Agenda
Critical Infrastructure Protection Committee
March 6, 2018 | 1:00 p.m. – 5:00 p.m. Eastern
March 7, 2018 | 8:00 a.m. – Noon Eastern

Hyatt Regency Jacksonville Riverfront
225 East Coastline Drive
Jacksonville, FL 32202

Introduction and Chair’s Remarks

NERC Antitrust Compliance Guidelines and Public Announcement

Agenda Items

1. Opening Remarks
2. Administrative – Tobias Whitney, CIPC Secretary, NERC
   a. Safety Briefing and Emergency Precautions – Hyatt Regency Jacksonville Riverfront Hotel Staff
   b. Declaration of CIPC Quorum
   c. CIPC Roster
   d. Parliamentary Procedures – In the absence of specific provisions in the CIPC charter, the committee shall conduct its meetings guided by the most recent edition of Robert’s Rules of Order, Newly Revised.
3. Consent Agenda – Marc Childs, Great River Energy, CIPC Chair
   a. Draft December CIPC Minutes – (Approve)
4. Chair’s Remarks – Marc Childs, Great River Energy, CIPC Chair
   a. Work Plan
5. Agency Updates
   a. Federal Energy Regulatory Commission
   b. Department of Energy
   c. Department of Homeland Security
6. Emerging Technology Roundtable Update* - Tobias Whitney, CIPC Secretary, NERC
7. E-ISAC Update* – Bill Lawrence, Director, E-ISAC
   a. Strategic plan, GridSecCon, and GridEx Updates – Bill Lawrence, Director, E-ISAC
   b. Notable cyber incidents past quarter – Zachary Fields, CRISP Analyst, E-ISAC
c. Notable physical incidents past quarter* – Charlotte de Siebert, Principal Physical Security Analyst, E-ISAC

8. **CIP Standards Update** – David Revill, CIPC Vice Chair, Georgia System Operations Corporation
   a. CIP Modification Team Update* - Steve Brain, Dominion Energy Services

9. **Supply Chain Update*** - Tobias Whitney, CIPC Secretary, NERC

10. **Idaho National Labs** – Andrew Bochman, Idaho National Labs

11. **Legislative Update*** – Kaitlin Brennan, Manager – Cyber and Infrastructure Security, EEI

12. **Electricity Subsector Coordinating Council Update*** – Kaitlin Brennan, Manager – Cyber and Infrastructure Security, EEI

13. **Reliability Issues Steering Committee Update** – John Moura, Director of Reliability Assessments and Systems Analysis, NERC


15. **Operating Security Subcommittee** – Lisa Carrington, Subcommittee Chair, APS
   a. Grid Exercise Working Group (GEWG) – Tim Conway, SANS

16. **Cybersecurity Subcommittee** – Brenda Davis, Subcommittee Chair, CPS Energy
   a. Control Systems Security Working Group (CSSWG) – Carter Manucy, Cyber Security Manager, Florida Municipal Power Agency and Michael Mertz, Vice President- Chief Information Officer, PNM Resources

17. **Physical Security Subcommittee** – Ross Johnson, Subcommittee Chair, Capital Power
   a. Physical Security Guidelines Work Group- Darrell Klimitchek, Manager of Technical Services, South Texas Electric Cooperative
   c. Security Management Program Guideline for the Electricity Subsector - Ross Johnson, Senior Manager, Capital Power
   d. E-ISAC Physical Security Advisory Group* – John Breckinridge, Chair, KCP&L

18. **Policy Subcommittee** – Jeffrey Fuller, Subcommittee Chair, AES Corporation
   a. Security Metrics Working Group (SMWG)* – Larry Bugh, SMWG Chair, ReliabilityFirst
b. Charter- (Approve)*

