Ohio | Public Utilities Commission






Cybersecurity in the Energy/Utility Sectors

Hon. Todd Snitchler
Chairman

Thomas Pearce
Senior Utility Specialist
Chair, NARUC Staff Subcommittee on Critical Infrastructure

Thursday, March 21, 2013
Ohio Gas Association Technical Seminar

Agenda

Purpose: to provide an introduction to issues, concepts, and vocabulary to facilitate action

- What is cybersecurity?
- Threats
- Principles of preparedness
- Role of government & regulators
- Where do we go from here?

Recent Headlines

- DHS: 40 percent of cyberattacks targeted energy sector (The Hill)
- Decoy ICS/SCADA Water Utility Networks Hit By Attacks (Dark Reading)

- U.S. Steps Up Alarm Over Cyberattacks (WSJ)
- Cyberattack leaves natural gas pipelines vulnerable to sabotage (CSMonitor)

- US Government Warns Over Vulnerable Control Systems (BBC)
- Obama Cybersecurity Order Lacks Bite, Security Experts Say (NetworkWorld)

- Cyber Threats To Energy Sector Happening At ‘Alarming Rate’ (WSJ)
- U.S. Homeland Chief: Cyber 9/11 Could Happen “Imminently” (Reuters)

- DHS Warns of Password-Cracker Targeting Industrial Networks (Nextgov)

Recent Headlines (cont'd)

- DHS Warns of Password-Cracker Targeting Industrial Networks (Nextgov)

- Malicious Virus Shuttered U.S. Power Plant – DHS (Reuters)
- Federal Reserve Hacked (Guardian UK)
- Hackers in China Attacked the NY Times For Last 4 Months (NYTimes)

- China Hacked the Wall Street Journal, Too (The Atlantic Wire)
- Chinese Army Unit Is Seen As Tied To Hacking Against U.S. (NYTimes)

- One-Third of Cyber Attack Traffic Originates in China, Akamai Says (Bloomberg)
- Nations Prepare For Cyber War (CNN)
- Hacktivist Campaigners Claim To Have Stolen Accounts From A Number Of Organizations Including NASA, The Pentagon And The Federal Reserve (ZDNet)

Cybersecurity

- What is it?
  - National Institute of Standards and Technology (NIST):

    "The ability to protect or defend the use of cyberspace from cyber attacks."

Cybersecurity

- "I think information sharing is a top priority."
  - Hon. Cheryl LaFleur, Commissioner, Federal Energy Regulatory Commission, when questioned about cybersecurity, Tuesday, March 19, 2013, before the U.S. House of Representatives' Energy & Commerce Committee hearings on Gas/Electric coordination

Cybersecurity

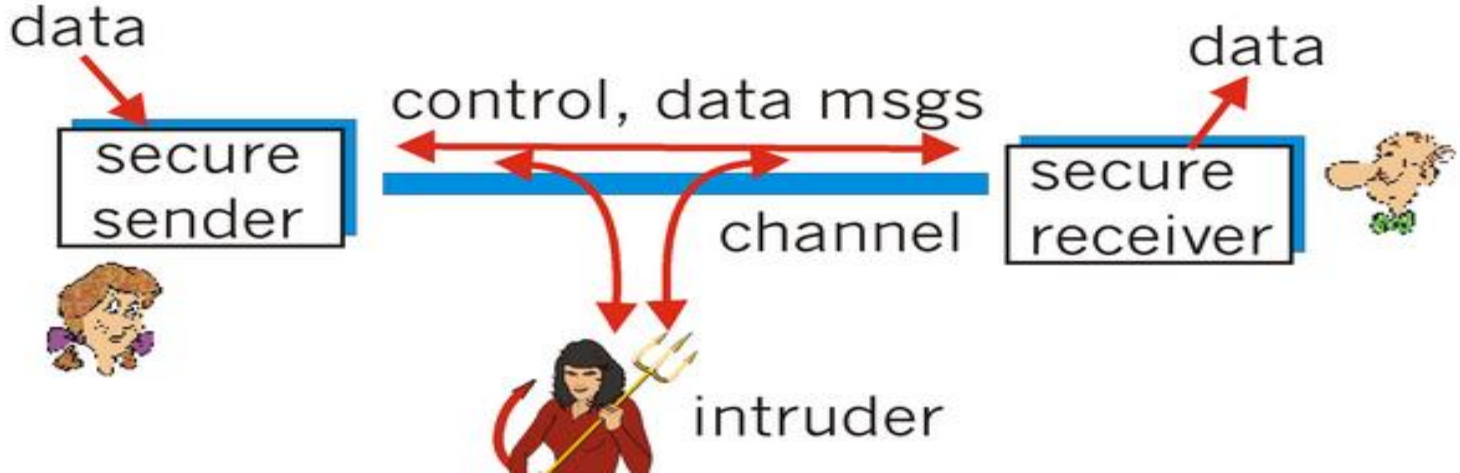
- There have been cyber attacks on systems that control plants being turned on/off; they are like FERC – fuel neutral. We need to guard against risks to energy management systems, wherever they are.
  - Hon. Cheryl LaFleur, March 19, 2013 testimony to House Energy & Commerce Committee

