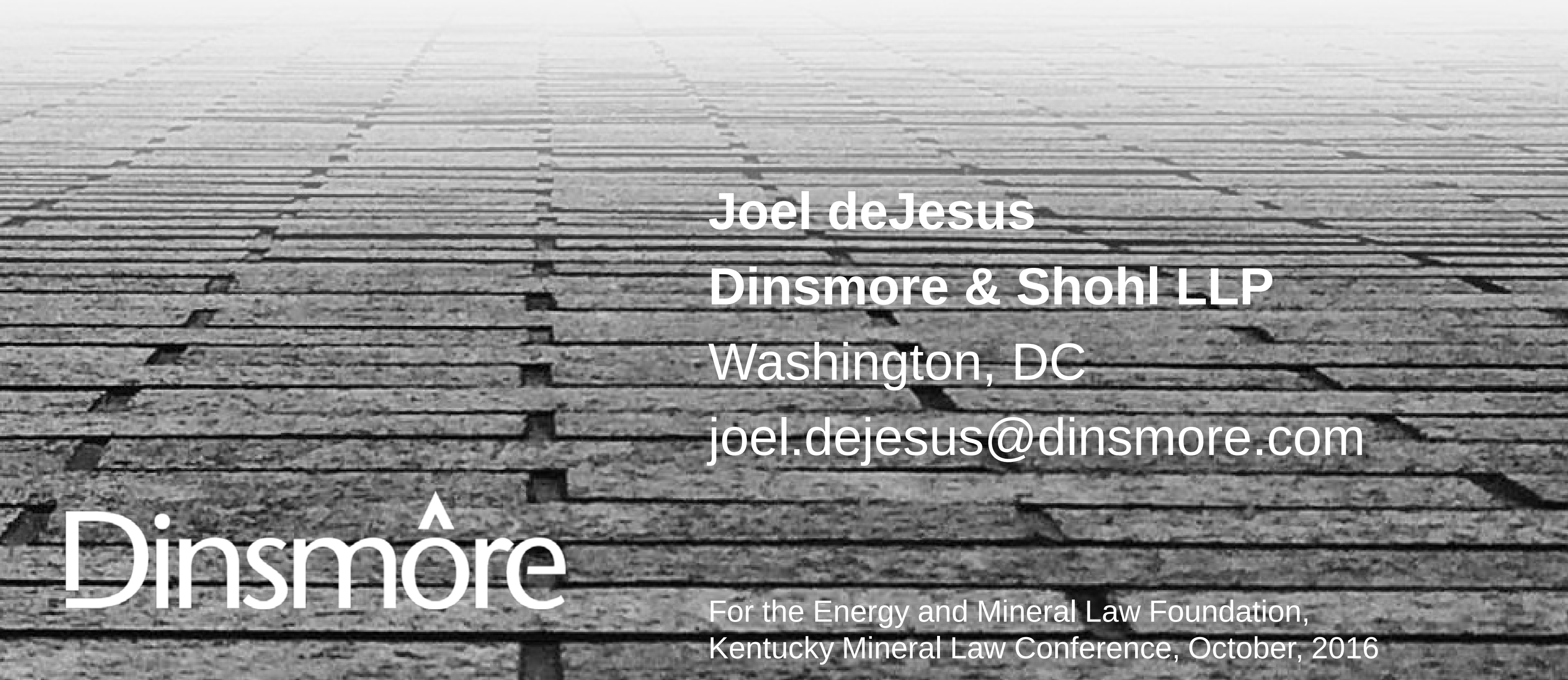
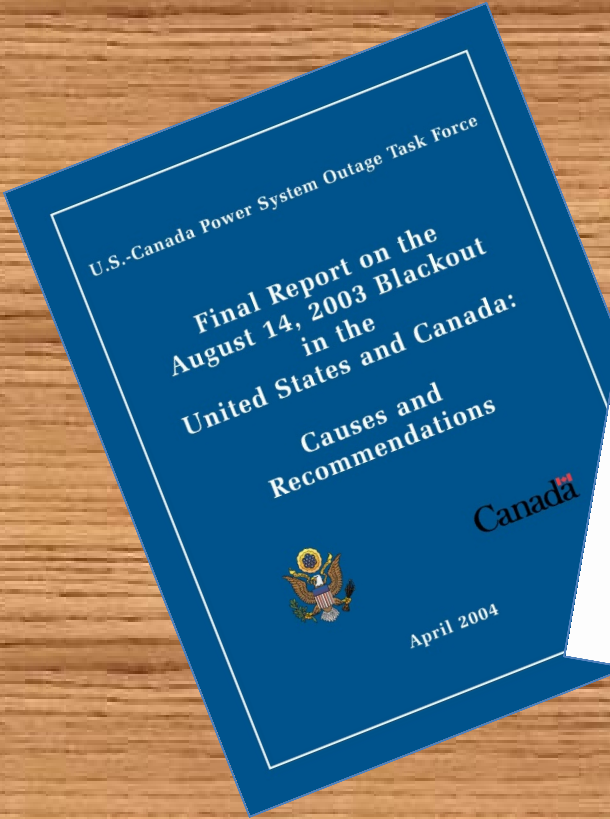
Cyber and Physical Security: Lessons Learned From the Electric Industry



Joel deJesus
Dinsmore & Shohl LLP
Washington, DC
joel.dejesus@dinsmore.com

For the Energy and Mineral Law Foundation,
Kentucky Mineral Law Conference, October, 2016



U.S.-Canada Power System Outage Task Force

Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations

Canada

April 2004

H. R. 6—348

(3) demonstrated responsiveness to workforce and training requirements in the electric power industry.

(c) Training and Continuing Education.—

(1) In general.—The Center shall provide training and continuing education in electric power generation, transmission, and distribution technologies and operations.

(2) Location.—The Center shall carry out training and education activities under paragraph (1)—

(A) at the Center; and

(B) through Internet-based information technologies that allow for learning at remote sites.

TITLE XII—ELECTRICITY

SEC. 1201. SHORT TITLE.

This title may be cited as the "Electricity Modernization Act of 2005".

Subtitle A—Reliability Standards

SEC. 1211. ELECTRIC RELIABILITY STANDARDS.

(a) In General.—Part II of the Federal Power Act (16 U.S.C. 824 et seq.) is amended by adding at the end the following:

"SEC. 215. ELECTRIC RELIABILITY.

"(a) Definitions.—For purposes of this section:

"(1) The term 'bulk-power system' means—

"(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

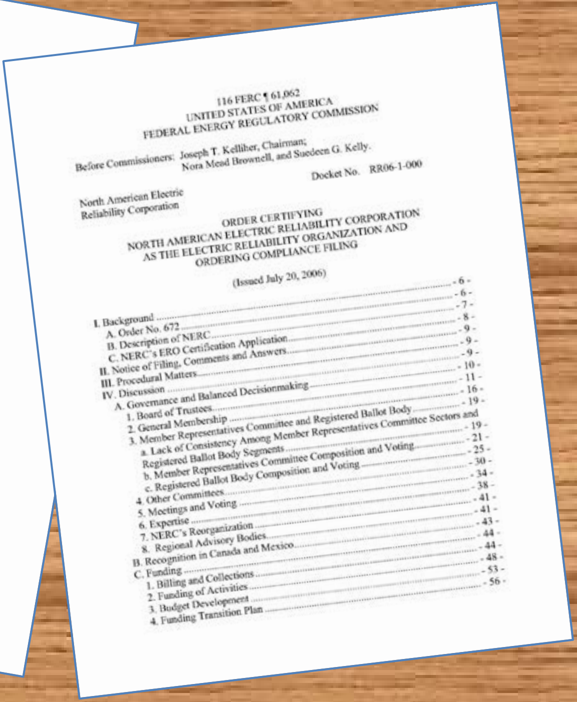
"(B) electric energy from generation facilities needed to maintain transmission system reliability.