SMWG Charter

c. Compliance Enforcement and Input Working Group (CEIWG)* – Paul Crist, CEIWG Chair, Lincoln Electric System

i. Cloud Computing Pilot Plan

ii. Charter, Deliverables, and Work Schedule (Approve)*

CEIWG Charter

19. Schedule of Important Dates:

<table>
<thead>
<tr>
<th>Dates</th>
<th>Time</th>
<th>Type</th>
<th>Location</th>
<th>Hotel</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 6, 2018</td>
<td>8:00 a.m. – Noon</td>
<td>CIPC Training</td>
<td>Jacksonville, FL</td>
<td>Hyatt Regency Jacksonville Riverfront</td>
</tr>
<tr>
<td>March 6-7, 2018</td>
<td>12:00 p.m. – 5:00 p.m.</td>
<td>CIPC Meeting</td>
<td>Jacksonville, FL</td>
<td>Hyatt Regency Jacksonville Riverfront</td>
</tr>
<tr>
<td>March 7, 2018</td>
<td>1:00 p.m. – 5:00 p.m.</td>
<td>Emerging Technology Roundtable</td>
<td>Jacksonville, FL</td>
<td>Hyatt Regency Jacksonville Riverfront</td>
</tr>
<tr>
<td>June 5-6, 2018</td>
<td>12:00 p.m. – 5:00 p.m.</td>
<td>CIPC Meeting</td>
<td>New Orleans, LA</td>
<td>The Ritz-Carlton New Orleans</td>
</tr>
<tr>
<td>September 11-12, 2018</td>
<td>12:00 p.m. – 5:00 p.m.</td>
<td>CIPC Meeting</td>
<td>Minneapolis, MN</td>
<td>Hyatt Regency Minneapolis</td>
</tr>
<tr>
<td>December 11-12, 2018</td>
<td>12:00 p.m. – 5:00 p.m.</td>
<td>CIPC Meeting</td>
<td>Atlanta, GA</td>
<td>The Whitley, Buckhead</td>
</tr>
</tbody>
</table>

20. Closing Remarks and Action Items
21. Adjournment
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.
Any other matters that do not clearly fall within these guidelines should be reviewed with NERC’s General Counsel before being discussed.

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.
Public Announcements

Face-to-face meeting version:
Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

August 10, 2010
Emerging Technology Roundtable Update

Action
Review and Discussion

Background
North American Electric Reliability Corporation (NERC) is hosting an “Emerging Technology Roundtable,” an afternoon event with in-depth discussions about the integration of technologies to improve the reliable operation of the Bulk Electric System (BES), while addressing and mitigating cyber and physical security risks. The Roundtable will be held on March 7, 2018, immediately following the Critical Infrastructure Protection Committee (CIPC) meeting at Hyatt Regency Jacksonville Riverfront.

Summary
NERC staff and guest presenters will focus on BES technology and its reliability benefits, business case matters, cyber/technology risks, and regulatory implications. The objective is to make participants aware of strategies and considerations related to technologies integration that could be used to improve operations and reliability in a secure manner that supports compliance. Vendors and asset owners are invited to attend to share ideas and develop solutions to help advance the assessment and adoption of emerging technologies. March’s ETR will address SCADA security for natural gas-fired generation and related pipeline infrastructure.
E-ISAC Update

Action
Discussion

Background
The E-ISAC is in the first year of a five-year long-term strategic plan. Working with NERC leadership and the Electricity Subsector Coordination Council’s Member Executive Committee (MEC,) the E-ISAC’s vision is to become a world-class, trusted source of quality analysis and rapid sharing of electricity industry security information. The three major areas of focus in the increase of E-ISAC capabilities are: information sharing, analysis, and engagement.

Summary
E-ISAC staff will present on the strategic plan, preparations for GridSecCon 2018, and lessons learned from GridEx IV. Updates on notable cyber and physical security incidents will also be shared.

1 E-ISAC Long-term Strategic Plan, 2018 NERC Business Plan and Budget, Exhibit F, page 156.
E-ISAC Physical Security Update

**Action**
Informational

**Background**
The E-ISAC provides quarterly briefs to the Critical Infrastructure Protection Committee regarding the current industry threat surface.

**Summary**
Charlotte de Sibert, Principal Physical Security Analyst, will present an overview of recent physical security events, trend analysis, and current lines of effort.

