Exercise of FERC Authority for Cybersecurity of the North American Electric Grid

Thomas S. Popik
Joseph M. Weiss
George R. Cotter

FERC Docket RM15-14-000

Agenda

- **Overall Concerns with FERC Authority and Grid Security**
- **Thomas Popik: Non-Implementation by NERC and FERC of Cybersecurity Provisions in Section 215 of the Federal Power Act**
- **Joseph Weiss: Industrial Control System Vulnerabilities in Interdependent Infrastructures—Electric Grid and Gas Pipelines**
- **George Cotter: Regulatory Commissions' Roles in Cybersecurity of the North American Electric Grid**
- **Conclusions and Recommendations**

Concerns with Use of FERC Authority

- **FERC Given Limited Authority in Section 215: "A Bad Law"**
- **NERC Standards Give False Assurance of Security to Public**
- **In FERC Order 822, NERC Once Again Allowed to Stonewall**
  - **Federal Power Act Mandates for Reliability Extend Beyond §215 Cybersecurity**
  - **Broader FERC Duties and Specific §215 Mandates Remain Unexercised**
  - **Supply Chain Threats Deferred Until Technical Conference (and Longer?)**
- **FERC Has "Partnership" and "Mutual Trust" with NERC?**
- **No, NERC Is Playing the Commission: "Captive Regulator"**
- **FERC Commissioners Work for the Public, Not Industry**
- **Looming Security Issues Likely To Cause Devastating Blackouts**
  - **Ukraine Grid Cyber-Attacks Demonstrate U.S. Vulnerabilities**
  - **PG&E Westpark Intrusion & Continuing Attacks on Bay Area IP Networks**
  - **Electromagnetic Pulse Probes of Critical Grid Facilities?**
  - **Abysmal Progress on Real Protection—Not Just Paper Standards—for Geomagnetic Disturbance, Physical Security, Cybersecurity**
- **What Will Be the FERC Docket Record When Blackouts Hit?**

FERC Under-Utilizes Broad Authority for Reliable Operation of the Bulk Power System and Neglects Specific Mandates To Protect "Communication Networks" per Section 215 of the Federal Power Act

Thomas S. Popik

Federal Law vs. NERC

Case Example

Provisions of Section 215

- **"The term 'reliability standard' means a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection…"**
- **"The term 'reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."**
- **"The term 'cybersecurity incident' means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."**

CIP-005-5—Cyber Security – Electronic Security Perimeter(s)

- **"3. Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."**
- **"4.2.3 Exemptions: The following are exempt from Standard CIP-005-5:**
  - **4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters."**

No "Reasoned Path" Between Critical Substation Protection in NERC Standard CIP-014-1—Physical Security and FERC Order 822 on Secure Communications

"CIP-014-1—Physical Security" for Transmission Substations

3. Purpose: To identify and protect transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

Section 4 Applicability

The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or cascading within an Interconnection.

FERC Order 822 on Secure Communications for Transmission Substations

"With regard to [Resilient Societies'] argument that the Commission should do more to promote grid security by mandating secure communications between all facilities of the bulk electric system, such as substations, the record in the immediate proceeding does not support such a broad requirement at this time. However, if in the future it becomes evident that such action is warranted, the Commission may revisit this issue."

Control System Cyber-Threats in Interdependent Infrastructures— Electric Grid, Natural Gas Pipelines, Water Transmission and Distribution

Joseph M. Weiss

Cyber-Threats for Grid Control Systems

- **Grid cyber threats are real**
  - **250 North American electric grid cyber incidents**
  - **5 major North American cyber-related outages**
  - **Most not identified as cyber by utilities or NERC**
  - **Many incidents outside North America (e.g., Ukrainian attacks)**
- **Size vs. connectivity**
  - **Loss of many "small" sites same as loss of "big" site**
  - **Small site can cause cyber compromise of big site (Section 215)**
- **Aurora Impacts**
  - **DHS declassified Aurora – "bad guys know"**
  - **Aurora causes long-term damage – months to years**
  - **Ukrainian attack is step 1 of 2-step Aurora process**
  - **Can happen here**
- **Inadequacy of NERC CIP**
  - **National Guard hacked CIP-compliant utility in less than 30 minutes with no indication by monitoring system**

Utilities Not Meeting Existing CIP Reporting Requirements

NERC Standard CIP-008-5 — Cyber Security — Incident Reporting and Response Planning

Summary: CIP-008-5 will mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Proposed Requirement R1 now includes an obligation to report Cyber Security Incidents within 1 hour of recognition. Requirement R2 adds testing requirements to verify response plan effectiveness and consistent application in responding to a Cyber Security Incident.