Cybersecurity

- Isn't just stopping bad guys…
- Vulnerabilities include:
  - Software bugs
  - User errors
  - Control system equipment malfunctions
  - Communications equipment failures
- Deliberate intrusions and sabotage

Information Security 101

- Devices generate & transmit data; converted to intelligence; someone or something takes action based on that intelligence
- Being "smarter" introduces new vulnerabilities that need to be managed
- Connectivity: how systems talk to each other can be exploited and should be protected at each stage of communication



Information Technology Systems

- Corporate IT/business systems
- Industrial Control Systems/Supervisory Control And Data Acquisition (ICS/SCADA)
  - (SCADA – e.g., power generation, gas transmission, water treatment, telecommunications)

Current Topics & Trends

- Vulnerabilities
- Increasing threats
  - Stuxnet, Duqu, Gauss, Flame, miniFlame, Shamoon

- Types of actors

- Types of threats
- SmartGrid






Shodan

- Have you heard of it?
- What is it?

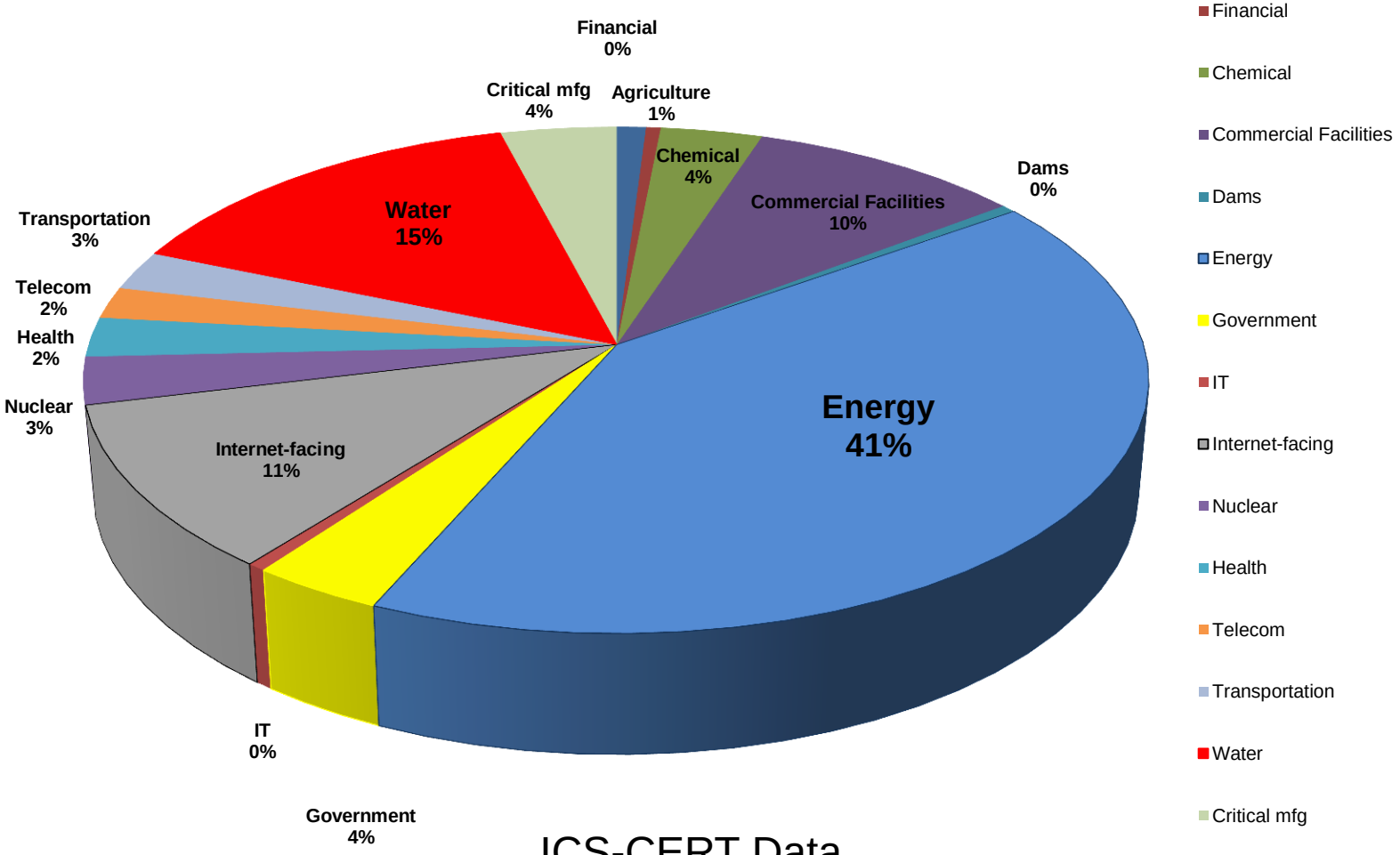
- Who? John Matherly
- There's an app for that

