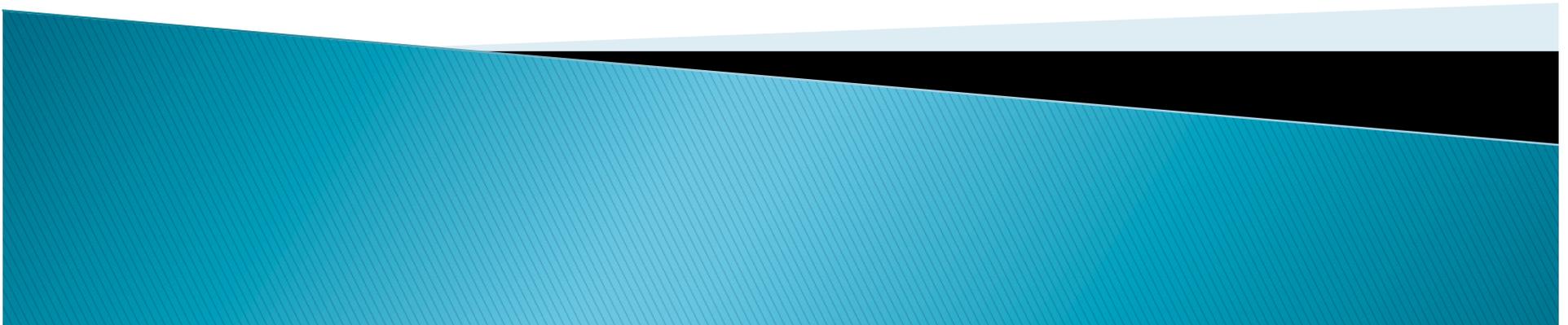


# Security in the National Grid

**NASA Goddard Space Flight Center  
IS&T Colloquium  
10 Oct 2012**

[grcotter@comcast.net](mailto:grcotter@comcast.net)



# Disclaimer

I take complete responsibility for this study. The data is totally from the public domain; the interpretations and judgments are mine. There has been no endorsement by any organization and none is implied.

George R. Cotter



# Motivation for this Study

- ▶ Enormous National, Industrial, Societal Dependencies
- ▶ Prime Target in Cyber Operations vs Intelligence Operations
- ▶ Much More Important than the DIB
- ▶ Curiosity–
  - What are the Security, Technical Challenges?
  - Can the National Grid be Defended?
  - What are Implications for Nuclear Facilities?
  - Is the Industry up to the Challenges?



# What This Study is About

- ▶ Industry and Federal Roles – Structures for Security of the Grid
- ▶ The Evolving Grid Cybersecurity Strategy
- ▶ Legal and Regulatory Issues
- ▶ Vulnerabilities of the Grid
- ▶ Major Threats – An Assessment
- ▶ Prospects for Change
  - Industry–Federal Roles
  - Legislation Picture
  - Structural, Competitive, Technical Complexity



# Background

- ▶ PDD-63 ('99) & NSCD-54/NHSD-23 ('06/'07)  
Critical Infrastructure Protection
  - ▶ Critical National Cybersecurity Infrastructure  
(CNCI) Program ('07 ->fy09)
  - ▶ Energy Designated a High Priority “CIP” Issue
  - ▶ Concerns – Bulk Energy Systems, Nuclear  
Facilities, Transmission Systems, Networks
  - ▶ Industry –Focus on Reliability, not Security
  - ▶ Federal Game Plan – “Rely on the Industry”
  - ▶ 13 years After PDD-63, Little Real Progress
- 

# This is a Huge Infrastructure!

- ▶ 1900+ Utilities, 5500 Generating Facilities
- ▶ 4 Major Continental Interconnections
- ▶ Over 1 Million Megawatts Generation Capacity
- ▶ Over 211,000 Miles of High Voltage Xmsn Lines, Increasingly Cyber Switchable
- ▶ Serving Needs of 340 Million People
- ▶ A Continental Infrastructure is Still Evolving
- ▶ Interoperability & Reliability Key Collaboration Drivers
- ▶ Operational Integration was Likely Possible Only with Substantial Deregulation



# North American Electric Reliability Corporation – 1968

- ▶ NERC – Voluntary Non-profit Corporation
  - Reliability and Standards Organization
  - Interconnectivity was a Key Objective
- ▶ ERO Charter – Federal Energy Regulatory Commission – 2003 Blackout, 2005 FPA
  - Reliability Standards made Mandatory
  - Cybersecurity Standards are an “Overlay”
- ▶ Significant Company, Regional Independence
- ▶ FERC, NERC, NRC – Legal, Regulatory Issues

