SECURICON
Information Security Solutions

Critical Infrastructure Protection & Industrial Cybersecurity

The Electric Grid as a Model

Ernie Hayden CISSP CEH
Executive Consultant
October 10, 2013 v0

SECURICON
Information Security Solutions

Information Security Professional Services

- 12-Year Old Company
- Headquartered in Alexandria, VA
- Industry Verticals
  - Power & Energy
  - Oil & Gas
  - Airport & Seaport
  - Finance & Banking
  - State & Local Governments
  - Federal Agencies – DOD, DHS, NSA, DISA, DARPA, FAA, DOE, NRC
- Areas of Expertise
  - Critical Infrastructure Protection and Security
  - Industrial Controls Security
  - Cybercrime & Cyberwarfare Analysis
  - Business Continuity / Disaster Recovery Planning
  - Security Strategy, Analysis and Planning
  - Security Training

Contact Us

Securicon Corporate Headquarters
5400 Shawnee Road
Suite 206
Alexandria, Virginia 22312

Toll Free : 877-914-2780
Phone: 703-914-2780
Fax: 703-914-2785

General
info@securicon.com

Sales
sales@securicon.com

SECURICON
Information Security Solutions

History of Grid Security

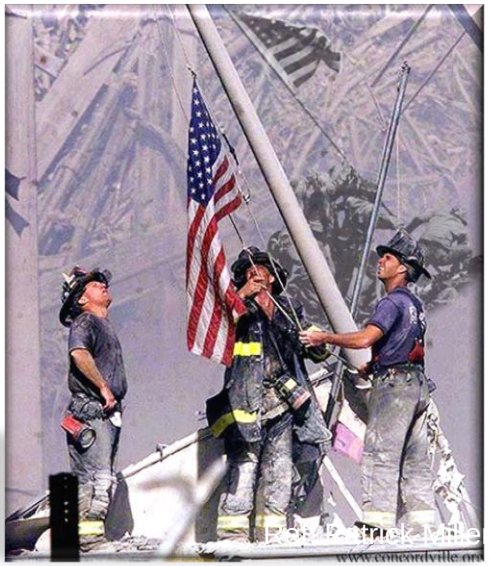
Security – Pre NERC CIP

- Until NERC CIP
  - Emphasis on Physical Security to Protect Assets
  - Military / Police Mindset
    - **Guards**
    - **Gates**
    - **Fences**
    - **Cameras**
  - Cyber Not Commonly Considered
  - Some Concerns with Copper Theft

Driving Factors for Grid Security

- **History**
  - FERC Appendix G
  - NERC UAS-1200
  - NERC 1300
  - NERC CIP-001 – Sabotage Reporting
  - NERC CIP 002-009
  - FERC Order 706 – January 2008

- **Influential** Events
  - Interdependency Studies
  - NE Blackout 2003
  - "Aurora" – Generator Destruction via Remote "Hack"