The term does not include facilities used in the local distribution of electric energy.

"(2) The terms 'Electric Reliability Organization' and 'ERO' mean the organization certified by the Commission under subsection (c) the purpose of which is to establish and enforce reliability standards for the bulk-power system, subject to Commission review.

"(3) The term 'reliability standard' means a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.

"(4) The term 'reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.



116 FERC ¶ 61,062
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

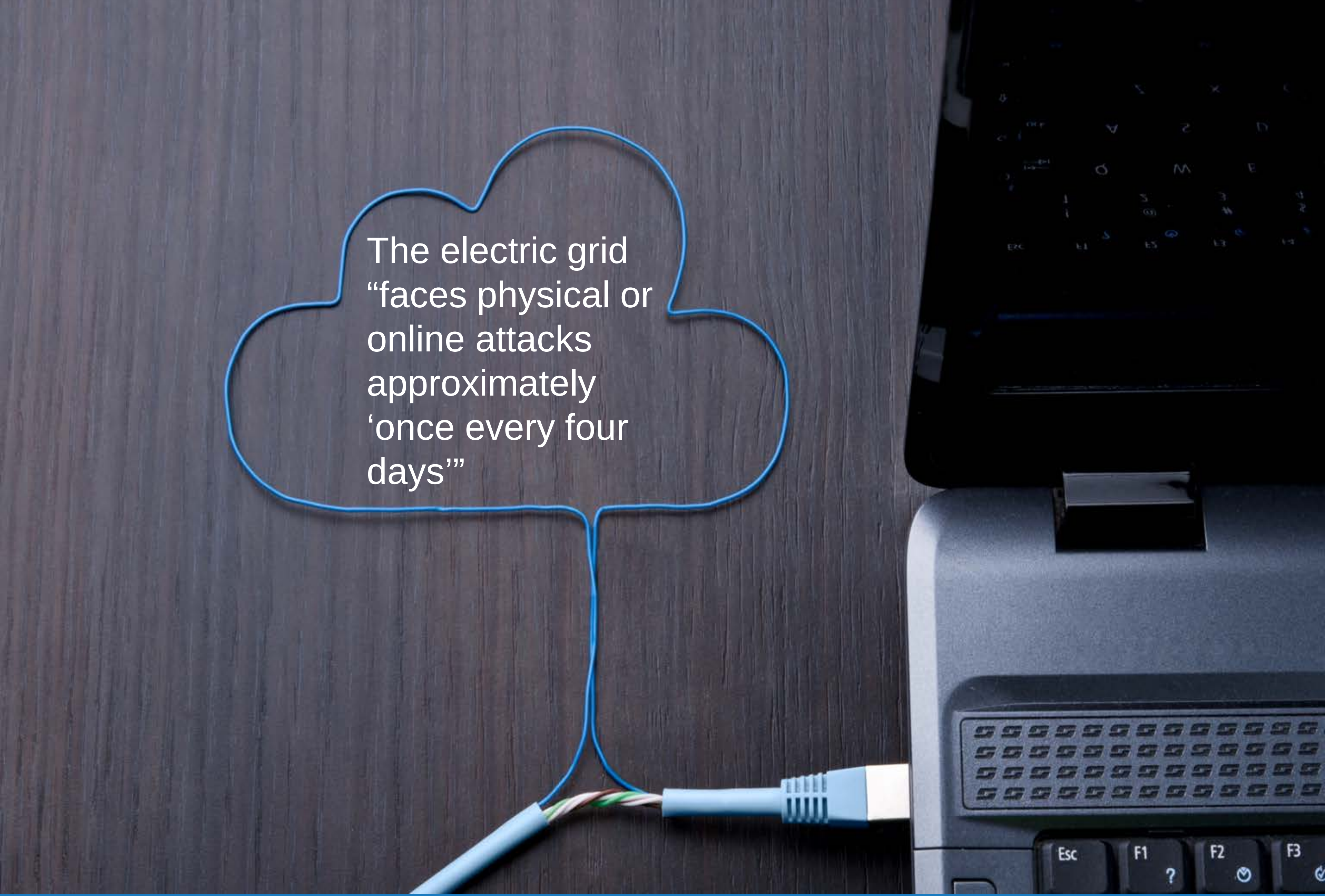
Before Commissioners: Joseph T. Kelliher, Chairman;
Nora Mead Brownell, and Suedeen G. Kelly.

North American Electric
Reliability Corporation

Docket No. RR06-1-000

ORDER CERTIFYING
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
AS THE ELECTRIC RELIABILITY ORGANIZATION AND
ORDERING COMPLIANCE FILING

(Issued July 20, 2006)



The electric grid “faces physical or online attacks approximately ‘once every four days’”

CIP Reliability Standards - Cybersecurity

- CIP-002 –Asset Identification/Categorization
- CIP-003 – Security Management Controls
- CIP-004 – Personnel & Training
- CIP-005 – Electronic Security Perimeters
- CIP-006 – Physical Security
- CIP-007 – Systems Security Management
- CIP-008 – Incident Reporting and Response
- CIP-009 – Recovery Plans
- CIP-010 – Configuration Change Management
- CIP-011 - Information Protection

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DEPARTMENT OF ENERGY • FEDERAL ENERGY REGULATORY COMMISSION

CIP Standards Evolution – 7 Versions in 10 years?

- 2003 – **Urgent Action 1200** – Voluntary pre-ERO cybersecurity standards
- 2008 – **Version 1** – First set of mandatory CIP standards approved (Order No. 706)
- 2009 – **Version 2** – Eliminated “reasonable business judgment” and “acceptance of risk” criteria; added rigor in critical cyber asset identification

CIP Standards Evolution – 7 Versions in 10 years?

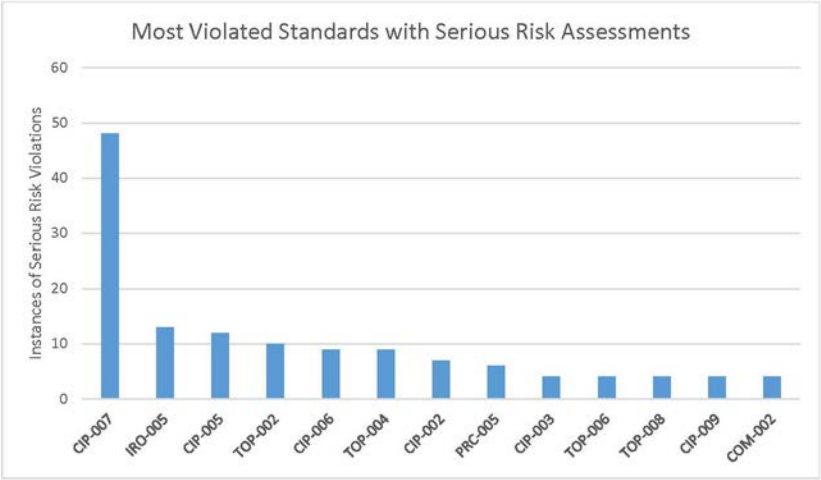
- 2010 – Version 3 –Addressing FERC directives to clarify standards and implementation plans
- 2012 – Version 4 – Added “bright line” criteria for identifying critical cyber assets (Order No. 761)
- 2013 – Version 5 – Shifted from critical cyber assets to BES Cyber Systems; added configuration change management (Order No. 791)

CIP Standards Evolution – 7 Versions in 10 years?