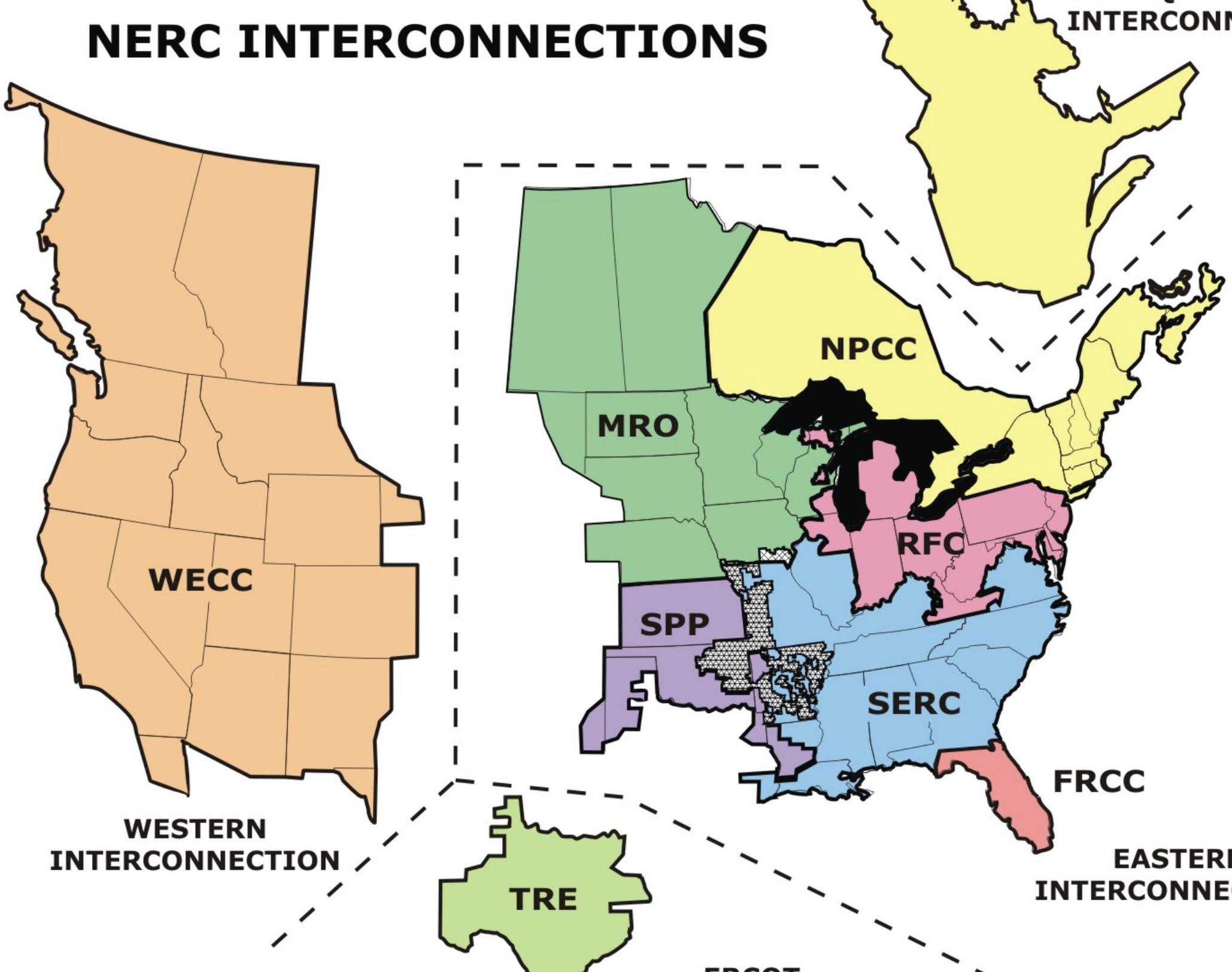


# Complications of Note

- ▶ EROs have no Legal Authority for Distribution Facilities (Transmission System Feeds)
- ▶ NERC's Actions, Other than Standards, are not Legally Enforceable
- ▶ FERC Cannot "Develop" Standards, Must Task ERO, FERC "Approves" Standards
- ▶ Hawaii, Alaska, Major Urban Areas (e.g., NYC) Not Covered (Not "Bulk Energy System")
- ▶ NERC and Industry Oppose Most Legislation—"Status Quo"; Hence so Does US Chamber of Congress