- Recent incidents of note
- Incident type and regional threat trend analysis
- Activist/Eco-Terrorist/Foreign Terrorist threat update
- Physical Security Advisory Group items
CIP Modification Team

Action
Informational

Background
The CIP Modification Team will provide an update on the progress of the 2016-02 CIP Modifications Standards Drafting Team. This update will focus on the issue areas currently posted for industry feedback as well as an update on future development on the topic of virtualization.
Supply Chain Standards Implementation

Action
Information

Background
On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829, directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations, as follows:

[The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. (P. 45)

The Commission established a filing deadline of one year from the effective date of Order No. 829, which is September 27, 2017.

Following the issuance of Order No. 829, NERC staff initiated Reliability Standards Project 2016-03 to develop a set of Critical Infrastructure Protection (CIP) supply chain risk management standards (“Supply Chain Standards”). The Supply Chain Standards, CIP-005-6, CIP-010-3, and CIP-013-1, support reliability by requiring entities to implement plans and processes to mitigate supply chain cyber security risks to high and medium impact assets. The requirements target risks in four objective areas: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Following industry approval of the Supply Chain Standards on July 20, 2017, the Board adopted the Supply Chain Standards at its August 10, 2017 meeting. NERC staff filed the Supply Chain Standards with the Commission on September 26, 2017, where they are currently pending action by the Commission.

In adopting the Supply Chain Standards, the board concurrently adopted additional resolutions related to implementation and risk evaluation.¹ The resolutions outlined in detail six actions by

¹ The Proposed Additional Resolutions for Agenda Item 9.a: Cyber Security – Supply Chain Risk Management – CIP-005-6, CIP-010-3, and CIP-013-1, NERC Board of Trustees Meeting, August 10, 2017, is available at:
NERC management and stakeholders to assist in the implementation and evaluation of the Supply Chain Standards as well as other actions to address potential supply chain risks for assets not currently subject to the standards. Collectively, the activities to address the Board supply chain resolution will establish a common understanding of the supply chain risk to the Bulk Electric System and initiate activities to mitigate those risks. The resolutions, in summary form, include:

**Support Effective and Efficient Implementation:** NERC to commence preparations for implementation of the Supply Chain Standards using similar methods during the CIP V5 transition, and regularly report to the Board on those activities.

**Cyber Security Supply Chain Risk Study:** Study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address identified risks. (Interim report 12 months after adoption of the resolutions and a follow-up final report 18 months after adoption).

**Communicate Supply Chain Risks to Industry:** NERC should communicate supply chain risk developments and risks to industry and in connection with the Cyber Security Supply Chain Risk Study.

**Forum White Papers:** The Board requested that the North American Transmission Forum and the North American Generation Forum (the “Forums”) to develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management, as described in the resolution.

**Association White Papers:** The Board requested that the National Rural Electric Cooperative Association and the American Public Power Association (the “Associations”) to develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management, as described in the resolution, focusing on smaller entities that are not members of the Forums, for the membership of the Associations.

**Evaluate Supply Chain Standard Effectiveness:** Collaborating with NERC technical committees and other experts, NERC should develop a plan to evaluate the effectiveness of the Supply Chain Standards, as described in the resolution, and report to the Board.

As part of NERC’s petition to FERC requesting approval of the Supply Chain Standard, NERC referenced the Board resolution and provided a detailed outline of activities to support each of the resolution requests. These specific activities maintain focus and engagement of the ERO.

[http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Minutes%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf](http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Minutes%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf)
Enterprise and its stakeholders, to understand and share the complexities of the supply chain with industry, while mitigating the associated risks.

At the March CIPC meeting, NERC staff will provide an update on the plans and status to address the supply chain resolution, and will continue to do so at each scheduled meeting.
Legislative Update

**Action**
Informational

**Background**
Discuss the legislation and current climate of the U.S. Government and its relation to the Energy Sector with updates on government issues.
Electricity Subsector Coordinating Council

Action
Informational

Background
Discuss the activities of the Electricity Subsector Coordinating Council (ESCC), which includes representatives from government, industry, and other groups. Committees of the council focus on strategies that address threats and vulnerabilities on a collaborative basis.
Review of RISC’s ERO Reliability Risk Priorities Report

**Action**
Discussion

**Background**
On February 8, 2018, the NERC Board accepted the 2018 ERO Reliability Risk Priorities Report (RISC Report). The RISC Report reflects the RISC’s determination of the most pressing risks to the BPS taking into account input from stakeholders, particularly from discussions held during the Reliability Leadership Summit on March 21, 2017.

