Agenda
Technology and Security Committee
February 6, 2019 | 11:30 a.m.-12:15 p.m. Pacific
(Please note the Schedule may be adjusted real-time should meetings conclude early and/or extend past their scheduled end time.)

westdrift Manhattan Beach, Autograph Collection
1400 Park View Avenue
Manhattan Beach, California 90266

Conference Room: Loftlight – Lobby

Introductions and Chair’s Remarks

NERC Antitrust Compliance Guidelines and Public Announcement*

Agenda Items

1. Minutes* — Approve
   a. November 6, 2018 Meeting

2. E-ISAC Update* — Review

3. ERO Enterprise Information Technology Strategy and IT Projects Update* — Review

4. Annual Review of Committee Mandate* — Review

5. Adjournment

*Background materials included.
Antitrust Compliance Guidelines

I. General
It is NERC’s policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC’s compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC’s antitrust compliance policy is implicated in any situation should consult NERC’s General Counsel immediately.

II. Prohibited Activities
Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants’ expectations as to their future prices or internal costs.
- Discussions of a participant’s marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.
III. Activities That Are Permitted
From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC’s Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.
Chair George S. Hawkins called to order a duly noticed open meeting of the Technology and Security Committee (the “Committee”) of the Board of Trustees (“Board”) of the North American Electric Reliability Corporation (“NERC” or the “Company”) on November 6, 2018, at 11:15 a.m. Eastern, and a quorum was declared present. The agenda is attached as Exhibit A.

Present at the meeting were:

Committee Members
George S. Hawkins, Chair
Janice B. Case
Kenneth W. DeFontes, Jr.
Suzanne Keenan
Roy Thilly

Board Members
Robert G. Clarke
Frederick W. Gorbet
David Goulding
Robin Manning
Jan Schori
James B. Robb, President and Chief Executive Officer

NERC Staff
Charles A. Berardesco, Senior Vice President, General Counsel, and Corporate Secretary
Tina Buzzard, Associate Director
Stan Hoptroff, Vice President, Chief Technology Officer, and Director of Information Technology
Scott Jones, Senior Vice President, Chief Financial and Administrative Officer, and Treasurer
Bill Lawrence, Vice President, Chief Security Officer, and Director of the E-ISAC
Mark G. Lauby, Senior Vice President and Chief Reliability Officer
Janet Sena, Senior Vice President and Director of Policy and External Affairs
Michael Walker, Senior Vice President and E-ISAC Chief of Staff

NERC Antitrust Compliance Guidelines
Mr. Hawkins directed the participants’ attention to the NERC Antitrust Compliance Guidelines included in the agenda, and indicated that all questions regarding antitrust compliance or related matters should be directed to Mr. Berardesco.

Chair’s Remarks
Mr. Hawkins welcomed the Committee members and described highlights from the annual NERC Grid Security Conference held on October 16-19, 2018 in Las Vegas, Nevada. He thanked Ms. Keenan for attending and commended Mr. Lawrence on his efforts to promote the visibility of his team during the conference. Mr. Hawkins noted the Committee’s continuing focus on enterprise wide system
implementations and the continued effective interaction with the E-ISAC Members Executive Committee (the “MEC”), and thanked Mr. DeFontes for chairing the August Committee meeting.

Minutes
Upon motion duly made and seconded, the Committee approved the minutes of the August 9, 2018 meeting as presented at the meeting.

ERO Enterprise Information Technology Strategy and IT Projects Update
Mr. Hoptroff provided an overview of the ERO Enterprise information technology projects, referencing the materials that had been included in the advance agenda package. He provided an update on the Compliance Monitoring and Enforcement Program (“CMEP”) Technology Project, the common registration tool, and the proposed SAFNR upgrade. Mr. Hoptroff stated that ongoing priorities include CMEP process harmonization efforts, the development of the business case for SAFNR, and the portal enhancements and other tools for the E-ISAC. He noted that he would provide additional detail regarding the standards portion of the CMEP tool at a future meeting. Mr. Robb commended the work of Regional Entity staff regarding process harmonization for the CMEP tool.