# NERC INTERCONNECTIONS

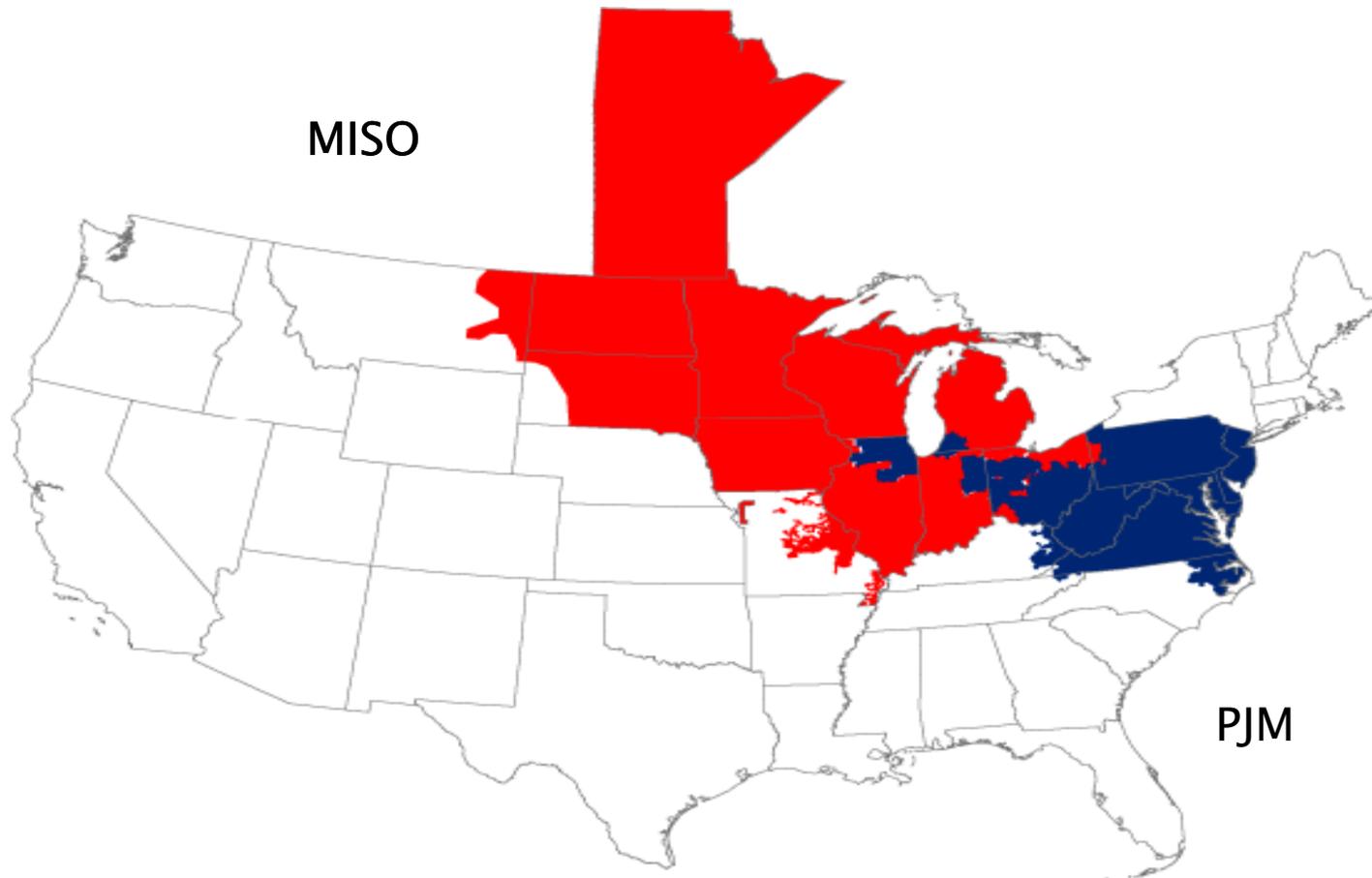


# NERC Registered Entities

- ▶ NERC
- ▶ Regional Entity
- ▶ Reliability Coordinator
- ▶ Balancing Authority
- ▶ Interchange Authority
- ▶ Distribution Authority
- ▶ Planning Authority
- ▶ Purchaser–Sell Authority
- ▶ Reserve Sharing Authority
- ▶ Transmission Service Provider
- ▶ Transmission Owner
- ▶ Transmission Operator
- ▶ Transmission Planner
- ▶ Generator Operator
- ▶ Generator Owner
- ▶ Load Serving Entity
- ▶ Resource Planner

Any Utility Performing These Functions is Considered by NERC to be Bound by the Critical Cybersecurity Standards

# Growth of Wholesale Markets



# ES Information & Analysis Center

- ▶ PDD-63 => 16 ISACs Currently in Existence
- ▶ Sharing of Information on Threats, Incidents
- ▶ Operational Roles Unclear but Vary
- ▶ ES ISAC – Somewhat Broader Mission
  - Compliance “Enforcement”
  - Violation Risk Factors, Violation Severity Levels
  - Annual Audit Report to FERC
  - Situational Bridge Between Feds and Industry
- ▶ Essentially, the Operational Arm for NERC



# NERC Cybersecurity Strategy

- ▶ Risk-Based Security Policy for Cyber Assets
- ▶ Standards-based Compliance, **However.....**
  - Each Owner Decides Risks and Exposure
  - Determines Policy, Systems, Response
  - Based on Asset Ownership, Utility Architecture
  - **Focus is Facility Protection, not the Grid !**
- ▶ Anonymous Incident Reporting, 1-48 Hours
- ▶ “Resiliency” is NERC’s Objective for Security
- ▶ FERC is Very Critical of CIP Standards Process
- ▶ But Has Limited Authority to Direct Change