A "Process", not a "Standard"!

NIST Definition of a Cyber Incident

"Cyber Incident - An occurrence that actually or potentially jeopardizes the Confidentiality, Integrity, or Availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional."—(FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.)

However, utilities still won't acknowledge cyber incidents in their quarterly "Lessons Learned" reports.

Aurora Vulnerability

Programmable Digital Relay

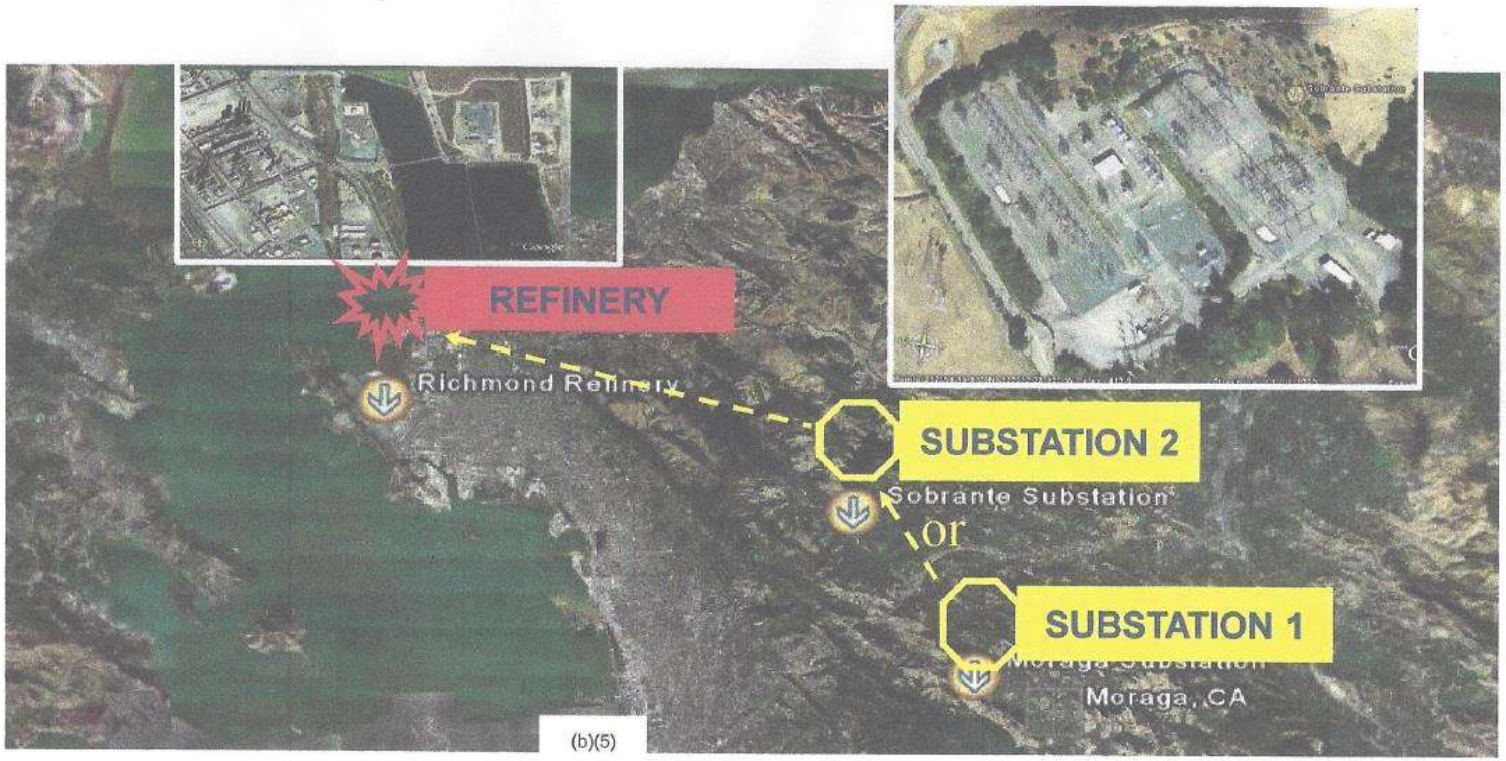
- The Elements Necessary for an Attack
  - Programmable Digital Relay
    - Or other device that controls the breaker
  - High-Speed Breakers
  - Access (front panel, modem, Internet, wireless, or SCADA)
  - Laptop/Desktop Computer
- Knowledge Necessary:
  - Power Engineering (attack planning and device setting skills)
  - Hacking Skills (exploit the relay and conduct the attack)
- Time Required to Conduct the Attack (after gaining access):
  - Less than one minute
  - No additional software is introduced
  - Uses the internal settings of the imbedded relay software

