

## **WESTERN CYBER-SECURITY WEBINAR: June 2, 2011**

Western Interconnection Regional Advisory Body (WIRAB)

The presenters were:

- Patrick Miller: President of EnergySec and Principal Investigator for NESCO, the National Electric Sector Cyber-security Organization. Patrick was formerly the WECC Manager of CIP Audits and Investigations.
- Mark Weatherford: NERC Vice-President and Chief Security Officer. Formerly, Mark was chief information security officer in California and in Colorado. (Mark was joined by David Cook, NERC General Counsel.)

The PowerPoint presentation is attached. The recorded webinar can be accessed using the following link: <http://westgov.adobeconnect.com/p6ddmek9bqe/>

### **SUMMARY:**

**The Threat:** Patrick Miller discussed the cyber security threat, linking it to the increasingly digital, connected, and embedded technology landscape of the 21<sup>st</sup> century. The current adversaries have sufficient motive, much improved means, and increasing opportunity. The threat can be addressed by consistent efforts to improve protection, detection, and response, by regular drills and exercises, and by planning for options and spare equipment. Mark W. added that the “insider threat” (involved in over half of cyber events) also needs to be acknowledged and addressed.

**The Institutional Landscape:** Mark Weatherford discussed NERC initiatives to improve cyber security in the bulk power system. His office has three divisions—one focused on risk management, another on security standards and training, and the third on policy and coordination. His 2011 objectives include a North American cybersecurity exercise (scheduled for November 15-17), several capabilities development initiatives conducted in partnership with federal agencies or DOE labs, and several Task Force initiatives resulting from NERC’s June 2010 “High-Level, Low-Frequency Event Risk” report. Responding to the criticism that CIP standards don’t cover everything, NERC is developing voluntary cyber security guidelines for the electric sector, with a draft expected later this month.

**Legislation:** Dave Cook, NERC General Counsel, was on the call, but time did not permit discussion of the several legislative initiatives under consideration in Congress. FERC is seeking additional authorities, which would extend to distribution systems under specified circumstances. Some consolidation may occur as the several bills are considered. Whatever the results, the implications for states could be significant.

**What PUCs Can/Should Do:** After recognizing the complex sets of regulations faced by utilities, Patrick outlined several areas for improvement of cyber security. One involves management practices--who has access to what for what purposes. Another involves developing awareness and understanding (including actuarial data) to guide effective response. A third involves a set of questions to ask of regulated entities.

**California Smart Grid Deployment Plans:** Wendy Al-Mukdad (CPUC) mentioned the Smart Grid Deployment Plans required of larger utilities under Senate Bill 17. Initially submissions are scheduled for July 2011. The plans will address eight elements, including “grid security and cyber security strategy.”

**Next Steps:** Doug Larson asked for thoughts regarding useful next steps. Initial thoughts include:

- Participation in the “Smart Grid and Energy Assurance Planning” online workshop (June 29, 1:00-3:00 EDT) offered by the Institute for Public Utilities at Michigan State University. The instructor is Jeff Pillon, Director of Energy Assurance for the National Association of State Energy Officials (NASEO). Link: <http://ipu.msu.edu/programs/online/smart-grid-assurance-planning.php>
- A review of current cyber security legislation, including implications for states.
- Exploratory discussion with the WECC Critical Infrastructure and Management Subcommittee. How does the subcommittee’s program reflect interconnection-wide reliability and cost concerns?
- A review of the differences in jurisdiction among western state PUCs, considering implications for state-level cyber security initiatives.
- Other thoughts invited.