# NERC CIP Standards

<b><i>CIP-001</i></b>	<b><i>Sabotage Reporting</i></b>
<b><i>CIP-002</i></b>	<b><i>Critical Cyber Asset Identification</i></b>
<b><i>CIP-003</i></b>	<b><i>Security Management Controls</i></b>
<b><i>CIP-004</i></b>	<b><i>Personnel &amp; Training</i></b>
<b><i>CIP-005</i></b>	<b><i>Electronic Security Perimeter</i></b>
<b><i>CIP-006</i></b>	<b><i>Physical Security of Critical Cyber Assets</i></b>
<b><i>CIP-007</i></b>	<b><i>Systems Security Management</i></b>
<b><i>CIP-008</i></b>	<b><i>Incident Reporting &amp; Response Planning</i></b>
<b><i>CIP-009</i></b>	<b><i>Recovery Plans for Critical Cyber Assets</i></b>



# FERC, NERC and CIP-002 (Assets)

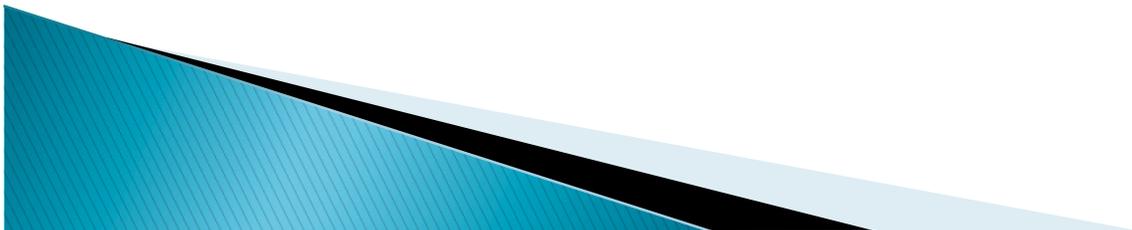
- ▶ FERC Order 706 Jan 08 Ok'd NERC Plan (Interim)
- ▶ Clearly Stated That Standards Were Minimum
- ▶ Directed Review:
  - Critical Asset Assessment Methodology
  - Scope of Critical Assets (Data, Control Systems)
  - Management Approval Process
  - External Review Process
  - Interdependencies
- ▶ Asset Issues Unresolved – Years of Debate
- ▶ Led to CIP v4 Brightline Proposal –> v5 to Follow
- ▶ NERC Approved v4 but Directed NERC to Resolve all Remaining Order 706 Issues with v5



# Critical Assets – CIP 002-4

## “Bright Line” Revision

- ▶ “Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection”
- ▶ Transmission Facilities operated at 500 kV or higher, or at 300 kV with 3 or More Connections....
- ▶ Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