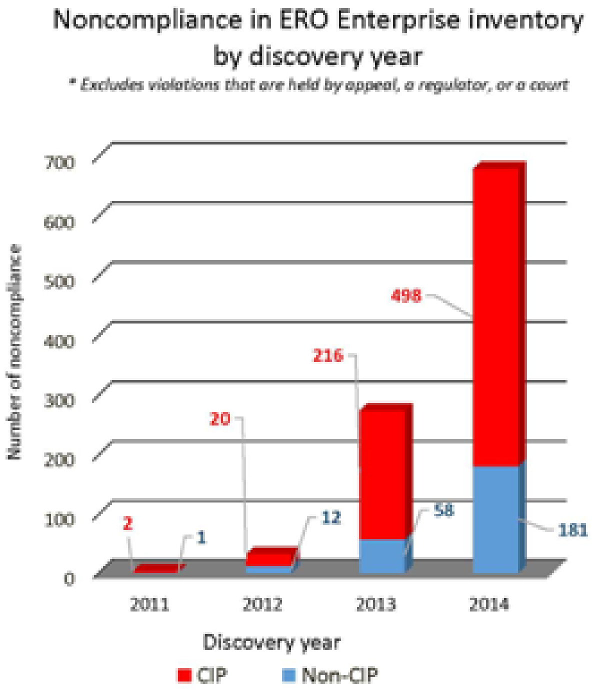
- 2015 – **Physical Security** and CIP-014
- 2016 – **“Revisions to Version 5”** – Eliminated “identify, assess, and correct” language; enhanced security controls for Low Impact assets; addressed transient devices and nonprogrammable components of communications networks
- 2017 – **Supply chain risk management standard?** (Order No. 829)

Enforcement of CIP Standards

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Source: NERC Compliance Monitoring and Enforcement Program Quarterly Update, Q3 2015

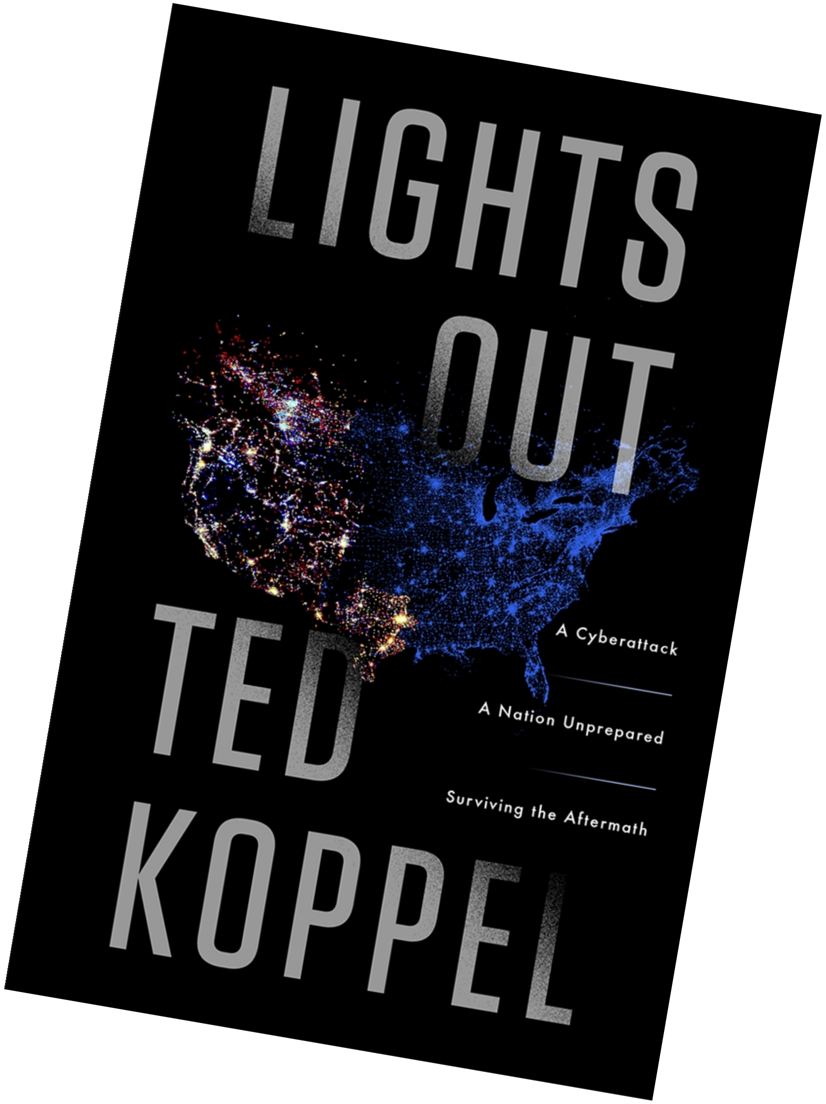


Source: NERC, Key Compliance Enforcement Metrics and Trends, February 11, 2015

Physical Security

Physical Security?

“While cyberattack is the most serious threat to our electric power system and is the primary focus of this book, it is not the only threat”



Physical Security?

Matt Farrell: You just killed a helicopter with a car!
John McClane: I was out of bullets.

- *Live Free or Die Hard (2007)*

Metcalf Substation
California, April 16, 2013

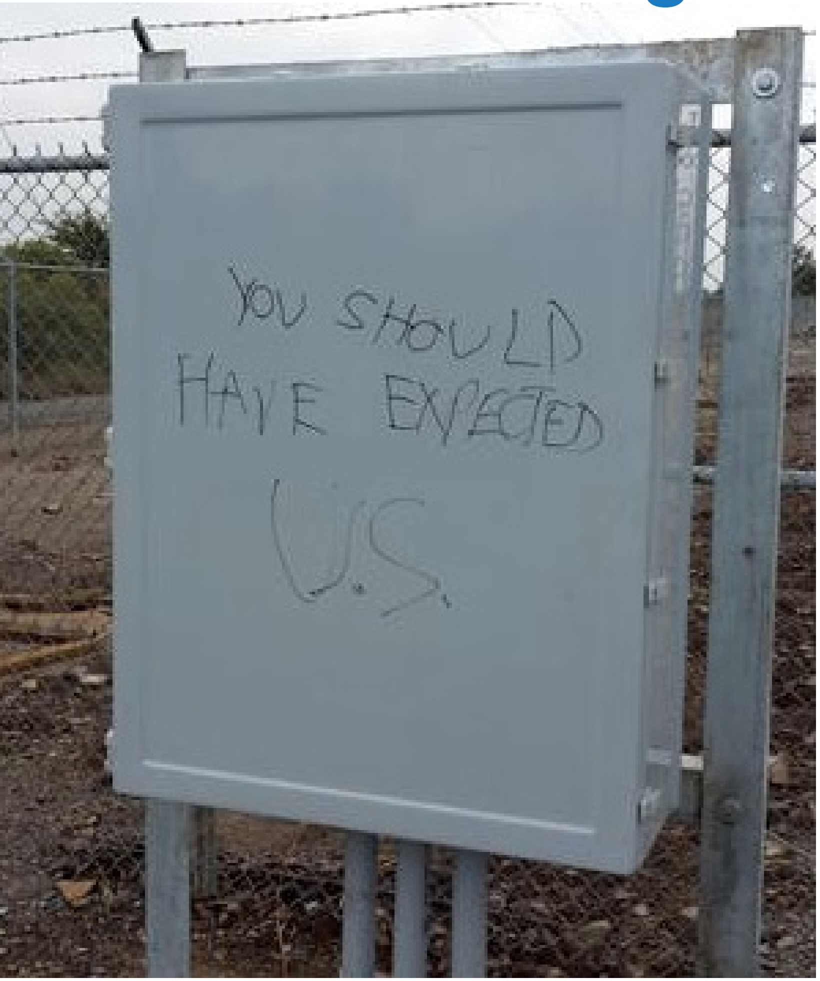
- Coordinated attack
- Nearby fiber optic cables cut
- >100 shell casings from AK-47s
- 17 transformers damaged
- 52,000 of oil leaked
- $15 million damage
- Still under investigation

Metcalf Substation
California, April 16, 2013

The Metcalf incident was “the most significant incident of domestic terrorism involving the grid that has ever occurred.”