E-ISAC Update
Mr. Lawrence provided an update on recent E-ISAC activities, referencing the materials that had been included in the advance agenda package. His update highlighted the E-ISAC’s progress executing its long-term strategy, including in the areas of member engagement, information sharing, and analysis. Mr. Lawrence highlighted the E-ISAC’s membership growth in 2018, increases in information sharing through the portal, and the E-ISAC’s plans to improve engagement with Canadian members. He reported that the membership of the MEC was revised to allow for an additional voting representative from Canada, and that the MEC was creating focused working groups to enhance support for the E-ISAC. Mr. Lawrence also provided an update on E-ISAC technology projects and the E-ISAC’s success in expanding staffing levels and capabilities. He recognized the new role for Mr. Walker as the E-ISAC’s chief of staff, thanked NERC Human Resources for their support in recruitment, and noted the ongoing work to develop security focused metrics.

Mr. Lawrence stated that the 2019 priorities for the E-ISAC include enhancing information sharing through the Cybersecurity Risk Information Sharing Program, sharing of machine-readable cyber indicators, increasing analysis capabilities, and continuing efforts to engage industry. Mr. Hawkins noted that the Cyber Automated Information Sharing System went online on November 6, 2018.
Adjournment
There being no further business, and upon motion duly made and seconded, the meeting was adjourned.

Submitted by,

\[Signature\]

Charles A. Berardesco
Corporate Secretary
Long-Term Strategy Update

Bill Lawrence, Vice President and CSO
Technology and Security Committee Meeting
February 6, 2019
Topics

• Strategic Plan Update
  ▪ Engagement
  ▪ Information Sharing
  ▪ Threat Analysis
• Resource Planning
• Key Challenges
7,070 E-ISAC Members
- 17% increase in 2018 (Average of 22 added per week)
- Increased focus on customer relationship management

Industry Engagement Program
- 2018
  - 21 analysts from 16 organizations (Ameren, ConEd, CPS, Duke, Exelon, GRDA, Hydro Quebec, JEA, LES, LADWP, NYPA, NPPD, OPPD, SMUD, Southern, SRP)
- 2019
  - 6 sessions planned (January, March, May, July, September, December)
  - Expand participation to all asset owner and operators
  - Increased support and participation from Trade Associations
  - Utility Technology Council--planning to host a webinar on the IEP
  - Ongoing industry engagement in cooperation with Regional Entities
• U.S. Government Agencies
  ▪ DOE—quarterly meetings
  ▪ DHS—NCCIC attendance. Periodic meetings with DHS leadership
  ▪ FERC—engagement with Office of Infrastructure Security
  ▪ DOD—focused on USCYBERCOM support to sector

• Canadian Government Agencies
  ▪ Ongoing meetings with Canadian security establishment to enhance reciprocal information sharing
• Three Main Strategic Objectives
  - Highlight the value of the E-ISAC through discussion and demonstration of increased capabilities
  - Provide a deeper understanding of the benefits of E-ISAC membership
  - Strengthen the E-ISAC’s relationship with Canadian members

• Outreach Efforts
  - Kickoff in November 2018, met with Atlantic Provinces Regulators and New Brunswick Power, Emera
  - Canadian Electricity Association, Hydro Quebec, Canadian Center for Cyber Security, IESO, Centre for Energy Advancement through Technological Innovation (CEATI)
• 2019 Outreach Efforts
  ▪ CEA Security & Infrastructure Protection Meetings (Quarterly)
  ▪ Continue Focused Engagement Across Canada
    o British Columbia
    o Calgary
    o Nova Scotia/Newfoundland
    o Toronto/Quebec
  ▪ Direct engagement with IESO
  ▪ Energy and Utility Sector Network Meeting in St. Johns
  ▪ CEATI and Infrastructure Protection and Security Interest Group engagement
  ▪ GridSecCon 2019 Classified Briefing
  ▪ CIPC 2019 Classified Briefing
• Portal
  ▪ Approximately 17% increase in registered users
  ▪ Cyber and physical bulletins posted
    o Cyber--297 thru Q4 2018
    o Physical--207 thru Q4 2018
  ▪ Two private User Communities in soft-launch phase
  ▪ Additional portal enhancements under development
• CRISP
  ▪ Membership continues to increase, which also reduces participant costs
  ▪ Public power pilot under development
  ▪ Evaluating additional software for CRISP data analysis

• Cyber Automated Information Sharing System
  ▪ Machine-speed sharing of cyber indicators of compromise
  ▪ Operational in Q4 2018-29 participants