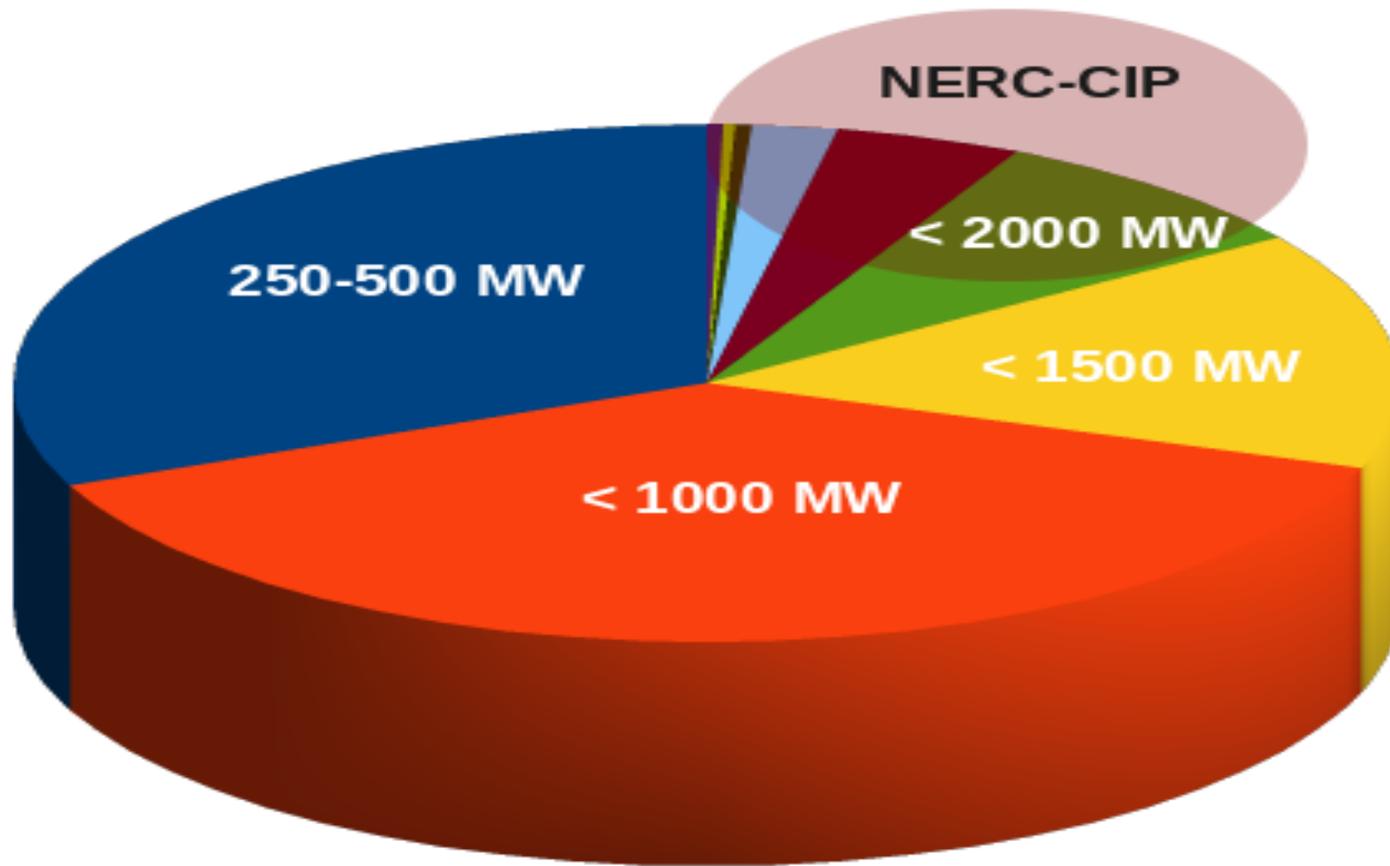


# Exempt from CIP 002-4 Standards

- ▶ Cyber Assets associated with communication networks and data communication links between discrete (i.e., Local) Electronic Security Perimeters.
- ▶ Cyber Assets that do not use a routable protocol to communicate outside the Electronic Security Perimeter or within a control center or are not dial-up accessible (i.e., legacy communications systems).