– “Assault on Power Grid Raises Alarms,” *WSJ*, February 5, 2014

Arkansas – August/September 2013



- Jason Woodring - acted alone
- Attempted to take down a 500 kV tower using a train
- Set fire to and destroyed an EHV switching station
- Cut down two power poles, which led to outage for approximately 9,000
- Pleaded guilty on March 2015

NERC and Physical Security

- January 2014 – Interviews by former FERC Chair Wellinghoff regarding Metcalf Incident
- March 7, 2014 – FERC ordered NERC to file a Physical Security Standard within 90 days
- May 23, 2014 - NERC filed proposed standard
- July 17, 2014 – FERC issued NOPR
- November 20, 2014 – FERC issued Order No. 802
- October 15, 2015 - CIP-014-1 Enforcement Date

CIP-014-1

R1 - Risk assessment

R2 - 3rd party verification of risk assessment

R3 - Coordination between TO and TOP

R4 - Evaluation of threats and vulnerabilities

R5 - Physical security plan

R6 - 3rd party review of evaluation and plan

Supply Chain Risk

Source: NERC Compliance Monitoring and Enforcement Program Quarterly Update: Q3 2015

Source: NERC, Key Compliance Enforcement Metrics and Trends, February 11, 2015

“Separately, we are concerned that changes in the bulk electric system cyber threat landscape, identified through recent malware campaigns targeting supply chain vendors, have highlighted a gap in the protections under the CIP Reliability Standards. These malware campaigns represent a new type of threat to the reliability of the bulk electric system where malicious code can infect the software of industrial control systems used by responsible entities.”

Revised Critical Infrastructure Protection Reliability Standards, 80 Fed. Reg. 43,354 (July 22, 2015), 152 FERC ¶ 61,054 (2015)

NOPR – Identified Risks

- Such supply chains are complex, globally distributed and interconnected systems that have geographically diverse routes and consist of multiple tiers of outsourcing.
- Supply chain risks may include the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices.

Supply Chain Risk Management - What is Really at Stake?

ICS-ALERT-14-176-02A – ICS focused malware campaign

- Software installers were infected with Havex Trojan
- 3 known ICS vendors
- Indicators of compromise to critical infrastructure owners and operators

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Supply Chain Risk Management
- What is Really at Stake?

ICS-ALERT-14-281-01E – Ongoing malware campaign compromising ICS

- Ongoing since 2011
- Variant of BlackEnergy malware (BE3)
- Various vendors have been targeted (GE Cimplicity, Advantech/Broadwin WebAccess and Seimens WinCC)
- 2016 Update: BE3 was present in Ukraine Attack

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Supply Chain Risk Management - What is Really at Stake?

E-ISAC, Analysis of the Cyber Attack on Ukrainian Power Grid (March 18, 2016)

- Spear Phishing/Theft of credentials
- Used VPNs from business network to enter ICS network
- Mitigation – Procurement/licensing of trusted hardware/software; network monitoring; strategic technology refresh

Order No. 829

- On July 21, 2016, FERC directed NERC to develop a standard within one year
- Four security objectives
  - Software integrity and authenticity
  - Vendor remote access
  - Information system planning
  - Vendor risk management and procurement controls

Order No. 829

Objective 1: Software Integrity and Authenticity

- Verify identity of software publisher
- Verify integrity of software and patches prior to installation
- Avoid “Watering Hole” Attack

Order No. 829

Objective 2: Vendor Remote Access

- Logging and controlling all third-party initiated remote access sessions
- User initiated and machine-to-machine remote access
- Theft of credentials and remote persistent connections were central to Ukraine Attack

Order No. 829

Objective 3: Information System Planning

- Include security considerations as part of IS planning
- Document role of CIP Senior Manager
- ICS-CERT
  - BlackEnergy Malware alert – “minimize network exposure for all control system devices/subsystems”
  - Ukraine incident – strategic technology refreshes

Order No. 829

Objective 4: Vendor Risk Management and Procurement Controls

- Verification of security concepts in future contracts
  - Security event notification and coordinated incident response
  - Personnel termination
  - Vulnerability disclosures

Order No. 829 - What is Really Required?

Software Integrity and Authenticity	→	CIP-007 R2 CIP-004 R3	+	Secure transmittal of patches Validate patch integrity
Vendor Remote Access	→	CIP-005 R2	+	Machine-to-machine logging Monitor/terminate sessions
Information System Planning	→	CIP-010	+	Procurement controls
Vendor Risk Management & Procurement Controls	→	Include security concepts in future contracts		

Voluntary Sharing

NationalCouncilofISACs
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
ONG-ISAC
DNG-ISAC
U.S. DEPARTMENT OF HOMELAND SECURITY
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER
NCCIC
ICS-CERT | NCC | US-CERT
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Argonne
NATIONAL LABORATORY
Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

ISACs

ISAOs, NCCIC, CISCP, AIS

CRISP

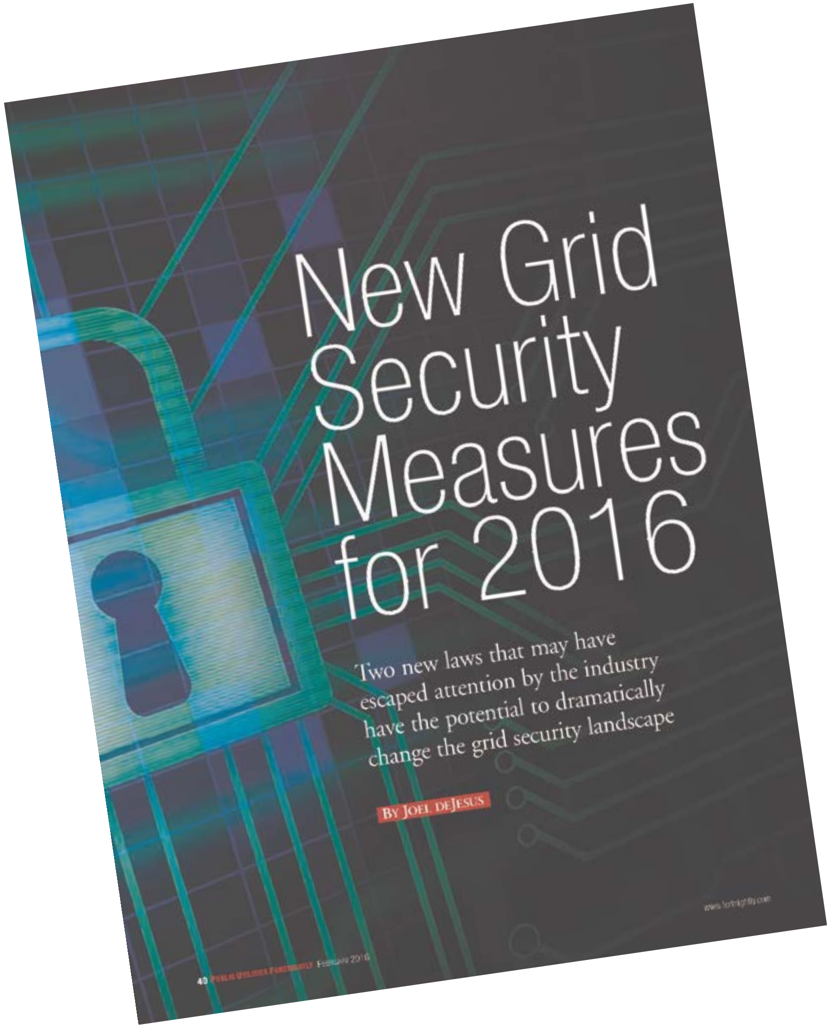
OEIS

Voluntary Sharing

- What type of information is being shared?
- Is the sharing performed manually or automatically?
- Who is responsible for screening for personally identifiable information?
- Are there liability protections for the “sharer” and the “receiver”?

