



University of Colorado  
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

### Electricity Infrastructure

CS 4950/5950  
Homeland Security &  
Cybersecurity

### Lesson 19 Electricity Infrastructure

Rick White, Ph.D.  
University of Colorado, Colorado  
Springs



1

Esc

1



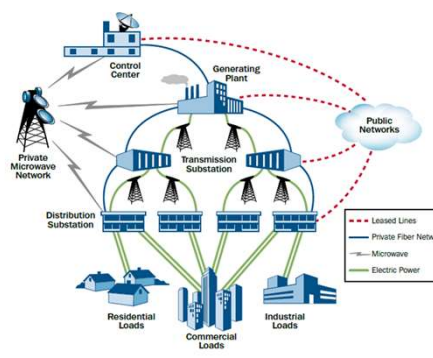
University of Colorado  
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

### Electricity Infrastructure

- The US electricity segment is comprised of more than **6,413 power plants** with approximately 1,075 gigawatts of installed generation.
- They serve 143 million customers by means of 30,320 substations, 203,930 miles of high-voltage Alternating Current transmission lines, 6,222 miles of high-voltage Direct Current transmission lines.



2

Esc

2



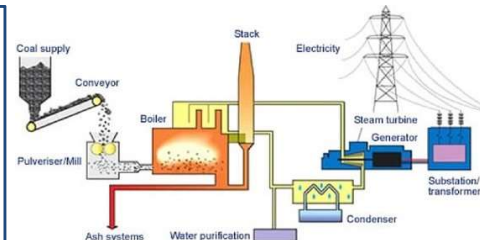
University of Colorado  
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

### Electricity Infrastructure

- About 48% of electricity is produced by coal power plants, 20% by nuclear power plants, and 22% by natural gas generators.
- Less than 10% of the nation's electricity is provided by renewable sources including hydroelectric, geothermal, wind, and solar power.



3

Esc

3



University of Colorado  
Colorado Springs

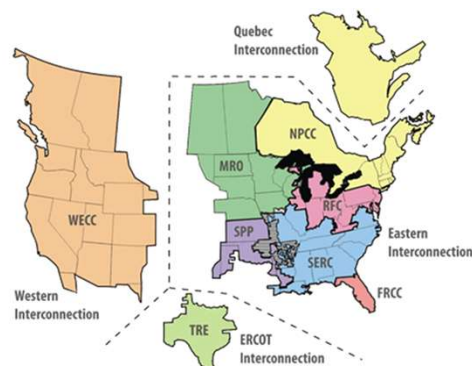
CS4950/5950

Homeland Security & Cybersecurity

### Electricity Infrastructure

The North American Grid is segregated into four regions serving both the United States and Canada:


1. Eastern Interconnection,
2. Western Electricity Coordinating Council
3. Electricity Reliability Council of Texas
4. Quebec Interconnection.



4

Esc

4




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**Electricity Infrastructure**

- The four power grids form an integrated system that has been described as the world's largest machine.
- There is no doubt that the loss of this system would be catastrophic.**



5  
 Esc

5



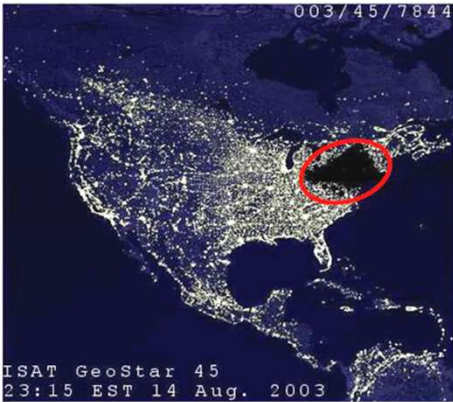
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**Electricity Infrastructure**


- In August 2003, a power outage affected 50 million people in the northeastern United States and Canada for most part of a week.
- The cause was accidental, but that didn't make the consequences any less severe.



ISAT GeoStar 45  
23:15 EST 14 Aug. 2003

6  
 Esc

6



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**Electricity Infrastructure**


- \$4-\$10 billion in economic losses are attributed to the blackout, as was a 0.7% drop in Canada's gross domestic product.
- A John Hopkins study determined that 90 people in New York City died as a direct result of the power outage.

**2003 NE Blackout**

- \$4-\$10 billion economic loss
- 0.7% drop in Canada GDP
- 90 NYC residents died

7  
 Esc

7




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**Electricity Infrastructure**

- In 2006, DHS and DOE conducted a joint experiment called Project Aurora.
- In this experiment, researchers demonstrated how an electricity generator could be remotely commanded over the Internet to self-destruct.
- **The video can be found on You Tube.**



8  
 Esc

8



### Electricity Infrastructure

- The implications were shocking because it can take months or even years to replace a generator.
- Consider the greater consequences if the 2003 blackout had lasted not just a week, but for months?

### Project Aurora

- Remotely commanded generator to **self-destruct**.
- Generators can take months or even **years to replace**.
- What if the 2003 blackout had **lasted for months**?

