



The Cyber House Rules

What Regulators Need to Know
about Cybersecurity

Kevin Gunn – Missouri Public Service Commission

November 17, 2009



Media Reports

THE WALL STREET JOURNAL
WSJ.com

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

Chicago Tribune

December 26, 2008

Russian hackers target U.S., Europe for profit and politics

CNN.com

Sources: Staged cyber attack reveals vulnerability in power grid



Cyber Security Initiative

- Initiated by MoPSC Chairman Robert Clayton
- Contemplated opening a docket
- Highly confidential information
- Ultimately decided letter certification was most appropriate



Cyber Security Initiative

- Send letters to all IOUs
- Responses to be “verified” and certify compliance or steps taken to become compliant
- Good Faith estimates on timetable for compliance
- What organizations IOU participates in for security issues



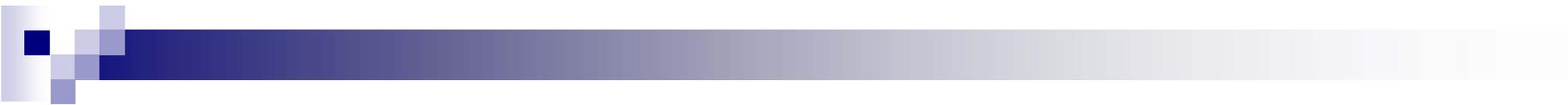
North American Electric Reliability Corporation (NERC) Standards NERC Order No. 706

- CIP-002-1 – Critical Cyber Asset Identification
- CIP-003-1 – Security Management Controls
- CIP-004-1 – Personnel & Training
- CIP-005-1 – Electronic Security Perimeters
- CIP-006-1 – Physical Security of Critical Cyber Assets
- CIP-007-1 – Systems Security Management
- CIP-008-1 – Incident Reporting and Response
Planning
- CIP-009-1 – Recovery Plans for Critical Cyber Assets



Responses

- All Missouri's IOUs certified compliance with NERC Order 706
- List of organizations IOU involved with on security issues broad and diverse



Utilities participation with Organizations

- Federal Agencies

- Department of Homeland Security
- Federal Energy Regulatory Commission
- Federal Bureau of Investigation

- State Agencies

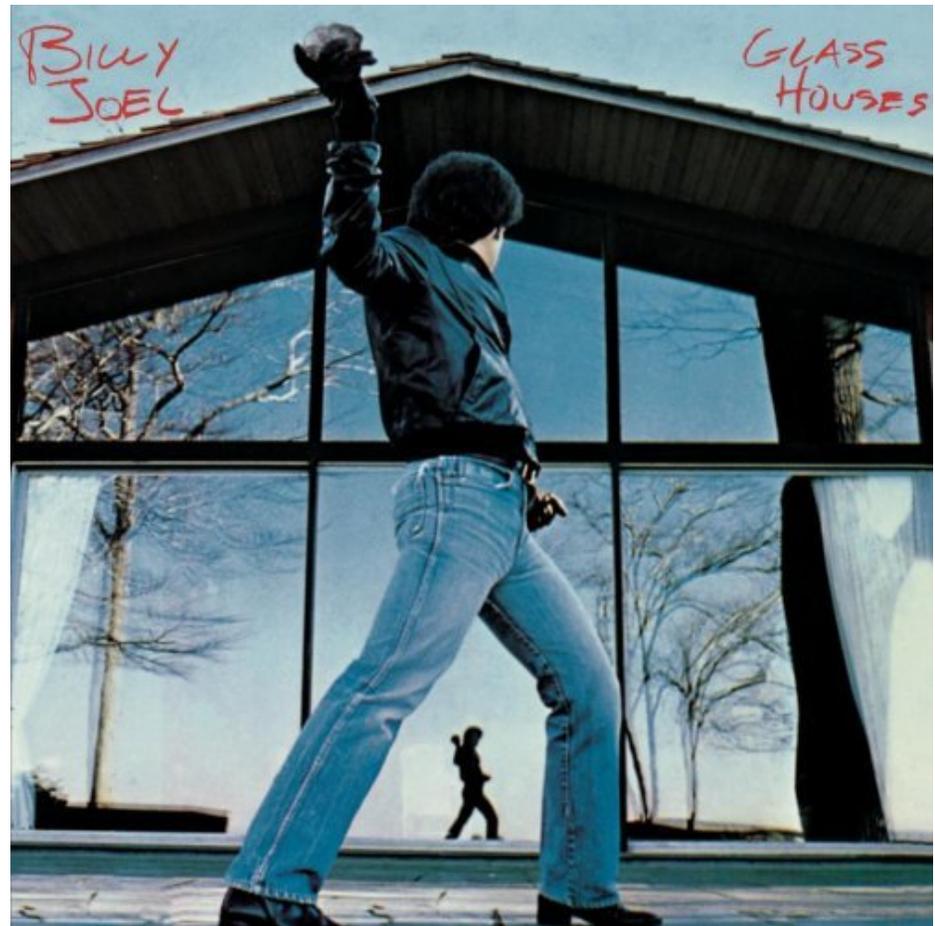
- Missouri State Highway Patrol
- State Emergency Management Agency