Interdependency Studies 2001

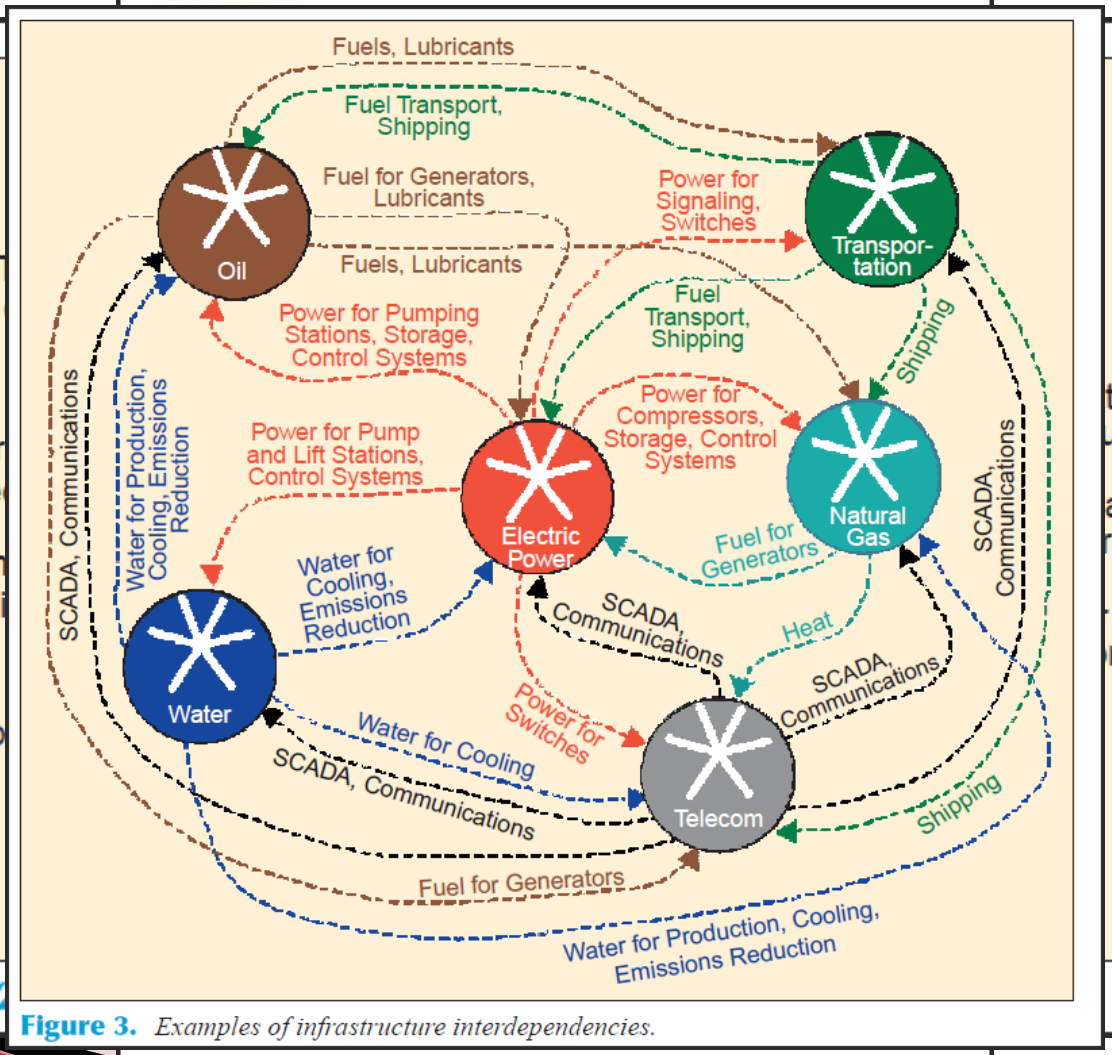