SHODAN

Ohio | Public Utilities Commission

THREAT LANDSCAPE

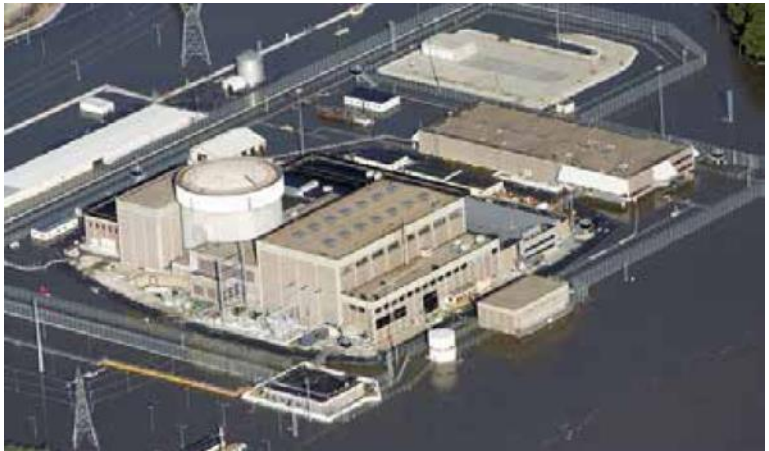
Incidents By Sector FY2012



ICS-CERT Data

Ohio | Public Utilities Commission

Cybersecurity is one element of all-hazards preparedness



Implications for Utilities

- Delivery of services
  - Reliability (& $)

