

Critical Infrastructure Protection & Industrial Cybersecurity

The Electric Grid as a Model

Ernie Hayden CISSP CEH
Executive Consultant
October 10, 2013 v0



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

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



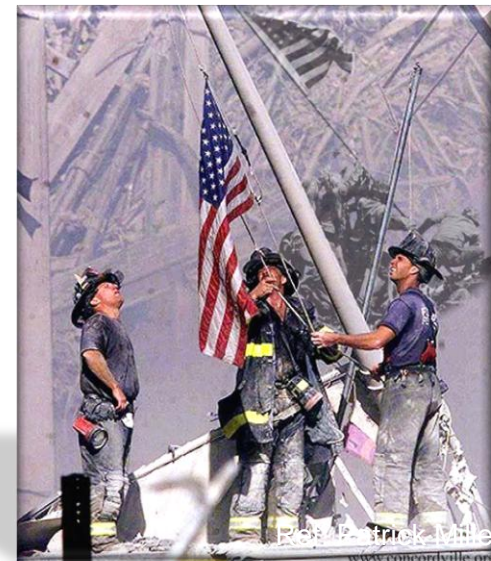
Driving Factors for Grid Security

► History

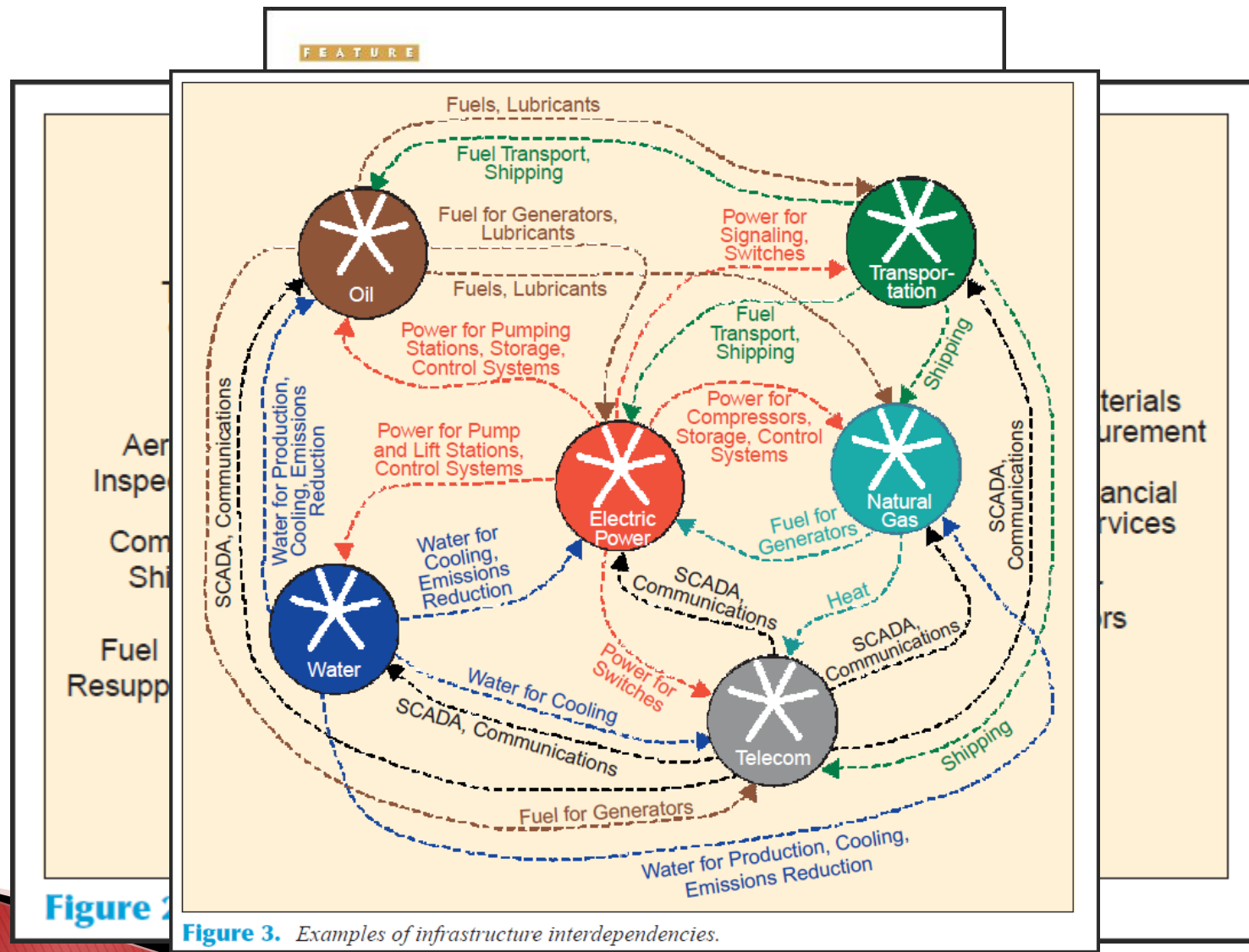
- FERC Appendix G
- NERC UAS-1200
- NERC 1300
- NERC CIP-001 – Sabotage Reporting
- NERC CIP 002-009
- FERC Order 706 – January 2008