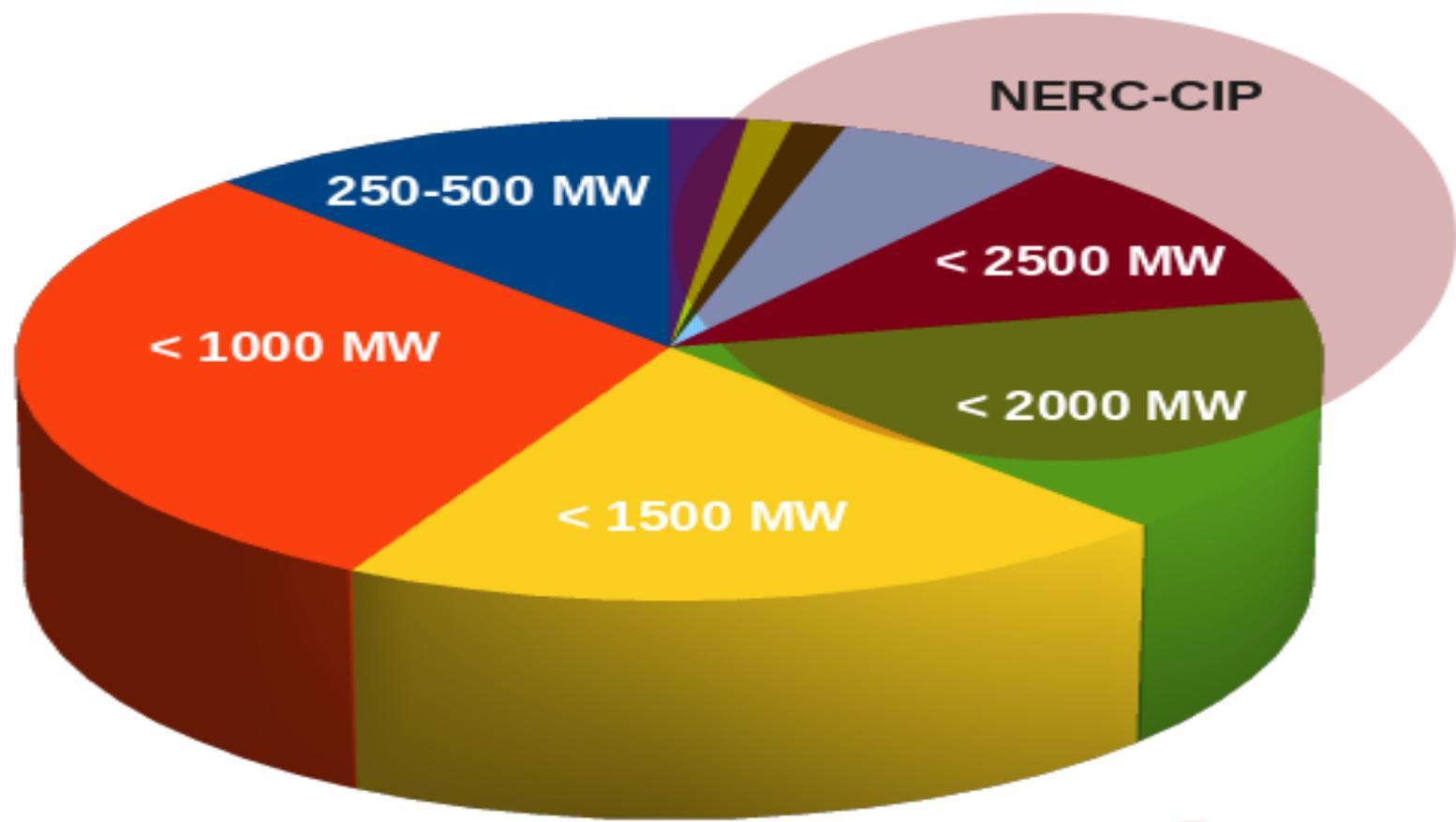
# Less Than 15% of Plants Within CIP



Number of Plants



# Less than 30% Grid Capacity in CIP



Aggregate Capacity



# Resiliency – How Effective? SW U.S. Cold Spell Feb 2011

- ▶ Three NERC Regions: ERCOT, WECC, SPP
- ▶ Shortage Forecasted but Reserves Planned
- ▶ But 29,000 MW Capacity
  - Committed to “Day Ahead” Market
  - “Tripped”, “Derated” or “Failed to Start”
  - Interdependencies; Natural Gas and Electricity
- ▶ Worse Day: 4000 MW Load Shed Causing Rolling Blackouts
- ▶ 3.2M Customers Affected Across Three “Reliability Regions”



# FERC/NERC and NRC/NEI

- ▶ FERC – NRC MOAs for Shared Cybersecurity
- ▶ Split Responsibility for Nuclear Facilities
- ▶ Covers Protection of Safeguard Information
- ▶ NERC: Need Considerable Resources for NRC CIP Compliance Audit
- ▶ GAO Audit Found Serious Flaws in TVA Nuclear Facility Control Systems
- ▶ Nuclear Energy Institute (NEI) Opposed Major Security Initiatives re. Fukushima



# Quote From NEI Website “FAQ”

- ▶ Myth: Nuclear Plants Vulnerable to Attack
- ▶ Facts: –
  - Never a Cyber Attack on NRC Facility (**Vulnerable?**)
  - No Two-way Data Flows (**Not Essential – Stuxnet**)
  - Control Systems not Connected to Internet (**TVA Audit by GAO Proves Otherwise**)
  - Control Computers under Strict Security Controls (**IT Penetrations Bypass Physical Security Controls**)
  - Reactor Controls not Affected by *Off-Site Power Losses* (**Fukushima? New NRC Study on Backup Systems**)



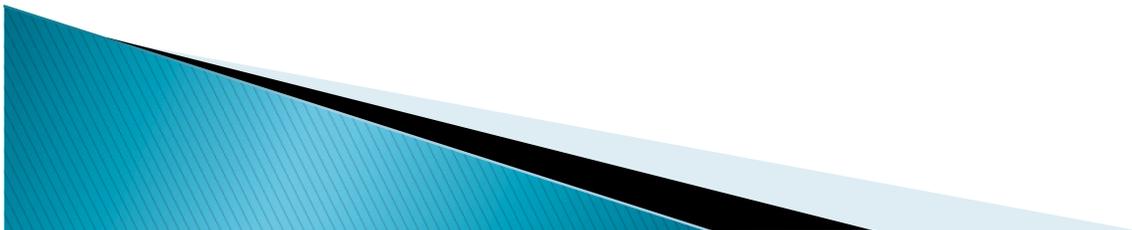
# Strengthened NRC Cybersecurity Regulations

- ▶ Linked to Safety Rules, 1948 Law, Everything in Between!
- ▶ NIST Standards, SP 800–53, SP 800–82
- ▶ 10 CFR 73.54 Protection of Digital Computers and Communications Systems & Networks
- ▶ Regulatory Guide 1.152 Criteria for Use of Computers in Safety Systems of Nuclear Plants
- ▶ Regulatory Guide 5–71 Cybersecurity Programs for Nuclear Facilities

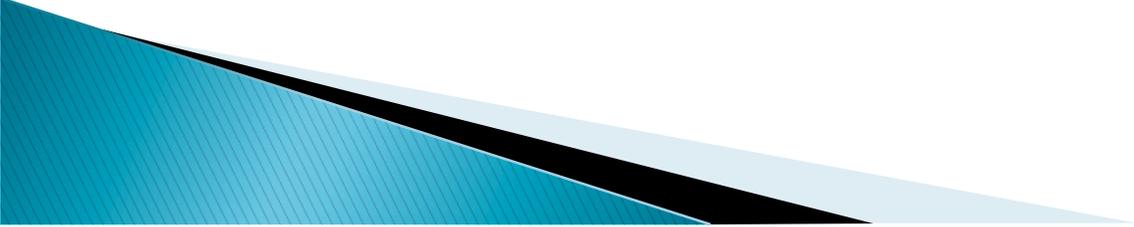


## Post-Fukushima RG 5-71 Status

- ▶ Short Deadline for Submission: All Submitted
- ▶ Probably all SGI: No Public Disclosures
  - Nuclear Sensitivities
  - Intellectual Property
- ▶ Critical Part of Safety Inspections-3 Year
- ▶ Competent NRC Resident Oversight
- ▶ But Sites Share National Grid Vulnerabilities
  - Restoration of External AC Power
  - Network, Control Systems
  - And What Else ? (GAO TVA Audit)
- ▶ Probes from Abroad a Virtual Certainty