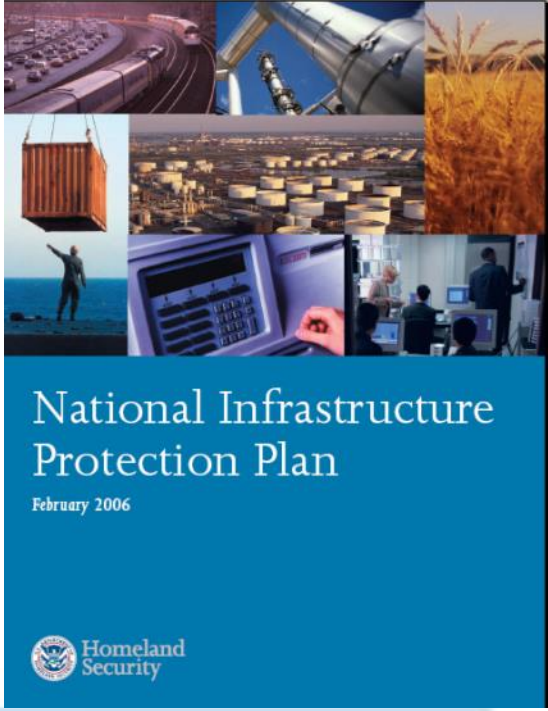
- Industry actions & response
  - OGA
  - AGA: ONG SCC & CSWG (Denbow)

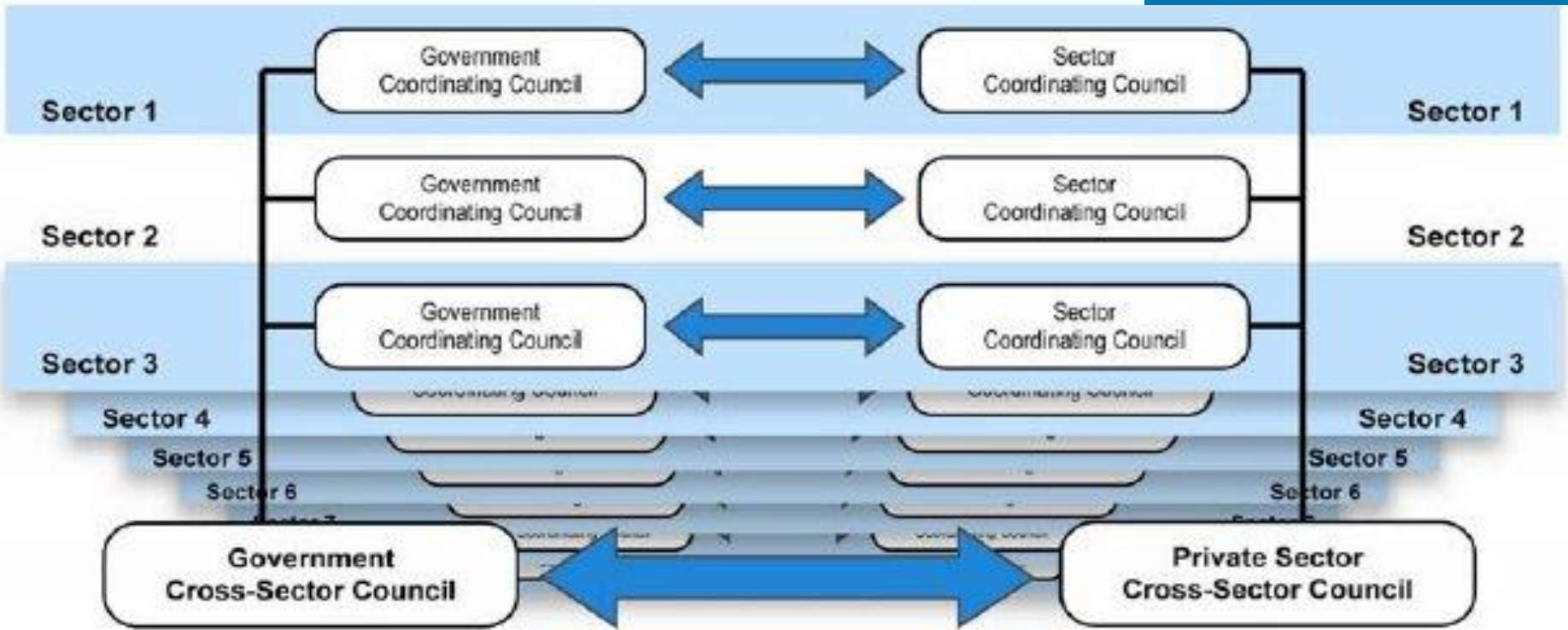
Industry Actions & Response

- NIST/SGIP CSWG
- NERC
- AGA
- ONG SCC

National Infrastructure Protection Plan (NIPP)