Homeland Security

UNCLASSIFIED/FOR OFFICIAL USE ONLY

8

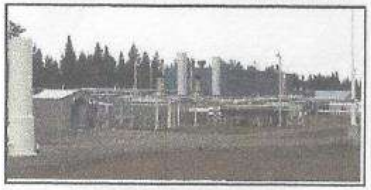
Aurora Vulnerability

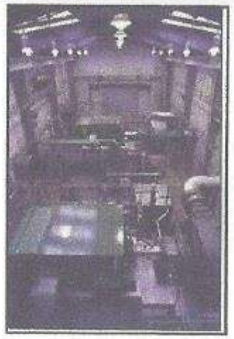


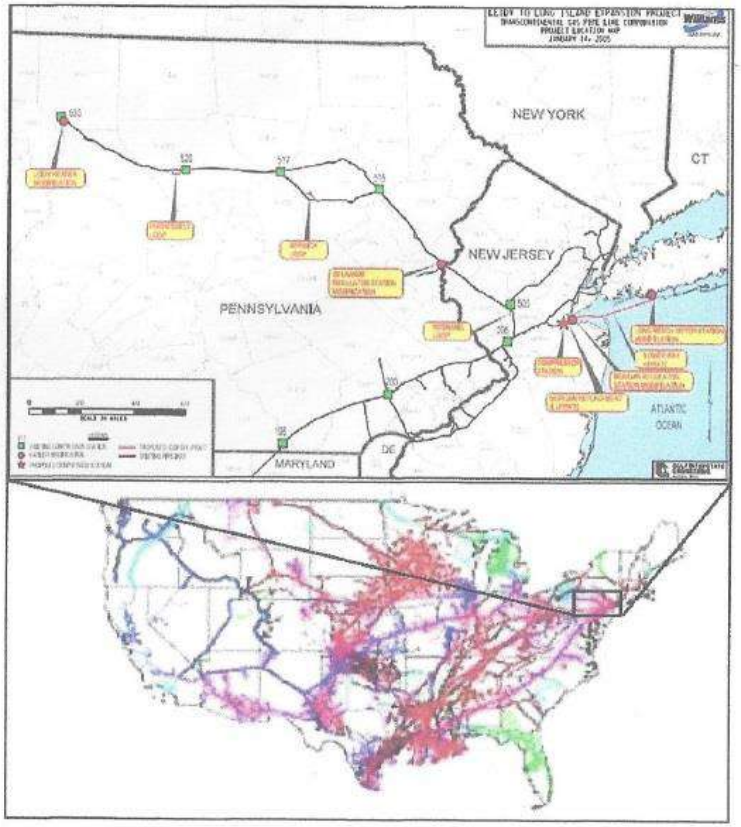
Homeland Security

Aurora Vulnerability Example

Gas Line Compressor Stations Use Large AC Induction Motors Near Cities



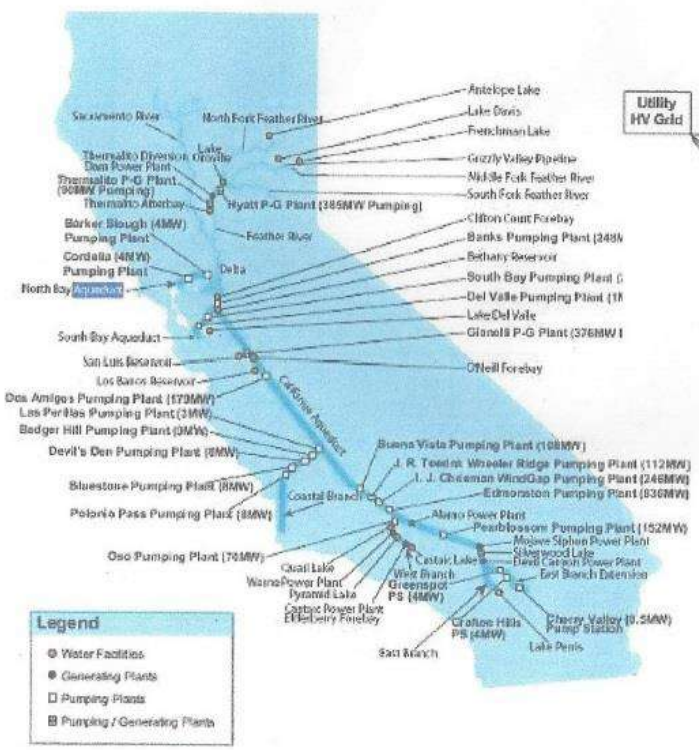


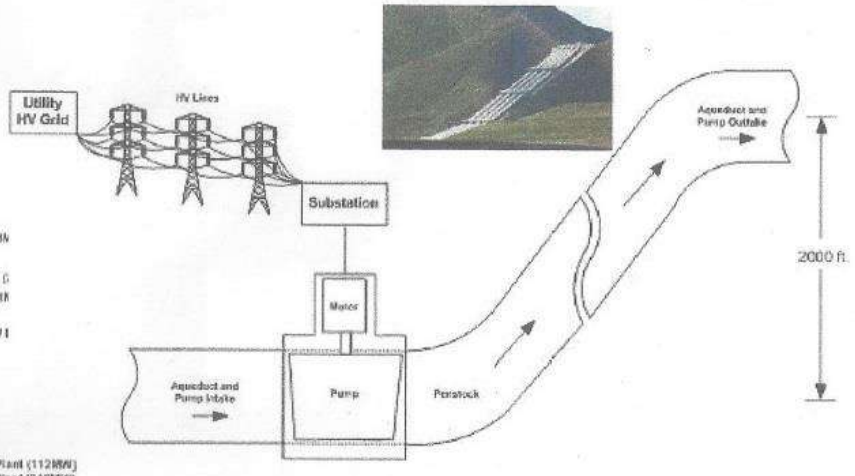


Homeland Security

Aurora Vulnerability Example

Water Pumping Plants Use Large Motors in Series





Homeland Security

~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~

Regulatory Commissions' Roles in Cybersecurity of the North American Electric Grid

George R. Cotter

Cyber Threats

- **The North American Grid – Very High Impact Target for Adversary Nation/States**
  - **Doing Reconnaissance in Depth; Targeting Vulnerabilities**
  - **Attack Development: Prudent Preparation for Crises; Goal is Grid Takeover**
  - **Russia: BlackEnergy Supply Chain Attacks on US Grid, Ukrainian Grid Attack**
  - **Foreign Policy: An Intimidating Element in Russia's International Agenda**
  - **China: Axion Threat Organization. Most Stealthy. Reportedly in US Grid**
  - **NERC/Industry: Playing Russian Roulette with Putin; Federal Agencies are Bystanders**
- **Cyber Terrorists – Only a Question of "When", Not "If".**
  - **Destructive Cyber Tools - Readily Available on Internet; Goal is Major Loss of Life**
  - **Advantage Terrorists: Significant Hardening of Grid Defenses is Only Real Option**
  - **Can US/Allied Programs Delay the Inevitable? And for How Long?**
- **Hactivists – It Only Takes a "Cause"; Note Silicon Valley Cyber Incidents**
- **The Real Targets – Critical High Impact National Security, Industrial, Social and Urban Infrastructures**

