NERC CIP Information Protection

Eric Ruskamp
Manager, Regulatory Compliance

September 13, 2017

Agenda

- NERC History
- NERC Compliance
  - Overview of Reliability Standards
  - Compliance with Reliability Standards
  - Penalty for noncompliance
- CIP Reliability Standards
- CIP Information Protection

NERC | History

Nov 9, 1965 Blackout

- A single wrongly set relay in Ontario caused a key transmission line to trip
- Escalating line overloads... more trips
- 25 Million people were without electricity for 12 hours
- Reason: varying operating standards

NERC | History

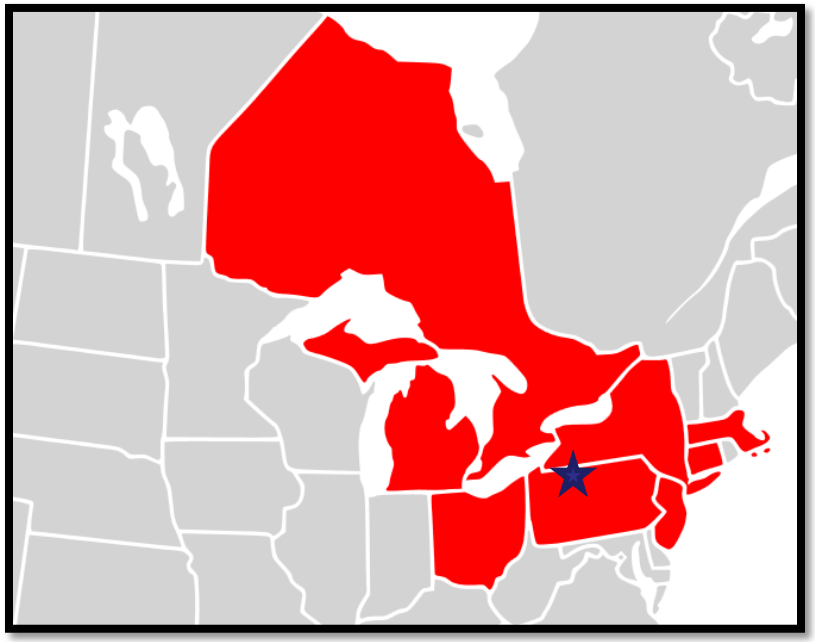
