Critical Infrastructure Protection Committee
Strategic Plan 2018-2019
CI PC Executive Committee

Updated: xxxxxxxxx
Table of Contents

Preface ...................................................................................................................................................................... iii
CIPC Organizational Structure................................................................................................................................. iv
Introduction ............................................................................................................................................................... v

Chapter 1: Mission, Vision, and Guiding Principles.................................................................................................... 1
  CIPC Mission............................................................................................................................................................ 1
  CIPC Vision.............................................................................................................................................................. 1
  Guiding Principles ................................................................................................................................................... 1

Advisory Panel to Board.......................................................................................................................................... 1
Cyber and Physical Security Guidelines and Technical Reports................................................................................. 1
NERC Reliability Standards Implementation and Compliance Input ........................................................................ 2
BES Security Metrics ............................................................................................................................................... 2
Public-Private Partnership....................................................................................................................................... 2
Information Sharing ................................................................................................................................................ 3
Risks and Emerging Issues.................................................................................................................................... 3
CIP Training and Educational Outreach................................................................................................................... 3
CIPC Member and Industry Observer involvement ................................................................................................. 3

Chapter 2: Areas of Strategic Focus in Support of ERO Goals.................................................................................... 5
  Major Activity 1: Advisory Panel to the NERC Board ............................................................................................. 5
  Major Activity 2: Cyber Security Risk Management .............................................................................................. 5
  Major Activity 3: Physical Security Risk Management .......................................................................................... 5
  Major Activity 4: NERC Standards Implementation Input ..................................................................................... 6
  Major Activity 5: BES Security Metrics ................................................................................................................... 6
  Major Activity 6: CIPC Training, Outreach and Industry Communications ........................................................ 6

Chapter 3: Strategic Plan Descriptions....................................................................................................................... 8
  Alignment with NERC Enterprise Operating Plan ................................................................................................. 8
  CIPC Work Plan ................................................................................................................................................... 8
  Major Activity #1: Advisory Panel to the NERC Board ........................................................................................... 8
  Major Activity #3: Physical Security Risk Management ........................................................................................ 9
  Major Activity #4: NERC Standards Implementation Input ............................................................................... 9
  Major Activity #5: BES Security Metrics ............................................................................................................... 10
  Major Activity #6: CIPC Training, Outreach and Industry Communications ........................................................ 10
Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC’s area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC’s jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.

The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRCC</td>
<td>Florida Reliability Coordinating Council</td>
</tr>
<tr>
<td>MRO</td>
<td>Midwest Reliability Organization</td>
</tr>
<tr>
<td>NPCC</td>
<td>Northeast Power Coordinating Council</td>
</tr>
<tr>
<td>RF</td>
<td>ReliabilityFirst</td>
</tr>
<tr>
<td>SERC</td>
<td>SERC Reliability Corporation</td>
</tr>
<tr>
<td>SPP RE</td>
<td>Southwest Power Pool Regional Entity</td>
</tr>
<tr>
<td>Texas RE</td>
<td>Texas Reliability Entity</td>
</tr>
<tr>
<td>WECC</td>
<td>Western Electricity Coordinating Council</td>
</tr>
</tbody>
</table>
The Executive Committee members of the Critical Infrastructure Protection Committee (CIPC) developed the CIPC Work Plan and comprehensively reviewed the work activities and deliverables to be produced for each CIPC subcommittee. This level of Executive Committee involvement promotes firsthand knowledge of group activity. CIPC Executive Committee engaged all subgroup leadership in appropriate discussion of deliverables to be produced by each group, and the expectations of the analysis and reports.

**Executive Committee**

- Marc Child, Chair, Great River Energy
- David Grubbs, Vice Chair, City of Garland
- David Revill, Vice Chair, NRECA
- Tobias Whitney, Secretary, NERC
- Melanie Seader, EEI
- APPA (vacant)
- EPSA (vacant)
- IPC (vacant)

**Physical Security Subcommittee** (David Grubbs)

- Physical Security WG (PSAG) (Ross Johnson)
- Physical Security Guidelines TF (Darrell Klimitchek)

**Cybersecurity Subcommittee** (David Revill)

- Control Systems Security WG (Mike Mertz) (Carter Manucy)
- Security Training WG (David Godfrey) (Amelia Sawyer)

**Operating Security Subcommittee** (open)

- Grid Exercise WG (Tim Conway)
- Planning Committee Joint Project Criticality Reduction (Vacant)
- Supply Chain Working Group (Vacant)

**Policy Subcommittee** (open)

- Security Metrics WG (Larry Bugh)
- Compliance and Enforcement Input WG (Paul Crist)
**Introduction**

This is a living document, meant to address the current and future CIPC strategic issues. The landscape in which the electric industry operates is dynamic and rapidly changing. Therefore, a regular review of the strategic plan by the CIPC Executive Committee should be conducted to ensure that it remains accurate.