► Influential Events

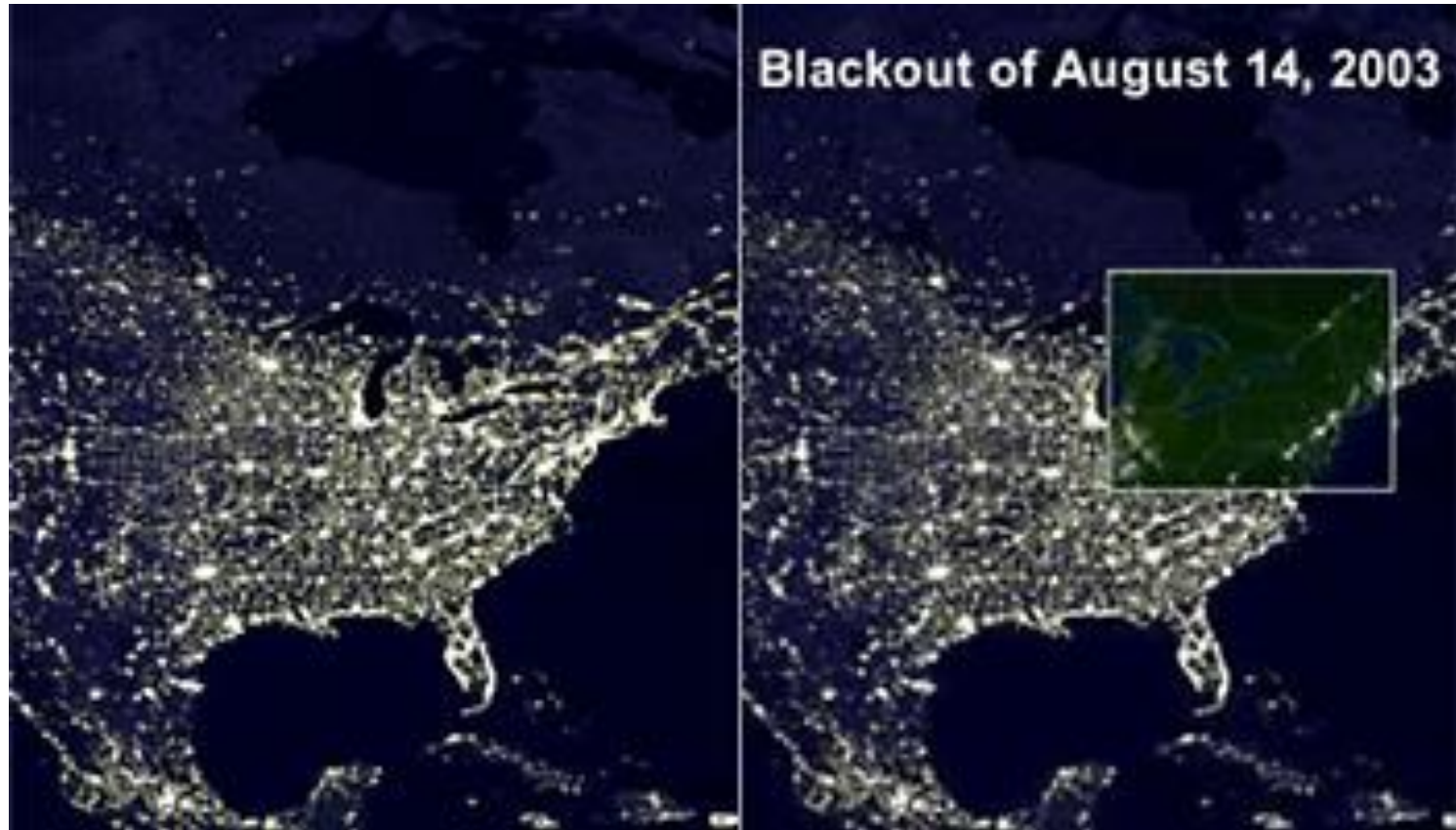
- Interdependency Studies
- NE Blackout 2003
- “Aurora” – Generator Destruction via Remote “Hack”