Cybersecurity Information Sharing Act of 2015, Title I of the Cybersecurity Act of 2015, which was part of Consolidated Appropriations Act of 2016, 114 Pub.L. No. 113, 129 Stat. 2242.

Section 215A of the Federal Power Act, Section 61,003 of Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 129 Stat. 1312 (December 4, 2015)



New Grid Security Measures for 2016

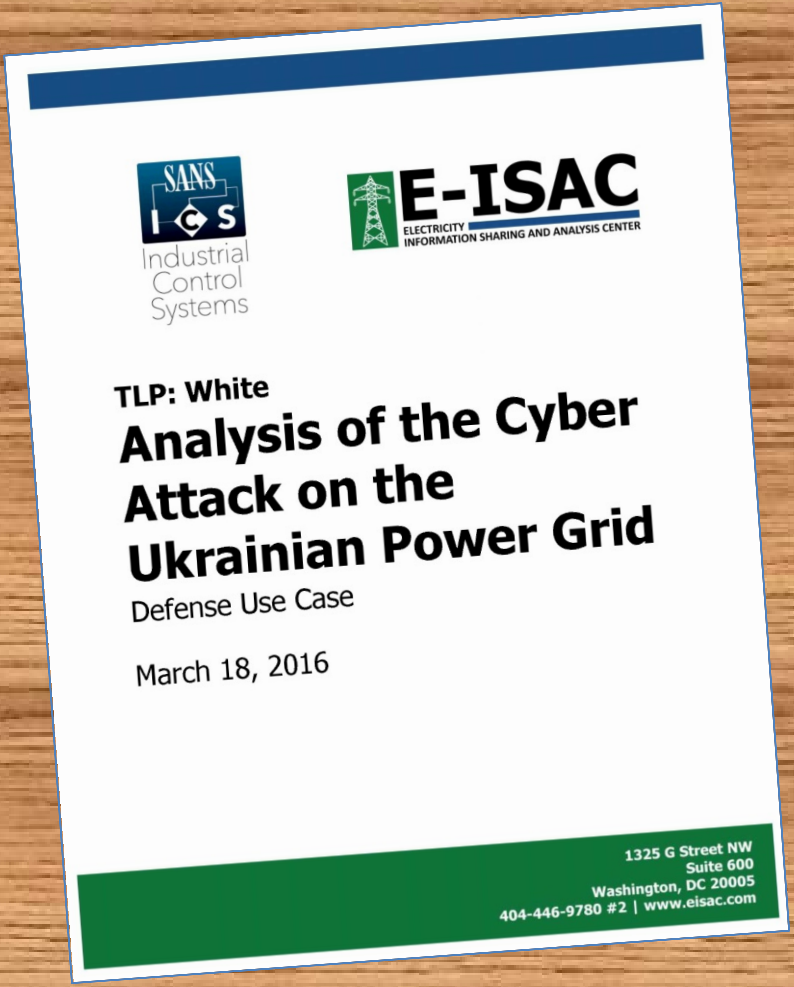
Two new laws that may have escaped attention by the industry have the potential to dramatically change the grid security landscape

By Joel deJesus

www.fortnightly.com

40 Public Utilities Fortnightly February 2016

Emerging Issues



SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

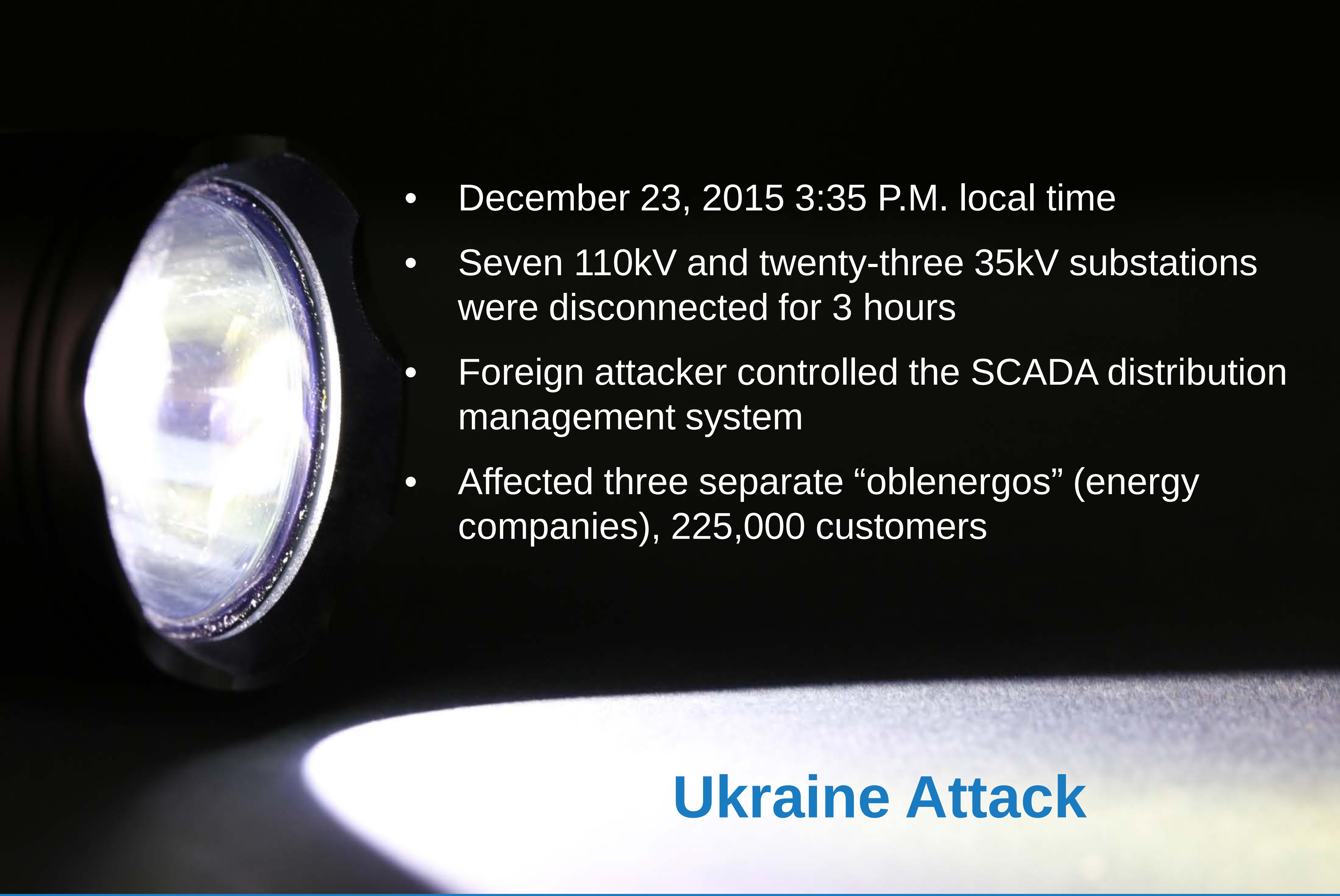
Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