The CIPC chair will provide regular strategic plan updates to the CIPC members, and will send status reports to the NERC Board of Trustees (Board).

Furthermore, if there are any key changes that emerge, CIPC will revisit the work plan to ensure alignment with the strategic plan of the Electric Reliability Organization (ERO) Enterprise. This work plan addresses activities, interests, and concerns of the ERO Enterprise related to critical infrastructure planning of the interconnected bulk power system (BPS).

This document is created to identify strategic activities as well as highlight the alignment of CIPC activities from several perspectives, including:

- Conforming to priorities of the ERO Enterprise, the Reliability Issues Steering Committee (RISC), and Federal, state/provincial regulators;
- Providing a technical foundation for reliability issues;
- Matching CIPC resources with priorities; and
- Efficiently using CIPC resources.
Chapter 1: Mission, Vision, and Guiding Principles

CIPC Mission
The CIPC will support the objectives of the NERC Board and standing committees by serving as an expert advisory panel on physical and cyber security, focusing on operations, compliance and policy matters. The CIPC will advance the reliability of the critical bulk electricity infrastructure of North America by addressing the technical and organizational dimensions of security; through collaboration and sharing of best practices and by identifying and quantifying emerging risks.

CIPC Vision
Foster information sharing, provide industry leadership and a forum for exchanging ideas, and promote dialogue on key issues regarding the critical infrastructure protection of the BES.

Guiding Principles
- Coordinate with the RISC on priorities and align the CIPC Strategic Plan with the ERO Strategic Plan;
- Maintain relationships and promote information sharing with other committees;
- Maintain high levels of expertise;
- Maintain the structure, processes and relationships with other NERC standing committees, and foster relationships with other forums, to maintain and foster high levels of reliability for the BES;
- Ensure CIPC resources are used efficiently;
- Maintain a focus on identification and mitigation of emerging technology risks;
- Maintain and enhance reliability through the pursuit of clear Technical Reports, Security Guidelines, and NERC Alerts;
- Maintain high levels of industry specific expertise to provide sound conclusions and opinions on security issues;
- Strive for a high level of industry awareness and accountability as related to security risks, mitigation strategies and lessons learned;
- Serve as advocate for voluntary information sharing.

Advisory Panel to Board
CIPC will fulfill this commitment with the following activities:
1. Provide reports of CIPC activities at the Board meeting.
2. Provide a representative to serve on the Reliability Issues Steering Committee (RISC).
3. Coordinate across all NERC committees and working groups to assure the highest degree of collaboration possible.
4. Encourage and solicit CIPC engagement and assist NERC staff as appropriate.

Cyber and Physical Security Guidelines and Technical Reports
CIPC will continue to support the NERC Reliability Standards with the following activities:
1. Create and maintain appropriate Task Forces and Working Groups to develop, periodically review, and revise CIPC security guidelines.
2. Issue guidelines in accordance with the work plan activities.
3. Develop and issue technical reports that contribute to the reliable operation of the BPS.

**NERC Reliability Standards Implementation and Compliance Input**

CIPC will continue to support the NERC Reliability Standards with the following activities:

1. Assist in the development of guidance and implementation of NERC Reliability Standards.
2. Assist the standards development process by providing expertise in support of the development of critical infrastructure protection standard authorization requests and standards.
3. Assist the standards development process by providing a forum for education, sharing of views, and informed debate of critical infrastructure protection standards.
4. Facilitate the implementation of critical infrastructure protection standards by developing reference documents and performing other activities.
5. Contribute to the Compliance Operations and Enforcement initiatives at NERC through the Compliance and Enforcement Input Working Group (CEIWG) by providing timely topical expertise on matters related to cyber and physical security.

**BES Security Metrics**

The CIPC will provide technical insight and advice into the development and improvement of BES security metrics, and identify a set of security performance measures to benchmark BES security. CIPC will utilize the expertise of its members, NERC staff and others to provide direction, technical oversight, feedback on the collection of industry metrics, and reporting of BES security performance metrics.