• Malware Analysis Repository and Threat Information Exchange
  ▪ “Dropbox” for submitting suspected malware files for advanced analysis
  ▪ DOE and E-ISAC conducting vendor capabilities gap analysis
• Data Storage and Management System
  ▪ Central data repository
  ▪ Early stages of requirements and business case development

• Customer Relationship Management System
  ▪ Evaluating RFP responses

• DHS Shared Resources HF Radio Disaster Recovery Capability
  ▪ Enhanced disaster communications capability
  ▪ Expected delivery of equipment Q1 2019
• Unclassified Threat Briefings (2018 and 2019)
  ▪ Two unclassified threat workshops (June and December)
  ▪ Two unclassified briefings at ESCC meetings (May and October)
  ▪ CRISP – two workshops
• Classified Threat Briefings (2018 and 2019)
  ▪ Coordinated three non-CRISP classified briefings
• Launched Critical Broadcast Program (2018)
• Significant Increase in Unique Publications in 2018- (9 Cyber, 6 Physical)
• 2019 Planned Resource Additions
  ▪ 4 watch officers
  ▪ 5 cyber security analysts
• Additional corporate services support (IT, legal, finance)
• Strategic Plan Refresh – including long-term projections
• March – Preliminary 2020 budget review with MEC
Key Challenges

- Properly positioning the E-ISAC relative to other external government and private sector initiatives
- Pace and resource demands
- Competition for top analyst talent
- Integration of resource additions
- Multiple IT initiatives running in parallel-prioritization process in place, additional IT resources being put in place to support
- Space to accommodate planned 2019 resources additions--planning underway
Questions and Answers
ERO Enterprise Information Technology Strategy and Projects Update

**Action**

Information

**Background**

At the November 6, 2018 open meeting of the Technology and Security Committee, an update was provided on the ERO Information Technology (IT) Strategy. Additionally, updates were provided on several IT projects:

- The Compliance Monitoring and Enforcement Program (CMEP) Technology Project \(^1\) update included the status of the process harmonization workshops, the change management plan, and stakeholder engagement, including the relationship with the Certification and Compliance Committee (CCC) and the Alignment Working Group (AWG).

- The Entity Registration solution was reviewed and the Standards and Registration data integration with BWise will be completed in the third quarter of 2019.

- The business case for the upgrade of Situation Awareness for FERC, NERC and the Regional Entities (SANFR) was discussed and was completed by the end of 2018.

- A review of the Southwest Power Pool Regional Entity (SPP RE) Dissolution was provided and all data migration requirements were reported as being successfully completed.

- An update was given on the Electricity Information Sharing and Analysis Center (E-ISAC) Portal, highlighting that the first portal community was delivered in late June 2018.

**Summary**

Since the November meeting, additional CMEP Technology Project configuration and testing work has been completed for the first release scheduled for Q3 2019.

In addition, work supporting the scheduled investments in the Entity Registration process has continued, along with planning for integrations necessary to exchange Entity Registration and Reliability Standards data between the CMEP Technology solution (BWise) and the xRM-based Centralized Organization Registration ERO System (CORES).

NERC IT, along with NERC’s Situational Awareness department and the E-ISAC, completed the business case for SAFNR version 3. The ERO Enterprise Technology Leadership Team endorsed and NERC’s CEO approved the business case on January 4, 2019.

Highlights of the business case include:

- The investment will enable NERC to continue to undertake situational awareness activities consistent with Section 1000 of the Rules of Procedure.

---

\(^1\) The CMEP Technology Project is a strategic initiative designed to support the ERO Enterprise as it continues to evolve as a risk-informed regulator. It supports three ERO Enterprise goals: implementation of a risk-informed CMEP (Goal 2), reduction of known risks to reliability (Goal 3), and improving the efficiency and effectiveness of the ERO (Goal 6).
• Implementing a new solution will eliminate the risk of unplanned outages associated with the current system.

• Funds are available in the 2019 and 2020-2022 budget forecasts to support the required investment.

• Competent vendors with viable functional and technical options for this investment were identified through a Request for Proposal.