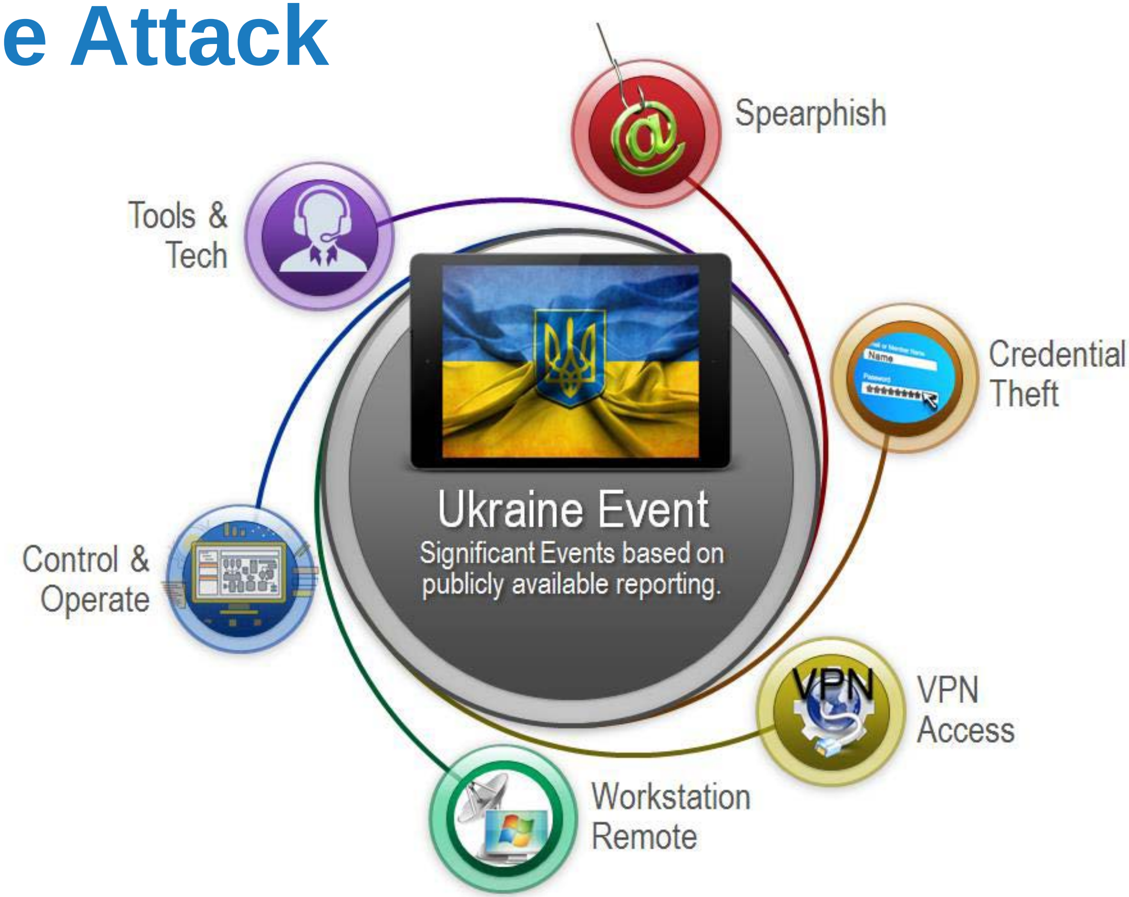
"The cyber attacks in Ukraine are the first publicly acknowledged incidents to result in power outages. As future attacks may occur, it is important to scope the impacts of the incident."



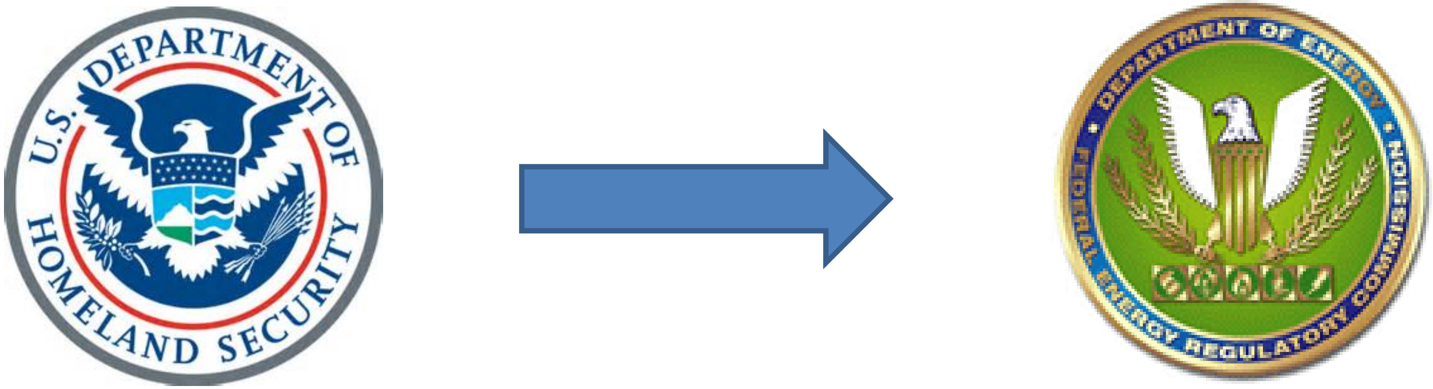
Ukraine Attack

- December 23, 2015 3:35 P.M. local time
- Seven 110kV and twenty-three 35kV substations were disconnected for 3 hours
- Foreign attacker controlled the SCADA distribution management system
- Affected three separate “oblenergos” (energy companies), 225,000 customers

Ukraine Attack



Response to Ukraine Attack

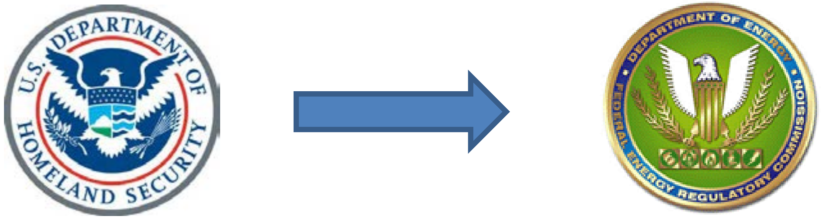

U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

DHS, ICS CERT IR-ALERT-H-16-056-01

(February 25, 2016)

Response to Ukraine Attack: Supply Chain Risk Management

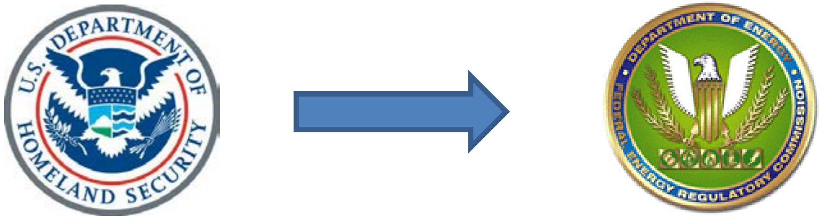
“The first, most important step in cybersecurity is implementation of information resources management best practices. Key examples include: procurement and licensing of trusted hardware and software systems; knowing who and what is on your network through hardware and software asset management automation; on time patching of systems; and strategic technology refresh.”


U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY • FEDERAL ENERGY REGULATORY COMMISSION

Response to Ukraine Attack: Application Whitelisting

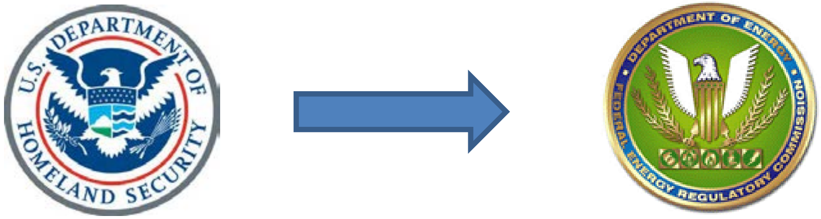
“Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by malicious actors. The static nature of some systems, such as database servers and HMI computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.”

FERC NOI re Cyber Systems in Control Centers, 156 FERC ¶ 61,051 (July 21, 2016)


U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY • FEDERAL ENERGY REGULATORY COMMISSION

Response to Ukraine Attack: Isolation

“Organizations should isolate ICS networks from any untrusted networks, especially the Internet. All unused ports should be locked down and all unused services turned off. If a defined business requirement or control function exists, only allow real-time connectivity to external networks. If one-way communication can accomplish a task, use optical separation (‘data diode’). If bidirectional communication is necessary, then use a single open port over a restricted network path.”


