NERC CIP Overview

Center for Advanced Power Engineering Research

Chip Moore

Clemson University

October 30th 2015

- Overview
- Scope
- History of CIP
- Past Attacks
- NERC-CIP Standards Review

NERC-CIP Overview

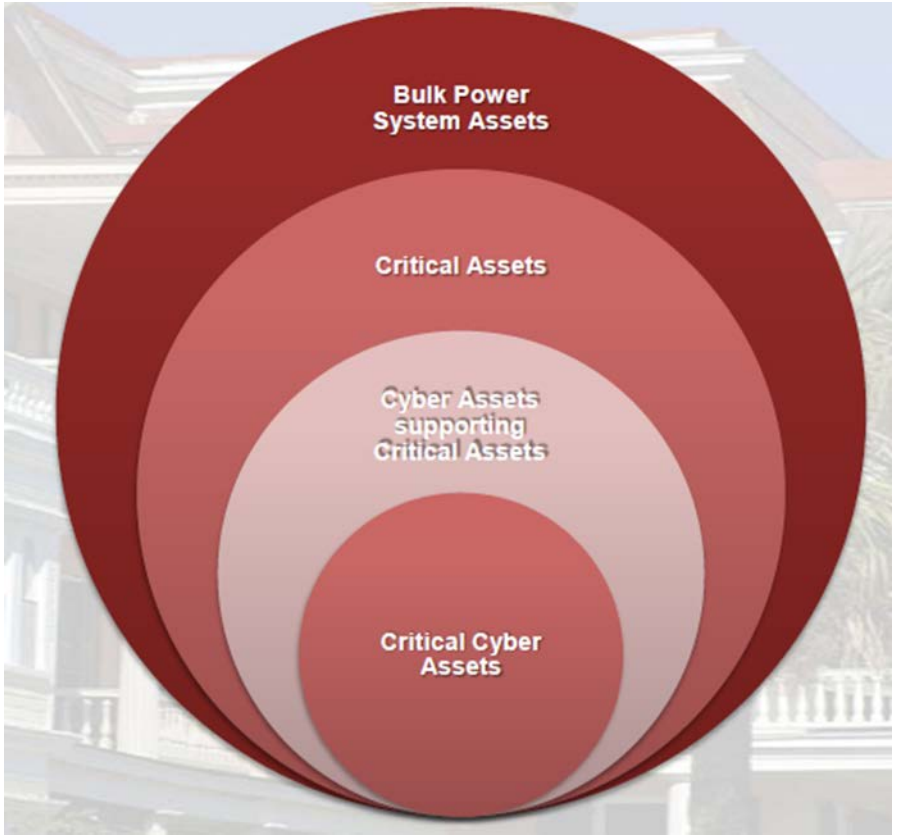
- The North American Electric Reliability Corporation (NERC) has adopted standards for the protection and security of Critical Cyber Assets supporting the Bulk Electric System (i.e., the power grid). This set of standards is known as the Critical Infrastructure Protection (CIP) standards CIP-002 – CIP-011.

- These standards for cyber security are mandatory and enforceable. Failure to comply with any NERC CIP Standard may result in penalties or fines of up to $1,000,000 per day/per incident.

- Critical Infrastructure Protection (CIP) continues to be a prominent issue in the utility industry and a significant area of focus for the energy sector. ”Critical Infrastructure,” for Duke Energy includes our energy delivery system (Generation, Transmission, Distribution) as well as the information systems and processes that support all businesses.