The RISC Report includes nine risk profiles, and each is mapped against the likelihood and impact further described in the RISC report. This mapping represents the unmitigated or inherent risks of each risk profile as determined by the RISC. Regardless of the categorization, all risk profiles warrant attention as the rapidly changing BPS can quickly raise the risk. Each risk profile includes a description of the risk and recommendations for mitigation.

The RISC Report is used by the Planning Committee (PC) and other industry stakeholders as input to strategic planning processes. PC leadership is reviewing the report recommendations and identifying PC objectives and activities that should be considered by the PC for inclusion in the PC Strategic Plan and other guiding documents.

Click [here](#) to download the RISC Report

**Summary**
*Leave Blank for meeting participant notes*
**Resilience Framework**

**Action**
Discussion

**Background**
During the Member Representatives Committee’s February 2018 meeting, Peter Brandien, RISC Chair, presented the following framework proposed by the RISC regarding BPS resilience:

1. Develop a common understanding and definition of the key elements of BPS resilience;
2. Understand how these key elements of BPS resilience fit into the existing ERO framework; and
3. Evaluate whether there is a need to undertake additional steps within the ERO framework to address these key elements of BPS resilience beyond what is already in place and underway in connection with ongoing ERO Enterprise operations, including work being undertaken by each of the NERC standing committees.

The RISC suggested the National Infrastructure Advisory Council’s (NIAC’s) Framework for Establishing Critical Infrastructure Goals¹ is a credible source for further understanding and defining resilience. The NIAC framework includes four outcome-focused abilities:

1. Robustness – the ability to absorb shocks and continue operating;
2. Resourcefulness – the ability to skillfully manage a crisis as it unfolds;
3. Rapid Recovery – the ability to get services back as quickly as possible; and
4. Adaptability – the ability to incorporate lessons learned from past events to improve resilience.

The RISC highlighted ERO Enterprise activities within these four areas, as shown in the table below. The NERC Board of Trustees (Board) requested that the RISC move forward with the resilience framework, with the next step being to request input from the standing committees on respective activities addressing resilience. Specifically, the RISC is requesting the following input on or before March 28, 2018, using the table below as a reference:

1. The committee’s views on how bulk power system (BPS) resilience is currently being addressed within the scope of the committee’s responsibilities; and
2. Any additional activities the committee believes should be undertaken.

---
The RISC will then review and summarize this information, together with any additional views and recommendations it may have, for discussion at the May 2018 MRC meeting.

<table>
<thead>
<tr>
<th>NIAC Resilience Constructs</th>
<th>Key Programs and Activities</th>
<th>Specific Efforts/Tools</th>
</tr>
</thead>
</table>
| **Robustness**—The ability to continue operations in the face of disaster. In some cases, it translates into designing structures or systems to be strong enough to take a foreseeable punch. In others, robustness requires devising substitute or redundant systems that can be brought to bear should something important break or stop working. Robustness also entails investing in and maintaining elements of critical infrastructure so that they can withstand low probability but high consequence events. | • Reliability and Emerging Risk Assessments  
• Risk, Event and Performance Monitoring  
• Technical Committee work, including special projects  
• Mandatory Reliability Standards  
• Reliability Guidelines  
• Operator Certification and Training  
• E-ISAC information sharing programs | • Alerts  
• State of Reliability Report  
  o GADS  
  o TADS  
  o DADS  
  o Protection system misoperations  
  o TEAMS  
  o FR Performance  
• Long-Term Reliability Assessment  
• Key Reliability Standards:  
  o TPL (Extreme)  
  o EOP  
  o Blackstart Restoration  
• GridEx  
• Security conferences and information sharing (e.g. GridSecCon) |
| **Resourcefulness**—The ability to skillfully manage a disaster as it unfolds. It includes identifying options, prioritizing what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Resourcefulness depends primarily on people, not technology. | • Situational Awareness and Industry Coordination  
• Government Coordination  
• Cross-Sector Information Sharing  
• Mandatory Reliability Standards/Functional Model | • BPSA information sharing tools and processes  
• E-ISAC information sharing tools and processes  
• Formation of a Crisis Action Team to support industry and governmental coordination  
• Standards requirements  
  o Reliability Coordinators  
  o Transmission Operators |
| **Rapid recovery**—The capacity to get things back to normal as quickly as possible after a disaster. Carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right places are crucial. | • Situational Awareness, Industry Coordination  
• Government Coordination  
• Cross-Sector Information Sharing | • Support for Electric Sector Coordinating Council activities |
| **Adaptability**—The means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis. | • Reliability Assessment  
• Event Analysis  
• Event Forensics | • Technical Committee Recommendations  
• Reliability Guidelines  
• Lessons Learned  
• Event Analysis, Investigations  
• Audit Recommendations  
• Reliability Assessments  
• State of Reliability Report |
NATF Update for NERC CIPC