Interdependency Studies 2001



Northeast Blackout 2003



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

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



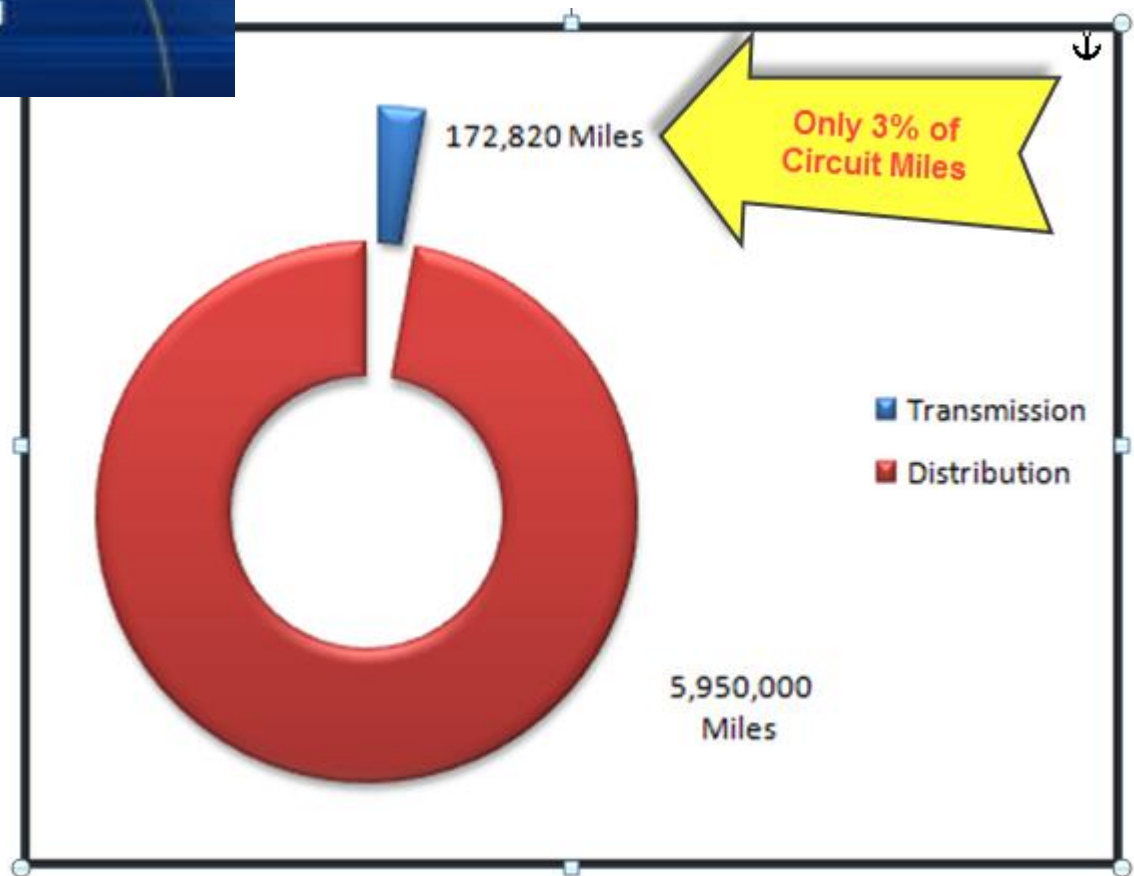
<http://www.cnn.com/2007/US/09/26/power.at.risk/>

