# NERC Critical Infrastructure Protection Committee (CIPC)
# Report to Southwest Power Pool Regional Entity Trustees
### Submitted by Robert McClanahan, Chair, SPP Critical Infrastructure Protection WG
### July 18, 2011

## *NERC CIPC Meeting*

- The NERC CIPC held its quarterly meeting in Toronto, Ontario, CA on June 8-9, 2011. The agenda for this meeting can be found at http://www.nerc.com/docs/cip/CIPC_Agenda_08Jun11.pdf.
- Mark Weatherford, NERC Chief Security Officer, gave an update on his involvement with the Electric Sector Coordinating Council (ESCC) and the Partnership for Critical Infrastructure Security (PCIS), where he serves as Vice Chair. Efforts are underway to reenergize PCIS, which brings together representatives from all 18 critical infrastructure sectors.
- Stuart Brindley, a Contractor for NERC, led an update on NERC's Coordinated Action Plan. This included updates on: the Severe Impact Resilience Task Force (SIRTF), chaired by Tom Bowe, PJM; the Geomagnetic Disturbance Task Force (GMDTF), chaired by Don Watkins, BPA; the Spare Equipment Task Force (SETF), vice chaired by Mark Westendorf, Midwest ISO; the Coordinated Attack Task Force (CATF), chaired by Mark Engels of Dominion.
- Tim Roxey of NERC Staff gave an overview of the operation of the Electric Sector Information Sharing and Analysis Center (ES-ISAC). He also explained the lifecycle of a NERC alert.
    - Mr. Roxey also provided additional information on the Stuxnet worm. There is great concern that it will be used as a platform for further attacks.
- Ralph Anderson of NERC Staff reported on the CIP Sufficiency Review Program. The program was deemed a success in 2010 and was carried forward in 2011. As of the CIPC Meeting, eight Registered Entities had volunteered for the program, and NERC is seeking additional volunteers.
- NERC Staff announced a grid security conference, known as GridSecCon, to be held at the JW Marriott in New Orleans, LA on October 19-21, 2011. This summit will bring industry, law enforcement and homeland security officials, and regulators to one venue to discuss physical and cybersecurity.
- CIPC continues work to revisit and update its Security Guidelines for the industry. These guidelines are not guidelines in support of standards, but are intended to provide general guidance and best practices on security-related matters.
    - John Breckenridge of Kansas City Power and Light has been appointed Chair of the Substation Security Guideline Task Force.
    - The Business Continuity Guideline was approved by CIPC to be posted for a 45-day broad industry review and comment period.
- The schedule for CIPC meetings for the remainder of 2011 follows:
    - September 14-15, 2011 (St. Louis, MO)
        - NERC will be sponsoring an Improvised Explosive Device (IED) Awareness/Bomb Threat Management Workshop in conjunction with this meeting to help CIPC members better manage the risks associated with IEDs.

- December 14-15, 2011 (Atlanta, GA – tentative)
    - NERC and the Department of Homeland Security (DHS) are working to schedule a classified briefing for cleared CIPC members and alternates in conjunction with this meeting. These briefings provide additional detail on emerging threats.

- Dave Batz of EEI gave an overview of the work being done by various committees of the US House and Senate on grid security legislation. There are still numerous pieces of legislation circulating around the Congress, though none has yet reached a vote.
- The CSO706 SDT continues work on addressing the remaining 50+ FERC directives in Order 706. The team continues development work on what has now been renamed CIP Version 5, which would replace Standards CIP-002-4 through CIP-009-4.

## *SPP CIPWG Meeting*

- The SPP Critical Infrastructure Protection Working Group (CIPWG) held its quarterly meeting at Kansas City Power & Light Headquarters in Kansas City, MO on June 14, 2011. The agenda for this meeting can be found at http://www.spp.org/publications/CIPWG%20Agenda%20-%206-14-2011.pdf.
- The CIPWG elected Eric Ervin as Cybersecurity Alternate for the NERC CIPC, replacing Joe Doetzel, who recently left Kansas City Power & Light. An updated CIPC roster will be forwarded to the SPP Regional Entity Board of Trustees for approval.
- Philip Huff, Vice Chair of the CIP Standards Drafting Team gave an update on the CIP Version 5 Standards and other CIP-related activities.
    - The NERC Order 706 Drafting Team continues developing version 5 of the CIP Standards to address all remaining directives in FERC Order 706. This next version builds on the version 4 bright line criteria for defining Critical Cyber Assets. The primary change in version 5 is that Cyber Systems are classified as High, Medium and Low based on the relative impact of the cyber system to the BES.
    - The SDT recently completed a 3-day workshop with regional CIP auditors to improve the measurability and clarity of the Standard requirements. This month the team will perform a walk-through of applying the requirements to generation and substation requirements. Then NERC will perform a full quality review in advance of the posting in October. NERC anticipates filing version 5 with FERC by the 3rd quarter of 2012.
    - There has been no action by FERC on the version 4 Standards. The drafting team will meet with FERC staff on July 28 to discuss the version 5 Standards.
    - Other CIP standards activities at NERC include the establishment of a standing CIP interpretations team and a joint risk management project with the DOE and NIST. The DOE expects to post this work by the end of July.
- Rick Goins, DHS Protective Security Advisor for Missouri, was present to discuss recent activities within DHS.