- NERC/Regional Entity

- Industry Groups

Those in glass houses ...

Missouri PSC
took the opportunity
to look internally
at our cyber security
procedures

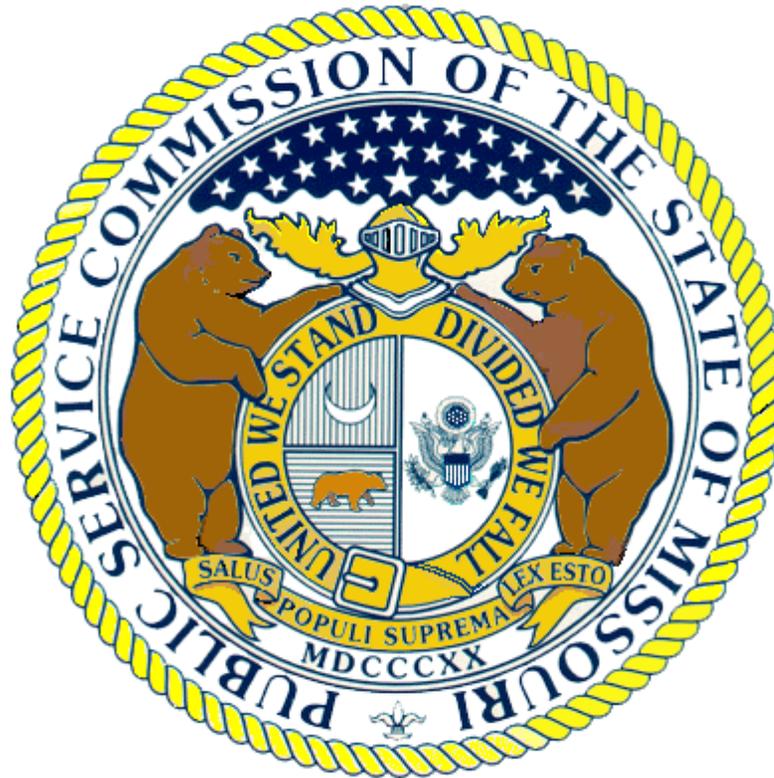




PSC Internal Assessment

- Make sure MoPSC aligned with National Institute of Standards and Technology (NIST) and Certification for Information System Security Professional (CISSP)
 - Information Security and Risk Management
 - Access Control
 - Applications Security
 - Business Continuity & Disaster Recovery Planning
 - Cryptography
 - Legal, Regulations, Compliance and Investigation
 - Operations Security
 - Physical (Environmental) Security
 - Security Architecture & Design
 - Telecommunications & Network Security

Questions?



Thank You