The CIPC will continue to deliver recommendations with the following actions:

1. The BES Security Metrics Working Group (BESSMWG) will develop measurable security metrics of cyber and physical security threats to the BES and industry responses.
2. The BESSMWG will provide BES security metrics to the NERC annual State of Reliability report.
3. The BESSMWG will continue to develop additional context to existing metrics to assist asset owners and NERC to understand and react to dramatic changes in trends.
4. The BESSMWG will develop and implement one new metric for the 2018 NERC State of Reliability Report.

**Public-Private Partnership**

The protection of the BPS requires the prompt dissemination of security-related information between public and private stakeholders and across international boundaries.

The CIPC will deliver recommendations by the following actions:

1. Contribute expertise to government initiatives.
2. Act as a coordinating body for dissemination of information from government to CIPC members.
3. Develop and test logistics for holding closed-session meetings when needed.
4. Foster relations with the DOE National Labs to identify collaboration opportunities.
Information Sharing
Common information-sharing protocols will enhance passage of information, ensuring that vital actionable information is disseminated quickly and accurately.

1. CIPC will study present protocols existing between industry and government. The Committee will continue to identify and research the information sharing structures, methods and requirements, and search for efficiencies and alternatives to improve or recommend changes in protocols.

2. CIPC will present recommendations to E-ISAC and NERC staff for consideration and improvement of the Public-Private Partnership, streamlining of the event reporting process for the industry with the E-ISAC, and the sharing of actionable information between government and industry.

3. Propose solutions that will build on practices and tools already in place.

4. CIPC quarterly meetings will be enhanced by the inclusion of regional information-sharing briefings. Once every two-years, voting members from each of the eight regions will deliver a briefing to CIPC (closed session if necessary) with the stated purpose of sharing security successes and challenges faced by each region.

Risks and Emerging Issues
CIPC, utilizing the expertise of its members and NERC staff, will stay abreast of new and emerging issues related to Critical Infrastructure Protection of the BPS and take action where appropriate to address these issues, and provide expertise, and direction to NERC and the electric industry.

1. CIPC will respond to the issues raised from the biennial GridEx by developing CIPC actions to address lessons learned by tasking CIPC Task Force and Work Group to develop recommendations.

2. CIPC will modify its work plan to directly address emerging technology, cyber security and physical security recommendations.

CIP Training and Educational Outreach
The CIPC will deliver with the following actions:

1. CIPC will conduct exercises, forums, and workshops related to the scope of CIPC and in cooperation with NERC.

2. CIPC will collaborate with the E-ISAC to:
   a. Identify and prioritize current topics related to the scope of CIPC.
   b. Coordinate by requesting NERC resources, if necessary, to support its activities for the forums and workshops.
   c. Schedule security training and education.

CIPC Member and Industry Observer involvement
The CIPC will deliver on this strategy by:

1. Encouraging and engaging CIPC voting member active participation.

2. Encouraging and engaging CIPC alternate members as active participants.

3. Encouraging and engaging industry observers as active participants.

4. CIPC Executive Committee will identify potential leadership candidates for subgroups.
5. CIPC subcommittees will review Task Force and Work Group rosters to identify gaps in expertise.
6. CIPC subcommittees will review Task Force and Work Group deliverables.
7. CIPC Executive Committee will encourage and recognize excellence.
Chapter 2: Areas of Strategic Focus in Support of ERO Goals

The majority of the strategic areas of focus that support ERO goals are derived from the ERO Reliability Risk Priorities, the ERO Enterprise Long-term Strategy and the E-ISAC Long Term Strategic Plan. In addition, other ERO activities are considered as input to the CIPC’s Strategic Plan. The activities listed below are driven from initiatives in association with Supply Chain Risk Management Program, NERC’s Remote Access Study, CIP-014- High Impact Control Center Report and other CIPC priority topics that warrant inclusion in the Strategic Plan. The resulting activities from these program documents address information sharing, security vulnerability risk management, and risk reduction methods to improve the reliability of the BES. This section summarizes the major activities the CIPC will pursue in support of the strategic program documents.

Major Activity 1: Advisory Panel to the NERC Board
CIPC serves as an expert advisory panel to the NERC Board, E-ISAC, RISC, and standing committees in the areas of physical and cyber security. The CIPC Chair or the designee will brief the NERC Board with regard to Strategic Plan progress, areas of risk that may impact the BES any significant updates to the CIPC program documents.