<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





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

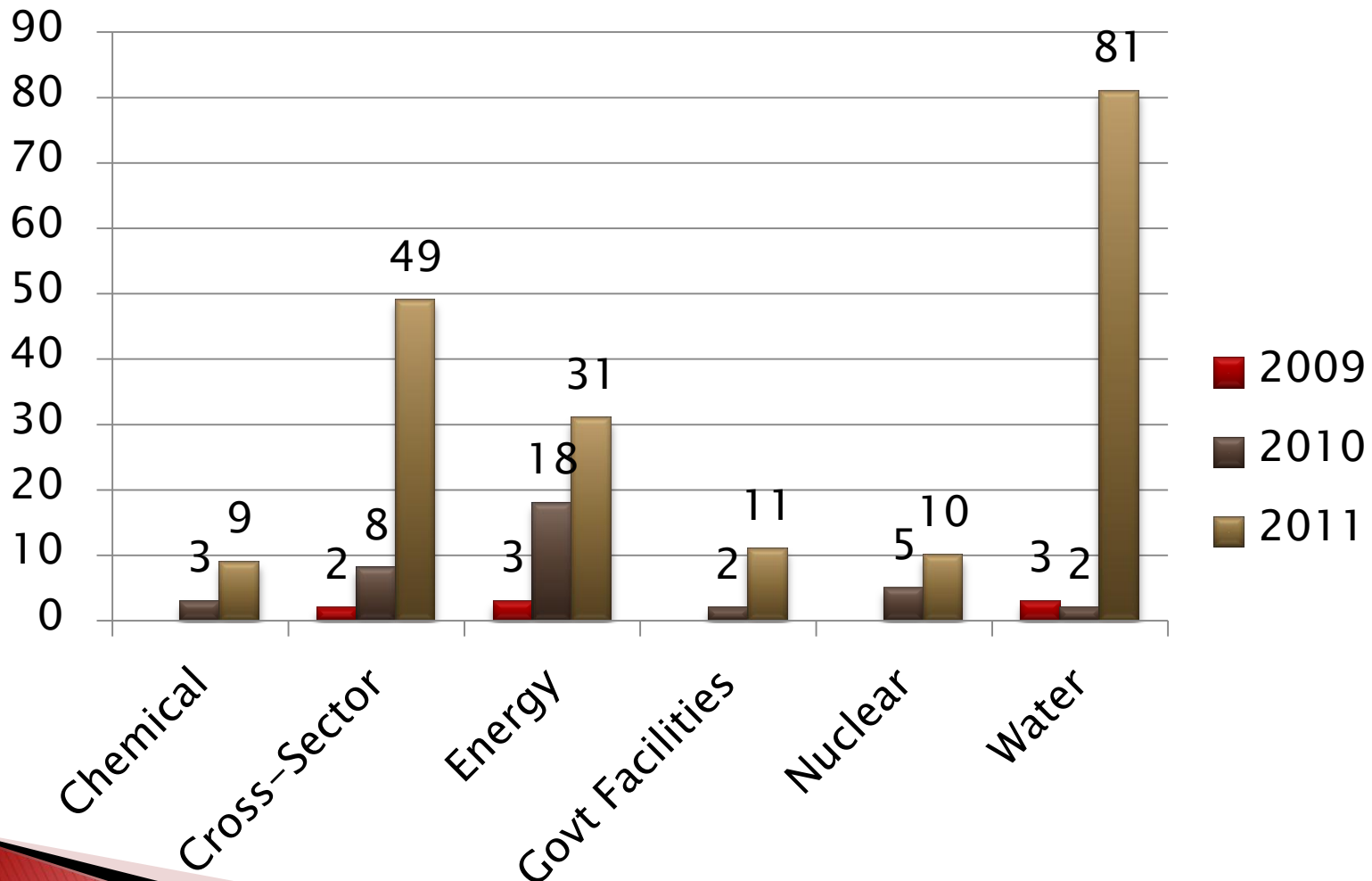


INDUSTRIAL CONTROL SYSTEMS

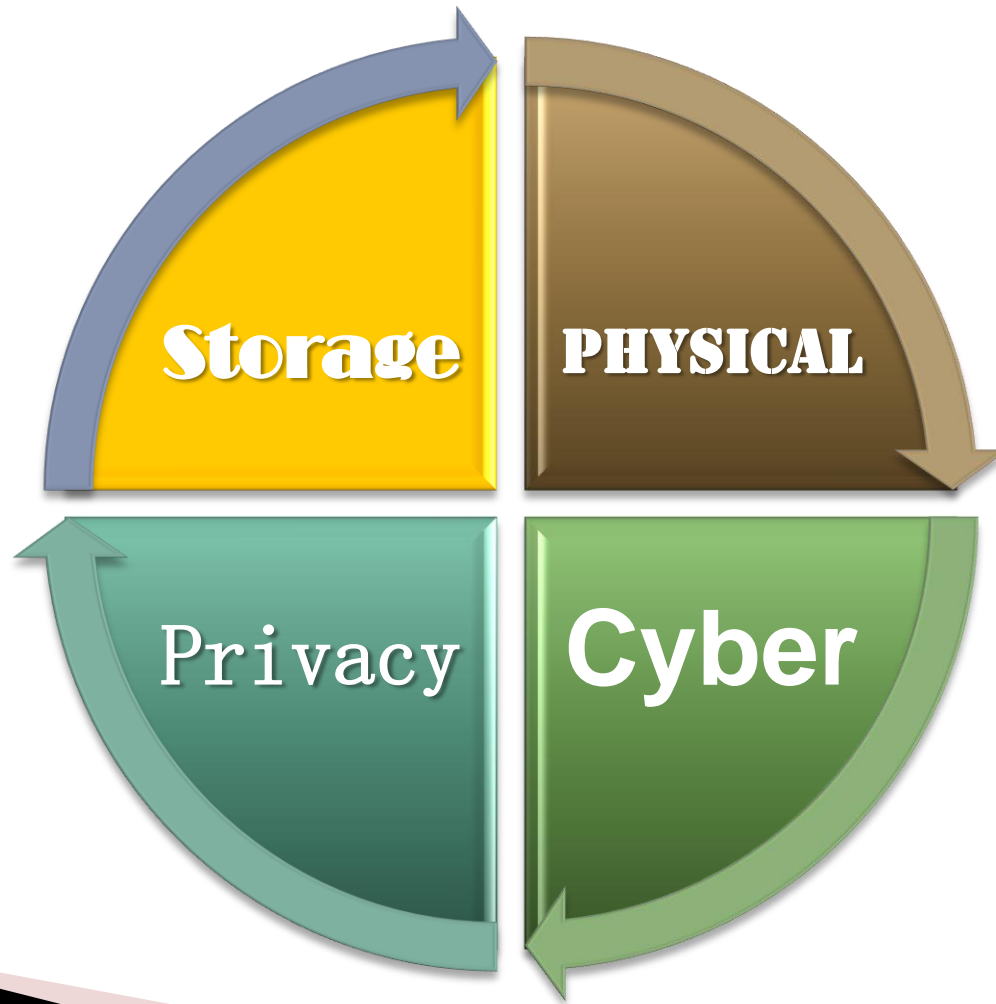
- ▶ **Control System Vulnerabilities**
- ▶ **New Modes of “Operational Attack”**
 - Stuxnet
 - DuQu
 - Flame
 - Shamoon
- ▶ **Legacy “Knowledge”**
- ▶ **Regulatory Focus...But**
 - Compliance vs. Security
 - TCP/IP Centric
- ▶ **New Emphasis by Congress**
- ▶ **New Emphasis Globally**
- ▶ **And...Moving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



