Security in the North American Grid

A Brief Update

CSLAC Random Access
October 2020

Hidden CyberSecurity Vulnerabilities

Threats to Critical Infrastructures Including Election Systems have not Diminished. Regrettably, the Industry & its Regulators are Complicit in the Threat.

grcotter@comcast.net

Not a New Random Access Talk…….

CSLAC 2018 - The Rest of the Dragonfly Story

CSLAC 2019 - Vulnerabilities vs. Threats – 2016 Election

CSLAC 2020 – "Hidden" Cybersecurity Vulnerabilities

Regulatory Background

GRID is Regulated in 3 Parts – Nuclear/NRC, Transmission/FERC, Distribution (States/Local)

Hugely Fragmented, ISOs, RTOs, Coops, Conglomerates, Mom & Pops, etc. But it Functions

4000+ Firms in "Bulk Electric Systems", 1500 Registered Entities, under NERC (the ERO) and FERC

NERC Historically Managed "Self Regulated" Bulk – Reliability (Engineering) Standards

In 2005, Congress Gave Responsibility for Bulk CyberSecurity (CIP) Standards to NERC i.e., ERO

CIP Standards Implemented in 2008, added to "Relibility Standards" but as Separate Category

First Effective Implementation Delayed until 2016

CIP covers Cyber Assets Categorized as Critical to BES Transmission/Generation "Resiliency".

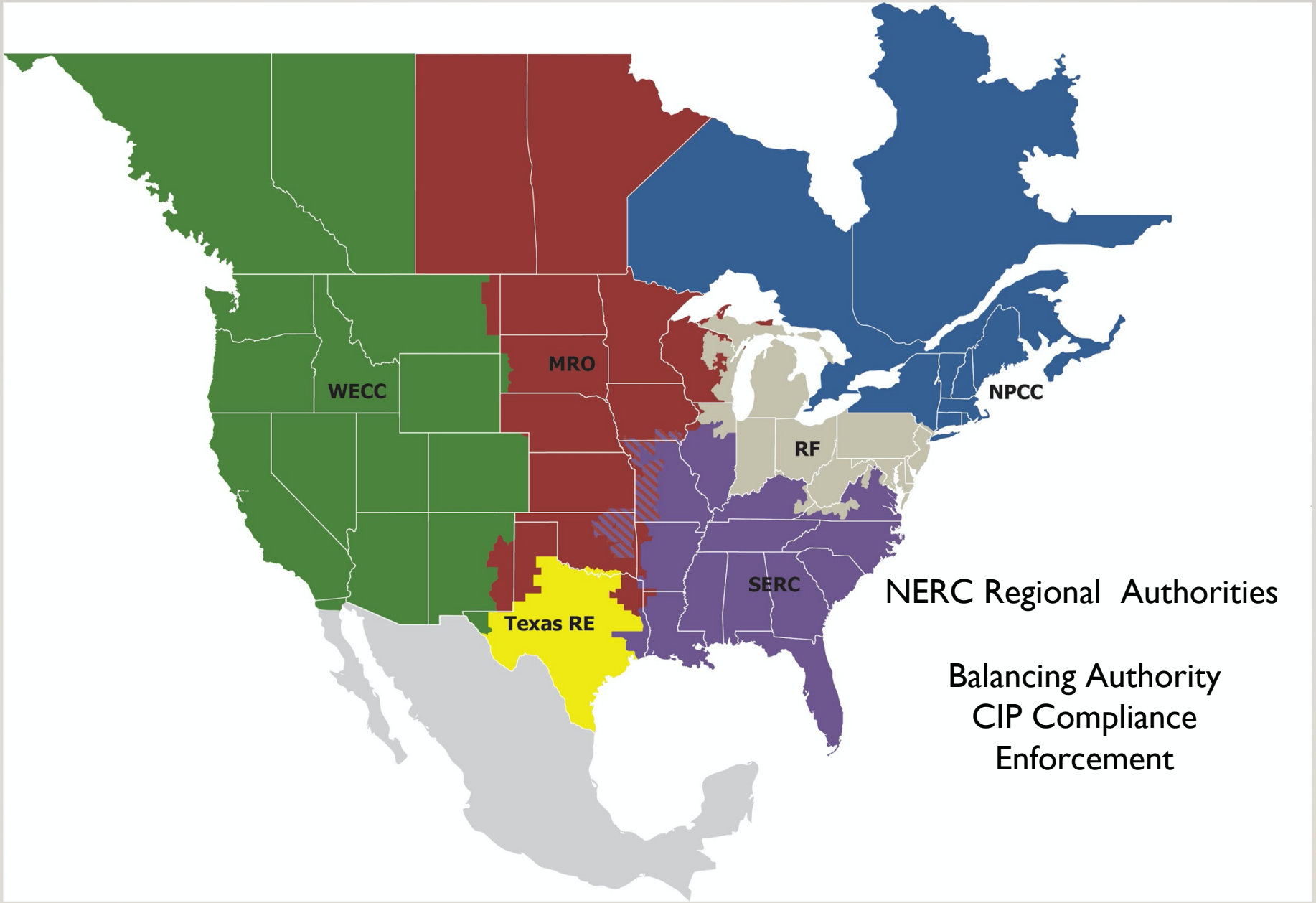
Several Exclusions Including "Communications & Networks", a Significant Exception!