# Grid Vulnerability Concerns

- ▶ Fragmentation – Across the Board
    - Site Independence
    - Application of Standards
    - Exclusions All “Distribution” Facilities; Urban, Hawaii, Alaska
    - Grid Defenses, Technology, Networks, BES and Controls
    - 104 Nuclear Generation Facilities + Plans for 29 more.
  - ▶ Situational Awareness
    - Dissemination to Participants, Security Issues
    - Information Flow to Federal Government; Anonymity
  - ▶ Control Systems–DCSs, PLCs, SCADA Linkages to Web
  - ▶ Nuclear Facilities–Linkages to Web; Laptops, PDAs
  - ▶ NERCnet–Vulnerabilities, Portals to Control Sys
  - ▶ Reliability Centers–Protection for Recovery
  - ▶ Balancing Authorities–Protection for Critical Nodes
- 

# Potential New Network Vulnerability

- ▶ Frequency Stability (60 Hz) Critical to Balance
- ▶ Provide Stable Frequency Reference to ISO's
- ▶ Techniques: Flywheels, Batteries
- ▶ Both are Computer Controlled
- ▶ Directly Support Demand/Supply Fluctuations
- ▶ A \$485M Industry and Growing!
- ▶ NERCnet is Coordination Resource Within Grid
- ▶ But Freq & Cyber Resources, Control Systems, Transmission Systems are Outside CIP
- ▶ A Key Theoretical Attack Vector for Cyber Attack



## Beacon Power Co. Flywheel Frequency Control; Stephentown NY



**REVVED UP:** A flywheel generator is lowered for high-speed tests.  
PHOTO: BEACON POWER CORP.

# Fukushima – Diet Final Report



- ▶ Government Totally Co-opted by Nuclear Industry
- ▶ Nuclear Explosions, Area Contamination Deemed Related
- ▶ Disorganized, Incompetent Disaster Planning & Recovery

# US Nuclear Site Vulnerabilities

- ▶ 104 U.S. Nuclear Facilities are AC Dependent
- ▶ NRC Study – Tighten Electric Safety Rules
  - New Minimums on Diesel, Battery Backup
  - Questionable Rule on External AC Sourcing
  - 72 Hours Maximum – Restoration Cooling Systems
- ▶ No Control Over NERCnet & Xmsn Systems
- ▶ Attack Vectors on Nuke Sites, Power Systems:
  - DDOS Thru BOTnets
  - STUXNET Clone Against SCADA, DCS, PLC Systems
  - No Significant Defenses Deployed
  - Extent of Penetration is Unknown



# Stuxnet

- ▶ A Siemens' Application Time Bomb
- ▶ Attacks DCS, PLC, SCADA Control Systems
- ▶ Undiscovered for at Least a Year
- ▶ Targeted Specific Features of Nuclear PLCs
- ▶ Exploited Vulnerabilities in Base IT Systems
- ▶ Could Communicate with its Masters
- ▶ Had High Level of Survivability, Replication
- ▶ An Extreme Example of Lethality
- ▶ New Control Vulnerabilities Coming to Light



# Threats to the Grid

- ▶ **Terrorism/International Hacktivist Teams**
  - Energy Infrastructure is a Very High-Value Target
  - Only Open Question-Cyber Attack Capabilities
  - Grid is Potential High-Value Hostage
- ▶ **Nation/State**
  - Ideal Asymmetric Target
  - Significant Military Value
  - “Must” Target for a Zero-Day Attack Planning
- ▶ **Response; Rapid Recovery Highly Uncertain**
- ▶ **OBTW – EMP, Solar Flares a Major Concern**



# Legislative Efforts

- ▶ **Senate DHS Committee Bill**
  - Immunity on Info Sharing
  - DHS Help on CIP Plans
  - Entity's Own Framework
  - Third Party Commercial Audit
  - DHS (with NIST) Could Modify Framework
- ▶ **HPSCI Info Sharing Bipartisan Bill**
- ▶ **Senate Armed Services Committee Bill**
  - ▶ Neutered DHS
  - ▶ Empowered NSA