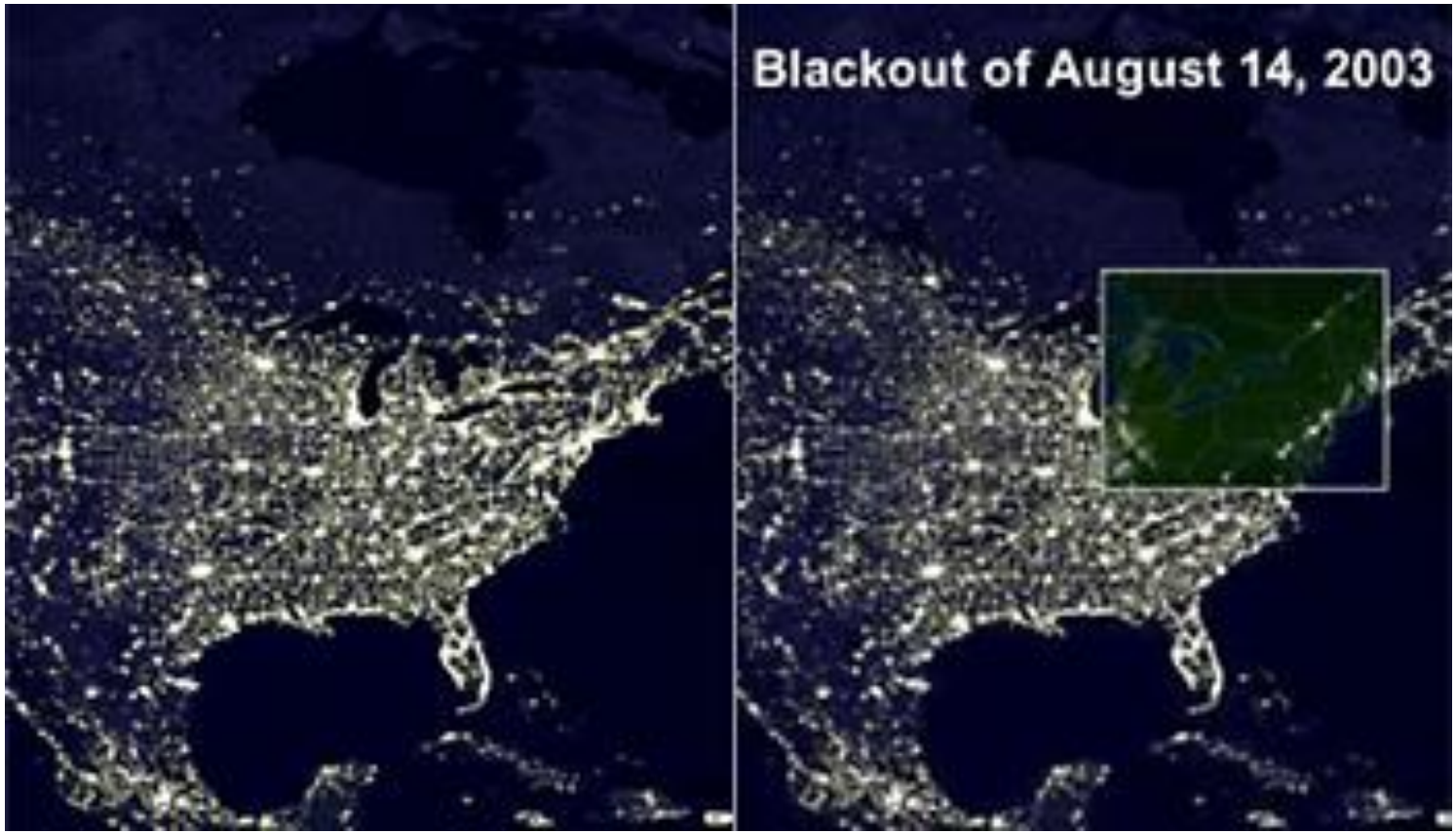