U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY • FEDERAL ENERGY REGULATORY COMMISSION

Beyond the Electric Industry

Voluntary Standards and Guidelines

AGA
American Gas Association

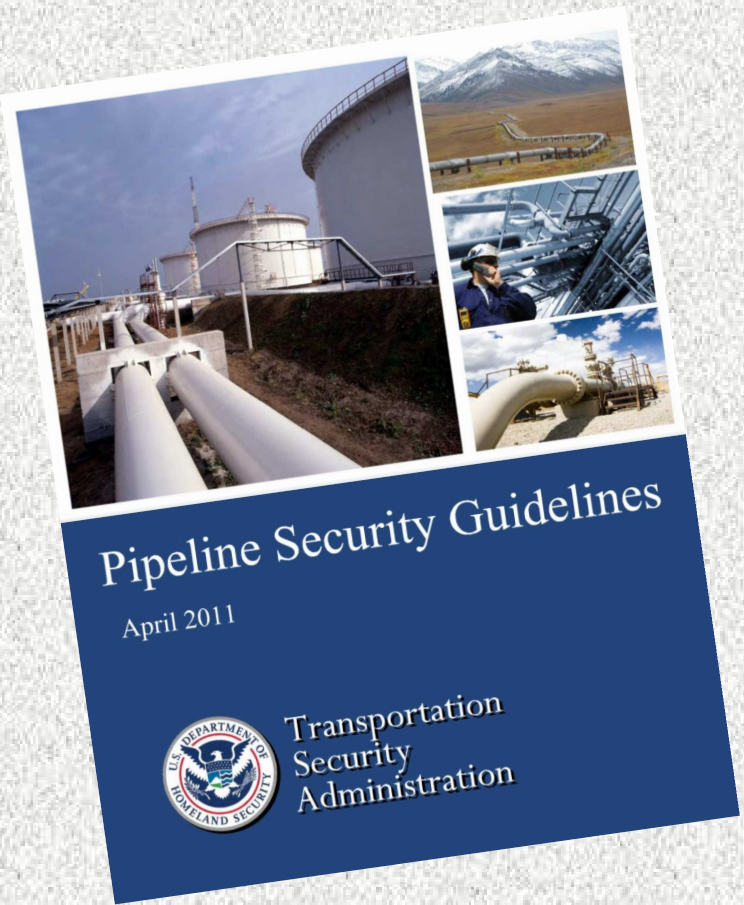
INGAA

energy API

U.S. DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

- "This document is guidance. It does not impose mandatory requirements on any person."
- Provides framework for:
    - o Corporate Security Plan
    - o Risk Analysis/Criticality
    - o Facility Security Measures
    - o Cyber Asset Security Measures
    - o National Terror Advisory System



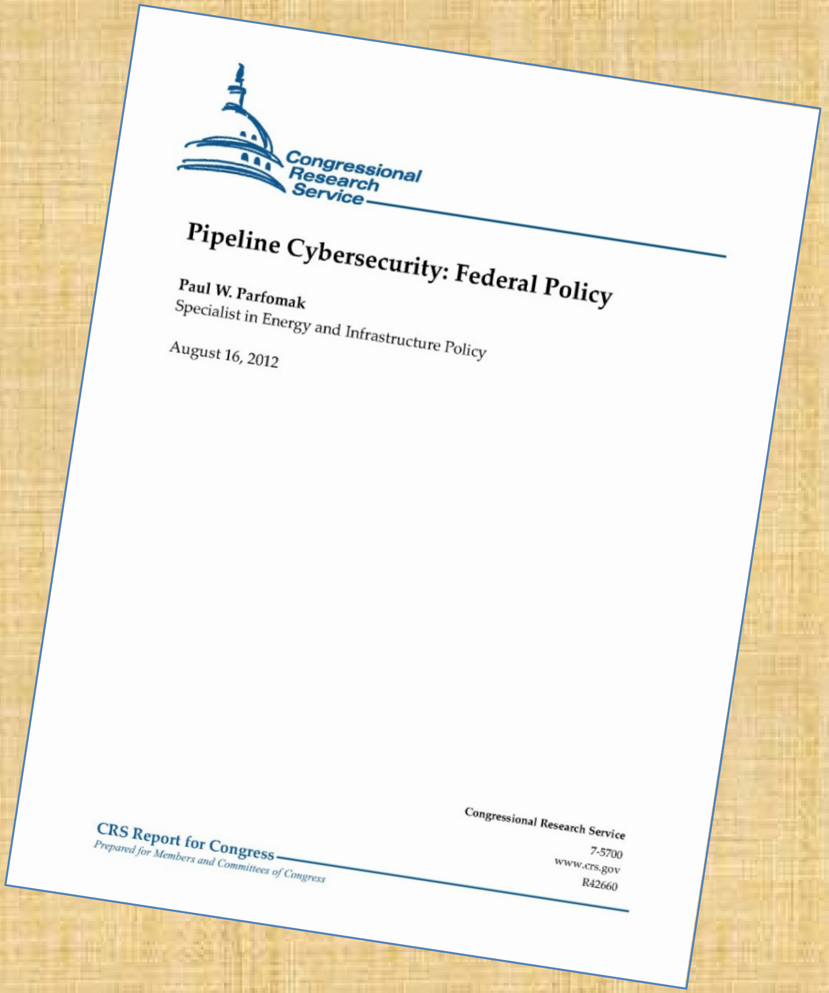
Pipeline Security Guidelines

April 2011

Transportation Security Administration

https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf

- TSA has statutory authority to promulgate pipeline physical and cybersecurity regulations
- TSA believes that voluntary standards are better, and is concerned that mandatory standards will reduce security
- Pipelines have been the target of attempted attacks and terrorist threats (Al Qaeda)
- Although no cyber attacks, there have been a number of SCADA-related incidents (inc. San Bruno)



Congressional Research Service

Pipeline Cybersecurity: Federal Policy

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

August 16, 2012

Congressional Research Service
7-5700
www.crs.gov
R42660

CRS Report for Congress
Prepared for Members and Committees of Congress

http://fas.org/sgp/crs/homesec/R42660.pdf

Pipelines Are Already Subject to

PHSMA Facility Security Regulations

- Security for LNG Facilities - 49 C.F.R. Part 193, Subpart J
- Security for Transportation of Hazardous Liquids by Pipelines- 49 C.F.R. §195.436

PHMSA
U.S. Department of Transportation
Pipeline and Hazardous Materials
Safety Administration
1203
3