Action
(Discussion)

Background
The North American Transmission Forum (NATF) is an organization of 87 members representing a total of 153 transmission owning and/or operating companies across North America. Collectively, NATF member companies own and operate 80 percent of the 200 kV and above transmission mileage and serve about 90 percent of the North American peak demand. The NATF promotes the highest levels of reliability, security, and resiliency in the operation of electric transmission systems, built on the principle that the open and candid exchange of information among its members is the key to improving the reliability of the transmission systems in the U.S. and Canada.

These periodic reports from the NATF to the NERC technical committees are intended to brief committee members on NATF efforts, identify areas of overlap, and establish dialogue on coordination to reduce duplicative efforts by industry subject-matter experts.

Summary
Ken Keels, NATF director of practices and initiatives, will provide an update focused on NATF’s work on supply chain cybersecurity risk management.

A cross-functional team of NATF members is working to develop industry supportive supply chain cybersecurity risk management guidance and practices. This work is focused on creating a common set of criteria by which to assess supply chain vendors’ security controls as an effective component of a cost-effective and efficient supply chain cybersecurity risk management program. Initial discussions have been conducted among representatives from NATF, EEI, NRECA, APPA, ISO/RTO Council, and NAGF regarding each organization’s related supply chain cybersecurity risk management efforts and the potential for coordination and collaboration.
STWG Update

**Action**
Review and Discussion

**Background**
Review the Security Training Session (Security/Incident Response During and After Natural Disasters) that was conducted on March 6, 2018 prior to the Critical Infrastructure Protection Committee (CIPC) Meeting and discuss future CIPC training opportunities.

**Summary**
The Security Training Working Group (STWG) will have three outstanding speakers discussing three uniquely different natural disasters. The CIPC STWG will host a training session on the lessons learned from natural disasters. Three unique case studies from the California wildfires, Hurricane Harvey in Texas, and Hurricane Irma in Florida natural disasters will be discussed. Industry experts will describe their challenges, effected operations, and the security issues presented during these circumstances.

**Presenters:**
- Chris Vicino – Los Angeles Department Water & Power – Corporate Security Response and Challenges to the Southern California Wildfires
- Bert Sausse III – CenterPoint Energy – Corporate Response and Challenges to Hurricane Harvey
- John R. Large & Carlos Morales – Florida Power & Light - Corporate Security Response and Challenges to Hurricane Irma
SMWG Update

Action
Review and Discussion

Background
The Security Metrics Working Group (SMWG) will provide an update with regard with activities to develop the security section of State of Reliability report. In addition, an update will provided regarding the efforts to improve security metrics and reporting. The CIPC will be provided a new charter for CIPC approval.

Summary
The SMWG is continuing its effort to develop quality metrics that provide a record of security issues associated with the Bulk Electric System. The group is reviewing approaches to use data derived from the CIP Standards as a means to obtain security metrics. In addition, the SMWG is working closely with the E-ISAC to develop metrics for use in the annual State of Reliability report. Enclosed is the modified SMWG charter which includes membership updates, additional details regarding the objectives of the group and the rationale for security metrics.
1. **Statement of Need**

The industry relies on physical facilities and cyber systems to be in place and operating as designed in order to support the reliable and resilient operation of the bulk power system (BPS). The industry needs a way to measure and trend the effectiveness of the security controls used to secure these facilities and systems. The Security Metrics Working Group (SMWG) will work closely with the E-ISAC to recommend and develop metrics and periodically review, assess, and report the results. The metrics and other information prepared by the SMWG will help inform industry executives and senior managers and provide answers to questions such as:

- How often do physical and cyber security incidents occur?
- To what extent do these reported incidents cause a loss of customer load?
- What is the extent of security information-sharing across the industry?
- Are cyber security vulnerabilities increasing?

