NERC Critical Infrastructure Protection Committee (CIPC)
Report to Southwest Power Pool Regional Entity Trustees
Submitted by Robert McClanahan, Chair, SPP Critical Infrastructure Protection WG
April 21, 2013

NERC CIPC Meeting

- The NERC CIPC held its quarterly meeting in Albuquerque, NM on March 5-6, 2013. The materials for this meeting can be found at:
  - Agenda: http://www.nerc.com/docs/cip/CIPC_Package_December_1213_2012_Final.pdf
  - Presentations: http://www.nerc.com/docs/cip/Presentations_March_2013_CIPC_Meeting.zip
  - Draft Minutes: http://www.nerc.com/docs/cip/CIPC_March_5_6_2013_Posting_Final.pdf
- Corporate Risk Solutions, Inc. hosted a physical security workshop for CIPC Members and Alternates prior to the CIPC meeting.
- Chuck Abell, CIPC Chair, discussed several items of interest to CIPC.
  - He noted that he is pleased with the quantity of work product that was accomplished by CIPC in 2012, but feels that more could have been done. The level of participation in CIPC Task Forces and Working Groups had improved over past years.
  - The CIPC Charter is currently under review and potential changes are in the works. The charter will undergo legal review before approval.
  - Based on the percentage of Net Energy for Load (NEL) for Canadian entities, those entities are under-represented on CIPC. The Canadian Electricity Association (CEA) will nominate two additional voting Members to CIPC, bringing the total Canadian representation to four.
  - The Electric Sector Coordinating Council (ESCC) conducted closed and open conference calls on January 24th. (Closed and open calls were also held on April 18th.)
- Matt Blizard, Director of NERC's Critical Infrastructure Protection Division, discussed NERC's strategic goals for 2013-2016 and how they intersect with CIPC's efforts.
  - NERC has a goal of conducting 10-12 cyber risk preparedness assessments (CRPA) in 2013.
  - NERC has a goal of conducting 25 sufficiency reviews (SRP) in 2014.
  - NERC is participating in the Electric Sector Public Private Partnership (ES3P) with DOD related to national security facilities.
- Nathan Mitchell of APPA provided an overview of the recent Executive Order (EO), signed by President Obama and its impact on CIPC work product. The EO is intended to:
  - Promote information sharing between the Federal Government and owners/operators of critical infrastructure.
  - Expand the Enhanced Cybersecurity Services program beyond the Defense Industrial Base (DIB) and into the critical infrastructures.
  - Identify Critical Infrastructure owners/operators/assets by July 12, 2013.

- FERC – report to POTUS on sufficiency of existing regulations by January 10, 2014; request for additional authority to address cyber risk by May 13, 2014; report to OMB any ineffective, conflicting or excessively burdensome requirements by February 12, 2015.

- Mr. Mitchell also provided an overview of the current state of cyber legislation in the Congress.
  - The Rogers-Ruppersberger Cybersecurity Bill is very similar to the 2011 Cyber Intelligence Sharing and Protection Act (CISPA). The bill has reported out of committee and is waiting to be introduced on the floor. There is no complimentary bill on the Senate side.
  - GRID Act passed the House in 2012, but had no corresponding Senate bill. Has not been reintroduced in this Congress.
  - Waxman and Markey sent a letter to numerous electric utilities asking highly-sensitive questions related to critical infrastructure and cyber security. The letter was not coordinated with industry and provided no assurance that the answers to these questions would be protected from public disclosure. Most utilities opted not to respond to the request. A copy of this letter is attached below.
  - Securing America's Future: The Cybersecurity Act of 2012 failed to pass the Senate. Has not been reintroduced.
- Jim Brenton, CIPC Vice Chair, provided an update on the NERC Reliability Issues Steering Committee (RISC), which is working on strategic efforts to sustain reliability. RISC is prioritizing the issues that are before them.
  - The high priority items are: Cyber Attack, Workforce Capability/Human Error, Protection Systems, Monitoring & Situational Awareness.
  - The medium priority items are: Operational Modeling, Equipment Maintenance and Management, Coordinated Attack, Generator Availability, Increased Dependencies on Natural Gas.
  - Many other issues are currently rated low priority, including: GMD/EMP, Climate Change, Pandemic, Extreme Weather/Acts of Nature, SmartGrid. These will be monitored and periodically reviewed.
- Stuart Brindley, contractor for NERC, provided an update on the final steps in the HILF project.
- Stephen Diebold, Chair of the Electric Sector Information Sharing Task Force (ESISTF), provided an update on the efforts of the Task Force.
  - The task force's report is nearing completion and should be available in draft form for the ESCC's face-to-face meeting on April 18th.
- Nathan Mitchell, CIPC Vice Chair, chairs the Personnel Security Clearance Task Force (PSCTF). With the issuance of the Executive Order, which highlights the need for security clearances, the efforts of the group to develop a model for management of security clearances within the industry have been accelerated. The PSCTF draft report has been circulated to CIPC for comment.
- Mike Mertz reported on the progress of the BES Security Metrics Task Force.
- Paul Crist, Chair of the Compliance and Enforcement Input Working Group (CEIWG), provided an update on the work by the group.