Figure 3. *Examples of infrastructure interdependencies.*

Reference: 10.1.1.89.2276.pdf

Northeast Blackout 2003



http://www.earthinstitute.columbia.edu/news/2005/story06-01-05e.html

CNN.com /US

HOME | WORLD | U.S. | POLITICS | CRIME | ENTERTAINMENT | HEALTH | TECH | TRAVEL | LIVING | MONEY | SPORTS | TIME.COM

Hot Topics » Cheating Death • Money & Main St. • Latino in America • What If? • What Matters • more topics »

Breaking news Once-missing Cleveland women released from hospital, go home to families

updated 11:06 p.m. EDT, Wed September 26, 2007

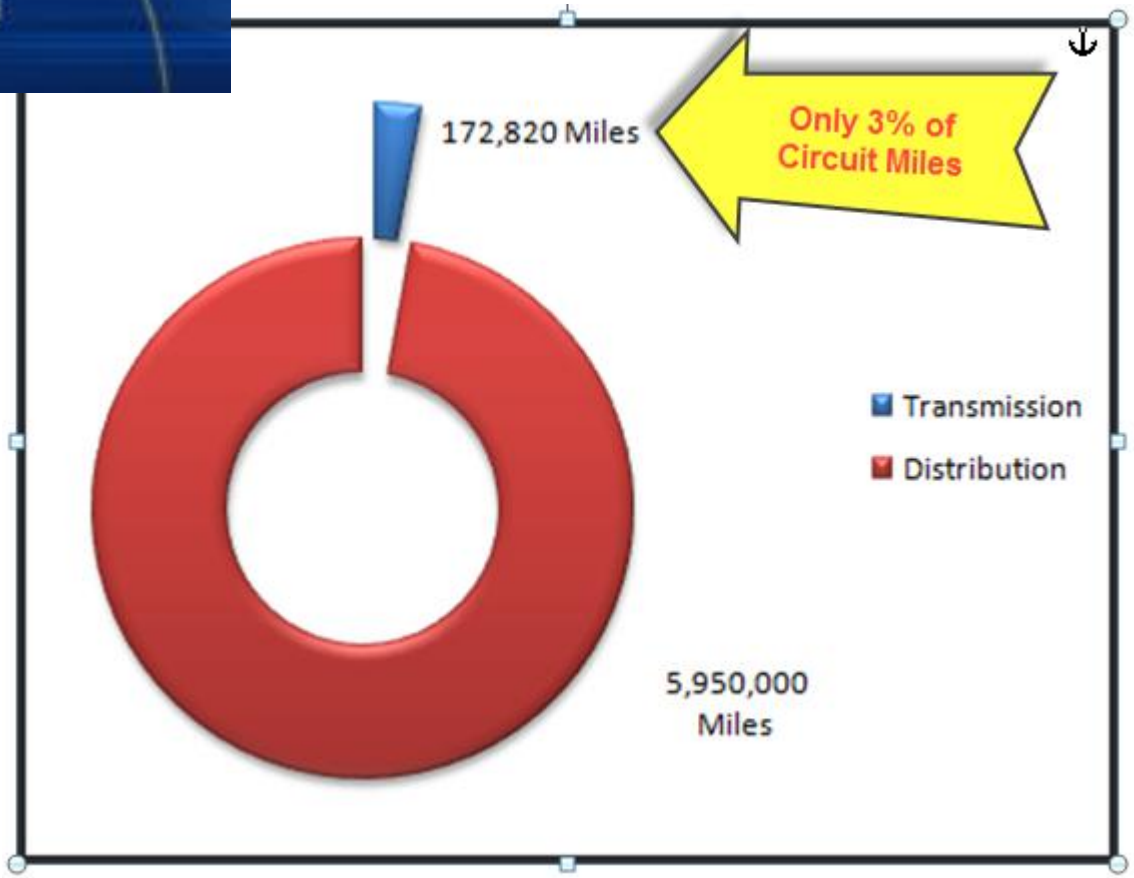
Sources: Staged cyber attack reveals vulnerability in power grid

