I. Meeting Packet

State of Florida
Public Service Commission
INTERNAL AFFAIRS AGENDA
Tuesday, August 9, 2016
1:30 PM
Room 105 - Gerald L. Gunter Building

---

1. ~~"Cybersecurity for State Utility Regulators" (Presentation and Report)~~
   ~~Miles Keogh – Director, Research Lab, National Association of Regulatory Utility Commissioners (NARUC)~~
   ~~(Attachment 1)~~

   NOTE: Speaker unable to attend.

2. Staff Briefing on the U.S. Environmental Protection Agency's Proposed Rule Addressing The Clean Energy Incentive Program
   (Attachment 2)

3. General Counsel's Report

4. Executive Director's Report

5. Other Matters

BB/ks

OUTSIDE PERSONS WISHING TO ADDRESS THE COMMISSION ON ANY OF THE AGENDAED ITEMS SHOULD CONTACT THE OFFICE OF THE EXECUTIVE DIRECTOR AT (850) 413-6463.

Attachment 1

Cybersecurity & the Florida PSC

Miles Keogh, Research Lab Director, NARUC

Aug 9, 2016

The Plan For Today

- Today's Purpose: to provide an introduction to issues, concepts, and vocabulary to help take action.

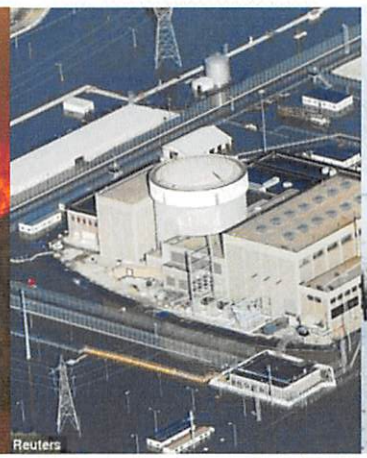
- Today's Agenda:
  I. What is cybersecurity?
  II. How does it affect utilities?
  III. What are the threats?
  IV. What does good security look like?
  V. Where do regulators fit?

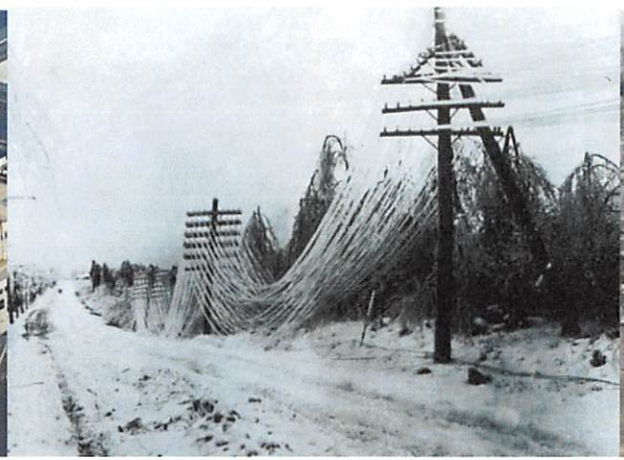
Infrastructure Protection is a risk management problem

- Enterprise risk management applies to any decision-making being made under conditions of uncertainty.
  - Financial risk
  - Regulatory risk
  - Critical Infrastructure protection risks:
    - An interruption to service, no matter what the origin, interrupts service.
    - An "all hazards" approach to preparedness helps deal with interruptions no matter the origin.

Risk management means considering a continuum:

Vulnerability: how prepared are we?
Threat: what could exploit the vulnerability?
Likelihood: how often does the event occur?
Consequence: how bad would it be?



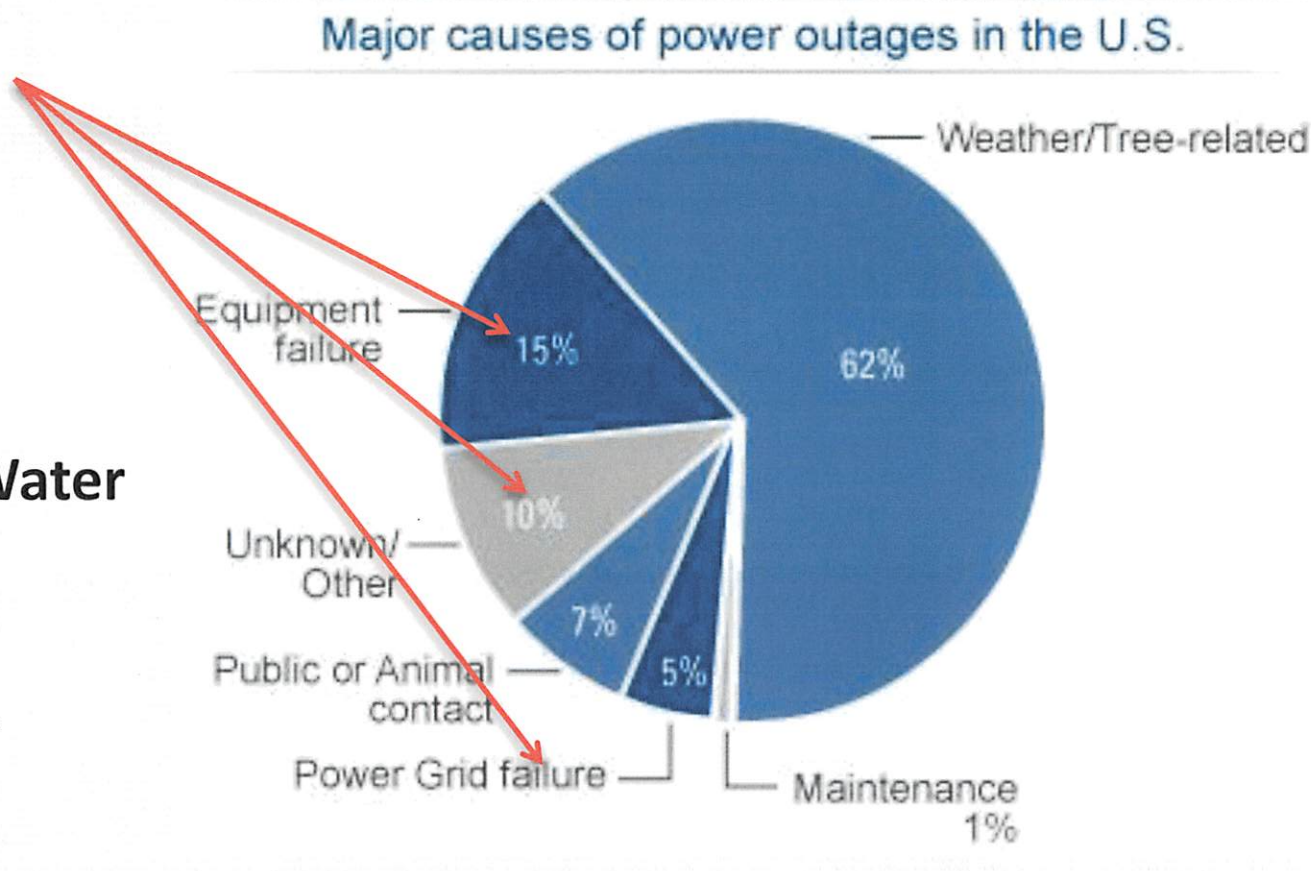


Ask the Audience!
What do you think is the biggest threat to electric service in the US?

Final Answer!

Cyber is mixed in here somewhere.

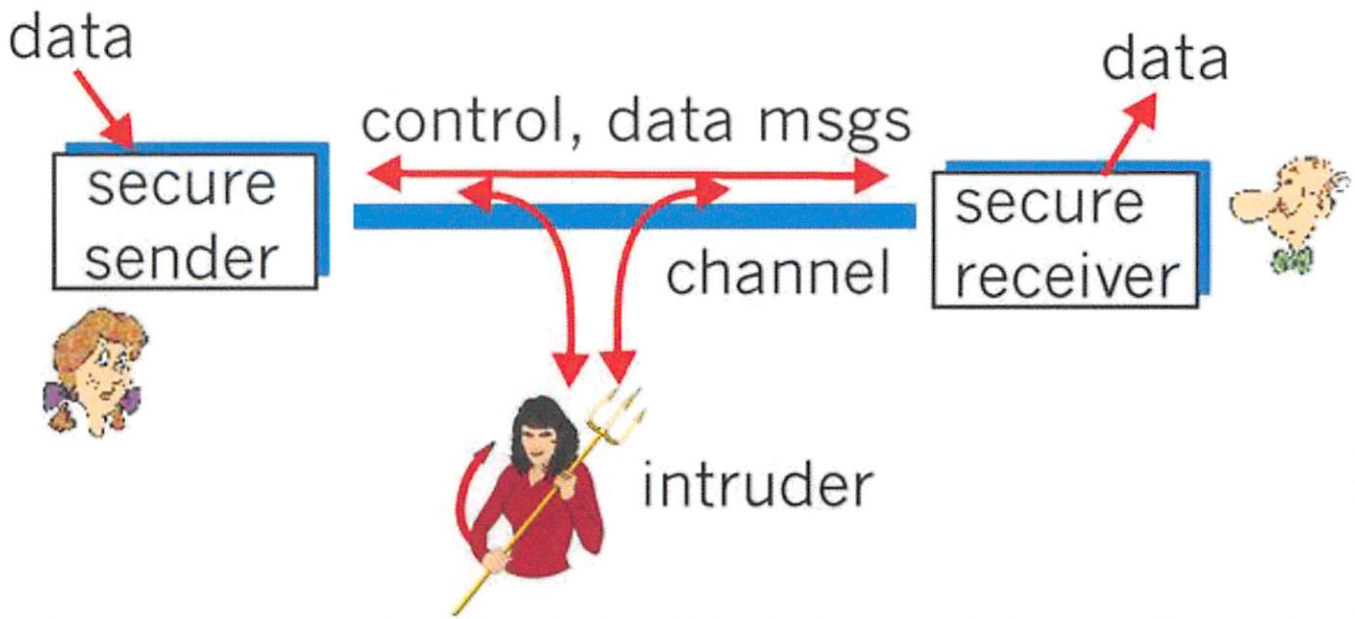
Power, Telco, Water and Gas have analogous, but different, risks.



What is cybersecurity?

"Cyber" just means "Connected"

- "Cyber" connectivity occurs when devices generate and transmit data.
- Data becomes intelligence when someone or something takes action based on that data.