- The group is currently addressing industry concerns related to CAR-005 and the numerous violations that have been seen as a result of that CAR being used for compliance – even though CARs were said not to be used for compliance.
- The group is working with NERC to identify how CARs are developed, if they can be modified, what could be done to withdraw one.

- Mark Engels, Chair of the Attack Tree Task Force, provided an update of the efforts of his group.
  - The TF is currently identifying systems and sub-systems within generation and control centers that could negatively impact the grid within three hours.
  - The TF will be participating in training on attach tree analysis software, which will aid in the development of a plan to address.
- Mr. Engels, Chair of the CSSWG, recommended that the existing CIPC cyber security guidelines be retired, given that there is no electric sector-specific information contained within them. In their place, the WG has created an authoritative list of other resources that provide more detailed information than the existing guidelines. CIPC approved the retirement of the following guidelines.
  - Business Network Electronic Connectivity
  - Control System Cyber Security Incident Response Planning version 1.0
  - Cyber Response version 3.0
  - Threat and Incident Reporting Guideline
  - Access Controls
  - Intrusion Detection
  - IT Firewall
  - Risk Management
  - Patch Management for Control Systems
  - Securing Remote Access to Electronic Control and Protection Systems
- Mark Child provided an update on the Cyber Security Events Analysis Working Group.
- John Breckenridge, Chair of the Physical Security Response Guideline Task Force, discussed the work in progress to develop the guideline. The group is currently researching the new DHS threat level.
- Marc Child discussed the efforts of the Cyber Training Working Group. CIPC approved the combining of the Cyber and Physical Training Working Groups.
- Tim Conway and Brian Harrell presented on the Grid Exercise II and Grid Security Conference. NERC and the TF have reviewed proposals from five contractors to conduct the exercise. Booz Allen Hamilton was chosen to lead the exercise, which is scheduled for November 13-14, 2013. The exercise plans to engage individual organizations' response plans.
  - NOTE: The SPP CIPWG is planning to develop a regional plan to allow SPP Member Companies to participate in both the National and a Regional exercise simultaneously.
- GridSecCon 2013 will be held on October 15-17, 2013 in Jacksonville, FL. The first day will be a full-day of training on cyber and physical security topics. Days 2-3 will be a workshop on current security-focused issues.

- Fred Hintermister, NERC CIP and Cybersecurity Specialist, provided an overview of the ES-ISAC's mission and future goals.
- Tim Roxey, NERC Chief Cyber Security Officer, provided an overview of recent attacks and threats against critical infrastructure.
- Steve Noess of NERC provided an overview of current and active interpretation requests on the CIP standards.
- Michael Assante of the National Board of Information Security Examiners (NBISE) provided an overview of the Secure Power Systems Professional (SPSP) workforce development program. NSBIE is working to identify critical cyber security roles in the electric industry and mapping them to certifications and training opportunities that are currently available. The goal of the effort is to identify a development roadmap for creating the security-trained professionals that will be required in the industry going forward.
- Dave Norton of FERC provided a report on FERC activities. FERC's Office of Energy Infrastructure Security (OEIS), McClelland's new group, will have nothing to do with standards and compliance, but will focus on industry interaction and outreach. The existing Office of Electric Reliability (OER) will retain focus on compliance, audits, NOPRs, etc.
- CIPC Meeting Schedule for 2013:
  - June 11-12 in Atlanta, GA
  - September 17-18 in Denver, CO
  - December 10-11 in Atlanta, GA