FERC has Failed to Order CIP Standards for Major Industry Developments

Green Energy (Solar, Wind, Nuclear Generation)

Modernization e.g, Synchrophasors

Federal Corporations, Nuclear Sites Exempt



NERC Regional Authorities

Balancing Authority
CIP Compliance
Enforcement

CIP STANDARDS

CIP- 002 Asset Categorization,

CIP-003 Security Management Controls CIP-004 Personnel & Training

CIP-005 Electronic Security Perimeters CIP-006 Physical Security, BES Cyber Systems

CIP-007 Systems Security Management CIP-008 Incident Reporting, Response Planning

CIP-009 Recovery Plans, Cyber Systems CIP-010 Configuration Change Management

CIP-011 Information Protection

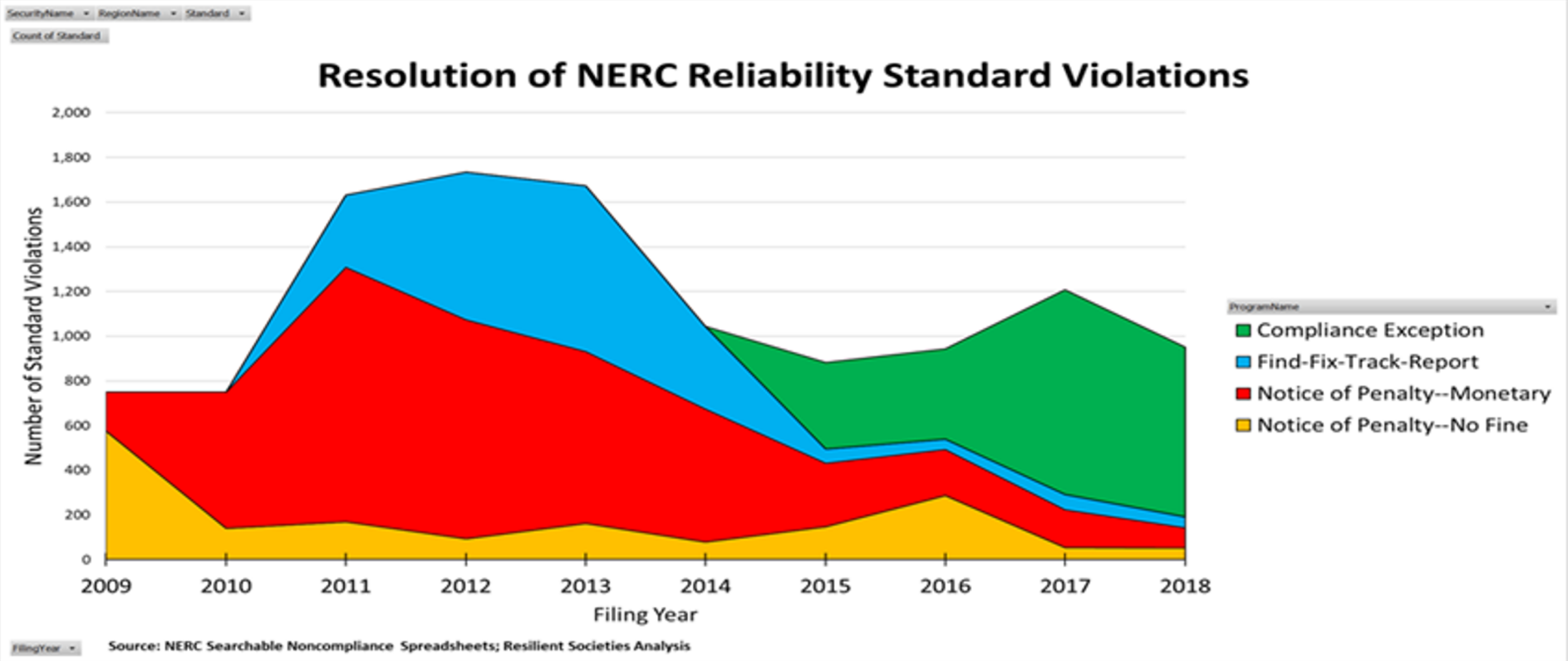
Bottom Line: Physical Facilities, Security Management, Access Controls, Configurations, Personnel,