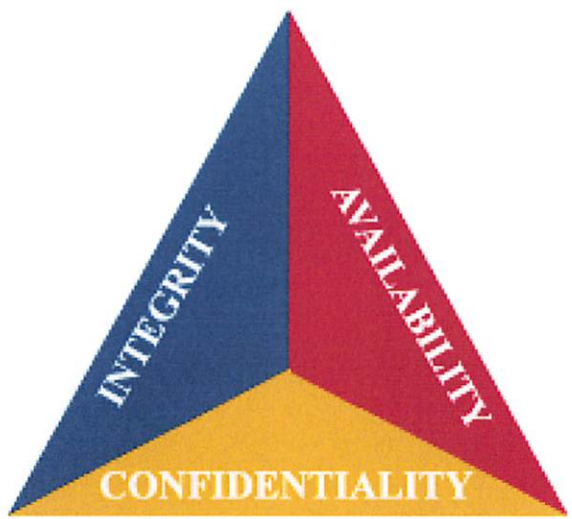
Information Security 101 (cont.)

- Traditional cybersecurity has focused on the C-I-A Triad – Protecting 3 Aspects of Information:
  - 1: **C**onfidentiality – prevent unauthorized access to information
  - 2: **I**ntegrity – prevent the unauthorized modification or theft of information
  - 3: **A**vailability – prevent the denial of service and ensuring authorized access to information

Protection methods we usually think of:

Antivirus, passwords, firewalls, etc.

Parts of this breaks down when we talk about operational devices instead of data.



Cybersecurity isn't just stopping bad guys – failures can be caused by:

- Software Bugs
- User Errors
- Power System Equipment Malfunctions
- Communications Equipment Failure

- Deliberate Intrusions and Sabotage
  - This can lead to data exfiltration, alteration, removal, and system operation

Grid Security: 3 Components

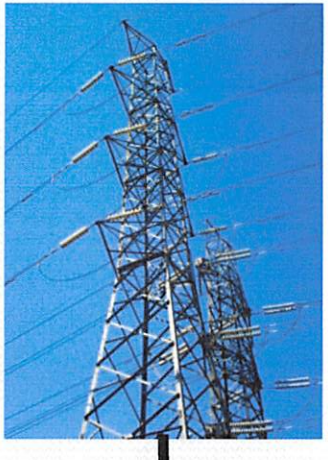
Protect + **Protect** + **Protect** = **Protect**

Conventional IT Systems

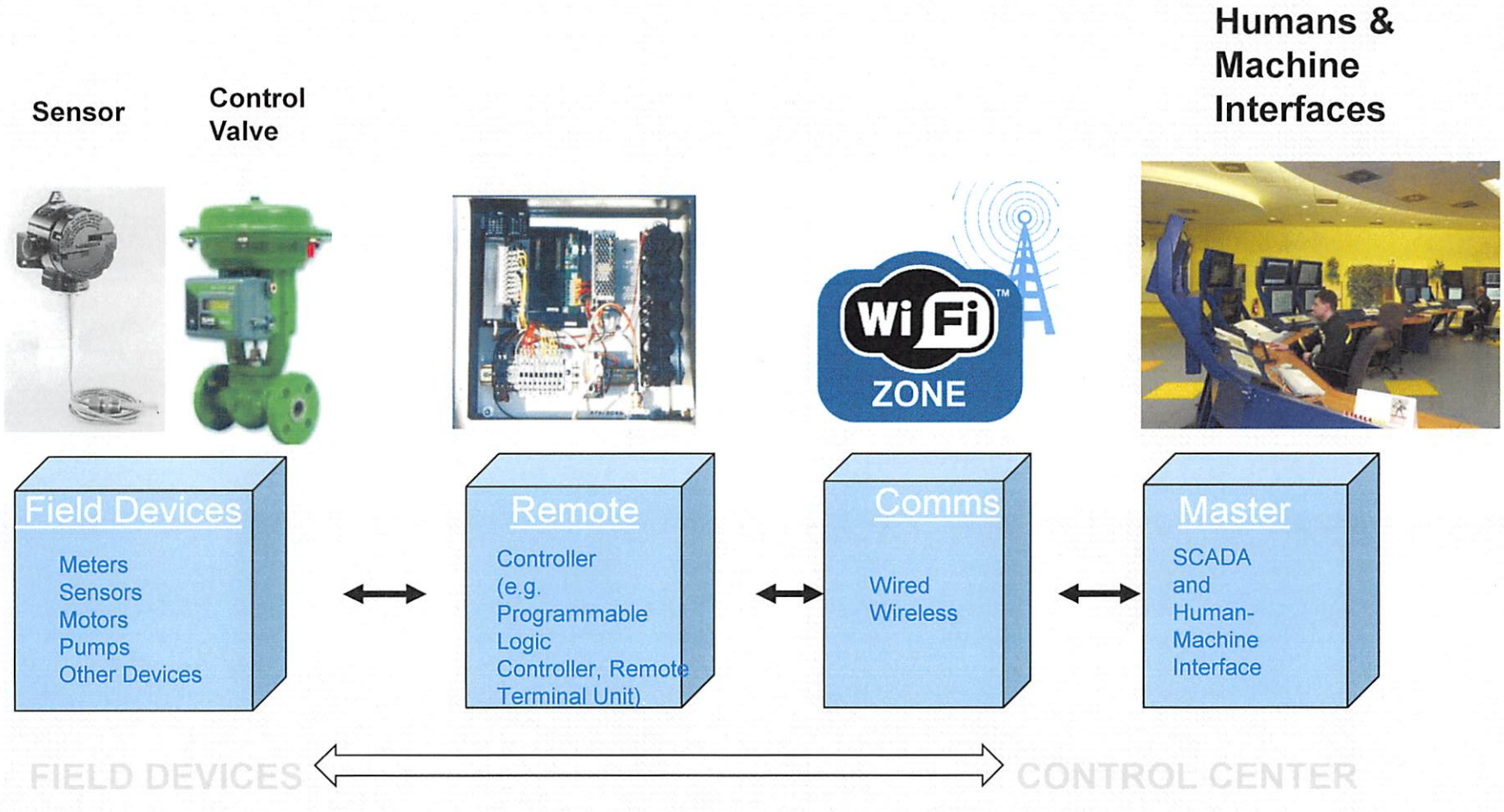
Control Systems

Electrical Infrastructure

"Smart Grid"



What is a control system?



IT Security vs. Control System Security

	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus/Mobile Code	Common/widely used	*Uncommon/impossible to deploy*
Support Technology Lifetime	3-5 years	*Up to 20 years*
Application of Patches	Regular/scheduled	*Slow (vendor specific)*
Time Critical Content	Generally delays accepted	*Critical due to safety*
Availability	Generally delays accepted	*24 x 7 x 365 x forever*
Physical Security	Secure	*Remote and unmanned*

© 2002 PA Knowledge Limited

Threats

Cyber Attacks Exist on a Continuum

Low impact:

- *Nuisance – low consequence*
- *Routine cyber attack common to all business networks*
- *Usually easier to detect and defend against*

Intermediate impact:

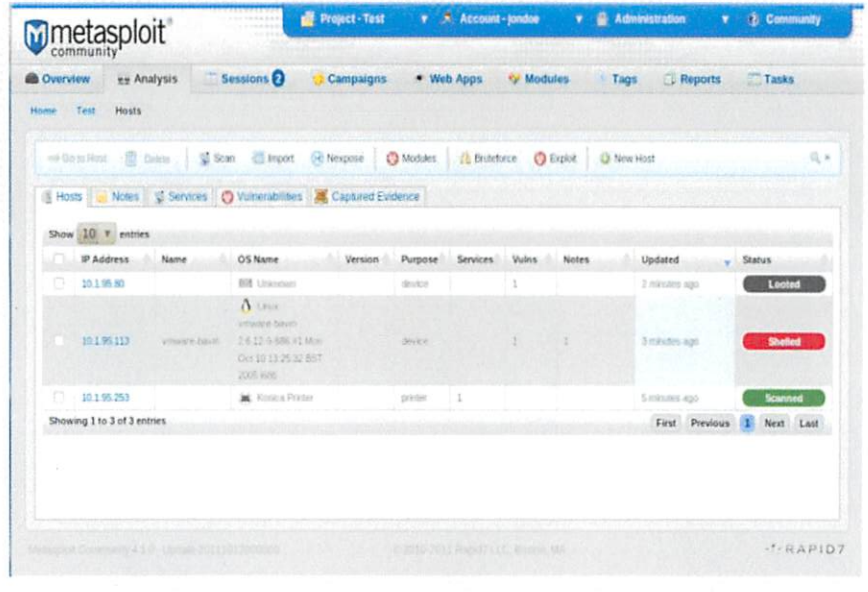
- *Events that may involve damage to a single system component*
- *Unsophisticated, unstructured*

High impact:

- *Directed against multiple assets designed to disable the system*
- *Highly-coordinated, well-planned*
- *Advanced Persistent Threat*

A couple examples of how it's done

- Techniques: Spearphishing,, Waterholing, Social engineering



- Software: "Malware", SHODAN, METASPLOIT, GLEG Agora SCADA+, RATs, worms

Example of spearphishing

Gmail by Google

Dale Peterson <peterson@digitalbond.com>

(no subject)

