GridEx II
Lesson’s Learned

Don Wallin
Sr. Lead System Operator Trainer
NERC sponsored GridEx II occurred November 13 - 14, 2013. Objectives included:

- Exercising the current readiness of the electricity industry to respond to a security incident, incorporating lessons learned from GridEx 2011
- Reviewing existing command, control, and communication plans and tools for NERC and its stakeholders
- Identifying potential improvements in physical and cyber security plans, programs, and responder skills
- Exploring senior leadership policy decisions and triggers in response to major grid reliability issues
• 200+ Organizations
• 35 PJM member companies
• Internal PJM Teams:
  – Dispatch Training Team and Simulator
  – Corporate Incident Response Team
  – Cyber Security Incident Response Team
  – Physical Security Incident Response Team
  – Crisis Communications
  – Additional Response and Recovery Teams as required by the scenario
• Nation-state sponsored attacks against the BES:
  – Distributed denial of service (DDoS) attacks against shared service websites (OATI, IDC, and SDX)
  – “Shamoon” like malware that exfiltrated sensitive information and locked corporate desktops/laptops
  – Physical attacks against transmission and generation
  – Active shooter attacks against first responders
  – RTU malware
• Copycat physical and cyber attacks from lone individuals and groups
What went well

- Interaction between PJM and members – real operators talking to real operators
- External Interaction (FBI, DHS, ES-ISAC, etc.)
- ES-ISAC / BPSA Conference Calls
- Discussions around critical substations / assets
- High level of awareness regarding sensitive information/facility names
• Non-standard communications channels
• Stagger exercise injects from members
• Consider review of all operations related materials for information security (i.e. Manual 3)
• Add similar “unplanned injects” to future PJM drills (Emergency procedures, restoration, etc.)
• Joint PJM and TO exercise in 2014
• GridEx III in 2015