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

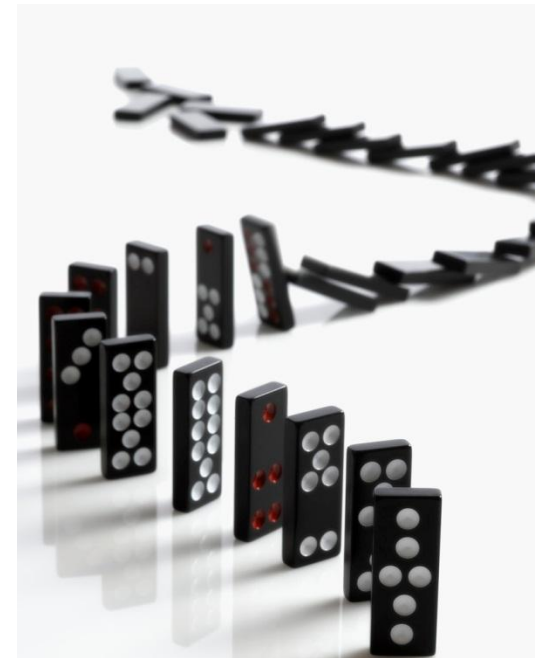


SMART GRID LAYERS OF CONCERN



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>





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

THE WHITE HOUSE

Office of the Press Secretary

By the authority vested in me as President by the Constitution and the laws of the United States, I hereby order as follows:

Section 1. Policy. Repeated cyber intrusions threaten the cybersecurity of the United States. The cyber threat to critical infrastructure is a national security challenge we must confront. To ensure the reliable functioning of the Nation's critical infrastructure, the United States must enhance the security and resilience of the environment that encourages efficiency, innovation, and business confidentiality, privacy, and civil liberties. Owners and operators of critical infrastructure must develop and implement risk-based standards for cybersecurity.

Sec. 2. Critical Infrastructure. As used in this Order, the term "critical infrastructure" means any physical or virtual system, whether physical or virtual, so vital to the United States that the incapacity or destruction of such system would have a debilitating impact on national security, including economic, public health, or safety, or any combination of those matters.

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

February 12, 2013

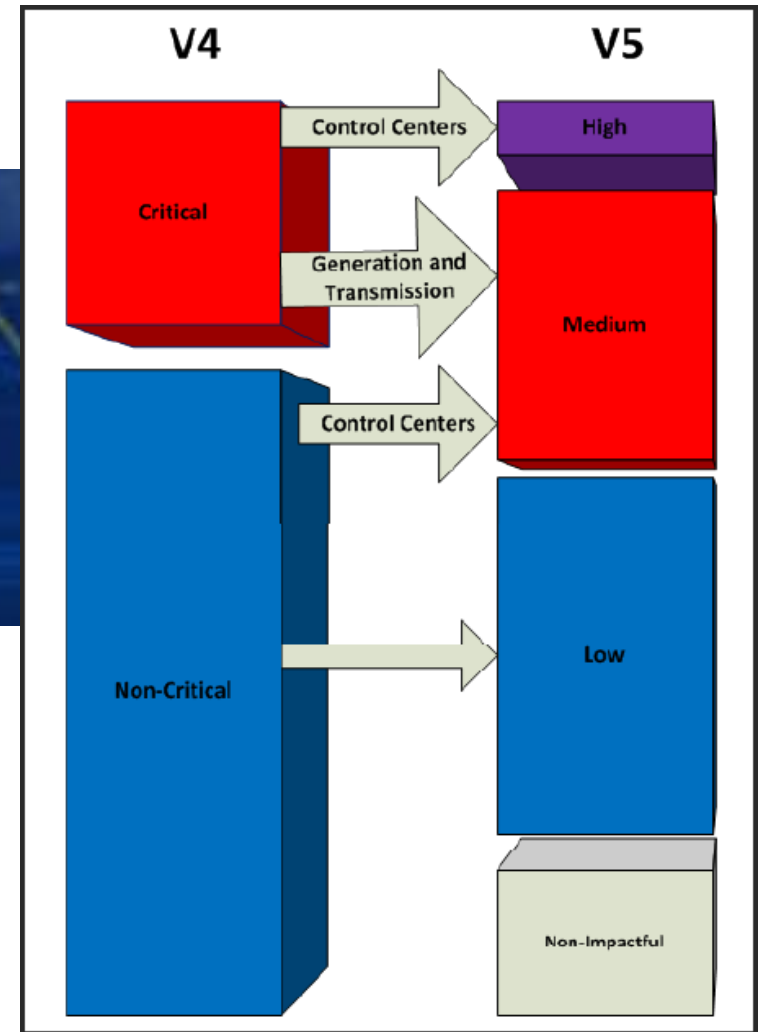
PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

