions regarding interpretation or clarification of this Code of Conduct should be directed to the General Counsel.

8.2
The General Counsel shall investigate any claims of breach of this Code of Conduct.

8.3
NERC employees who wish to report a potential violation of this Code of Conduct should contact the General Counsel. In accordance with the "Policy on Reporting Complaints Regarding Accounting and Code of Conduct Matters," NERC prohibits retaliation against employees who submit code of conduct complaints in good faith.

8.4
A NERC employee must immediately notify the General Counsel upon learning that he or she has violated this Code of Conduct.

8.5
Any NERC employee who is found to have willfully violated this Code of Conduct and/or knowingly failed to report such a violation will be subject to disciplinary measure up to and including termination.

9.0 Records and Records Retention

9.1

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

9.1.1

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;

9.1.2

The electronic log, maintained by the CSO or his designee, of all Attributed Protected Information that is shared outside of the ES-ISAC; and

9.1.3

The list of Authorized Personnel maintained and updated by the CSO annually.