Utility Organizations but not Cyber Assets Used in Operational Power Flows!!!!!!

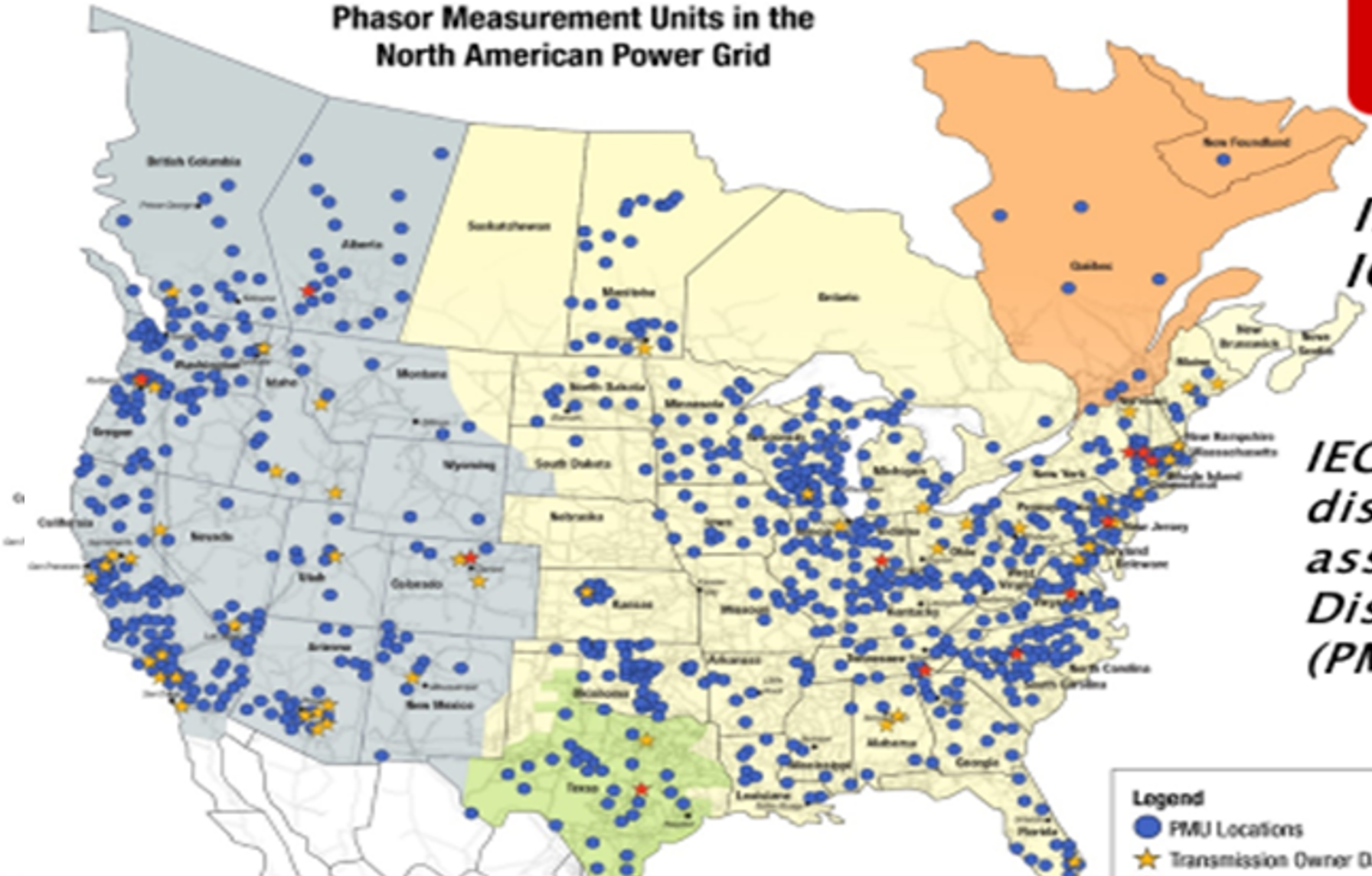
Took until 2016 to Fully Implement this Set, Subject to CIP Compliance Assessments