Work is continuing on additional E-ISAC portal user communities and portal security enhancements on E-ISAC.com. Machine-to-machine security sharing, through the software solution ThreatConnect, has been opened up for expanded use and, as of November 2018, any utility stakeholder can enroll in the program. Frequently asked questions and guidance on enrolling in ThreatConnect has been posted to the E-ISAC portal.

NERC IT continues in its mission to deliver technology solutions supporting the effective and efficient use of resources for registered entities, the ERO Enterprise, and the E-ISAC.
Annual Review of Committee Mandate

Action
Review

Background
As part of the annual review of all Board committee mandates, the NERC Legal Department has reviewed the current Technology and Security Committee (TSC) mandate. The current TSC mandate is attached.

The Legal Department is not recommending any further revisions at this time.
Board of Trustees Technology and Security Committee Mandate
Approved by the Board of Trustees: February 2, 2018

Committee Membership
The Board of Trustees Technology and Security Committee (TSC or the Committee) of the North American Electric Reliability Corporation (NERC) shall be composed of not less than three and not more than six of the independent members of the Board of Trustees (Board). The members of the TSC shall be appointed or reappointed by the Board at the regular meeting of the Board immediately following each Annual Meeting of the Members Representative Committee. Each member of the TSC shall continue to be a member thereof until a successor is appointed, unless a member resigns, is removed, or ceases to be a trustee of the corporation. When a vacancy occurs at any time in the membership of the TSC, it may be filled by the Board.

Purpose
The purpose of the TSC is to assist the Board by providing oversight to the corporation’s (i) information technology program, (ii) information security program, and (iii) Electricity Sector Information Sharing and Analysis Center (E-ISAC), as well as performing such other responsibilities as directed by the Board or this Mandate.

Committee Authority and Responsibilities
To carry out its purpose, the TSC shall have the following authority and responsibilities:

Technology and Information Security:

1. As part of the annual business plan and budgeting process, provide the Finance and Audit Committee and the Board with recommendations regarding management proposed resource requirements and funding for (i) the design, procurement, installation, operation, and maintenance of information technology hardware, software and applications, including hardware, software, and applications hosted by third parties, supporting NERC’s operations and program area initiatives; and (ii) investments in, or supporting, the development of new technology to improve and ensure the reliability of the bulk power system in North America, historic examples of which included funding for the development of transmission system awareness tools, synchrophaser technology, technology used to monitor and manage transmission congestion, and data reporting tools providing information regarding generator, transmission system, and demand side resource availability and performance.

2. Provide oversight on behalf of the Board with respect to the corporation’s overall computer systems environment, including procedures to keep the systems secure and contingency plans
developed to deal with possible computer failures.

3. Respond to the Board’s requests to the Committee for advice and recommendations on any technology-related issues.

E-ISAC:

1. Provide oversight on behalf of the Board of the E-ISAC and its related programs.

2. Respond to the Board’s requests for advice and recommendations on any E-ISAC related issues.

Additional Responsibilities:

1. Recommend to the Board such actions as may further the purposes of NERC’s technology and information security, and NERC’s E-ISAC and related programs.

2. Perform such other functions as may be delegated from time to time by the Board.

Committee Meetings

The TSC shall meet at least twice a year by conference call or in person. Meetings may occur at the same place in conjunction with the regular Board meetings of the corporation, or as determined by the members of the TSC, using the same meeting procedures established for the Board. Meetings may be held in either open or closed session as set forth in the Bylaws of the corporation.

A majority of the Committee members shall constitute a quorum. Except where prescribed differently by law: (a) any action or decision of the TSC requires a vote of a majority of the Committee members then in attendance at any Committee meeting provided a quorum is present; and (b) participation may be telephonic or by Action Without a Meeting. The Committee may hold special meetings as circumstances require. Minutes of each Committee meeting shall be maintained as part of the Committee’s record.

Governance

The Board, or in the event of their failure to do so, the members of the TSC, shall appoint a chair from among their members. The TSC Chair shall be responsible for leadership of the Committee, including scheduling of meetings, setting agendas, presiding over Committee meetings, and making reports to the Board. A member(s) of the NERC staff shall assist the Chair and shall serve as the non-voting secretary.

Review

The TSC shall review this mandate annually and recommend to the Board Corporate Governance and Human Resources Committee any changes it considers advisable. Any changes must be approved by the full Board. The TSC shall complete a self-assessment annually to determine its effectiveness.