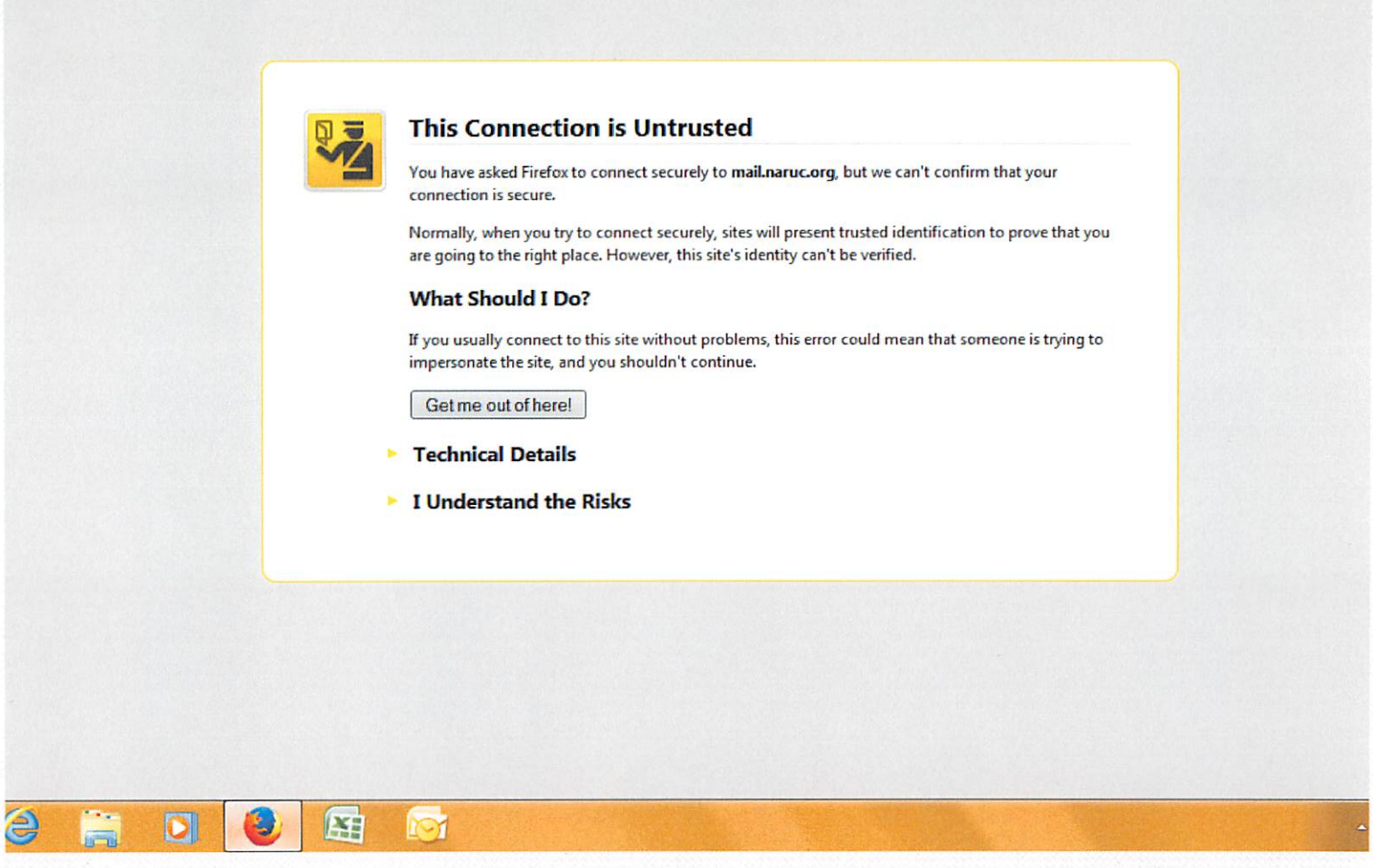
1 message

Dale Peterson <dale.peterson111@yahoo.com> Thu, Jun 7, 2012 at 7:48 AM
Reply-To: Dale Peterson <dale.peterson111@yahoo.com>
To: "rvpasupuleti@yahoo.com" <rvpasupuleti@yahoo.com>

Dear All:
Field devices essential for the monitoring and control in DCS and SCADA systems are increasingly being deployed with Ethernet cards to connect these devices to local and wide area IP networks. Many of the Ethernet cards have their own CPU, memory, operating system and applications. Field device vendors are also providing the capability to upgrade or replace the firmware in these Ethernet cards. Unfortunately in most cases there is no effective security on the firmware upload to the field device Ethernet cards.
Details are available at: Leveraging_Ethernet_Card_Vulnerabilities_in_Field_Devices.pdf
Download it and have a look.
Regards,
Peterson

COURTESY: DIGITAL BOND

Example of suspected waterholing



The Emergence of Nation State Actors

- In 2001, reports that hackers penetrated the California Independent System Operator
- By March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems.
- April / May 2007: Estonian economy reportedly shut down by cyber attacks originating in Russia over the relocation of a statue!
- In April 2009, the Wall Street Journal stated Chinese and other spies hacked into the U.S. electric grid and left behind computer programs that could allow them to disrupt service (since discredited)
- 2009 cyber attacks on nation of Georgia prompted NATO comment
- 2011: Stuxnet & IRI
- 2013: The Comment Crew (over 1000 orgs hit since 2002)
- 2013: Shamoon "bricks" business Saudi ARAMCO and RasGas systems
- 2015: Ukraine blackouts caused by Russian-supported hackers
- 2016: Bowman Dam power station in NY tied to Iran

What's Being Done About It?

NERC and the Bulk Power System

- The North American Electric Reliability Corporation - Standards CIP-001 through CIP-011
- http://www.nerc.com/page.php?cid=2|20

- The NERC standards are excellent but have limitations

What's Missing?

- Well-used and tested risk-management structures
- Enforceable Cybersecurity Rules for Distribution (though some States have led in this area)
- Enforceable rules that cover soup-to-nuts systems or "grey areas"
- Metrics to help with measuring cybersecurity effectiveness
  - So, how do you measure cost-effectiveness?
  - Maturity models help here (like DOE ESC2M2)
- Sufficient information-sharing structures (like ISACs)
- It may fall to State Commissions to ask questions and require performance

The NIST framework

A catalog of industry best-practices and standards that creates a voluntary template for companies to use in developing better security programs.

- The framework is built on three basic components:
  - **Core.** A set of common activities that should be used in all programs, providing a high-level view of risk management.
  - **Profiles.** These help each organization align cybersecurity activities with its own business requirements, and to evaluate current risk management activities and prioritize improvements.
  - **Tiers.** Tiers allow users to evaluate cybersecurity implementations and manage risk. Four tiers describe the rigor of risk management and how closely it is aligned with business requirements.
- It's "informative" rather than "normative" and leaves implementation choices up to the user.
- incentive options to promote the framework - might include cybersecurity insurance, rate recovery, process preference, and grants for adopters.
- http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

What Can Regulators Do?

Commissioners may play a big role

- Reliable service depends on cyber secure service
- A prudent cyber investment is a prudent investment

- In every area, Commissions oversee utility activity by asking questions and setting expectations…
- …So for utility cybersecurity you can ask questions and set expectations.

Cyber Questions

- PUC staff has to be knowledgeable enough about cybersecurity to know what questions need to be asked.
- Regulators primarily want to know:
  - Are the costs prudent?
  - Will the resulting system be more reliable?
    - Fewer outages
    - Faster to recover when outages occur
  - To what degree have cyber security requirements been met?
- Does this assure that the system is cyber-secure?
- Industry is doing a lot, so one early step is to ask what they are doing

Cybersecurity for systems

- We should expect risk-based systems for assuring security.
- The best cybersecurity is in the DNA of the system
  - Fail-safe: cause no harm; cause minimum harm
  - Integrated to core design of hardware, software, and institutions
- Line items may be hard to identify
- Human resources are so important! But aren't price-tagged.
- The "Volvo vs. not-a-Volvo" metaphor
- Many needed steps are questions of process, not of expenditure

What spending might look like

Again, cybersecurity line-items may be hard to single out

Might look like:

- Software, Consultants
- Employee types, i.e. for NERC compliance
- Training for employees
- More expensive hardware ("Volvo")
- Personnel surety steps (shifting, contracting, verification)
- Supply chain verification, certification
- Effects on value delivery to ratepayers (savings and costs)
- Settlements, fines

A "Management Audit" vs. a "Financial-style audit"

- Ask for:
  - Processes
  - Structures
  - Institutions
  - Decision criteria
  - Policies
  - Supply chain verification
  - "Sufficient"
- Be careful with:
  - "Plans"
  - Reports
  - Titles and Names
  - Brands
  - Companies
  - Specific schedules
  - Programs
  - "Perfect"

Protecting Critical Infrastructure Information

- There is tension between the transparency of the regulatory process and protection of critical assets
- Information itself is sometimes the asset
- If you can do this informally, it may work better.
- If it has to be in an open, docketed proceeding:
  - Establish a critical infrastructure information handling policy
  - Know your state's open records & FOIA rules & Implement exemption and protection procedures that properly address utility sectors and associated processes
  - Implement protections for security and cybersecurity info that is stronger than those for commercially sensitive info
  - Apply all protections to accommodate other parties in a case

Sample Approaches to Information Protection

1. "We can't protect it so don't share it"
2. "We can't protect it onsite but can see it at your site"
3. "We can protect it in a special case"
4. "We can protect it within a standard case with a secure hearing"
5. "We can protect it as a matter of course"

Some of these approaches require people with specialized skills, clearances, or professional relationships

Cyber Questions

- Vulnerabilities
- Threats
- Contingency-driven Consequence Analysis
- Prioritize Risks
- Cost-effectiveness Test
- Implementation
- Response & Recovery
- Process Questions
- Governance Questions

The questions are only as good as your ability to understand the answers and take intelligent action

The NARUC Primer Questions

- Pages 21-25 contain 48 questions that you can tailor to your own needs, and use as needed.

- http://www.naruc.org/grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf

- Questions focus on:
  - Planning: indicates response isn't haphazard, reactive, or fragmented
  - Standards: indicates awareness of best practices and compliance with obligations
  - Procurement: indicates systemic and interdependency-aware thinking
  - Personnel & policies: indicates integration of risk management across the enterprise, including people
  - Systems & Operations: indicates that the plan is cyclical and a process, not just a one-time check-box

YOUR Questions?

Miles Keogh, Director – Grants and Research, mkeogh@naruc.org, 202-898-2217

NARUC Grants & Research
1101 Vermont Ave NW Suite 200
Washington DC 20005

Available Resources

- Standards and Guidelines:
  - Bulk Power System: NERC CIP Standards
  - Smart Grid: NIST Interagency Report 7628 (NISTIR 7628) http://csrc.nist.gov/publications/PubsNISTIRs.html
  - NIST framework : http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

- NARUC has developed:
  - Cybersecurity for State Regulators *with Sample Questions for Regulators to Ask Utilities: http://www.naruc.org/Grants/Documents/NARUC%20Cybersecurity%20Primer%20June%202012.pdf*
  - NARUC Critical Infrastructure Committee http://www.naruc.org/committees.cfm?c=46
  - Monthly Cybersecurity Threat Briefings
- National Electric Sector Cyber Security Organization (NESCO): EnergySec formed the NESCO organization as a Public-private partnership including Utilities, federal agencies, regulators, researches, and academics
- National Electric Sector Cyber Security Organization Resource (NESCOR): EPRI was selected to serve as a research and analysis resource to the NESCO program and develop mitigation strategies, best practices and metrics
- DOE Smart Grid Investment Grant (SGIG) Program: Required grant recipients to gather info and implement cyber security plans http://energy.gov/oe/technology-development/smart-grid/recovery-act-smart-grid-investment-grants

Available Resources (cont'd.)

- AMI-SEC Task Force *Advanced Metering Infrastructure (AMI) System Security Requirements*, December 2008. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology, 2007.* See http://csrc.nist.gov/publications/fips/fips199/FIPSPUB-199-final.pdf.
- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 2: Establishing a Manufacturing and Control Systems Security Program*, 2009. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
- Federal Bureau of Investigation, InfraGard program, *InfraGard FBI Cyber Security Collaboration*. See http://www.infragard.net/.
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006. See http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Available Resources (cont'd.)