The Result

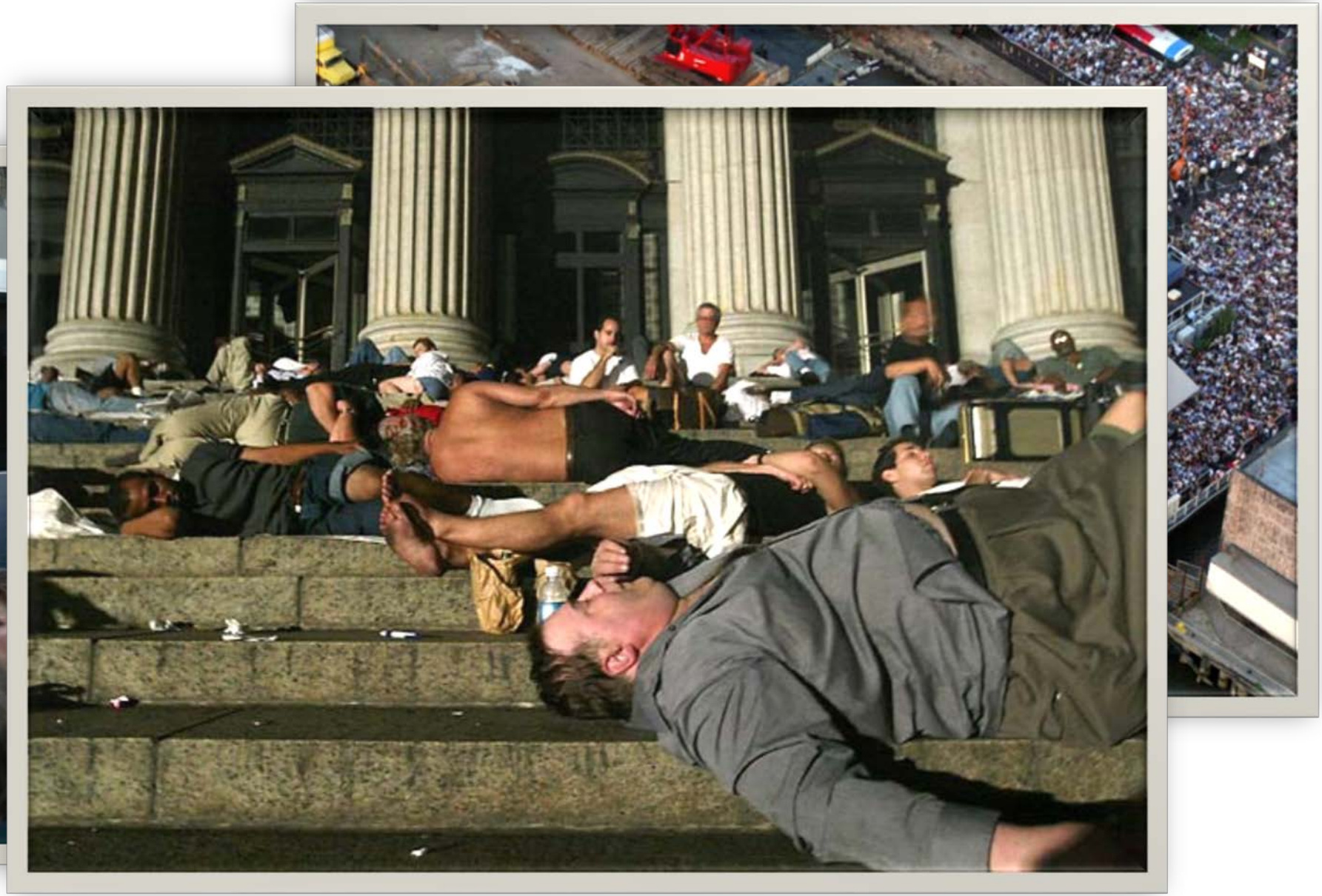
- North American Electric Reliability Council (NERC) formed on June 1, 1968 under the Electric Power Reliability Act of 1967
- Began developing Operating Policies
- Adopted Planning Standards in 1997

NERC | History

August 14, 2003 Blackout

- Largest Blackout in North American history
- Affected 50 million people
- Financial loses estimated at $6 Billion

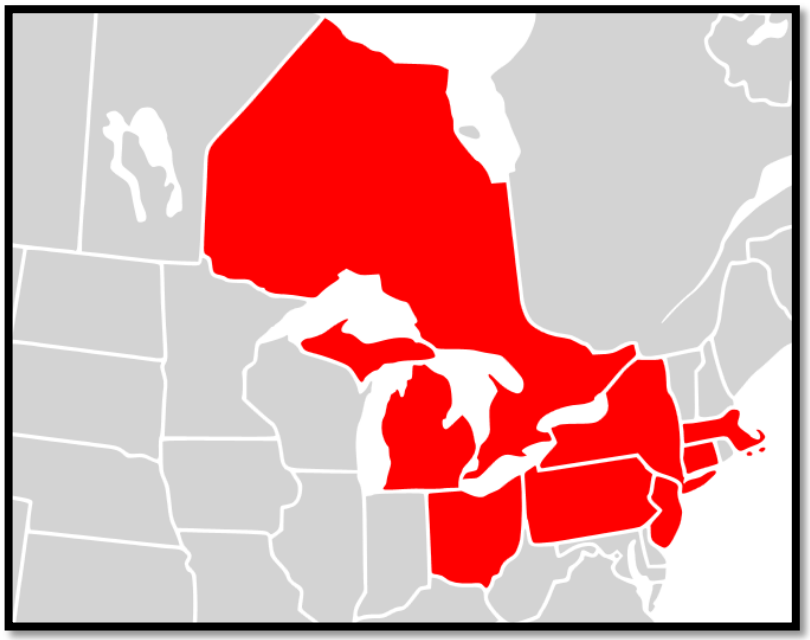




NERC | History

1965

2003



NERC | History

Enforcement Needed

- EPACT 2005 signed by President Bush
- June 18, 2007 Mandatory Enforcement began

