Sterne Kessler Goldstein Fox
ATTORNEYS AT LAW

Power Grid Resiliency

PTO Pilot Program Proposal

Theodore A. Wood

February 7, 2011

INNOVATION

"The first step in winning the future is encouraging American innovation. (…) What we can do -- what America does better than anyone else -- is spark the creativity and imagination of our people."

President Barack Obama
State of the Union Address, 25 January 2011

Specific “carve-out” for the Grid

- The grid is vulnerable

  “The next Pearl Harbor is likely to be a cyber attack going after our grid…and that can literally cripple this country.” CIA Director Leon Panetta

- Proposing a mechanism with entrepreneurial appeal
- Spur innovation to reduce grid vulnerabilities
- PTO becomes catalyst for grid innovations

Grid Pilot Highlights

- Similar to Green Pilot Program
  - Covers new applications
- Grid resiliency-enhancing technologies
  - Added to existing grid components and systems
  - Integrated into next generation components and systems

Proposed Grid Resiliency Technologies

- Cyber (Hardware and Software) Resiliency Strategies coupled with Power Grid Infrastructure Technologies
- Physical Infrastructure Resiliency Strategies
- Techniques for Validating and Certifying Grid Resiliency

Proposed Grid Technologies (cont.)

A. Cyber (Hardware and Software) Resiliency Strategies	B. Power Grid Infrastructure Technologies	C. Physical Infrastructure Resiliency Strategies	D. Techniques for Validating and Certifying Grid Resiliency
1)Access Control 2)Authentication 3)Cryptography 4)Public Key Infrastructure (PKI) 5)Elliptic Curve Cryptography 6)Certificate Authority 7)Trust and Key Management 8)Software Upgrading 9)Patch Management 10)Rootkit Detection 11)Firewalls 12)DMZ (Demilitarized Zone) 13)Proxy 14)Network Access Control (NAC) 15)Anti Virus (AV) 16)Virtual Private Network (VPN) 17)Intrusion Detection System (IDS) 18)Intrusion Protection System (IPS) 19)Intrusion-Tolerance 20)Diversity Strategies 21)Replication Strategies 22)Intrusion Response System (IRS)	**SCADA Systems (Transmission & Operations)** 1)Intelligent Electronic Device (IED) 2)Remote Terminal Unit (RTU) 3)Programmable Logic Controller (PLC) 4)DNP-3 (Distributed Network Protocol 3) 5)MODBUS (serial communications protocol for PLCs) 6)IEC 61850 7)Inter-Control Center Communications Protocol (ICCP) 8)Energy Management System 9)Data Historian 10)Human Machine Interface (HMI) **Wide-area Measurement Systems** 1)GPS (Global Positioning System) Clock Synchronization 2)Phasor Measurement Unit (PMU) 3)Synchrophasors 4)Gateways 5)Phasor Data Concentrator (PDC) **Distribution Systems** 1)Advanced Metering Infrastructure (AMI) 2)Smart Meter 3)Meter Data Management System (MDMS) 4)Head End **Consumer-Area Energy Systems (Customer Oriented Technologies)**	1) Physical plant security 2) Grid physical component security 3) Data center facilities security 4) Security event detection and correlation 5) Electricity generation physical plant security 6) Substation physical security 7) Electric power transmission and distribution plant security 8) Grid decentralization strategies 9) Grid transformer and power line security 10) Microgrids 11) Physical threat resiliency strategies	1)Fuzzing 2)Penetration Testing 3)Red Teaming 4)Simulation 5)Validation Techniques 6)Verification Techniques 7)Conformance Testing 8)Modeling 9)Formal Proof 10) Modeling Checking

Proposed Next Steps

- Preliminary PTO Approval
- Finalize Program Details
  - Technical categories
  - Patent landscape assessment
- Get The Word Out
- Take Steps for Formal Implementation

QUESTIONS/COMMENTS?