http://www.cnn.com/2007/US/09/26/power.at.risk/
http://www.militaryphotos.net/forums/showthread.php?121081-AURORA-test-validated-fears-of-Dept-of-Homeland-Security

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002 to CIP-009



SECURICON
Information Security Solutions

The Present

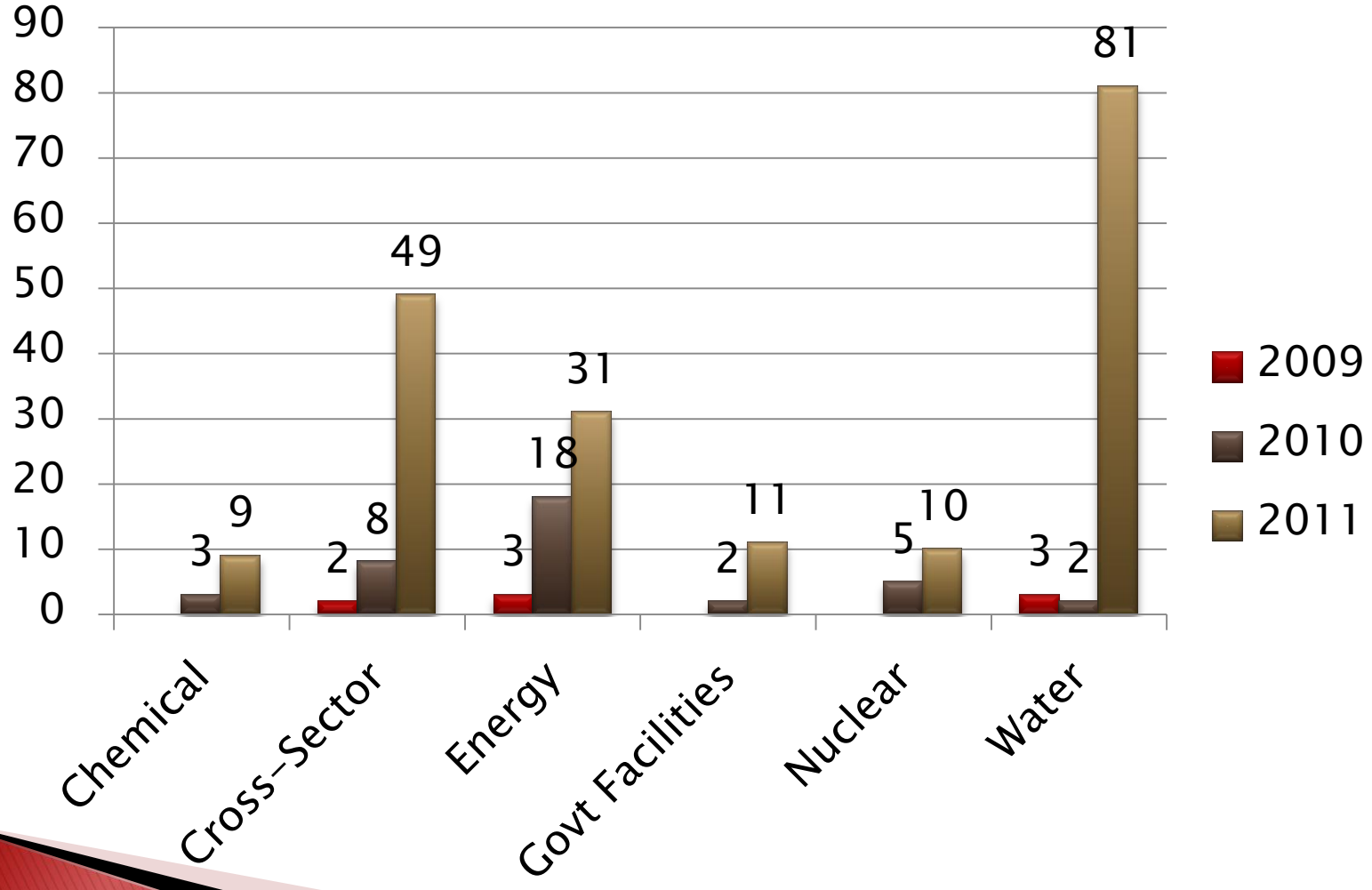
LOTS TO FIX AND PROTECT

- Too Many Opportunities for Harm
  - Ubiquity of Data
  - Internet Not Designed for Security
  - Legacy Systems
  - Complexity of Modern Software and Hardware
  - Reliance on Third Parties