- Idaho National Laboratory, *Cyber Assessment Methods for SCADA Security*, 2005. See http://www.naseo.org/eaguidelines/documents/cybersecurity/SCADA_Security.pdf.
- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, April 2008. See http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spdsz.pdf.
- North American Electric Reliability Corporation (NERC), *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, June 2002. See http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
- *Smart Grid Cyber Security Blog*. See http://smartgridsecurity.blogspot.com/.
- U.S. Department of Homeland Security *National Infrastructure Protection Plan*, 2009. See http://www.dhs.gov/nipp.

Available Resources (cont'd.)

- U.S. Department of Homeland Security IT, telecommunications, and energy sectors sector specific plans (SSPs), and updated tri-annually. See http://www.dhs.gov/files/programs/gc_1179866197607.shtm
- U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) and the Energy Sector Control Systems Working Group, Roadmap to Achieve Energy Delivery Systems Cybersecurity, September 2011. See http://www.cyber.st.dhs.gov/wp-content/uploads/2011/09/Energy_Roadmap.pdf
- U. S. Computer Emergency Readiness Team (US-CERT), U.S. Department of Homeland Security. See http://www.us-cert.gov/.
- American Petroleum Institute *Security Guidelines for the Petroleum Industry,* April 2005. See http://new.api.org/policy/otherissues/upload/Security.pdf
- Idaho National Engineering and Environmental Laboratory *A Comparison of Oil and Gas Segment Cyber Security Standards*, November 2004. See http://www.naseo.org/eaguidelines/documents/cybersecurity/Comparison of Oil and Gas Security.pdf

Cybersecurity for State Regulators 2.0

With Sample Questions for Regulators to Ask Utilities

Miles Keogh
Christina Cody
NARUC Grants & Research

February 2013

NARUC

The National Association of Regulatory Utility Commissioners

With support from the U.S. Department of Energy

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Acknowledgements and Disclaimers

The report you are reading was created under the State Electricity Regulators Capacity Assistance and Training (SERCAT) program, a project of the National Association of Regulatory Utility Commissioners (NARUC) Grants & Research Department. This material is based upon work supported by the U.S. Department of Energy under Award Number DE-OE0000123 and by the U.S. Department of Homeland Security.

This report was authored by the Grants and Research Department. Throughout the preparation process, the members of NARUC provided the authors with editorial comments and suggestions. However, the views and opinions expressed herein are strictly those of the author(s) and may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Special thanks to:

Denis Bergeron, *Maine Public Utilities Commission*
Edison Electric Institute
Commissioner Terry Jarrett, *Missouri Public Service Commission*
Annabelle Lee, *Electric Power Research Institute*
Patrick Miller, *EnergySec & National Electric Sector Cybersecurity Organization*
NARUC Staff
Thomas Pearce, *Public Utility Commission of Ohio*
Jeffrey Pillon, *National Association of State Energy Officials*
Bridgette Remington, *Vermont Public Service Board*
Alan Rivaldo, *Public Utility Commission of Texas*
Daniel Searfoorce, *Pennsylvania Public Utility Commission*
Christopher Villarreal, *California Public Utilities Commission*

Please direct questions regarding this report to Miles Keogh, NARUC's Director of Grants & Research, mkeogh@naruc.org; (202) 898-2200 and Christina Cody, Program Officer, Grants & Research, ccody@naruc.org; (202) 898-9374.

© February 2013 *National Association of Regulatory Utility Commissioners*

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Executive Summary

This primer was prepared by the National Association of Regulatory Utility Commissioners as a tool for policy-makers who are charged with making decisions about the electric, gas, water, communications, and transportation systems that are vital to everyday life. Increasingly, these systems are being interconnected with the ability to generate, share, and act on data. With these cyber-capacities come new cyber-vulnerabilities that must be managed by regulators and the infrastructure operators they regulate.

Cybersecurity is unlike many other areas that have historically fallen under the purview of regulators, and the pace of change in this area can be dauntingly fast. Still, Public Utility Commissioners and others already have many of the tools they need as risk managers to meet these emerging challenges. The primer includes an introductory explanation of the issues, identifies the jurisdictional landscape and highlights some of the characteristics of good cybersecurity that policy-makers should look for. This document also proposes that States engage strategically with cybersecurity to enable and support a thoughtful, risk-based approach that encourages prudent investments by infrastructure operators. It includes sample questions for States to customize and ask their regulated entities and points to other resources that policy-makers can turn to as they engage with cybersecurity more deeply.

Introduction

We often hear reports of cyber attacks in the news, but how serious are the threats to our country's essential utility infrastructure, such as electricity, gas, water and telecommunications?[1] Many State utility regulators have begun asking how to best protect the services, information and data that are valuable to customers, companies, as well as the country. These regulators are charged with assuring that utility companies provide reliable and affordable service to their customers, and putting cybersecurity into the field of view of State regulators. Cybersecurity threats challenge the reliability, resiliency and safety of the electric grid, and utility spending to address cyber vulnerabilities can impact the bills that customers pay.

This primer addresses cybersecurity – particularly for the electric grid – for State utility regulators, though we hope that it will be useful for a wide audience of policymakers in this field. The primer provides some conceptual cybersecurity basics for the electric grid and provides links to how regulators can:

- Develop internal cybersecurity expertise;
- Ask good questions of their utilities;
- Engage in partnerships with the public and private sector to develop and implement cost-effective cybersecurity; and
- Begin to explore the integrity of their internal cybersecurity practices.

We find ourselves at a critical juncture for infrastructure protection as the grid transitions from a previously isolated environment to a complexly interconnected one. Today's electrical grid interconnects components of our traditional physical electrical infrastructure with less tangible

[1] DHS Critical Infrastructure Sectors are the following: Food and Agriculture; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Transportation Systems; Water (http://www.dhs.gov/files/programs/gc_1189168948944.shtm)

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

information technology (IT) components such as networks, software and data. For the purposes of this primer (in which our primary concerns are areas pertinent to State regulators' jurisdiction) when we talk about cybersecurity and infrastructure, we are referring to the cybersecurity of not only the physical distribution and transmission grids, substations and offices, but also equipment and systems that communicate, store and act on data. Cybersecurity must encompass not only utility-owned systems, but some aspects of customer and third party components that interact with the grid, such as advanced meters and devices behind the meter. And more than simply being a function of hardware, cybersecurity is critically important as a function of software, data and the networks that use data to keep the system operating. Finally, there are human elements to cybersecurity, including system operators, customers and "bad guys" interacting at all levels of a system. With such a dynamic and broad landscape to consider, cybersecurity cannot be a stagnant prescription handed down from experts. It should evolve as technology, threats and vulnerabilities evolve, introducing the building blocks that stand the test of time while still being flexible enough to meet changing cybersecurity requirements.

Why Cybersecurity?

Cyber attacks that cripple the power grid or shut down other infrastructures may be rampant in Hollywood, but to date there have been no reports of a cyber attack successfully crippling critical utility infrastructures in the United States – it is harder to do in the real world than in the movies. With all the attention given to impossible fictional attacks, it might be helpful to imagine an improbable but realistic scenario.

> *Imagine that one Sunday afternoon you turn on the TV to find major news reporting a troublesome, though not devastating blackout affecting a number of areas in your region. In the subsequent days, police and the system operator report that the information about load and generation the grid's regional transmission operator receives had been snuck out – exfiltrated – by parties unknown, and replaced with erroneous data. Dispatchers had to rely on conservative operations in dispatching power plants because they could not trust the data they were receiving without careful review. A few days later, a similar exploit occurs in a vertically-integrated utility's service territory, and soon it is occurring widely and regularly enough, regionally, that careful data review, cross-checking and expensive conservative dispatch become standard practices while the perpetrators are tracked down. Soon thereafter, utility officials report massive denial of service attacks directing tens of thousands of emails an hour to the mobile email systems of their experts and executives, clogging up the flow of information to coordinate response. The situation worsens when substations in the region begin experiencing equipment malfunctions, creating load management problems at the very time that system operators are addressing the system operations data integrity and denial of service problems. Checks of the substations reveal that the firmware in the programmable logic controllers of key sensor devices has been rewritten. It will take ongoing digital forensics to determine what the rewritten firmware even contains, much less how it was overwritten, or by whom.*
>
> *Internal utility emails forwarded to the Public Service Commission warn their staff that malevolent programs are spreading on a peer-to-peer basis within the utility's business process systems looking to exfiltrate customer data, and the utility alerts the regulator that their system may be at risk as well because of the frequency of communications. The Public Service Commission orders an audit of its own internal data systems and IT staff reports that the State system has been successfully penetrated by intruders, but the vendor cannot be certain whether legally protected, commercially sensitive or even detailed utility infrastructure data has been*

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

taken. Market-driven system operations are on the shelf for the time being, distribution level reliability is regionally affected and customers are wondering if they can rely on their electric service. Companies and citizens alike are asking hard questions about whether their data is safe. Experts believe they have determined a remedy for breach, but as of now, they cannot be sure who perpetrated the attack and whether more attacks are planned. Service interruptions continue over the next few months, customers' information is still at large and the GDP has contracted significantly after months of stunted power provision across the interconnection.

This is a pretty bad scenario, but far from the worst case. A dedicated hacker group could accomplish the situation above. A nation-state or well-funded criminal syndicate could theoretically accomplish worse. The more likely scenario is a smaller attack that compromises data without necessarily affecting the operation of the grid. While the above scenario is realistic, the likelier reality may be much easier to address and mitigate. If regulators (and utilities) can imagine the more drastic possibility, it might be easier to imagine – and be prepared for – scenarios of lesser consequence.

Responding to Threats and Vulnerabilities

State governments are already hard at work implementing energy assurance plans across the country that help respond to vulnerabilities, as well as preventing and protecting against threats. There is an important distinction to understand between threats and vulnerabilities. A threat is the potential for an actor, circumstance or event to adversely affect assets, people or organizational operations of the system. A vulnerability is a specific weakness at any point in the system that can be exploited by a threat source. A good example is the difference between leaving a door to your house unlocked (creating a vulnerability) and doing so when there are burglars on your street (who pose a threat). Providing true energy assurance in cybersecurity includes addressing vulnerabilities and responding to threats in a way that is timely and assures normal conditions for the near future. The responsibility of prevention, protection, detection and responding is multi-pronged and shared between industry, local, state and federal actors.