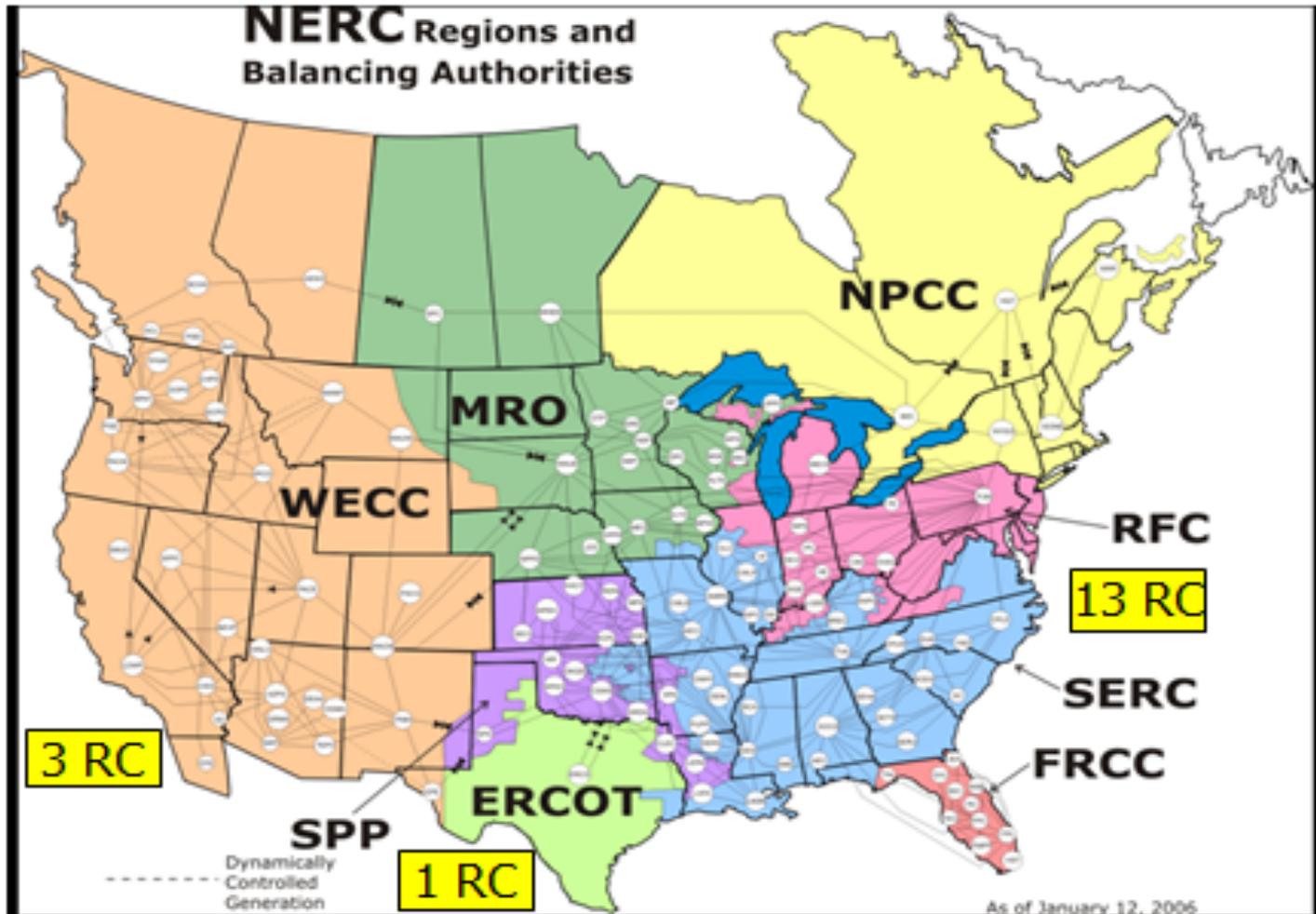
# Reliability Regions–A Way Ahead

- ▶ *Minimum security of the BES will remain elusive until NERC, the Industry and Federal Authorities address the **topology** of Grid communications and networks, aggressively **separate industrial control functions** from business and marketing functions, **rank nodes** in terms of criticality, and establish **an integrated efficient security structure**, with deep **protection at all external connections**.*



Thr Network Challenge

The Network Complexity



*3 NERC Regional Entities (Western, Eastern, Texas)  
 8 Balancing Authorities (NPCC, MRO, etc)  
 1, 3, and 13 Reliability Coordinators*

# Additional “Must Do’s”

- ▶ Formalize a National Deterrence Strategy
- ▶ Enact Enabling Legislation
  - Industry–Federal Roles & Responsibilities
  - Liability Protection
- ▶ Create a 24/7 Industry–wide Watch Operation
  - Real Time Information Exchange
  - Tied to Active Response Mechanisms (FEMA, DoD)
- ▶ Create a Viable Security Plan for the Grid
- ▶ Reconcile FERC–NRC Dichotomy
- ▶ Cybersecurity for Major Urban Areas. Hawaii
- ▶ Engage Industry Throughout



# Any Light at the End of the Tunnel?

- ▶ DoD “Act of War” Dictum
- ▶ Maturing of DoD Information Operations
- ▶ Technologies (Einstein-3, Cray XMT-2.....)
- ▶ Cybersecurity-Intelligence Linkages
- ▶ HPSCI Bipartisan Cybersecurity Unity
- ▶ Impending Presidential Memorandum
- ▶ Positive NRC Fukushima-Related Actions
- ▶ New FERC Security Organization (Cyber, EMP)



Questions?

Comments?