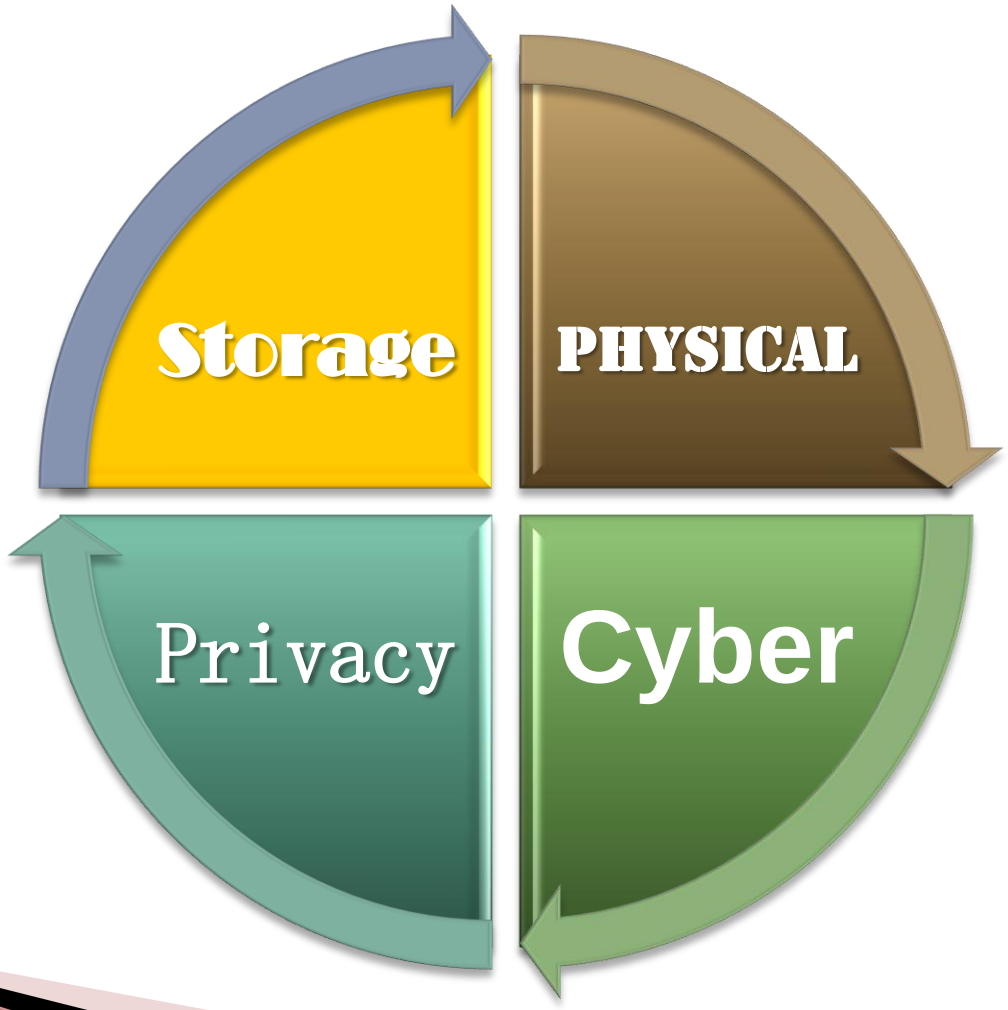
INDUSTRIAL CONTROL SYSTEMS

- Control System Vulnerabilities
- New Modes of "Operational Attack"
  - Stuxnet
  - DuQu
  - Flame
  - Shamoon
- Legacy "Knowledge"
- Regulatory Focus…But
  - Compliance vs. Security
  - TCP/IP Centric
- New Emphasis by Congress
- New Emphasis Globally
- And…Moving to TCP/IP

2009-2011 ICS-CERT Incident Response Trends - A Closer Look

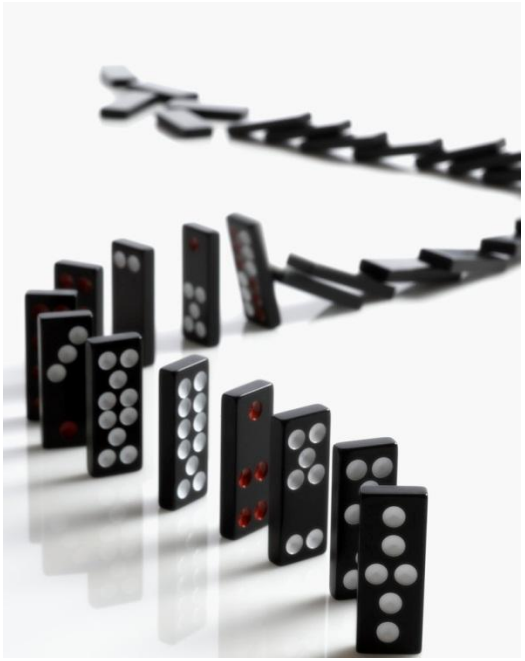


SMART GRID LAYERS OF CONCERN



SUPPLY CHAIN CYBER SECURITY

- Subtle Opportunities for Attack
- Examples:
  - Back Doors Included in Chip Sets for Smart Meters
  - Physical Addition of Chips on Mother Boards
  - Counterfeit Components
- Huge Concerns at Government Levels
  - Australia, Canada, UK, US – Telecommunications and Network Components Concerns