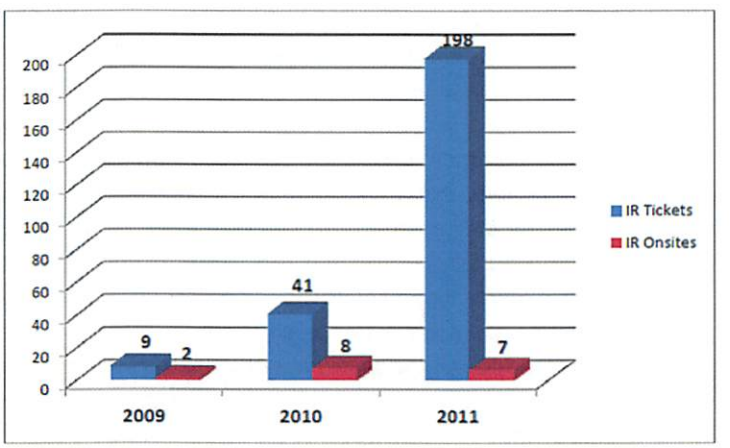


Figure 1 ICS-CERT incident response trends data; http://ics-cert.us-cert.gov/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf

Where Cybersecurity Fits

Cybersecurity vulnerabilities exist wherever computer systems and data exist. With the advent of smart grid technologies, which layer software on top of utility operations and computer systems, threats become increasingly likely and relevant. [2] While a smarter grid is generally more reliable, new vulnerabilities appear that must be managed as grids become two-way exchanges of kilowatts, as well as network and customer-usage data that may be valuable and desirable to bad actors.[3]

[2] Trusted sources have articulated that the ICS CERT incident response increase seen is in fact an increase in attacks and not due to better detection or increased reporting

[3] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," June 2010: 39.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

> ***"On the low-impact end of the spectrum are common events, such as copper theft and the types of routine cyber attack common to all business networks in the Information Age. In the intermediate-impact range are events that may involve damage to a single system component in an unsophisticated, unstructured attack. On the high-impact end of the scale are highly-coordinated, well-planned attacks against multiple assets designed to disable the system."***
> **High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," North American Electric Reliability Corporation (NERC), June 2010**

Threat Sources

While cybersecurity breaches can be caused by people, they are not always who we think of as "bad guys." Criminal threats to the bulk power system can range from those of minimal impact to those of great consequence. For the purpose of this primer, we will focus on cyber attacks from intentionally malicious actors and how to protect against them, although the steps taken to create cybersecure systems are only one part of an all-hazards approach. [4] Cybersecurity must protect against inadvertent sources – user errors (including accidents), hardware failure, software bugs, operator errors or plain negligence – as well as intentional attacks. Natural disasters can also play a role: a flooded server room cannot provide service any better than one flooded with data traffic from a denial of service attack. Other resources[5] may be helpful in establishing an all-hazards approach that addresses risks other than intentional cyber attacks.

The aims and implications of cybersecurity violations vary widely. Gaining system control – the ability to remotely modify and operate the system as a vehicle for attack – is just one of the possible consequences. Data theft (or "exfiltration") is also a known and ongoing problem. The scope of a cyber attack is also an important consideration. Attacks that affect one person's data or that cripple one meter will generally have less impact than attacks that exploit larger amounts of data or that attack not one component, but multiple components or the network that connects them.

What Are We Protecting? Three Flavors

While natural disasters, human error, software bugs or equipment breakdowns can be the origins of a system failure, deliberate attacks involve the element of intent – a person at the other end of the operation with the capability to bring down a system specifically outside its existing protective barriers.[6] Malicious attacks threaten utilities on multiple levels in ways that sometimes overlap and compound each other. It may be helpful to visualize the application of cybersecurity in three areas: IT, supervisory control and data acquisition (SCADA) systems, and smart grid. We'll explain each of these components of the data-connected grid and how cybersecurity relates to each.

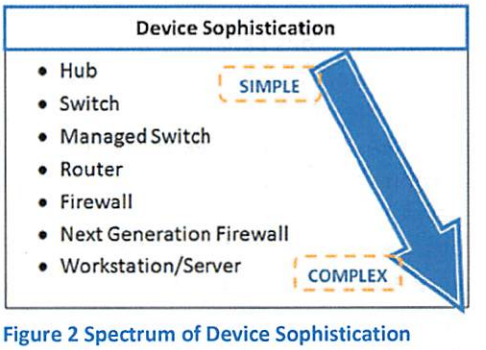


Figure 2 Spectrum of Device Sophistication

Information Technology Systems

This is the arena where cybersecurity has historically focused: business process systems such as those found on your laptop computer, as well as in more sophisticated

[4] All-hazards approach takes into account any threat to security, including unintentional or naturally-occurring ones

[5] Such as the NARUC/National Association of State Energy Officials (NASEO)/DOE Energy Assurance Guidelines: http://www.naruc.org/Publications/State_Energy_Assurance_Guidelines_Version_3.1.pdf

[6] NERC, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 29.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

systems and networks that connect data and perform intelligent tasks with that data. It includes both components, like individual workstations, and network components that allow interoperability between components. If IT is all about connectivity – how systems talk to each other – then IT security begins by protecting the network that enables the flow of data through the system, as well as by protecting the data itself. This data can be financial information, a customer's street address, phone number, or information about their power usage, to name a few. IT connects all systems, from simple to complex, including communications between systems like the hub or the switch all the way to the firewall and the server. Considering how valuable the data of utilities' systems are, the communication, transferences and actions based on this data compound its intelligence value. For IT, cybersecurity not only includes software and hardware strategies – passwords, antivirus systems, firewalls, logical and physical separation of servers, for example – but also training personnel and creating policies so that their interaction with the IT system enhances, rather than erodes, cybersecurity. Because of this human element, simply upgrading or making hardware more obscure does not equal improved cybersecurity.[7]

Crossing Over from Data Attacks to Physical Impacts: Aurora and Stuxnet

The most common target of cyber attack is sensitive data, but some examples are emerging that highlight the possibility of a successful physical attack that originates in the cyber arena.

In 2006, the Idaho National Laboratory (INL) staged a cyber attack nicknamed "Aurora" that crippled an electric power generator. The attack involved controlled hacking into a replica of a power plant's control system and misusing safety systems to change the operating cycle of the generator, sending it out of control and physically damaging and disabling it.

Emerging in 2009, "Stuxnet" was a self-replicating and –propagating software worm that also had the capacity to physically attack the grid. When an infected USB stick was inserted into a computer, malicious code awakened and surreptitiously dropped a large, partially encrypted file onto the computer, re-writing the programmable logic controller and changing the frequency of spinning drives that it controlled. By 2011, reports were circulating that it had been designed to attack specific centrifuges in Iran; it remains an example of software that can cause physical damage to the grid.

Control Systems

SCADA encompasses systems that monitor and control industrial, infrastructure or facility-based processes, such as utility operations. They include simple functions such as "on/off," sensor capability, communications capability and human-machine interface (HMI) that connects them to people operating the system. In other words, they are automatic (and often remote) control devices. SCADA security means the machine does what it is supposed to do and does it accurately. With a secure SCADA system, you can trust what your machine is telling you. However, according to executives with SCADA responsibilities, these systems more and more often have connections to Internet Protocol (IP) networks, including the internet in some cases.[8] Even those physically and logically disconnected from other systems may be locally or remotely accessible and have vulnerabilities to be exploited. SCADA access and control points are also frequently located in remote and unmanned areas of the utility system, and therefore may require either increased physical security or the ability to isolate those points from the overall system if they become compromised.

[7] Miles Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," *National Association of Regulatory Utility Commissioners*, May 2009: 6.

[8] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 31.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Security for SCADA systems requires a system-wide understanding of how each of the components fit together so that vulnerabilities can be prioritized and addressed at each point.[9] Depending on the situation, some devices may need to be remotely upgradeable, in which case these devices may need capability to use encryption, certificates and authentication. For other devices this may be impractical and access might be required in order to adjust to updated technology. When systems are remotely monitored and maintained, calibration and auditing can be important ways to ensure that they continue giving accurate information and perform functions in a trusted manner. Control systems are not like IT systems, however, in that they often have much longer deployment lifetimes with much rarer software updates and much scarcer physical security measures.

Smart Grid

The smart grid is defined differently depending on who you ask, but for this primer it represents the modernization of electricity infrastructure through added technology, allowing the grid to gather and store data, to create a "dialogue" between all components of the grid, and allowing for automatic command and response within the function of the grid. In concept, smart grid provides so many improvements in situational awareness, prevention, management and restoration that, in spite of the new vulnerabilities it introduces, it fundamentally makes the electric system more secure and reliable.[10] However, the smart grid enhances the need for cybersecurity because it adds a layer of computer systems and software – all with additional doors to be hacked – to existing utility infrastructure. It may increase the portals through which a cyber threat could enter the system. Keep in mind that the more systems communicate with each other and their human operators, the more channels across which data is shared and, therefore, the more the systems require an assessment of their cybersecurity.

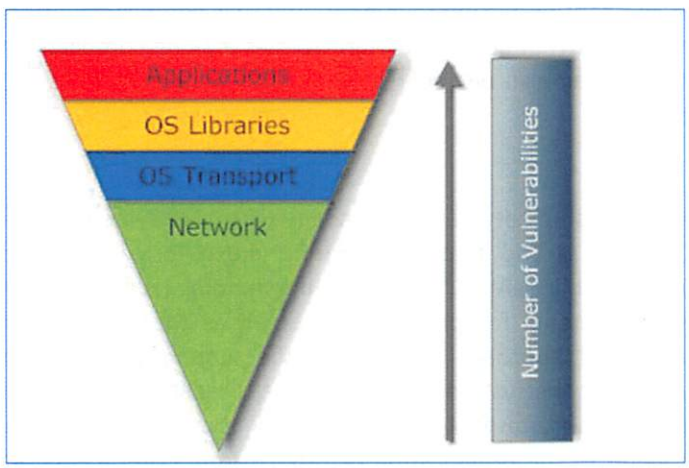


Figure 3 SANS: Number of Vulnerabilities in Network, OS and Applications

Smart grid technology touches a number of components–from transmission phasor measurement units to smart meters to home appliances. Therefore, the smart grid requires software to be installed in a way such that if an attack succeeds, components that are compromised do not threaten the network, and that infiltrators are only able to access data in such a way that the attack is unproductive, undesirable, not valuable and detectable by operators.[11]

Compliance-Based and Risk-Based Approaches to Cybersecurity

Using Compliance as a Basis for Cybersecurity

The owners and operators of critical infrastructure have not been sitting idly by while cyber threats mount. NERC has developed standards- and compliance-based structures that require the operators of

[9] Asset owners should be encouraged to do a risk assessment to determine which vulnerabilities to mitigate. Addressing all vulnerabilities may be cost and performance prohibitive.

[10] Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," 6.

[11] *Ibid.*

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

the bulk power system to take steps to conform to specific cybersecurity practices. These standards include assessing the systems you have, determining if there are specific vulnerabilities, and then taking action to address these as part of a compliance regime. In practice, these standards appear to be effective for motivating compliance, although some critics note that responding to a compliance regime does not necessarily overlap entirely with responding to a risk-assessed landscape of potential vulnerabilities and threats.