<table>
<thead>
<tr>
<th>Strategic Input</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarterly Board of Trustees Update</td>
<td>Board package, update and presentation materials.</td>
</tr>
</tbody>
</table>

Major Activity 2: Cyber Security Risk Management
CIPC has identified guidelines and technical reports to reduce the reliability risk due to system compromise from malicious threat actors. The CIPC will develop implementation guides or security guidelines depending on the best method to address the topic. CIPC will utilize the expertise of its members and collaborate with NERC staff to identify risks and emerging issues and to recommend timely and appropriate action. A CIPC representative will be nominated to the RISC to assist in the analysis and prioritization of risks and emerging issues for Board consideration. Additionally, CIPC will act on the lessons learned from the biennial NERC grid security exercise (GridEx) to improve industry’s security posture. A list of the proposed cyber security guidelines and technical reports are listed below.

<table>
<thead>
<tr>
<th>Strategic Input</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERO Enterprise Long-term Strategy Focus Area #5</td>
<td>Identification and reduction of cyber and physical security Risks while improving resilience.</td>
</tr>
<tr>
<td>ERO Reliability Risk Priority - Risk Profile #8 &amp; #9</td>
<td>Assess the cyber security risk of Fuel Handling SCADA systems for Generation.</td>
</tr>
<tr>
<td>FERC-Led Audits Compliance Report</td>
<td>Address Remote Access Security Findings #1-#18</td>
</tr>
<tr>
<td>Remote Access Study Report</td>
<td>Collaborate with E-ISAC and industry stakeholders to plan for next GridEx and share lessons learned.</td>
</tr>
<tr>
<td>Supply Chain Risk Management</td>
<td>Legacy system testing coordination with National Labs.</td>
</tr>
</tbody>
</table>

Major Activity 3: Physical Security Risk Management
CIPC has identified guidelines and technical reports to reduce the reliability risk due to physical damage initiated by malicious threat actors. The CIPC will develop implementation guides or security guidelines depending on the best method to address the topic. CIPC will utilize the expertise of its members and collaborate with NERC staff to identify risks and emerging issues and to recommend timely and appropriate action. A CIPC representative will be nominated to the RISC to assist in the analysis and prioritization of risks and emerging issues for Board consideration. Additionally,
CIPC will act on the lessons learned from the biennial NERC grid security exercise (GridEx) to improve industry’s security posture.

<table>
<thead>
<tr>
<th>Strategic Input</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-014 High Impact Control Center Report</td>
<td>Security practices for High Impact Control Centers.</td>
</tr>
<tr>
<td>CIPC Priority Topic in coordination with PC</td>
<td>Reduction in asset criticality by developing design standards.</td>
</tr>
<tr>
<td>CIPC Priority Topic</td>
<td>Security implications of UAVs and clarifying the rights of stakeholders.</td>
</tr>
<tr>
<td>CIPC Priority Topic</td>
<td>Key management security guideline.</td>
</tr>
<tr>
<td>GridEx Planning &amp; Preparation</td>
<td>Collaborate with E-ISAC and industry stakeholders to plan for next GridEx and share lessons learned.</td>
</tr>
</tbody>
</table>

**Major Activity 4: NERC Standards Implementation Input**

CIPC will support NERC standards and compliance initiatives, including implementation guidance, by providing timely topical expertise on matters related to cyber and physical security in association with the NERC CIP Standards. The Compliance and Enforcement Input Working Group (CEIWG) is established to solicit industry stakeholders for input to NERC staff to assist and clarify compliance monitoring or enforcement documents. CIPC will utilize the expertise of its members and collaborate with NERC staff to identify risks and emerging issues and to recommend timely and appropriate action.

<table>
<thead>
<tr>
<th>Strategic Input</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emerging Technology Roundtable</td>
<td>Implications of Cloud Services for CIP Assets (Pilot Study).</td>
</tr>
<tr>
<td>CIPC Priority Topic</td>
<td>Implications of Voice-over-IP and the CIP Standards.</td>
</tr>
<tr>
<td>CIPC Priority Topic</td>
<td>CIP Implications of Shared Transmission Facilities.</td>
</tr>
</tbody>
</table>

**Major Activity 5: BES Security Metrics**

CIPC will utilize the expertise of its members, NERC staff, and others to provide direction, technical oversight, feedback on the collection of industry metrics, and reporting of BES security performance metrics. The BES Security Metrics Working Group (BESSMWG) is established to develop measurable security metrics of cyber and physical security threats to the BES. The BESSMWG will collaborate with NERC to produce an annual security assessment of the BES.