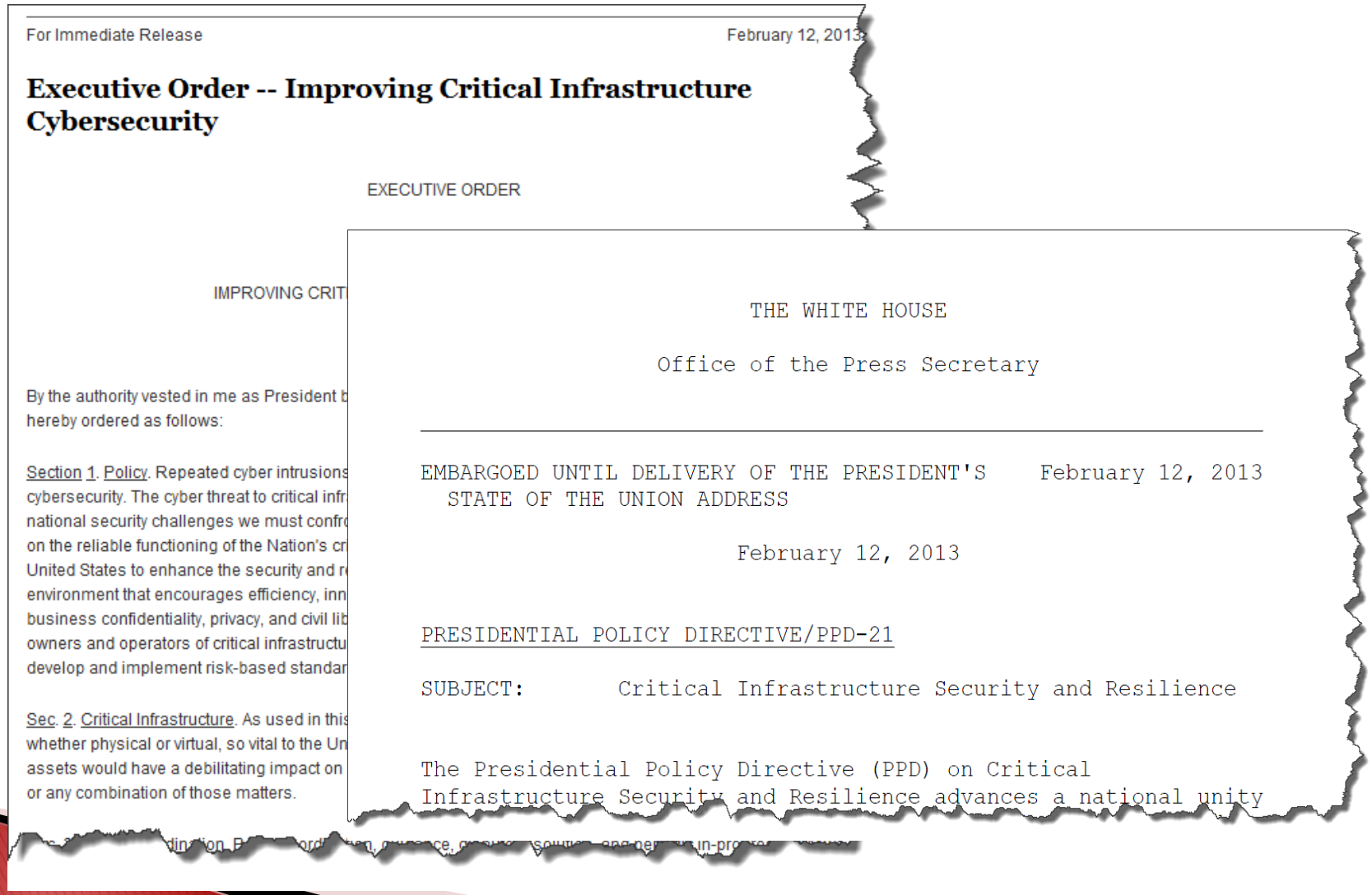
Physical Security is Still a Necessity

http://www.inedc.com/1-3747

SECURICON
Information Security Solutions

The Future

The Presidential Executive Order Improving Critical Infrastructure Cybersecurity



For Immediate Release February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRIT

By the authority vested in me as President b
hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions
cybersecurity. The cyber threat to critical infr
national security challenges we must confr
on the reliable functioning of the Nation's cr
United States to enhance the security and r
environment that encourages efficiency, inn
business confidentiality, privacy, and civil lib
owners and operators of critical infrastructu
develop and implement risk-based standar

Sec. 2. Critical Infrastructure. As used in this
whether physical or virtual, so vital to the Un
assets would have a debilitating impact on
or any combination of those matters.