Any regulator interested in cybersecurity will be well-served by becoming familiar with what the NERC Critical Infrastructure Protection (CIP) standards require for the bulk power system. The NERC CIP Standards are enumerated on the following page. NERC's board of trustees has approved the following standards, the proposed Version 5, and filed them with FERC.

While these standards are robust and a strong improvement over what existed before, State regulators should bear in mind that the NERC CIP Standards are still evolving as they relate to the bulk electric system. Those interested in improving upon these standards argue that distribution systems and other key areas where cybersecurity remain a concern to State regulators may not be entirely covered by the existing standards. Additionally, those who argue that the CIP standards are incomplete point out that compliance only proves *compliance*; utilities' cybersecurity should be based in *risk management*. Risk management includes assessment, mitigation and continuous improvement, whereas compliance offers a view of cybersecurity at a fixed point in time, not a dynamic picture of it. Utilities may be compliant to the CIP standards and still not be secure. Utilities may also be secure but not be compliant to the CIP standards. One is not the guarantee of the other.

Using Risk as a Basis for Cybersecurity

Understanding risk means understanding the relationship between vulnerability (such as a system with a known but unaddressed weakness), threat (such as a bad actor propagating viruses or worms) and consequence (such as physical damage and loss of public safety).[12] Simply understanding risks is just the first step: a risk-based approach prioritizes components for protection, as well as the threats and vulnerabilities that require attention. A risk-based approach starts with the assumption that an unauthorized user can and will gain access to data or the system, and thus designs responses based on the value of the data or system that could be compromised by the inevitable access. This calls for prioritizing data and systems based on their value to the organization or other useful criteria such as reliability and privacy. The utility or other organization can then decide which systems and programs should have the highest level of cybersecurity, best personnel resources, the right tools, and of course the right budget. Basing a cybersecurity strategy on a risk assessment that identifies and addresses the most significant cybersecurity issues across and within the system will always yield better security results than ineffective "outer wall" approaches to cybersecurity that only focus on denying access to the system. A risk-based approach includes understanding risks, prioritizing them by likelihood, consequence and potential interactions with other risks, and allocating resources accordingly.[13]

---

[12] U.S. Department of Energy, "Electricity Subsector Cybersecurity Risk Management Process," May 2012.

[13] Rich Baich and Ted DeZabala, "Cyber crime: a clear and present danger; Combating the fastest growing cyber security threat," *Deloitte Center for Security & Privacy Solutions* (2010), http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

NERC CIP Standards

Number	Title/Summary	Date
CIP-001-2a	Sabotage Reporting	02.16.2011
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	12.16.2009
CIP-002-3a	Cyber Security - Critical Cyber Asset Identification	05.09.2012
CIP-002-4	Cyber Security - Critical Cyber Asset Identification	01.24.2011
CIP-002-4a	Cyber Security - Critical Cyber Asset Identification	05.09.2012
CIP-002-5	Cyber Security - BES Cyber System Categorization	11.26.2012
CIP-003-3	Cyber Security - Security Management Controls	12.16.2009
CIP-003-4	Cyber Security - Security Management Controls	01.24.2011
CIP-003-5	Cyber Security - Security Management Controls	11.26.2012
CIP-004-3a	Cyber Security - Personnel & Training	05.24.2012
CIP-004-4a	Cyber Security - Personnel & Training	05.24.2012
CIP-004-5	Cyber Security - Personnel & Training	11.26.2012
CIP-005-3a	Cyber Security - Electronic Security Perimeter(s)	02.16.2010
CIP-005-4a	Cyber Security - Electronic Security Perimeter(s)	01.24.2011
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	11.26.2012
CIP-006-3c	Cyber Security - Physical Security of Critical Cyber Assets	02.16.2010
CIP-006-3d	Cyber Security - Physical Security of Critical Cyber Assets	02.09.2012
CIP-006-4c	Cyber Security - Physical Security of Critical Cyber Assets	01.24.2011
CIP-006-4d	Cyber Security - Physical Security of Critical Cyber Assets	02.09.2012
CIP-006-5	Cyber Security - Physical Security of BES Cyber Systems	11.26.2012
CIP-007-3	Cyber Security - Systems Security Management	12.16.2009
CIP-007-4	Cyber Security - Systems Security Management	01.24.2011
CIP-007-5	Cyber Security - System Security Management	11.26.2012
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	12.16.2009
CIP-008-4	Cyber Security - Incident Reporting and Response Planning	01.24.2011
CIP-008-5	Cyber Security - Incident Reporting and Response Planning	11.26.2012
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	12.16.2009
CIP-009-4	Cyber Security - Recovery Plans for Critical Cyber Assets	01.24.2011
CIP-009-5	Cyber Security - Recovery Plans for BES Cyber Systems	11.26.2012
CIP-010-1	Cyber Security - Configuration Change Management and Vulnerability Assessments	11.26.2012
CIP-011-1	Cyber Security - Information Protection	11.26.2012

Figure 4 http://www.nerc.com/page.php?cid=2%7C20

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

A Few Helpful Cybersecurity Concepts

State regulators are not responsible for building a strong cybersecurity capacity for critical infrastructure – utilities are responsible for this – but it is increasingly important that regulators be able to recognize underlying concepts of robust cybersecurity when it comes before them in a proceeding. A few of the concepts that should inform a regulator's assessment of a utility's cybersecurity proposal should include the following:

- Prioritizing systems and networks over components
- Ensuring that human factors are considered
- Deploying defense-in-depth
- Promoting system resilience

Securing Systems and Networks vs. Devices on the Network

Cybersecurity may call for securing entire networks, in addition to devices on that network. For example, the meters within a smart grid system can be fortified against attack, but in order to ensure the entire network of the smart grid system is secure, the components *linking* those meters, as well as every other component in between, must be secured as well. That way, if an attack occurs at one meter, the rest of the system linked to that meter is not also at risk because the components linking them have been protected.[14] This concept was explored in each of the three "flavors" of risk: IT, SCADA and smart grid.

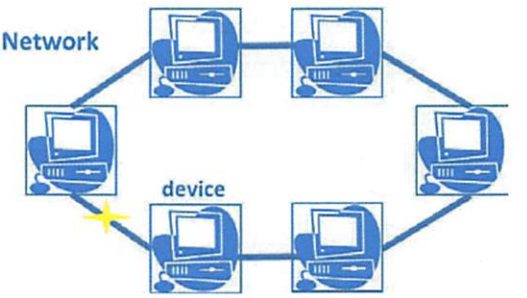


Figure 5 Networks vs. Devices

Personnel Surety: Securing People As Well As Systems

A system is only as secure as the people who run and operate it. Training is essential to ensure that in the event of a cyber attack, personnel are skilled in identifying and responding to the impacts. Personnel can also be "insiders" involved in a deliberate or accidental cybersecurity breach. Identifying key personnel and using background checks is a potential strategy to mitigate this, but once they have been hired, policies that limit an individual's ability to inflict harm may also be important. These policies, such as the Principle of Least Privilege and "Need to Know,"[15] segregate duties. Securing personnel may also include conducting background checks, ensuring expertise through education,[16] safe and supportive working conditions and finally, continual training to keep expertise up-to-date.[17] Lastly, effective separation policies for employees, regardless of the reason for separation, should ensure that separated employees' access to facilities, networks and SCADA systems are terminated as soon as it is appropriate.

Crown Jewels

Conventional wisdom in cybersecurity previously suggested a defense-in-depth approach, requiring many diverse barriers at each layer of potential attack surface. This is a great approach for those with

[14] It is worth mentioning that specific cybersecurity mechanisms will likely vary among devices and protection may be stronger or weaker across the devices in the system, depending on their importance and functionality.

[15] Principle of least privilege is defined as having access to the least information or fewest resources necessary to complete a legitimate purpose; "Need to know" is a practice that restricts information or resources in the execution of a task outside of what is critical in order to complete that task, despite clearance level.

[16] A good example is available from the State of Michigan's personnel protocol: www.michigan.gov/cybersecurity.

[17] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 15.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

well-developed risk-based resources, but for those just starting, or even those with a well-developed security apparatus, the quickly and ever-changing threats and vulnerabilities would suggest an updated approach. A "crown jewels" approach calls for identifying the ultimate priority assets within the attack surface (these may vary depending on context) and securing these first and most thoroughly. Effective cybersecurity often encompasses physical as well as technological measures – restricted access to server rooms, locks on smart meters, security fencing and cameras at key substations, for example, must be incorporated in the above approach. Once the security of the most important resources has been established, working out towards defense-in-depth is an useful direction. However, the time and cost necessary to identify, authenticate and authorize, admission control, encryption, integrity checking, detections of policy violations, data logging and data auditing could potentially distract from the security needed for the key assets. The "crown jewels" approach would suggest protecting these sufficiently first, after which resources should be spent in padding out security towards the overall security of defense-in-depth.

It is recommended that State Regulators proceed with the following steps:

1. *Convene an internal team of staff to set aside time in addition to normal duties to work on cybersecurity*
2. *Develop a strategy that outlines the commissions desired approach, goal and timeframe for proceeding*
3. *Promulgate guidance to regulated entities that falls in line with the desired goals and approach outlined in the strategy*
4. *Proceed with asking questions and motivating desired behavior from regulated entities*

Interdependencies

While this primer has focused mainly on the electric sectors, attackers will attack any area that seems less-prepared and cyber threats have been identified to gas, telecommunications, transportation and other State-regulated utilities. If the industry has and relies on control systems, then it also has vulnerabilities to exploit. In addition to having electrically-dependent control systems, regulators must consider the interdependencies of their regulated entities where an electric outage affects gas, telecommunications and other rate-payer services to an exponential degree on top of the acute affects on the electric grid.

Resilience and Recovery

The electric industry is an incredibly resilient industry. In the event of extreme storms in the past, power lines have been restored much sooner than homes are rebuilt. Resilience of the electric sector to cyber attack should be no less resilient than to a tornado. While defense-in-depth plans for the unexpected, resilience ensures that the unexpected will not persist indefinitely. A resilient system will not only be prepared for deterring, defending against and mitigating attacks, but also for ensuring quick and efficient restoration in the event that an attack compromises the system, through disaster recovery planning. Plans should be stored in a way that a cyber attack does not affect access to them, such as a backup hard copy in an accessible, but physically secured, location that is water- and fireproof.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Developing a Cybersecurity Team

Several States, including Iowa, Washington, Texas and Pennsylvania have already assembled a cybersecurity team, following similar approaches, outlined below. This primer endorses the below approach, to be tailored to the specifics of your State, whereby each State's team...