- FERC and Industry Resisted Identifying Specific Cyber Assets Covered by CIP Standards
- Major Omissions, Gaps e.g. Supply Chains, Control Centers, Synchrophasor Systems
- NERC Fought Public Release of Compliance Reviews
- But NERC Weakened Audit Rqmts & Suppressed Utility IDs and Violations as CEII

CIP COMPLIANCE HISTORY



Synchrophasor Sites In The North American Electric Grid



Russia FSB & MOD GRU

Industroyer ICS Malware

IEC61850-based attack can disable targeted ICS cyber assets at Transmission and Distribution Synchrophasor (PMU) equipped sites

CONNECTING THE DOTS

- Bulk Electric Systems Involve Two Sets of Standards, Engineering and Cybersecurity (CIP)
- Engineering Standards are Critical to Massive Interconnection of Thousands of Utilities
  - How do Non-CIP Engingeering Standards Interface with CIP Standards? (Nil Evident)
  - Extensive Study of Compliance Audits Reveals CIP is non-Operational, Deliberately
- Otherwise, How Could BES Secure Synchrophasor Power Flows be Massively Connected to non-Secure Distribution Sychrophasor Networks? (Map Shows they Connect!!)
- How do Non-CIP Engineering Standards Audits Address Synchrophasors? (Nil Cited)
- Do CIP Compliance Audits Address Synchrophasor Real Time Power Flows? (Ignored)

CONCLUSION

- 1. CIP Standards Only Protect Utility's Organization, Mgmt, and Support Functions
- 2. Bulk Electric System ***Operations*** (Cyber Assets) are not Subject to CIP Standards
- 3. ***Real-time Operational Power Flows (Cyber Assets)*** Including Synchrophasors are Excluded from all Compliance Audits, CIP and non-CIP
- 4. Therefore, There is Little or No Mandated Cybersecurity Protection for Power Feeds to:
  - Nuclear Generation Sites
  - Critical Infrastructures Including National Security Facilities
  - National Health Systems
  - The 2020 Election Process
- 5. But the ERA 2005 Section 215 ***Mandated*** Cybersecurity Protection for BES ***Operations,*** Intentionally Ignored by NERC and FERC for 15 years.