THE WHITE HOUSE

Office of the Press Secretary

EMBARGOED UNTIL DELIVERY OF THE PRESIDENT'S STATE OF THE UNION ADDRESS February 12, 2013

February 12, 2013

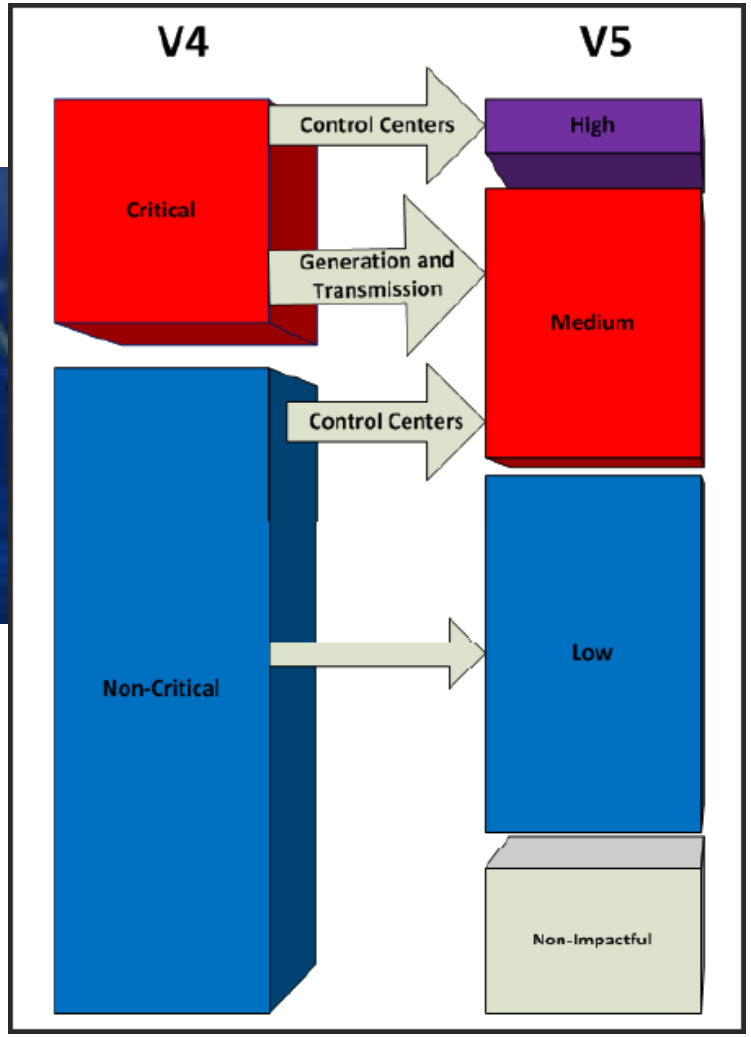
PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

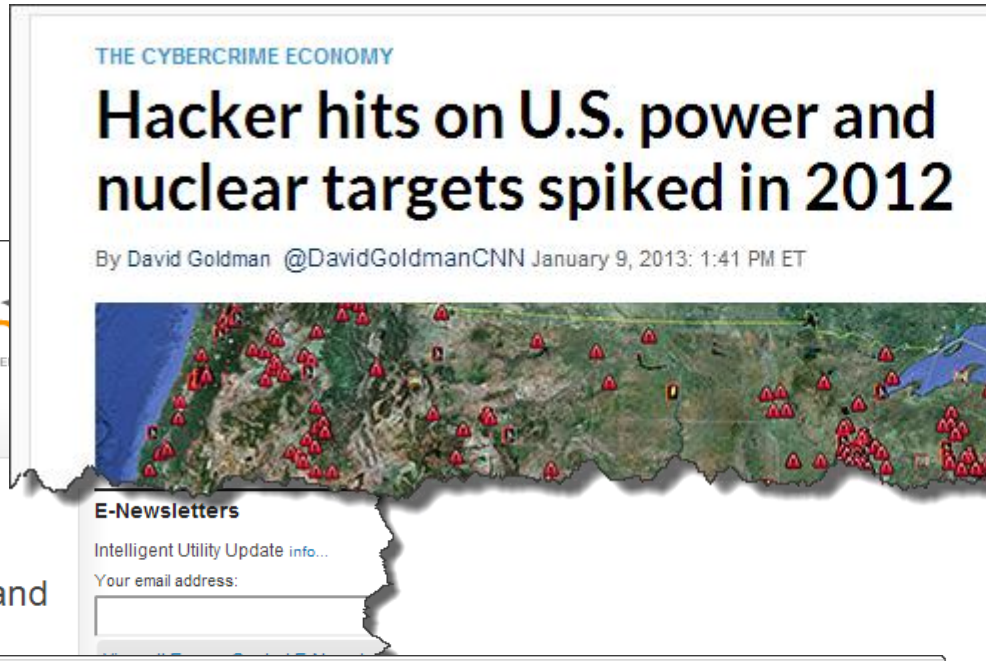
The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity

NERC CIP Version 5

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



New and Continued Attacks



New Philosophy – Assumption of Breach

How to Proceed?

- Have a Security Officer – Ensure a Security Conscience
  - Executive Team Support
  - Board Support
- Assume the Worst – Be Prepared
  - Cyber Incident Response Team
  - Practiced and Ready
- New Legislation and Executive Order Actions
  - Pay Attention
  - Don't Stand by the Sidelines – Participate
- Develop a Cyber Security Network
  - Compare Cyber Incidents with Your Peers
  - Talk to FBI, Secret Service
  - Have a "Go To" Security Resource

SECURICON
Information Security Solutions

THANK YOU!

Ernie Hayden CISSP CEH
Executive Consultant -- Securicon
ernie.hayden@securicon.com
425-765-1400