- *Begins by articulating the desired role that was most appropriate for their given regulated entities, State-specific assets and relationship*
- *Generates a strategy that reflected the above articulation* ***before taking action***

The starting point and end goal of developing a cybersecurity team were similar in most States, but the steps in between vary by State, given the varying nature of assets, relationships and regulated entities. Specifics are emerging and will be detailed in subsequent editions of this primer.

What Regulators Can Do

The regulatory role in this arena is increasing. More cyber attacks to business processes and NERC CIP Standards compliance are driving new cybersecurity expenditures by utilities that may be featured in future rate cases. The deployment of smart grid adds new cost and reliability elements to this puzzle. Regulators are already hard at work to address cybersecurity risks to the American power grid and the greater infrastructure of utilities. But there's more to be done and, in the face of shrinking budgets, fluctuating workforce and the absence of comprehensive legislation, regulators need a dynamic strategy to strike the right balance of security and resources.

Although regulators will not need to be experts at implementing utility cybersecurity, they will be well-served by asking smart cybersecurity questions of utilities, the entities responsible for conducting risk assessment. These questions are the basis of evaluating prudence, which we will discuss in the next section. Staff members who specialize in cybersecurity at commissions are invaluable resources for drafting the relevant cybersecurity questions for Commissioners to ask utilities during cases. It is very important that questions posed to utilities, however, do not reveal information that could be valuable to a cyber attacker, because answers submitted by utilities during a proceeding are subject to the Freedom of Information Act (FOIA) and can therefore be accessed by the public – potentially including people with malicious intent. Some States have a Critical Infrastructure Confidentiality Statute or other authority that protects against this vulnerability. Please see the Appendix for NARUC's *Sample Cyber Questions to Ask Your Utilities*. It is intended that you will customize these questions to each relevant scenario, while maintaining the phrasing of the questions, which avoids potential cybersecurity risk in the utility's response.

The NARUC Resolution Regarding Cybersecurity, adopted on February 17, 2010, calls for "continued vigilance against all potential sources of cyber threat to be both prepared to prevent cyber attacks capable of disrupting utility services and to mitigate the harmful consequences of such attacks in order to protect public health, public safety and the economy."[18] Key tenets of the resolution encourage Commissioners to prioritize the consistent monitoring and evaluating of cybersecurity in collaboration with agencies having expertise in cyber threat management and mitigation in order to remain effective in meeting

[18] NARUC Committee on Critical Infrastructure, "Resolution Regarding Cybersecurity," adopted at the NARUC Winter Meeting of 2010, February 17, 2010.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

evolving cyber challenges. Commissioners should regularly revisit their own cybersecurity policies and procedures "to ensure that they are in compliance with applicable standards and best practices."[19] Keep in mind that ensuring new investments in technologies that are designed with cybersecurity in mind at the front end will create cybersecurity more effectively than adding it to systems later.

The resolution encourages regulators to initiate a dialogue with their utilities to ensure that the utilities are also in compliance with standards. In order to properly review filings to this end, regulators may wish to develop and maintain staff expertise on cybersecurity as it relates to the following topics suggested by NASEO[20]:

1. What is the insider threat and what policies and procedures are in place to prevent intrusion and manipulation?
2. Technical solutions to cybersecurity should account for human behavior, which can be driven by both cultural and psychological factors;
3. Nature of the threat from employees, contractors, consultants or anyone with short or long term access to IT systems and knowledge about system vulnerabilities; and
4. Effect of new systems on consumer behavior – will it strengthen cybersecurity or incite actions to attack the system?

Training Resources

Regulators may wish to invest in training staff on cybersecurity standards and to provide regular updates to training as information changes and technology advances. Internal staff should also be responsible for understanding the cybersecurity of their agency. It may be valuable to have staff members fluent in the concepts of cybersecurity available to serve as a point person for the rest of the staff on all issues relating to cybersecurity. In this way, not only those with an information technology workload familiar with cybersecurity, but those involved with rate cases, siting cases, reliability oversight and planning will have access to cybersecurity concepts and principles so that this becomes a regular part of the content of a regulatory process when appropriate.

NARUC provides cybersecurity training free of charge through grant-funded programs once or twice per year and convenes cybersecurity expertise at its meetings. In partnership with the National Electricity Sector Cybersecurity Organization (NESCO), NARUC also hosts regular threat assessment teleconferences. It may also be worthwhile to explore what training options may be available through your State's homeland security department, or other in-state sources.

Other resources include:

- *U. S. Computer Emergency Readiness Team's* (U.S. Computer Emergency Readiness Team (CERT) and U.S. Department of Homeland Security (DHS) Control Systems Security Program training: http://www.us-cert.gov/control_systems/cstraining.html
- Pacific Northwest Control System training: http://eioc.pnnl.gov/training.stm
- INL "Red Team / Blue Team" training: http://www.inl.gov/scada/training/advanced_scada.shtml
- Multi-State Information Sharing and Analysis Center (MS-ISAC) http://msisac.cisecurity.org/
- FBI's InfraGard Program: http://www.infragard.net/

[19] *Ibid.*

[20] NASEO, "Smart Grid and Cyber Security for Energy Assurance," November 2011: 16.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Ask Questions

Standards, such as the NERC CIP Standards described later in this document, are important but should not be considered to be exhaustive. For example, specific technology standards will not address all the aspects of cybersecurity that are critical, such as high level policies and procedures, that are commonly excluded from standards. Furthermore, existing processes may cover many bulk generation and smart grid aspects of the system, but guidance, standards and other regulations may not currently suffice for elements of the distribution system. It may fall to regulators to ask questions of utilities to determine if there are gaps and facilitate action.

Information Protection

The line between knowing enough to determine that a utility's actions are prudent and knowing so much that the information held by the Commission can pose a cybersecurity risk is a line that commissions should walk carefully. In cybersecurity, the information itself is sometimes the asset worth stealing. To address this issue, States may wish to consider establishing a critical infrastructure information policy. This policy would govern not only the type of information the commission could take possession of (or refuse to take possession of), but also under what circumstances, as well as which access, handling and storage protocols would govern that data. For example, Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act allows public utilities to restrict certain information from public disclosure and Right-to-Know requests. The Act also puts the onus on State agencies to protect any confidential cybersecurity information belonging to the utility that the State has in its possession, including sensitive parts of emergency or cybersecurity plans.

Commissions should become familiar with their State's information access and transparency laws – such as the FOIA and Sunshine laws – and ensure that sensitive information is not gathered in a context which would enable it to be publicly accessible. Many States have good cybersecurity exemption rules that properly address utility sectors and associated processes while providing automatic protection of information related to cybersecurity. State agencies can develop and communicate their non-disclosure procedures and, where appropriate, may want to consider stronger protections for cybersecurity and information than for commercially sensitive information.

Finally, just because information is legally and procedurally protected does not mean that it's actually cybersecure. Commissions should carefully consider whether they need information before asking for it, because even if they can keep it out of the public record and exclude it from FOIA, it may still be vulnerable to theft via cyber attack.

This may be the key role for commissions in cybersecurity. Commissions do not need to become cyber industry authorities or enforcers, but asking a utility a question may motivate the development of a well-founded answer. NARUC is in the process of developing a series of sample questions that originate with some of the interrogatories developed by States with their utilities. These may prove a helpful starting point and are included in *Appendix A* of this primer.

Asking questions isn't enough – once good questions have been posed to utilities, regulators bear the responsibility of understanding the answers to determine whether they represent prudent activities and investments. Regulators have to determine whether the amount being invested is insufficient or excessive and whether it is allocated appropriately. Regulators must then help prioritize these investments along with all the other proposed spending that a utility proposes in a rate case. Regulators

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

must keep the cost of electricity affordable for customers while asking utilities to spend more on cybersecurity in the face of increasing media attention on stories of cybersecurity threats and vulnerabilities.

Developing Expertise: Resources for Regulators

Cybersecurity remains an area where a lot of work needs to be done, but it is worth noting that many institutions and frameworks have been set up that have already made an enormous amount of progress. Some of these are listed below. Many of these groups are open to State personnel to monitor, join and participate in, and this may be an important way to become appropriately engaged with companies and other stakeholders working on these issues before they emerge in the context of a hearing room. Particularly if a State has multiple regulated utilities, information sharing between utilities, and potentially PUCs, may be a very important step towards coordinated cyber defense.

Drivers for Cybersecurity Expenditures
Aside from good business practices by the utilities that dictate that they should prevent attacks on their systems, State regulators should understand three key additional areas that motivate and inform smart utility investments in cybersecurity: laws, enforceable standards and voluntary best-practice guidance.

Industry standards enforce legislation that utilities must meet, and these standards do not come cheaply. Standards require additional resources in the form of employees, hours and technology, all of which increases the cost of providing reliable electricity to the customer. Therefore, the standards of cybersecurity that protect the customer are then ultimately paid by the customer. So what are these standards and who sets them? Some of the most important sets of standards are described in this section.

NERC CIP
http://www.nerc.com/page.php?cid=6|69
The first step for developing cyber expertise is to understand, and where possible engage with, the NERC CIP Standards. These standards already drive a good deal of cybersecurity investments and, as greater coverage is applied to protection of the electric grid, this process will only become more important. NERC's CIP efforts include standards development, compliance enforcement, and supporting and providing technical subject matter expertise to the program. The committee consists of industry experts and reports to NERC's board of trustees in the areas of cybersecurity, physical and operational security. The U.S. Department of Energy (DOE) designated NERC as electricity sector coordinator for critical infrastructure protection.

NIST National Cybersecurity Center of Excellence
http://www.nist.gov/itl/csd/nccoe-022112.cfm
The National Institute of Standards and Technology (NIST) recently announced the establishment, in partnership with the state of Maryland and Montgomery County, Maryland, a National Cybersecurity Center of Excellence. The center will assume $12 million of NIST's 2012 budget and will bring together researchers, user and vendors in targeted tests to address cybersecurity issues.

NIST Smart Grid Interoperability Panel and Cyber Security Working Group
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG
NIST works collaboratively with industry and government agencies. A wide range of stakeholders and working groups make up the NIST Smart Grid Interoperability Panel (SGIP), responsible, through and

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

open consensus-based process, for interoperable standards aimed at enhancing economic security and quality of life. The SGIP's Cyber Security Working Group (CSWG) works to develop an overall cybersecurity strategy for the smart grid that includes a risk mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The CSWG has developed the NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, available here: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

The NARUC/NASEO Energy Assurance Guidelines
Along with NARUC, NASEO runs an energy assurance program to address state-level coordination on critical infrastructure protection, other national organizations are doing their part to address cybersecurity needs for the energy sector and to serve as resources to government decision makers.. More information about this program can be found here: http://naseo.org/energyassurance/.