NERC-CIP Scope

- What is NERC protecting?
- Bulk Electric System
  - Generation Plants
  - Transmission Stations
  - Transmission Lines
  - Transmission towers
- Critical Assets
  - Generation Plants
  - Transmission Stations
  - Control Centers
- Cyber Assets
  - Supervisory Control And Data Acquisition Systems (SCADA)
  - Energy Management Systems (EMS)
  - Plant Distributed Control Systems (DCS)



- Aurora Generator Test
  - 2007
  - Idaho National Labs
  - Department of Homeland Security
  - Independent power/SCADA engineers
  - Open and close generator's circuit breakers out of phase from the rest of the grid

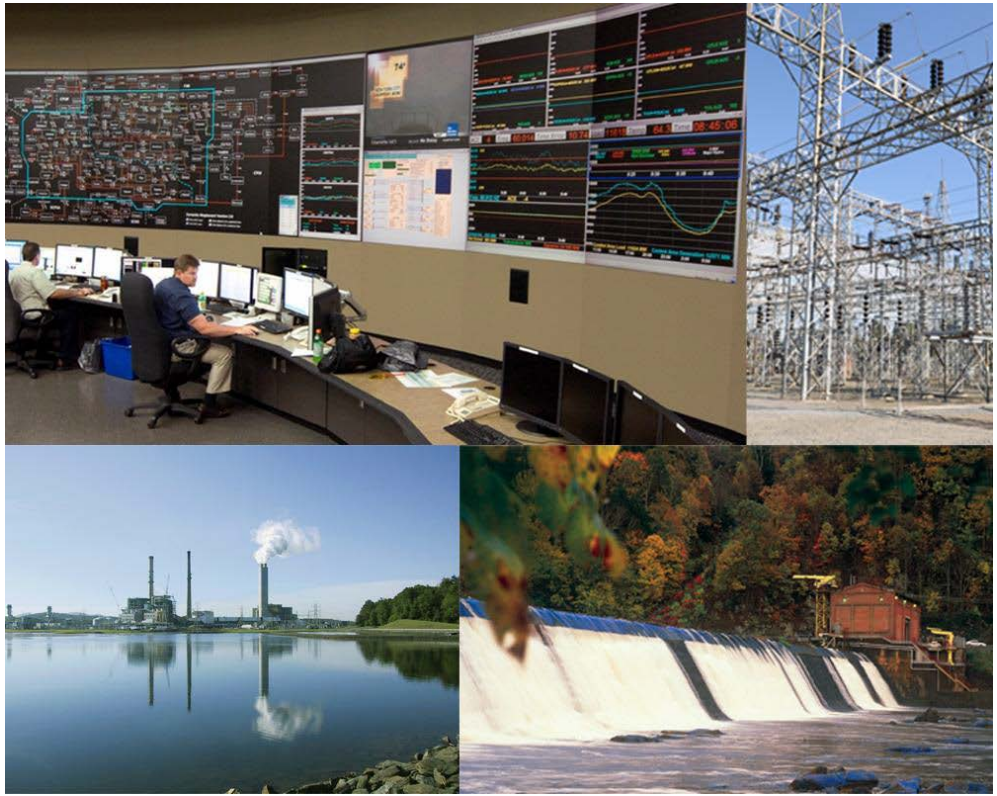
- https://youtu.be/fJyWngDco3g

NERC-CIP History

- 2008: CIP Version 1
  - First enforceable cybersecurity standards for the BES
  - RBAM (Risk-Based Assessment Methodology) to define Critical Assets
- 2009: CIP Version 2
  - Added annual review of additional processes
  - Enforced requirements rather than except risk
- 2010: CIP Version 3
  - Visitor escort updates
- 2012: CIP Version 4
  - Bright-Line Criteria
  - Never enforced due to timing of Version 5
- 2013: CIP Version 5
  - Impact Ratings (High, Medium, Low)
  - Include all communication devices (IP & Serial)

Past Cyber Attacks

- STUXNET
  - 2010
  - Attack Siemens PLCs
  - Iranian Uranium Factory
  - State sponsored
- SHAMOON
  - 2012
  - Attack Windows NT
  - Saudi Aramco
  - 30,000 Computers
  - No Control/Process Systems
  - "Cutting Sword of Justice"