<table>
<thead>
<tr>
<th>Strategic Input</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERO Enterprise Long-term Strategy Focus Area #5</td>
<td>Security Metrics derived from E-ISAC or Compliance data.</td>
</tr>
<tr>
<td>CIPC Priority Topic</td>
<td>Annual Security Assessment of the BES.</td>
</tr>
</tbody>
</table>

**Major Activity 6: CIPC Training, Outreach and Industry Communications**

CIPC, through its Outreach and Training Working Group (OTWG), will coordinate and communicate with those responsible for both physical and cyber security in all industry segments, including, among others E-ISAC, American Public Power Association (APPA), Canadian Electric Association (CEA), Edison Electric Institute (EEI), Electric Power Research Institute (EPRI), Electric Power Supply Association (EPSA), ISO/RTO Council (IRC), National Rural Electric Cooperative Association (NRECA), North American Standards Board (NAESB), the Nuclear Energy Institute (NEI), and
the NERC Regional Entities (REs). In addition, the CIPC will liaise with government, including the Department of Energy (DOE) national labs, about critical infrastructure protection matters. CIPC will provide to industry the opportunity to participate in physical, cyber and operational security training, and educational outreach activities.

- CIPC will support the training development through workshops and webinars.
- CIPC will develop or support outreach and training efforts related to NERC standards implementation.
- CIPC will ensure security related deliverables are accessible to CIPC members and industry.

<table>
<thead>
<tr>
<th>Strategic Input</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIPC Priority Topic</td>
<td>Update CIPC Website on NERC.com.</td>
</tr>
<tr>
<td>CIPC Priority Topic</td>
<td>Develop CIPC Collaboration Site on NERC.com.</td>
</tr>
<tr>
<td>E-ISAC Long-term Strategic Plan</td>
<td>Develop Information Sharing, Outreach and Training Plan.</td>
</tr>
<tr>
<td>ERO Enterprise Long-term Strategy Focus Area #3</td>
<td>Develop Information Sharing, Outreach and Training Plan.</td>
</tr>
</tbody>
</table>
Chapter 3: Strategic Plan Descriptions

Alignment with NERC Enterprise Operating Plan
As a NERC Board committee, CIPC is dedicated to the success of the ERO mission and works to ensure the goals of the committee maps directly to the goals of the enterprise.

CIPC Work Plan
The CIPC Executive Committee will annually assess its work plan and strategic imperatives in order to ensure that the work being performed by the committee will align to the areas of strategic focus.

Major Activity #1: Advisory Panel to the NERC Board

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description of Deliverable</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board package, update and presentation materials</td>
<td>The quarterly presentation made by the CIPC Chair or his/her designee to provide on the CIPC progress on strategy and work plan items.</td>
<td>On-going</td>
</tr>
</tbody>
</table>

Major Activity #2: Cyber Security Risk Management

<table>
<thead>
<tr>
<th>Activities</th>
<th>Description of Deliverable</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification and Reduction of Cyber and Physical Security Risks</td>
<td>The CIPC in coordination with the OC and PC will define measures to reduce cyber and physical security risks.</td>
<td>Q4 2019</td>
</tr>
<tr>
<td>Assess the cyber security risk of Fuel Handling SCADA systems for Generation</td>
<td>The CIPC, in coordination with the Operating Committee, will coordinate with stakeholders and perform a study on the risks associated with fuel handling systems that supply generation facilities. An emphasis will be place on natural gas-sourced facilities.</td>
<td>Q1 2019</td>
</tr>
<tr>
<td>Address Remote Access Security Findings #1-#18</td>
<td>The CIPC will coordinate with stakeholders and will either develop security guidelines or offer training (as necessary) on the topics identified in the Remote Access Study.</td>
<td>Q3 2019</td>
</tr>
<tr>
<td>GridEx Preparation and Planning</td>
<td>The CIPC, in coordination with industry stakeholders, develop lessons learned from the completed GridEx activities and begin preparing for the upcoming GridEx.</td>
<td>On-going</td>
</tr>
<tr>
<td>Vendor Essential Security Practices Model</td>
<td>In support of the Supply Chain Risk Management Program, the CIPC will work with vendors and industry stakeholders to develop a controls matrix that can be used to help industry work with vendors to address supply chain risks.</td>
<td>Q3 2018</td>
</tr>
<tr>
<td>Legacy system testing coordination with National Labs</td>
<td>In support of the Supply Chain Risk Management Program, the CIPC will work with vendors and industry stakeholders to test legacy systems and supply chain share lessons learned with industry.</td>
<td>Q4 2019</td>
</tr>
</tbody>
</table>
### Major Activity #3: Physical Security Risk Management