9

Esc

9



### Electricity Infrastructure

As with the Water Sector, protection of the Electricity Sector is also covered under **Presidential Policy Directive #21, Critical Infrastructure Protection**.

<https://www.whitehouse.gov/the-press-office/2013/02/12/2013-02-12-presidential-policy-directive-critical-infrastructure-security-and-resilience>

The White House

Office of the Press Secretary

For Immediate Release

February 12, 2013

#### Presidential Policy Directive -- Critical Infrastructure Security and Resilience

**PRESIDENTIAL POLICY DIRECTIVE #21**

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

#### Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure -- essential people, networks, and systems -- that are vital to public confidence and the Nation's safety, prosperity, and well-being.

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating modes (including institutional ownership), independent functions and systems in both the physical space and cyberspace, and governance constructs that involve multiple authorities, responsibilities, and regulators. Critical infrastructure owners and operators are uniquely positioned to manage risks to their institutional operations and assets, and to coordinate effective strategies to make them more secure and resilient.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, State, local, tribal, and territorial (S/L/T) entities, and public and private services and operators of critical infrastructure known referred to as "critical infrastructure owners and operators." This directive also defines and confirms the critical infrastructure-related functions, roles, and responsibilities among the Federal, State, local, tribal, and territorial (S/L/T) entities, and public and private services and operators of critical infrastructure. The directive also establishes the national unity of effort to strengthen the security and resilience of the Nation's critical infrastructure, for the continuity of national essential functions, and to organize and lead to greater efficiency with and across the security and resilience efforts of critical infrastructure owners and operators.

#### Objectives

It is the priority of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government must work with critical infrastructure owners and operators and S/L/T entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.

10

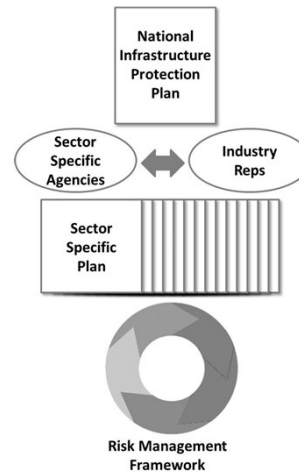
Esc

10



### Electricity Infrastructure

- PPD-21 assigns the **Department of Energy as the Sector-Specific Agency** responsible for the Energy Sector including electricity.
- DOE officials work together with industry representatives on the **Electricity Sector Coordinating Council** to implement provisions of the **2013 National Infrastructure Protection Plan** and update the corresponding **Sector-Specific Plan**.



11

Esc

11



### Electricity Infrastructure


- The **Energy Policy Act of 2005** created the **Federal Energy Regulatory Commission** giving DOE regulatory authority over the electricity sector.
- The **North American Electric Reliability Corporation**, an industry cooperative, maintains reliability of the grid through eight Regional Reliability Councils.
- **FERC works closely with NERC.**



12

Esc

12




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

### Electricity Infrastructure


Security cooperation is also facilitated through the **Electricity Sector Information Sharing and Analysis Center**.



13

Esc

13




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

### Electricity Infrastructure

- The Energy Policy Act of 2005 gave **FERC the authority to approve mandatory cybersecurity standards**.
- Accordingly, FERC developed a set of Critical Infrastructure Protection cybersecurity reliability standards.




14

Esc

14





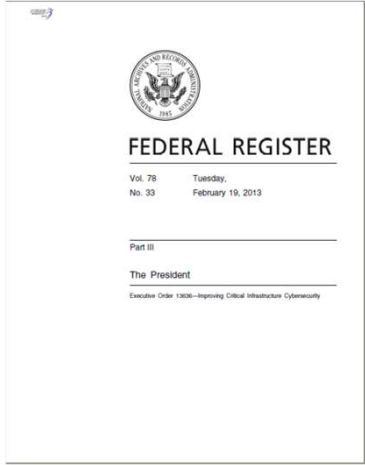
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**Electricity Infrastructure**

After President Obama issued Executive Order 13636 in February 2013, **FERC worked with NIST to help develop the NIST Cybersecurity Framework.**



15  
 Esc

15



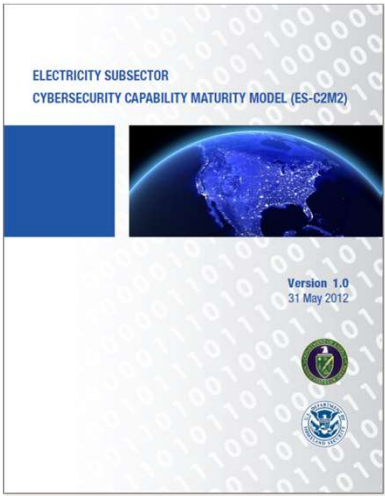
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**Electricity Infrastructure**

The resulting product, released in February 2014, is very similar to the **Electricity Subsector Cybersecurity Capability Maturity Model** created in 2012.



16  
 Esc

16




**UCCS** University of Colorado  
Colorado Springs

CS4950/5950  
*Homeland Security & Cybersecurity*

**Conclusion**

Questions?



17

Esc