Sector Partnership Model





Some Government Actions & Response

- NIST/SGIP CSWG
- U.S. Department of Homeland Security:
  - National Cyber Security Division (CSET Tool, US-CERT/ICS-CERT, ICSJWG)
  - ICS-CERT fly-away teams (Springfield MO water utility)
  - ICS-CERT "Active Cyber Campaigns Against the U.S. Energy Sector" Briefings (9 conducted @ US late fall 2012)
- U.S. Department of Defense: CyberComm

Government Actions & Response (cont'd)

- U.S. Department of Energy:
  - Cybersecurity for Energy Delivery Systems (CEDS)
  - Roadmap to Achieve Energy Delivery Systems Cybersecurity 2011
  - Cross-Sector Roadmap for Cybersecurity of Control Systems
  - The Vulnerability Analysis of Energy Delivery Control Systems - 2011
  - Guide to Developing a Cyber Security and Risk Mitigation Plan
  - ESC2M2 (Elec. Sector Cybersecurity Capability Maturity Model)
  - NESCO (Nat'l Electric Sector Cybersecurity Org)

Issues of Preparedness

- Assessments
  - Equipment
  - Policies: do you have a formal written employee internet security policy?

- Responses/action plans
  - **Do you have a cyber element/plan?**

- Standards
- Information sharing

What is a control system?

Biological Metaphor:	Eyes, ears	Hands, feet, muscles	Ganglia, nerve bundles	Spinal cord	Brain
	Sensor	Control Valve	Programmable Logic Controller	Communication Devices and Protocols	Human Machine Interface

Aurora & Stuxnet

- Aurora: DHS/DOE experiment to hack generator control system
- Stuxnet: computer worm targeting Mid-East nuclear infrastructure

Some Things You Can Do

- Know what you need to protect
- Enforce strong password policies

- Map out a disaster preparedness plan

- Encrypt confidential information

- Use a reliable security solution
- Protect information completely
- Stay up to date
- Educate employees

Roles of State Commissions

- ***Cost recovery*** guidelines – investment prudence
- ***Sensitive information*** – develop handling protocols

- Rapid ***information sharing*** methods

- Review utility ***emergency response plans***
- Regulatory oversight of ***reliability***

- Promote ***State emergency planning*** efforts
- Understand ***interdependencies***
- Engage in ***regional coordination*** and response

Some State Actions Regarding Cybersecurity

- NARUC: *Cybersecurity for State Regulators*
- State level actions:
  - MO PSC: current review and formal dialogue with state utilities
  - PA PUC: annual certification process; dialogue with state utilities
  - CPUC: SmartGrid & SGIP CS,
  - OH PUC: informal dialogue with state utilities
  - TX PUC: SmartGrid & SGIP CS; work w/ERCOT

Ohio Partnerships

- Chairman Snitchler: Co-Vice-Chair, NARUC Committee on Gas
- Thom Pearce: Chair, NARUC Staff Subcommittee on Critical Infrastructure
- Congress: Sens. Portman & Brown, Reps. Latta & Stivers, among others
- Federal agencies: DHS (including ICSJWG), DOE, FCC, DoD
- U.S. CIPAC member
- Energy GCC (w/ONG SCC)

Ohio Partnerships

- DOE CEDS Program Evaluation Panel
- DOE Labs: INL, PNNL, SNL
- OHS:
  - SAIC weekly briefings; monthly classifieds
  - OHSAC & CSWG
- DHS PSAs: Pat Shaw/Jim Emery
- DHS CSA
- NAESB Advisory Council & Cyber Task Force

Ohio | Public Utilities Commission

Private & Public Sector Responsibilities

- Cyber secure utility operations: utilities
- Defend against nation-state cyber attacks: national defense & law enforcement
- Effective cybersecurity: utility/regulator/federal partners

Where Do We Go From Here?

- [Dialogue/discussion]

Ohio | Public Utilities Commission

Questions?

Todd A. Snitchler, Chairman

Thomas Pearce, Senior Utility Specialist

thomas.pearce@puc.state.oh.us

614.466.1846