# NERC CIPC Report

SPP RE Trustees Meeting – July 25, 2011

# Topics

- Highlights from CIPC Meeting
- Status of CIP Standards
- Washington Update

# CIPC Highlights

- NERC CSO Mark Weatherford discussed a vulnerability in the ICCP protocol identified by the Idaho National Lab
  - Used by virtually every Registered Entity to transfer data in real-time to Transmission Operators, Balancing Authorities and Reliability Coordinators
  - No additional information has been provided

# CIPC Highlights (cont)

- Tim Roxey covered the “life cycle” of a NERC Alert, describing in detail the effort put into the process
  - Vulnerability or other issue is identified
  - Information is gathered
  - Classified information is “scrubbed out”
  - Product is vetted by subject-matter experts
  - FERC review if necessary
  - Alert is released

# CIPC Highlights (cont)

- NERC's Grid Security Conference, GridSecCon, was announced
  - Scheduled for October 19-21 in New Orleans, LA
  - Intended to bring industry, law enforcement, government agencies, etc. to discuss grid security issues
  - SANS will offer a pre-conference training session on October 18th

# CIP Standards Update

- The NERC Order 706 Drafting Team continues development of CIP Version 5
  - Addressing all remaining directives in FERC Order 706
  - 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

# CIP Standards Update (cont)

- 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
- NERC will then perform a full quality review in advance of the posting in October

# CIP Standards Update (cont)

- NERC anticipates filing Version 5 with FERC by the 3rd quarter of 2012
- The drafting team will meet with FERC staff on July 28 to discuss the Version 5 Standards
- There has been no action by FERC on the Version 4 Standards

# CIP Standards Update (cont)

- Other CIP standards activities at NERC
  - Establishment of a standing CIP interpretations team
  - Joint risk management project with the DOE and NIST
  - DOE expects to post this work by the end of July

# Washington, DC Update

- Sampling of recent security incidents
  - RSA breach (March)
  - Sony network breach (April-June)
  - China Blue Team (May)
  - Lockheed Martin breach (May)
  - Pentagon sources discuss kinetic response
  - InfraGard breach (June)
  - Citibank (June)
  - PayPal (July)

# Washington, DC (cont)

- Breaches like these have energized the House and the Senate to take some action on cyber security in this Congress
- Were it not for the current focus on raising the debt ceiling, we would likely have seen movement by now
- There are still numerous pieces of legislation floating around

# Questions?