<table>
<thead>
<tr>
<th>Activities</th>
<th>Description of Deliverable</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security practices for high impact Control Centers</td>
<td>The CIPC will perform a study to determine the types of operational control comprised by high impact controls centers and identify effective measures to mitigate risks.</td>
<td>Q1 2019</td>
</tr>
<tr>
<td>Reduction in Asset Criticality (in coordination with PC)</td>
<td>A security guideline will be developed to address effective practices to reduce the criticality or the risk of loss of any critical substation as a means to improve resiliency and reduce applicability to CIP-014-2.</td>
<td>Q4 2019</td>
</tr>
<tr>
<td>Security implications of UAVs</td>
<td>The CIPC will research and communicate current practices and considerations for drones and other unmanned aerial vehicles.</td>
<td>Q3 2018</td>
</tr>
<tr>
<td>GridEx Preparation and Planning</td>
<td>The CIPC, in coordination with industry stakeholders, develop lessons learned from the completed GridEx activities and begin preparing for the upcoming GridEx.</td>
<td>On-going</td>
</tr>
<tr>
<td>Key management security guideline</td>
<td>Identify and describe security best practices associated with the management of physical keys BES assets. Specific examples for low impact CIP assets will be considered.</td>
<td>Q2 2018</td>
</tr>
</tbody>
</table>

### Major Activity #4: NERC Standards Implementation Input

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description of Deliverable</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implications of Cloud Services for CIP Assets</td>
<td>The CIPC, in coordination with NERC and industry stakeholders will conduct a pilot to determine the CIP Standards implication of cloud services on the BES. The study may result in implementation guides, security guidelines or other deliverables to industry.</td>
<td>Q4 2018</td>
</tr>
<tr>
<td>Implications of Voice-over-IP and the CIP Standards</td>
<td>Provide implementation recommendations for the categorization of voice communications under Reliability Standard CIP-002-5.1. Provide suggested guidance for the use and protection of Cyber Assets used for voice communications, particularly within Control Center environments, including issues surrounding authenticity and integrity.</td>
<td>Q1 2018</td>
</tr>
<tr>
<td>CIP Implications of Shared Transmission Facilities</td>
<td>Provide a common understanding of the challenges surrounding shared facilities relating to CIP Reliability Standards and compliance. In addition, provide suggested solutions to some of the issues related to these challenges, specifically focused on ways to meet compliance obligations through joint agreements between entities.</td>
<td>Q2 2018</td>
</tr>
</tbody>
</table>
## Major Activity #5: BES Security Metrics

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description of Deliverable</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Metrics derived from E-ISAC or Compliance data</td>
<td>The CIPC, in coordination with NERC and industry stakeholders will develop additional metrics to improve security metrics used as part of NERC’s State of Reliability Report. The metrics can be derived from E-ISAC, compliance performance or 3rd party data sources.</td>
<td>On-going</td>
</tr>
<tr>
<td>Annual Security Assessment of the BES</td>
<td>The CIPC, in coordination with NERC and industry stakeholders will evaluate the process and approach for developing an assessment of Security of the Bulk Electric System.</td>
<td>Q4 2019</td>
</tr>
</tbody>
</table>

## Major Activity #6: CIPC Training, Outreach and Industry Communications

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description of Deliverable</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update CIPC Website on NERC.com</td>
<td>Consolidate all CIPC deliverables and content and post the content NERC.com website. The content should include guides, CIPC meeting materials or training documentation.</td>
<td>Q3 2018</td>
</tr>
<tr>
<td>Develop CIPC Collaboration Site on NERC.com</td>
<td>The CIPC will work with NERC to create and maintain a collaboration site used to facilitate the coordination and development of CIPC subcommittees deliverables and draft content.</td>
<td>Q2 2018</td>
</tr>
<tr>
<td>Develop Information Sharing, Outreach and Training Plan</td>
<td>The CIPC will develop a plan to manage training and outreach to CIPC members and industry stakeholders that will outline the timing, resources and topics for upcoming CIPC engagements.</td>
<td>Q1 2018</td>
</tr>
</tbody>
</table>