BPS Reliability

Global Energy Management Institute

Bauer, College of Business, University of Houston

March 11, 2015
Critical Infrastructure Scene Setter

1. Bulk Power System’s Reliability Challenges
2. Critical Infrastructure - Physical Security Threat
3. Critical Infrastructure - Cybersecurity Threat
4. BPS’ CIP Compliance Challenges
5. Recommendations to consider
6. Questions to consider
Bulk Power System’s Reliability Challenges

» Threats and Vulnerabilities – Cyber and Physical
» FERC and NERC Standards
» Workforce CIP (Supply and Demand)
» Changing Resource Mix
» Mother Nature
» Political, press and public pressures
» Aging infrastructure
» Legislation – (Environmental)
» Executive Orders, and PPD-21
Critical Infrastructure - Physical Security Threat

» PG&E’s Metcalf Substation (Sabotage)

» Arkansas – Lone Wolf… (Sabotage)

» Recent Substation Intrusion

» Explosive Devices (Terrorism)
  o Boston Marathon – soft targets
  o Maritime or Land - USS Cole

» Combined Physical and Cyber Attack (Terrorism)
  o GridEx Series
Critical Infrastructure - Cyber Security Threat

» Aurora

» Stuxnet Discovery – Iran Centrifuges (6/25/2010)

» DuQu, Wiper, Flame, Gauss, Mahdi – Cyber Espionage, Cyber Effects (9/1/2011- 7/1/2012)

» Shamoon - Saudi Aramco and RasGas (August 2012)

» U.S. Financial Institutions – Chase, BOA, NYSE, Wells Fargo, U.S. Bancorp, PNC (DDOS Attacks, September 2012)

» Mandiant APT1 Report (February 2013)


» Control Systems; SCADA – Biggest Concern…
» NERC and FERC Standards (rate of change, the amount, the variety, the overlap…)

» Clarity of NERC Standards (CIP v5 example)

» Compliance Risk is great - $1M/event/day

» Reducing NERC Standards compliance risk

» Aggressive NERC Standards implementation timelines (2015 and 2016)
Bulk Power System’s CIP Compliance Challenges (continued)

» Minimizing NERC Standards compliance risk

» Addressing concurrently CIP v5 and CIP-014 NERC Standards with aggressive and concurrent implementation timelines (2015 and 2016)

» Integration of Cyber and Physical Security Compliance needed

» Hardening of Critical Facilities

» Addressing political, media, and public pressures
Recommendations to Consider

» Get out ahead of regulation

» Establish Compliance Programs – CIP (Cyber and Physical)

» Pirate Lessons Learned from other sectors – Regulation, Security

» Implement CIP Best Practices (Cyber and Physical Security)

» Information Share – Leverage the Electric-Subsector Information Sharing and Analytics Center (ES-ISAC)

» Continuously conduct risk assessments and address highest risk –
  o Cyber: Maturity Assessment; and Penetration Testing and Forensics
  o Physical: Critical Facilities; Threat and Vulnerability Evaluation; Security Plans
Recommendations to Consider (continued)

» Expand DOE/DHS coordination nexus – NCCIC, ICS-CERT, US-CERT

» Build the CIP workforce – highly competitive

» Consider integration of compliance and security; physical and cyber early

» Prevent – if possible, next biggest security event (Metcalf lesson learned)

» Extremely proactive with security and tell the story… (NERC lessoned learned)
Questions to consider

» Where to spend the next incremental security dollar?

» How can you possibly direct/manage the CIP regulation machine?

» Any lessons learned from the BPS experience that could assist you?
Key Contacts

Ken Lotterhos | Managing Director  
Washington, DC  
(631) 678-7302  
Ken.lotterhos@navigant.com

Matthew Blizard | Director  
Folsom, CA.  
(360) 464-3944  
Matthew.Blizard@navigant.com

Celia David | Director  
Chicago, Illinois  
(312) 583-2139  
celia.david@navigant.com