Russian Cyber-Attack on the Ukrainian National Grid

- **December 23rd-Sophisticated Attack in 2 Regions, Probably 6 Others**
  - **Intruded into SCADA Systems, Damaged SCADA System Hosts and Workstations**
  - **Seized Control at Human Machine Interface (HMI) Level, Blindsided System Dispatchers**
  - **Opened Circuit Breakers, Cut Power to 80,000 Users, HMI was Undoubtedly Compromised (Precursor to Aurora?)**
  - **Initiated DDOS Attack on Call Centers to Prevent Users from Reporting Outages**
  - **Activated KillDisk, Erasing Presence, Denying Forensics**
  - **Multiple Attack Vectors But Much More to be Learned**
- **Earlier Intrusions March-July 2015 Evidence of Planning, Penetration**
- **Sandworm Team, BlackEnergy 2, 3 Techniques Are of Russian Origin**
- **Directly Related to 2014 BlackEnergy Supply Chain Intrusions in U.S.**
- **And Yet ES-ISAC Stated:**

"There is no credible evidence that the incident could affect North American grid operations and no plans to modify existing regulations or guidance based on this incident."

Vulnerabilities

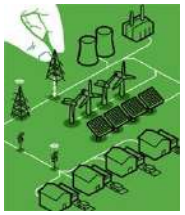
After 9 Years of CIP Standards, all Major Vulnerabilities Still Exist

- **Communications and Networks Largely Insecure**
- **Automation Systems (ICS et al) Largely Insecure**
- **Extensive Use of Internet, Totally Insecure**
- **Little or No Operational Cybersecurity Monitoring Effort**
- **Extensive Growth of Supply Chain Penetrations; No Effective Defense**
- **No Cyber Modeling and Simulation Studies, Red Team Efforts on Vulnerabilities**
- **No Effective Program for Grid-wide Cybersecurity Situational Awareness**
- **No Effective Regulatory Agreement on Power Assurance to Nuclear Sites**
- **Industry Remains on CIP V3; Standards Practically Worthless**
- **High, Medium, Low Cyber Asset Segmentation Ignores Attack Strategies**
- **CIP V5/6 Standards Mostly Process; Lack Technical Metrics**
- **Compliance Self-Regulated; No Structured Oversight, New "Exemptions"**

FERC's Cybersecurity Responsibilities*

- **For Past 15 Years; A Major Regulatory Challenge for FERC and NRC**
- **"In the Public's Interest" Should Mean "In the Overall Interests of the Nation"**
- **It's A Critical Element of FERC's Task–Ensuring and Monitoring Grid Reliability**
- **FERC Authority Should Be Exercised Within Larger Context of the Nation's Survivability Under Cyber-Attack**
  - **Build Competent Cybersecurity Support – Internally, and from Industry**
  - **Develop Active Partnerships With NRC, DHS, DoE, DoD, and Intelligence Community**
  - **Demand Federal Effort to Extract Foreign Implants from All Grid Systems**
  - **Initiate Major Federal Certification Program for Security of Grid Supply Chains**
  - **Develop Operational CIP Compliance Testing, Including Red Team Attacks**
  - **Ultimately, Overhaul CIP Standards to More Enforceable Set**
  - **Support Development of National Guard Role in "Active Defense" of Grid**
  - **Bring "Distribution" Assets into a North American Grid Security Program**
  - **Implement an Operational Cybersecurity Monitoring Program**
- **Do Not Avoid, But Seek Legislative Action if FERC Authorities Are in Doubt**

As Outlined in Our Joint Filing on Docket RM14-15-000



Conclusions and Recommendations

- **Complexity of NERC CIP Standards Gives <u>False Assurance</u>**
- **NERC and Its Standard Drafting Teams Are Stonewalling FERC**
  - **Example: Protection from Intrusion/Manipulation of Data Flows Between Substations and Control Centers**
  - **Example: Torturous Foot Dragging on Low-Impact Cyber Asset Standards**
- **If FERC Does Not Assert Regulatory Leadership, and a Cyber-Attack Results in a Major North American Blackout, FERC, *<u>not</u>* NERC, Will Take the Full Hit**
- **FERC Should Move Quickly To Fully Implement Section 215**
  - **Full Regulatory Control Over a Comprehensive Grid Cybersecurity Program**
  - **Assume a Leadership Role Across Federal Agencies**
- **Where FERC Authority is Inadequate:**
  - **Request Legal Remedies for Section 215**
  - **Executive Branch Actions—White House and Federal Agencies**