CYBER REGULATION: RENEWABLE ENERGY SECTOR USA

DeNexus Cyber Thought Leadership Retreat – Bermuda – October 10, 2022

INTRODUCTION

- CEO, Owner, Ampere Industrial Security – serial entrepreneur
- Former utility staff (telecommunications, water & electric)
- Drafter of NERC CIP standards and formal interpretations, Supply Chain Working Group contributor
- First NERC CIP auditor in North America
- Former Manager, CIP Audits and Investigations – WECC Region (NERC)
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Former Director, Former Instructor and President Emeritus
- SANS ISC456 Instructor: Essentials for NERC Critical Infrastructure Protection
- CS2AI Fellow
- US Coordinator, Centro de Ciberseguridad Industrial (CCI)
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- National Telecommunications and Information Administration (NTIA) and Idaho National Lab (INL) Software Bill of Materials (SBOM) Energy POC Stakeholders
- DOE Solar Energy Technology Office (SETO) and National Renewable Energy Lab (NREL) Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- Advisor to multiple industrial security hardware and software vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

THREAT CONDITION

- Infrastructure is a high-value target
- Your adversaries have three things you don't
- Who are you up against?
  - Organized crime
  - Nation states
  - Non-governmental organizations (NGOs)
  - Competitors, business partners and customers
  - Hanlon's Razor
- Attacker attribution is challenging
- Regulation is only getting more restrictive

RENEWABLE SECTOR SITUATION

- Market, integration, and political influences keep shifting
- Innovation is accelerating disruption
- OT looks more like IT each day
- Smart everything will be connected to smart everything
- Ever increasing dependence on technology and data
- Losing touch with manual options
- Age and skills of workforce are in transition
- Grid is turning inside out with renewables in many ways
- Regulation has a hard time keeping up

NERC/FERC FORECAST

- Wind is already at threshold for “big enough to regulate”
  - Solar and battery storage are close behind
- Inverter-based resources are regularly discussed
  - New dedicated working groups (indicators of new regulation)
  - Potential balance/disturbance effect for Bulk Electric System
- What was medium impact will become low impact over time
  - This has already happened many times; more is already approved
  - FERC has directed more studies from NERC on low impact
  - In every hearing, directive, RFI, NOPR, etc. this is mentioned
- Threat of DHS CISA takeover under ”national security” premise will motivate NERC/FERC in unusual ways

SNOWBALL EFFECT

- Electric power is the most critical infrastructure
- We are one “catalytic event” away from an avalanche
- NERC CIP moved the needle, but it doesn’t cover everything or everywhere
- Everyone who matters is getting wiser
  - Consumers
  - Boards and executives
  - M&A diligence, credit issuers, investors
  - Insurance firms
  - Legislators, regulators and federal agencies

MORE REGULATION IS COMING

- Clear signaling from U.S.
  - NERC standards drafting, FERC RFI, NOPR(s)
  - DOE RFI, NEW report: Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid
  - Executive Orders
  - National Security Memorandum (applies to “sector 5” verticals)
  - Neighboring critical infrastructure verticals (ONG, Water, Chemical)
  - TSA Pipeline Security Directives
  - 100-day Sprints for all sector 5 infrastructures
  - 140+ new cybersecurity bills introduced – so far (more to come)
  - “National Security” reach into distribution and small generation
- Global trend
  - NERC CIP, NIS2, CAF, BSI, IEC 62443, NIST 800-53/82, ENISA…

COMMON THREADS: STABILIZERS

- We have just enough actuarial data to drive regulation
- Whether direct regulation (NERC CIP, TSA, CFATS, EPA) or indirect "para"-regulation (NIST, EO, NSM), new normal is:
  - Buy only "trusted" hardware, software, services (supply chain)
  - Know all cyber assets in your environment
  - Know the security posture for all cyber assets, cradle to grave
  - Segment and restrict access (zero trust, MFA)
  - Monitoring and detection at asset and network level
  - Strong incident response capability
  - "Intelligent islanding" (turtle mode)
  - Strong recovery capability
- Aligns with any external interested party: risk knowledge and accountability/blame for subsequent posture and actions

CONTACT ME

@PatrickCMiller

linkedin.com/in/millerpatrickc

pmiller@amperesec.com

www.amperesec.com

+15032721414