NERC | Reliability Standards

- generation-load balance
- contingency reserves
- communication protocols
- cyber security
- physical security
- system restoration
- emergency operations
- interconnection requirements
- vegetation management
- facility ratings
- operating limits
- transmission loading relief
- outage coordination
- real-time assessments
- model development
- system operator training
- system protection
- underfrequency load shedding
- generator capability coordination
- operations planning
- transmission planning
- voltage control

NERC | Reliability Standards

- 99 enforceable NERC Reliability Standards
  - 69 applicable to LES
- 549 Requirements
  - 281 applicable to LES

- An additional **1,100** sub Requirements within the standards (not counting bullet points and attachments)

NERC | Enforcement

Mechanisms to monitor, assess, and enforce compliance with Reliability Standards:

1. Compliance Audits
2. Self-Certifications
3. Self-Reporting
4. Spot Checking
5. Compliance Violation Investigations
6. Periodic Data Submittals
7. Exception Reporting
8. Complaints

NERC | Enforcement

	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

NOTE: This table describes the amount of Penalty that could be applied for each day that a violation continues, subject to the considerations of Section 2.16 regarding frequency and duration of violations.

NERC | Reliability Standards

- BAL – Resource and Demand Balancing
- COM – Communications
- **CIP – Critical Infrastructure Protection**
- EOP – Emergency Preparedness and Operations
- FAC – Facilities Design, Connections and Maintenance
- INT – Interchange Scheduling and Coordination
- IRO – Interconnection Reliability Operations and Coordination
- MOD – Modeling, Data, and Analysis
- NUC – Nuclear
- PER – Personnel Performance, Training and Qualifications
- PRC – Protection and Control
- TOP – Transmission Operations
- TPL – Transmission Planning
- VAR – Voltage and Reactive

CIP | Critical Infrastructure Protection

1. Identify the cyber assets critical to operating the BES

2. Harden against physical and cyber threats
   - physical access
   - electronic access
   - incident response
   - recovery plans
   - change management
   - security patching
   - information protection

CIP | Information Protection

BES Cyber System Information (BCSI)

1. Identification of BCSI
2. Protecting and Handling BCSI
3. Reuse or Disposal of cyber assets containing BCSI

CIP | Information Protection

1. Identification of BCSI
   - ❑ Criteria:
     - Usernames and passwords
     - Known vulnerabilities
     - Network diagrams with IP addresses
     - Ports and services
     - Firewall access rules
   - ❑ Classification – “Internal Restricted: CIP BCSI”
     - Electronic Labeling – header/footer, watermark
     - Physical Labeling – stamp, handwritten
     - Filename
     - Login banner

CIP | Information Protection

2. Protecting and Handling BCSI
   - ❑ BCSI in Storage
     - Electronic storage – permitted cyber assets
     - Physical location of electronic storage
     - Hardcopy storage – designated file cabinets
   - ❑ BCSI in Use
     - LES owned device
     - Lock device when not in use
     - Return to Storage at end of day
   - ❑ BCSI in Transit
     - Signed confidentiality agreement
     - Approval from CIP Senior Manager
     - Secure share or tamper evident packaging
     - May result in creation of another Storage location

CIP | Information Protection

3. Reuse or Disposal of cyber assets containing BCSI
   - ❑ Proper storage
   - ❑ Sanitize or destroy per:
     - NIST SP 800-88,
     - Degaussing, or
     - Secure Erase
   - ❑ Cyber Security department validation
   - ❑ Record keeping of actions taken


Question?