2. **Background**

The NERC Planning and Operating Committees have promoted the development of performance metrics for the North American bulk power system through the Performance Analysis Subcommittee. The SMWG will contribute to this work by developing a set of metrics that measures the performance of the security controls that support the reliable and resilient operation of the BPS.

Definition of security from the perspective of BPS reliability:

> The state of actions taken by entities to detect, prevent, and respond to cyber and physical dangers or threats to the reliability or operability of the BPS.

3. **Objectives/Duties**

Provide an advisory role to NERC and its stakeholders regarding physical and cyber security metrics. Develop cyber and physical security metrics that:

- Align with and support the mission and goals of NERC and the E-ISAC.
- Help BPS operators understand the significance of evolving cyber and physical security risks that could affect the reliable operation of the BPS.
- Provide consistent metrics definitions, data collection, and reporting mechanisms.
- Measure the historic performance of security controls that support the reliable and resilient operation of the BPS.
- Provide leading indicators of incidents or events (e.g., technology, configuration, human factors) that could compromise the effectiveness of the security controls that support the reliable, resilient operation of the BPS.
• Contribute to an overall assessment of BPS reliability consistent with the Adequate Level of Reliability (ALR) framework.

Note: The SMWG will not develop metrics specific to the operational performance of the E-ISAC or individual entities.

4. Members and Structure

<table>
<thead>
<tr>
<th>Security Metrics Working Group Members</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Chair</td>
</tr>
<tr>
<td>Vice-Chair</td>
</tr>
<tr>
<td>CIPC EC Sponsor</td>
</tr>
<tr>
<td>NERC staff</td>
</tr>
</tbody>
</table>
| E-ISAC staff                        | Bill Lawrence  
Steve Herrin  
Laura Brown  
Kristen Worosz  
Sam Chanoski  
Stuart Brindley (consultant) |
| Members                             | Nathan Mitchell, APPA  
Chuck Abell, Ameren  
David Dunn, IESO  
Elizabeth Mairs, Xcel Energy  
David Revill, Georgia Transmission  
Joe Garmon, Seminole Electric |

5. Reporting

The SMWG will work closely with the E-ISAC to define, develop, and review security metrics. The E-ISAC will manage the data collection and quarterly reporting process. The SMWG will administratively report to the Critical Infrastructure Protection Committee (CIPC).

6. Deliverables and Work Schedule

Four to six meetings per year plus monthly conference calls and web-based meetings.

CIPC approved xx, 2017
Compliance Enforcement and Input Working Group Update

**Action**
Approve updates to Charter and new name.
Update on cloud implementation guidance requested by NERC.

**Background**
Critical Infrastructure Protection Committee (CIPC) will support the NERC Compliance Monitoring and Enforcement Program (CMEP) initiatives by providing timely technical expertise on matters related to cyber and physical security as requested by the NERC Compliance Assurance department and the NERC Compliance Enforcement department. The development of the compliance implementation guidance process, the role of the group will be changing slightly to provide CIPC with support in the process. We will also be revising the name to focus less on the enforcement aspect of compliance.

**Summary**
The proposed changes to the charter will be discussed and a vote will be requested to approve the changes. The group will also be presenting the approach that we will be taking for implementation guidance related to using cloud technologies for BCSI and BCS. The proposal includes developing the implementation guidance in phases to address the specific requirements in the NERC CIP standards.
Critical Infrastructure Protection Working Group Charter

Deliverables and Work Schedule

Date: 3/7/2018  Name: CIPC Compliance Input WG (CIWG)

1. Statement of Need

Critical Infrastructure Protection Committee (CIPC) will support the NERC Compliance Monitoring and Enforcement Program (CMEP) initiatives by providing timely technical expertise on matters related to cyber and physical security as requested by the NERC Compliance Assurance group.