Pipelines are Already Subject to

Voluntary Sharing

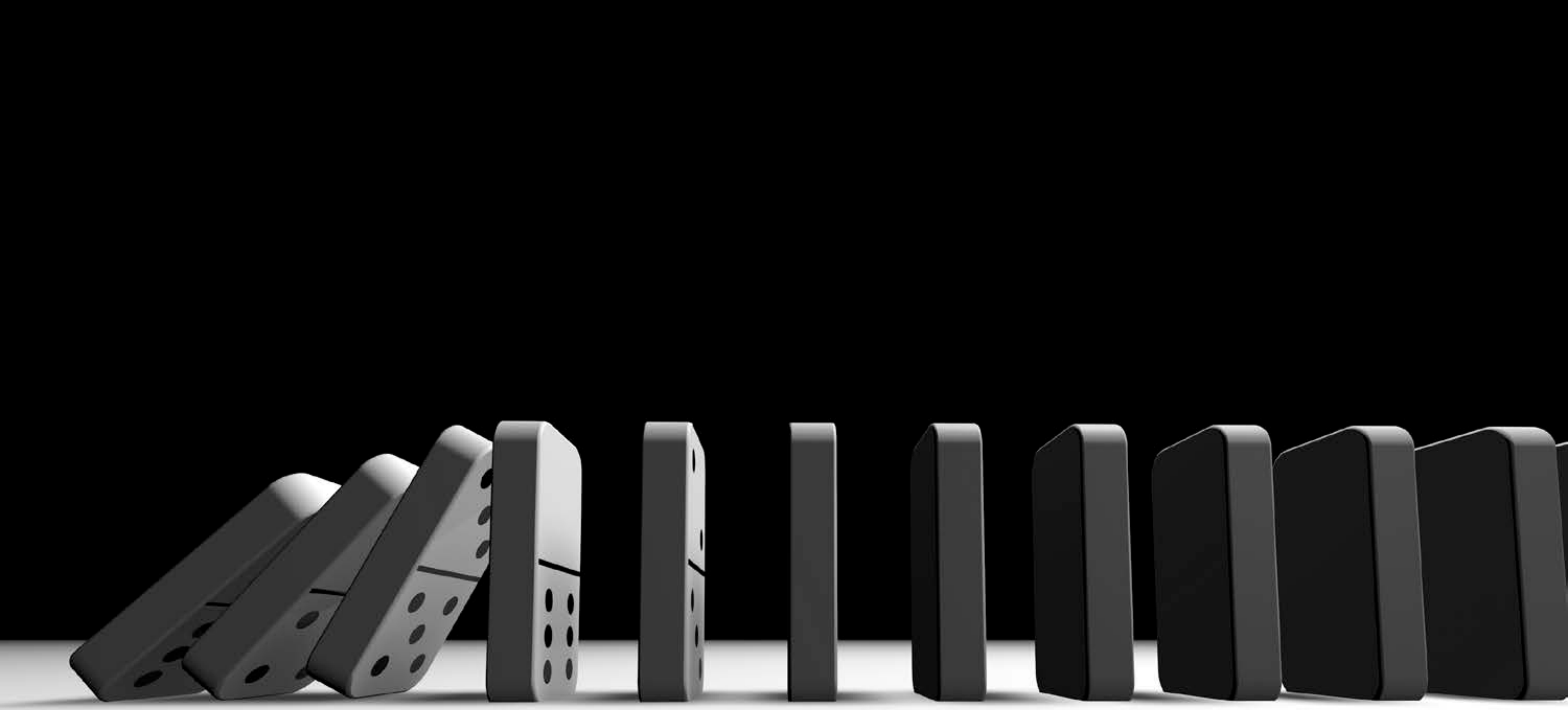
ONG-ISAC

NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER
NCCIC
ICS-CERT / NCC / US-CERT

DNG-ISAC

U.S. DEPARTMENT OF HOMELAND SECURITY
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Lessons Learned from the Electric Industry



Reactiveness

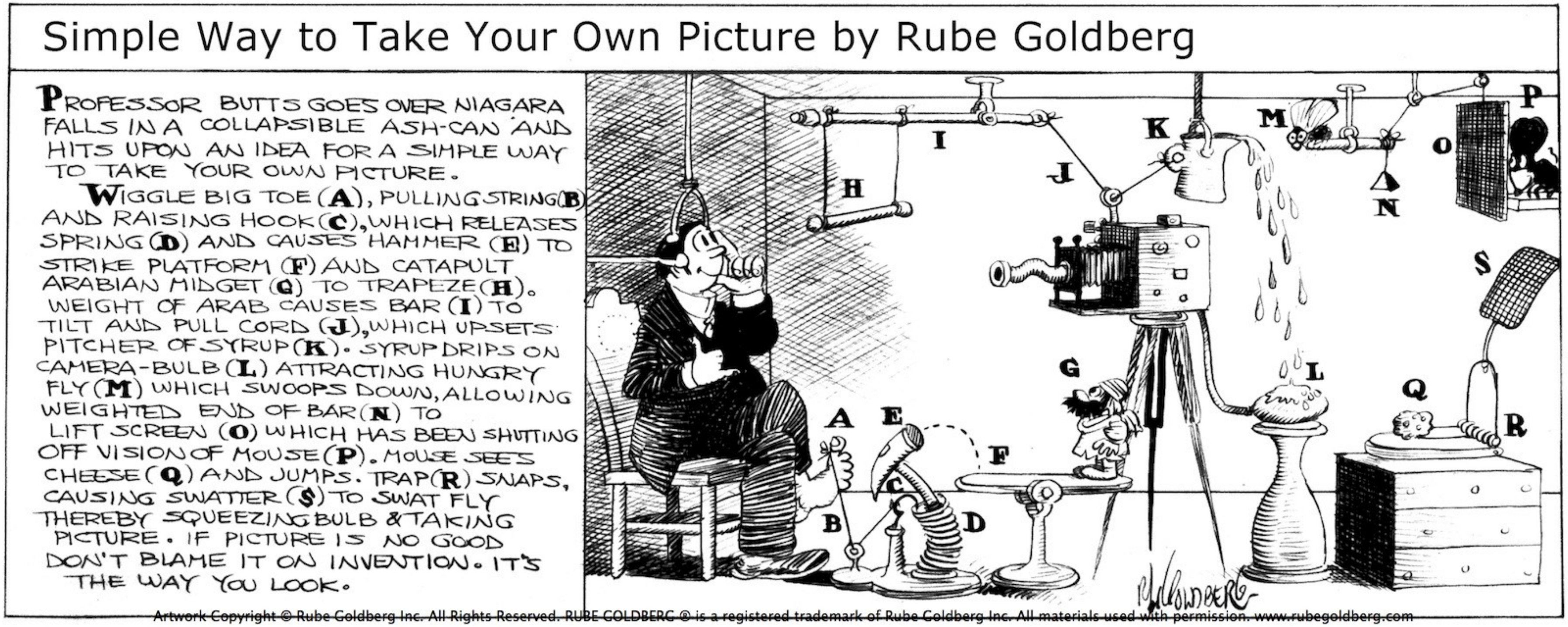
Scope Creep

- Voluntary Standards >> Mandatory Standards >> Voluntary Sharing
- Operational standards >> Security standards
- Cybersecurity >> Physical security
- Utility systems >> Supply chain
- ESPs and PSPs >> Isolation

Regulatory Uncertainty

Uniqueness Among Sectors

Familiar Process



Simple Way to Take Your Own Picture by Rube Goldberg

PROFESSOR BUTTS GOES OVER NIAGARA FALLS IN A COLLAPSIBLE ASH-CAN AND HITS UPON AN IDEA FOR A SIMPLE WAY TO TAKE YOUR OWN PICTURE.

WIGGLE BIG TOE (A), PULLING STRING (B) AND RAISING HOOK (C), WHICH RELEASES SPRING (D) AND CAUSES HAMMER (E) TO STRIKE PLATFORM (F) AND CATAPULT ARABIAN MIDGET (G) TO TRAPEZE (H). WEIGHT OF ARAB CAUSES BAR (I) TO TILT AND PULL CORD (J), WHICH UPSETS PITCHER OF SYRUP (K). SYRUP DRIPS ON CAMERA-BULB (L) ATTRACTING HUNGRY FLY (M) WHICH SWOOPS DOWN, ALLOWING WEIGHTED END OF BAR (N) TO LIFT SCREEN (O) WHICH HAS BEEN SHUTTING OFF VISION OF MOUSE (P). MOUSE SEES CHEESE (Q) AND JUMPS. TRAP (R) SNAPS, CAUSING SWATTER (S) TO SWAT FLY THEREBY SQUEEZING BULB & TAKING PICTURE. IF PICTURE IS NO GOOD DON'T BLAME IT ON INVENTION. IT'S THE WAY YOU LOOK.

Reliability & Security

Let's *Accomplish* more.SM Together.