Past Physical Attacks

- Pacific Gas & Electric
  - April 16th 2013
  - Metcalf 500/230kV Substation
  - 2 Auto Banks
  - Fiber communication cut
  - Transformers shot from outside of fence
  - 10,000 – 17,000 Gallon Spill (71 Trip)
  - No extended outages
  - Grid Reliability Alert
  - FBI Investigation
  - No arrest to date

- Entergy
  - August – October 2013
  - Arkansas
  - 3 Separate attacks
    - Transmission line cut
    - Substation fire
    - Transmission tower tied across railroad tracks
  - Actual outage
  - FBI Investigation
  - 15 years
  - $4.8 million in fines

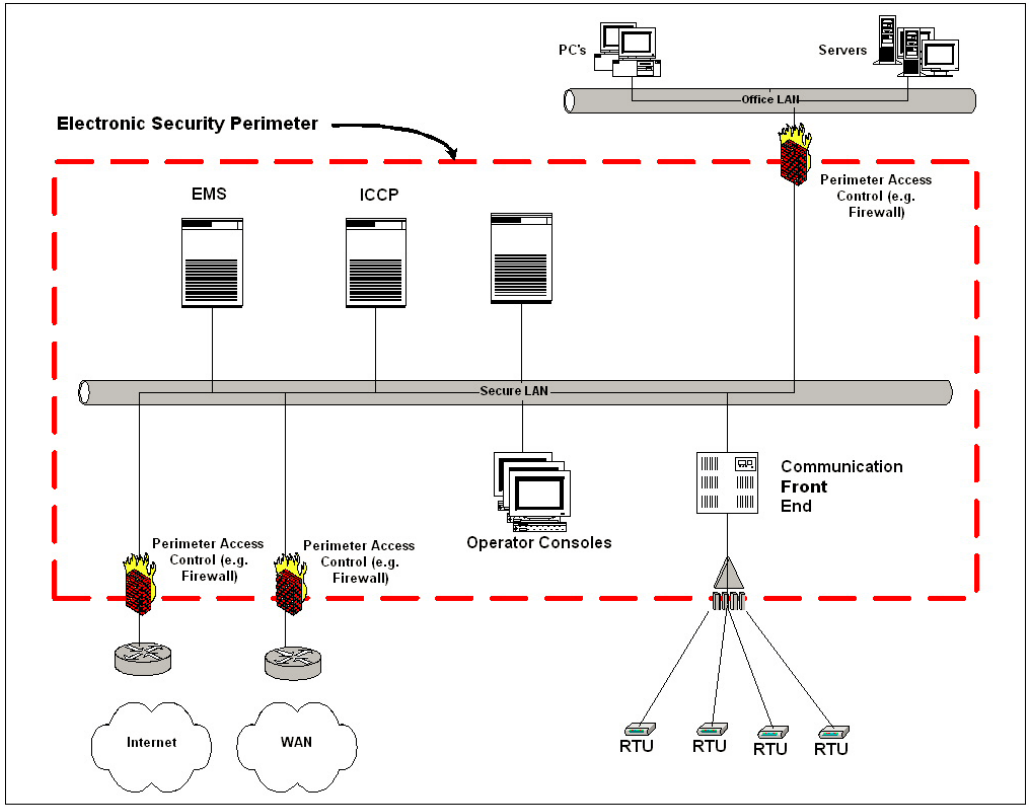
- CIP-002: BES Cyber System Categorization
- CIP-003: Security Management Controls
- CIP-004: Personnel and Training
- CIP-005: Electronic Security Perimeter(s) (ESP)
- CIP-006: Physical Security Perimeter (PSP) of BES Cyber Systems
- CIP-007: Systems Security Management
- CIP-008: Incident Reporting and Response Planning
- CIP-009: Recovery Plans for BES Cyber Systems
- CIP-010: Configuration Change Management and Vulnerability
- CIP-011: Information Protection
- CIP-014: Physical Security