2. Background

The NERC Compliance Assurance group may on occasion request technical expertise in developing and prioritizing Compliance products. CIPC has supported these requests through the CIPC Executive Committee (EC) on an ad hoc basis. The CIPC EC in developing the CIPC strategic plan, believes it beneficial to formalize the processing of Compliance input requests with an ongoing working group.

3. Objectives/Duties

- CIPC oversees the Compliance Input Working Group (CIWG).
- The CIWG will develop a roster of technical cyber and physical security experts from the CIPC voting members, alternate members and other willing participants and conduct the following activities:
  - Develop a process for handling requests from NERC Compliance Assurance staff.
  - Provide feedback from industry to the NERC Compliance Assurance staff to improve the CMEP.
  - Provide guidance to CIPC on prioritization of Compliance Assurance products under development.
  - Provide guidance on Compliance Monitoring and Enforcement Products (CMEP) that may be brought before the CIPC for discussion.
  - Provide timely technical reports to CIPC on CMEP matters related to cyber and physical security.
  - Utilize the CIPC face-to-face meetings to facilitate discussion and allow discourse on CMEP topic areas.
  - Encourage registered entity involvement in the NERC CIP Standards review and comment process.
  - Provide CIPC feedback to NERC Compliance Assurance on the effectiveness of the CMEP tools and processes when possible.
  - Reviews Lessons Learned published by NERC that the CIPC EC would like the CIWG to investigate for additional industry feedback.
  - Develop Implementation Guidance where needed under the direction of the CIPC EC.
4. Members and Structure
The CIWG will generally follow the organizational structure and voting rights of the Critical Infrastructure Protection Committee with the following additions:

- Non-voting members who are industry subject matter experts, for the work at hand.
- A NERC staff member will be assigned as the non-voting CIWG Coordinator. The CIWG chair and vice chair will be appointed by the CIPC EC for two-year terms.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tel</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair</td>
<td>Paul Crist</td>
<td>402-467-7615</td>
</tr>
<tr>
<td>Vice-Chair(s)</td>
<td>Damon Ounsworth</td>
<td><a href="mailto:dounsworth@saskpower.com">dounsworth@saskpower.com</a></td>
</tr>
<tr>
<td></td>
<td>Lisa Carrington</td>
<td><a href="mailto:Lisa.Carrington@aps.com">Lisa.Carrington@aps.com</a></td>
</tr>
<tr>
<td>EC Sponsor</td>
<td>Jeff Fuller</td>
<td>937-331-4057</td>
</tr>
<tr>
<td>NERC staff</td>
<td>Tom Hofstetter</td>
<td>404-446-9750</td>
</tr>
</tbody>
</table>

5. Reporting
The Compliance Input WG (CIWG) will administratively report to the Policy subcommittee of CIPC.

6. Deliverables and Work Schedule
- The work plan for the CIWG will be documented in the CIPC Strategic Plan and updated as needed by the CIPC EC.
- The CIWG will convene a monthly conference call as needed to address any issues raised by the NERC Compliance Assurance Department or CIPC EC.
- At a minimum the Working Group will conduct four meetings per year. Emphasis will be given to conference calls and web-based meetings prior to the CIPC quarterly meeting. If face-to-face is required every effort will be made to meet at the same location as the CIPC quarterly meeting.
- The CIWG chair/vice chair or their designee will provide a report at each CIPC quarterly meeting.
- Process for handling requests will be developed in consultation with EC Sponsor

7. References and Resources
To be completed by WG Chair

Approved by the NERC Critical Infrastructure Protection Committee (CIPC):
__________________________, 2018
Critical Infrastructure Protection Working Group Charter

Deliverables and Work Schedule

<table>
<thead>
<tr>
<th>Date:</th>
<th>Name: CIPC Compliance and Enforcement Input WG (CEIWG)</th>
</tr>
</thead>
</table>

1. **Statement of Need**
   Critical Infrastructure Protection Committee (CIPC) will support the NERC Compliance Monitoring and Enforcement Program (CMEP) initiatives by providing timely technical expertise on matters related to cyber and physical security as requested by the NERC Compliance Assurance group and the NERC Compliance Enforcement department.