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

dition on PPD-21, which provides guidance on the security and resilience of critical infrastructure.

NERC CIP Version 5



New and Continued Attacks

intelligentutility[®] WHERE THE SMART GRID MEETS BUSINESS AND REALITY

KN
INTELLIGENCE

[HOME](#) [NEWS & COMMENTARY](#) [CALENDAR](#) [RESOURCES](#) [MAGAZINE](#) [SUBSCRIBE](#)

MORE...

[SUBSCRIBE](#)

[Back Issues](#)

[Blogs](#)

[Case Studies](#)

[Commentary](#)

[Conferences](#)

[Home](#)

The Rise of Critical Infrastructure Attacks: Understanding the Privileged Connection and Common Thread

Yariv Lenchner | Aug 16, 2013

[Share / S](#)

Over the past two years, a growing number of headline-grabbing

THE CYBERCRIME ECONOMY

Hacker hits on U.S. power and nuclear targets spiked in 2012

By David Goldman @DavidGoldmanCNN January 9, 2013: 1:41 PM ET



E-Newsletters

Intelligent Utility Update info...

Your email address:



ALL TECH - ALL THE TIME

CYBERSECURITY

[Computing](#) [Internet](#) [IT](#) [Mobile Tech](#) [Reviews](#) [Security](#) [Technology](#) [Tech Blog](#)

[TechNewsWorld](#) > [Security](#) > [Cybersecurity](#) | [Next Article in Cybersecurity](#)

DHS Raises Alarm Over Cyberattacks on Critical Infrastructure



By Richard Adhikari
TechNewsWorld
05/13/13 2:15 PM PT

Private companies in the energy industry, as well as those providing critical infrastructure services like electricity and water, have been put on notice -- watch

A A Text Size
[Print Version](#)
[E-Mail Article](#)



[Newsletters](#)

[Most Popular](#)

[advertisement](#)

[OpManager Li](#)

[workise.net](#)

New Philosophy – Assumption of Breach



SearchSecurity

News | Premium E-Books & E-Zines | Multimedia Security Topics | Tutorials | Expert Advice | White Papers | Blogs | Certification Central

Home > Topics > Enterprise Data Protection > Identity Theft and Data Security Breaches > Assumption of breach: How a new mindset can help protect critical data

Assumption of breach: How a new mindset can help protect critical data

Ernie Hayden, Contributor

As a security professional for more than 12 years and a frequent speaker at security conferences, I've seen the concept of "assumption of breach" under the hood of many security professionals.

eWEEK **SELF STORAGE** Sometimes one p...

MOBILE CLOUD SECURITY STORAGE ENTERPRISE APPS INNOVATION

HOT TOPICS: Android Apple IT Management New Era Networks Slide Shows More

Security / Taking Heed to NSA's Assumption on Security Breaches Is Sound First Step

Taking Heed to NSA's Assumption on Security Breaches Is Sound First Step

By Wayne Rash | Posted 2010-12-17 | Email | Print

RELATED ARTICLES

- McAfee Buys Stonesoft to Bolster Content-

News Analysis: Real security depends on a belief that somebody, somewhere, will get into your network. The real question is, what do you do about it?

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





THANK YOU!

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