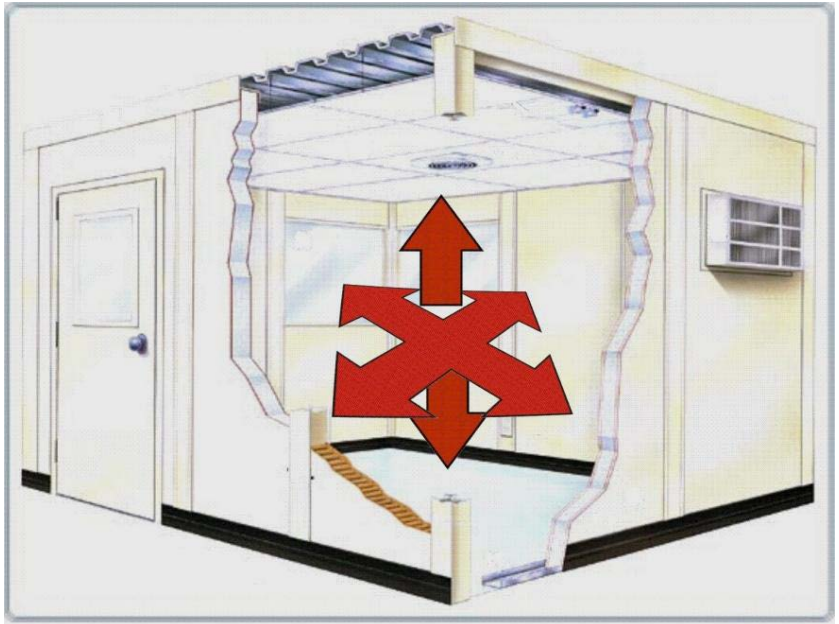
- CIP-002: BES Cyber System Categorization
  - Identify BES Facilities
    - High Impact (Control Centers)
    - Medium Impact (large Generation plants, larger Transmission stations)
    - Low Impact (everything else in the BES >100kV)
  - Identify Cyber Assets
    - Programmable with a communication interface (IP/Serial)
  - Identify BES Cyber Assets
    - Negative impact within 15 minutes
    - Degraded, Misused, Unavailable

- CIP-003: Security Management Controls
  - Document Cyber Security Policy & Program
  - Identify CIP Senior Manager

- CIP-004: Personnel and Training
  - Personnel Training on Cyber Security Program
  - Background Checks
  - Access Controls for Physical and Electronic

- CIP-005: Electronic Security Perimeter(s) (ESP)
  - Firewall rules and policies
  - Electronic Access Point
  - Protect all BES Cyber Assets





Six Wall Physical Security Perimeter

- CIP-006: Physical Security Perimeter (PSP) of BES Cyber Systems
  - Restrict access
  - Monitor access
  - Log activity
  - Escort visitors
  - Alarm
  - Built around all BES Cyber Assets

- CIP-007: Systems Security Management
  - Restrict IP ports & services
  - Security patch/firmware management
  - Intrusion detection/prevention
  - Antivirus/Malware
  - Alarm on cyber events
  - Account/Password management

- CIP-008: Incident Reporting and Response Planning
  - Cyber Incident Response Team
  - Program to track and report

- CIP-009: Recovery Plans for BES Cyber Systems
  - Recovery plan for failed/damaged assets
  - Storage of spares and associated data/configuration

- CIP-010: Configuration Change Management and Vulnerability
  - Maintain baseline configuration/settings
  - Track any changes
  - Verify configuration every year
  - Cyber Vulnerability Assessment
- CIP-011: Information Protection
  - Access control to repositories
  - Protect data in transit

- CIP-014: Physical Security
  - Identify most critical facilities on system
  - Assess potential physical attack vectors
  - Install protections
    - Fencing
    - Barriers
    - Cameras
    - Security
    - Alarms
  - 3rd party review

As cyberattack campaigns continue to multiply, our Critical Infrastructure, such as Generation and Transmission assets and our information and technology systems, must be prepared to protect against cyber threats and intrusions that could occur anytime, anywhere. The NERC-CIP requirements are the first step to insuring the safe and reliable operation of the Bulk Electric System.


DUKE
ENERGY®