2. **Background**
   The NERC Compliance Assurance and Compliance Enforcement departments may on occasion request technical expertise in developing and prioritizing Compliance and Enforcement products. CIPC has supported these requests through the CIPC Executive Committee (EC) on an ad hoc basis. The CIPC-EC, in developing the CIPC strategic plan, believes it beneficial to formalize the processing of Compliance input requests with an ongoing working group.

3. **Objectives/Duties**
   - CIPC oversees the Compliance and Enforcement Input Working Group (CEIWG).
   - The CEIWG will develop a roster of technical cyber and physical security experts from the CIPC voting members, alternate members and other willing participants and conduct the following activities:
     - Develop a process for handling requests from NERC Compliance Assurance and Compliance Enforcement staff.
     - Provide feedback from industry to the NERC Compliance Assurance and NERC Compliance Enforcement staff to improve the CMEP.
     - Provide guidance to CIPC on prioritization of Compliance Assurance and Enforcement products under development.
     - Provide guidance on Compliance Monitoring and Enforcement Products (CMEP) products that may be brought before the CIPC for discussion.
     - Provide timely technical reports to CIPC on CMEP matters related to cyber and physical security.
     - Utilize the CIPC face-to-face meetings to facilitate discussion and allow discourse on CMEP topic areas.
     - Encourage registered entity involvement in the NERC CIP Standards review and comment process.
Provide CIPC consensus feedback to NERC Compliance Assurance and Compliance Enforcement on the effectiveness of the CMEP tools and processes when possible.

- Reviews Lessons Learned published by NERC that the CIPC EC would like the CIWG to investigate for additional industry feedback.
- Develop Implementation Guidance where needed under the direction of the CIPC EC.

Some of the CMEP products that may be reviewed include: Implementation Guidance, CMEP Practice Guides, Regional Consistency Reporting Tool, Compliance Reports, Reliability Standard Audit Worksheets (RSAW), and Internal Controls Evaluation (ICE).

4. Members and Structure

The CEIWG will generally follow the organizational structure and voting rights of the Critical Infrastructure Protection Committee with the following additions:

- Non-voting members who are industry subject matter experts, for the work at hand.
- A NERC staff member will be assigned as the non-voting CEIWG Coordinator. The CEIWG chair and vice chair will be appointed by the CIPC EC for one two-year terms.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tel</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair</td>
<td>Paul Crist</td>
<td>402-467-7615</td>
</tr>
<tr>
<td>Vice-Chair(s)</td>
<td>Damon Ounsworth</td>
<td>413-540-4057</td>
</tr>
<tr>
<td></td>
<td>Lisa Carrington</td>
<td></td>
</tr>
<tr>
<td>EC Sponsor</td>
<td>John Galloway Jeff Fuller</td>
<td>413-540-4057</td>
</tr>
<tr>
<td>NERC staff</td>
<td>Sam Chanoski Tom Hofstetter</td>
<td>404-446-970650</td>
</tr>
</tbody>
</table>

5. Reporting

The Compliance and Enforcement Input WG (CEIWG) will administratively report to the Policy subcommittee of CIPC.

6. Deliverables and Work Schedule
The work plan for the CIWG will be documented in the CIPC Strategic Plan and updated as needed by the CIPC EC.

- The CEIWG will convene a monthly conference call as needed to address any issues raised by the NERC Compliance Assurance and Compliance Enforcement Department or CIPC EC.
- At a minimum the Working Group will conduct four meetings per year. Emphasis will be given to conference calls and web-based meetings prior to the CIPC quarterly meeting. If face-to-face is required every effort will be made to meet at the same location as the CIPC quarterly meeting.
- The CEIWG chair/vice chair or their designee will provide a report at each CIPC quarterly meeting.
- Process for handling requests will be developed in consultation with EC Sponsor.

### 7. References and Resources

To be completed by WG Chair

Approved by the NERC Critical Infrastructure Protection Committee (CIPC):

_______________________, 2016-2018