Securities and Exchange Commission Corporation Finance Disclosure Guidance: Cybersecurity
http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
In October 2011, the SEC released this guidance to clarify the cybersecurity responsibility of publicly traded companies. Federal securities law requires that publicly traded companies report "material" risk – something that was not clearly defined or followed for cybersecurity risks before this document was released.[21] This is a vital moment because now a publicly traded company can consider cybersecurity as a business investment.

DHS Cross Sector Working Group – CIPAC
http://www.dhs.gov/files/committees/gc_1277402017258.shtm
The DHS Cross-Sector Security Working Groups include the Critical Infrastructure Partnership Advisory Council (CIPAC), which facilitates coordination between federal IP programs and the equivalent programs of private sector, State, local, territorial and travel entities. It also operates a forum in which government and critical infrastructure – key resource owners can coordinate critical infrastructure protection.

DHS National Cybersecurity & Communications Integration Center
http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
The National Cybersecurity & Communications Integration Center (NCCIC) falls under the DHS Office of Cybersecurity and Communications, as the central location for coordinating and integrating operations of cybersecurity and communications reliance. NCCIC serves many functions, including providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation and recovery actions.

DHS CSET
http://ics-cert.us-cert.gov/satool.html
The Cyber Security Evaluation Tool (CSET) was created by DHS to support organizations in protecting their key national cyber assets. Cybersecurity experts, under the direction of the DHS National Cyber Security Division (NCSD) and with assistance from NIST developed this tool to provide users with a systematic and replicable approach for assessing the security posture of their systems and networks.

---

[21] Jay Rockefeller and Michael Chertoff, "A new line of defense in cybersecurity, with help from the SEC," *The Washington Post*, November 17, 2011, http://www.washingtonpost.com/opinions/a-new-line-of-defense-in-cybersecurity-with-help-from-the-sec/2011/11/15/gIQAjBX8VN_story.html.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

DHS Cyber Resilience Review

The Cyber Resilience Review (CRR) is a complimentary, voluntary program provided by the Cyber Security Evaluation Program (CSEP), within DHS NCSD, to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services and assets. The CRR pays special attention to protection and sustainment practices with their ten established key domains of cyber resilience, generating a report that summarizes observed strengths and weaknesses in each domain. The report also suggests general guidance or activities to improve the cybersecurity posture and preparedness of the organization.

EEI Principles for Cybersecurity and Critical Infrastructure Protection

The Edison Electric Institute (EEI) released the principles in 2010 to address the electric utility industry's mandate to provide reliable power. EEI prioritizes collaboration between the State and federal level, as well as distinguishing between the priorities of responses to threats and vulnerabilities. The *EEI Principles for Cybersecurity and Critical Infrastructure Protection* can be found here: http://www.eei.org/ourissues/ElectricityTransmission/Documents/cyber_security_principles.pdf).

National Electric Sector Cybersecurity Organization (Resource)

http://www.energysec.org/Websites/energysec/files/Content/840313/2011.02.22_WhatIsNESCO_Webinar.pdf

To meet the "exponential increase in complexity in securing an ever growing electric grid with an increasing number of stakeholders," National Electric Sector Cybersecurity Organization (NESCO) creates a "comprehensive public private partnership to coordinate the efforts in the industry to meet the growing challenge of securing the electric sector." The Energy and Water Development and Related Agencies Appropriations Act of 2010enabled DOE to establish "an independent national energy sector cybersecurity organization." EnergySec and Electric Power Research Institute (EPRI) received fund awards to form NESCO and the National Electric Sector Cybersecurity Organization Resource (NESCOR). The two organizations bring together experts to strengthen the cybersecurity posture of the electric sector by working with the DOE Electricity Sector Information Sharing and Analysis Center and industry.

Smart Grid Investment Grant Cybersecurity Requirements

The American Recovery and Reinvestment Act of 2009 (Recovery Act) authorized funding for the DOE to modernize the electric power grid, including accelerating smart grid development through competitive selection of investment projects in a number of areas, one of which was cybersecurity.[22] This program, called the Smart Grid Investment Grant (SGIG) program, currently supports initiatives like Critical Intelligence Inc.'s Intelligence Training for Targeted Cyber Attacks based in Idaho to train energy sector information security employees to detect and respond to cyber threats (http://www.smartgrid.gov/project/critical_intelligence_inc), and broader programs such as Pepco's "Smart Grid Workforce Training Project" in Washington, D.C., which includes a cybersecurity component through compliance training as part of their overall implementation program (http://www.smartgrid.gov/project/pepco). The SGIG program is just one example of the hardening of the US smart grid currently in place.

[22] www.smartgrid.gov

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

NRECA Guide to Developing a Cybersecurity and Risk Mitigation Plan
http://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf
The National Rural Electric Cooperative Association (NRECA) cybersecurity plan addresses general business operations for cooperatives addressing critical infrastructure needs in their systems. The plan is based on the NISTIR 7628, a survey of standards and security concepts specifically for the smart grid.

DOE/NIST/NERC Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline
The Electricity Subsector Cybersecurity RMP Guideline, resulting from a collaboration between DOE, NIST and NERC, is a resource geared toward strategic long-term risk management mapped specifically to the electric sector. Authorship of the document, which is still in the works, includes industry and utility-specific trade groups. Please find the document here: http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
This initiative will serve as a tool for the electric sector to assess their security posture at a given point in time. Driven by the highest levels of the US government the resulting resource should be relevant and important, though as of this writing it remains a work in progress. The latest can be found here: http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012.

Developing Legislation
Congress has been working on comprehensive legislation for the past four years. Regardless of federal actions in this arena, however, State commissions should be tackling this issue within their jurisdictions to ensure a secure cyber future. The Congressional Research Service (CRS) provides good information on relevant legislation in their latest report, *Cybersecurity: Authoritative Reports and Resources*, which can be found here: http://www.fas.org/sgp/crs/misc/R42507.pdf.[23]

[23] Rita Tehan, "Cybersecurity: Authoritative Reports and Resources," *Congressional Research Service*, April 26, 2012.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Conclusion

Absolute cybersecurity is neither attainable, nor is it the end goal. What's more, according to NERC, addressing high-impact, low-frequency risk like cybersecurity requires the re-allocation of "already strained human and financial resources available to the sector."[24] Therefore, cybersecurity is best approached through a nimble and complex balance of functionality, security and cost. The reality of a "perfect" defense against cyber attack has a cost that may, and often does, outweigh the value of the information it protects. Simply put, the energy sector cannot expect to "gold plate" the grid. Planning for, protecting against, detecting and responding to cyber attack must take into account a dynamic relationship of systems, physical components, people and their function.

State utility regulators can and should:

- Create expertise within their own organizations
- Ask the right questions of utilities
- Assess their own cybersecurity and information protection capabilities
- Engage with other efforts led by the private sector, State agencies or federal officials, as well as engaging with processes that link these sectors

Regulators are already doing significant work to protect the grid, but the key to successful cybersecurity may prove to be the development of a partnership between public and private actors to create a cybersecurity structure and culture that can meet current needs while also being flexible enough to meet the ever-evolving threat.

[24] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," pg. 23

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Appendix A:

National Association of Regulatory Utility Commissioner

Sample Cyber Questions to Modify and Ask Your Utilities

The following questions grew out of several PUCs efforts to ask critical cybersecurity questions of utilities in an effort to ensure reliable electricity for their rate payers. NARUC has built the following list from those original questions, editing where necessary for sensitivities, clarity and general usage so that these questions could be used in commissions across the country. These are general questions, they are not exhaustive, nor are they all appropriate for every scenario or region. You must adapt the questions to your own taste, but when you do so, make sure the answers will not create vulnerabilities. These questions not only generate answers from utilities, but inspire their action to meet any gaps in current operations. Your utilities may not be particularly forthcoming with some of their answers, but their answers create a dialogue of understanding and responsibility in the event of a cyber attack.

Your needs for your PUC will vary – please modify these questions before using them in order to suit your needs. For example, drop the questions that are too difficult or are unnecessary! You do not need to use questions below which you think will yield answers that contain unnecessary or overly complex information. Where questions below reference a process or a plan that the utility probably has in hard copy, you may want to ask to see a copy of it.

You may want to describe to the utility how you will handle and safeguard the responses to these questions. Lastly, and most importantly, *do not ask questions whose answers can create vulnerabilities.*

Planning

Having a plan indicates that the response isn't piece-meal, reactive or fragmented. Asking planning questions aims to encourage proactive and strategic action on the part of the utilities, rather than a patchwork response.

1. Does your company have a cybersecurity policy, strategy or governing document?
2. Is the cybersecurity policy reviewed or audited? Internally or by an outside party? What qualifications does the company consider relevant to this type of review?
3. Does your cybersecurity plan contain both cyber *and* physical security components, or does your physical security plan identify critical cyber assets? (See the *Glossary, Appendix 2*, for helpful definitions).
4. Does your cybersecurity plan include recognition of critical facilities and/or cyber assets that are dependent upon IT or automated processing?
5. Are interdependent service providers (for example, fuel suppliers, telecommunications providers, meter data processors) included in risk assessments?

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

6. Does your cybersecurity plan include alternative methods for meeting critical functional responsibilities in the absence of IT or communication technology?

7. Has your organization conducted a cyber risk or vulnerability assessment of its information systems, control systems and other networked systems?

8. Has your company conducted a cybersecurity evaluation of key assets in concert with the National Cyber Security Division of the Department of Homeland Security? Has your company had contact with the National Cyber Security Division of DHS or other elements of DHS that may be helpful in this arena?

9. Has your cybersecurity plan been reviewed in the last year and updated as needed?

10. Is your cybersecurity plan tested regularly? Is it tested internally or by or with a third party?

11. What is your process/plan for managing risk? (Example: DOE/NIST/NERC Risk RMP)

12. Has your company undergone a whole-system, comprehensive cybersecurity audit or assessment? When and by whom?

Standards

Standards are an important driver of enforceable action with which regulators can attempt to ensure utilities' compliance.

13. Describe the company's compliance status with NERC CIP-002 through CIP-009. *(Note: Be aware that this may create double-reporting).*

14. What collaborative organizations or efforts has your company interacted with or become involved with to improve its cybersecurity posture (such as NESCO, NESCOR, Fusion centers, Infragard, US-CERT, ICS-CERT, ES-ISAC, SANS, the Cross-Sector Cyber Security Working Group of the National Sector Partnership, etc.)?

15. Can your company identify any other mandatory cybersecurity standards that apply to its systems? What is your company's plan for certifying its compliance or identifying that it has a timetable for compliance? *(Note: PUCs might also need to first establish standards for compliance they find suitable)*

16. Compliance as a floor, not a ceiling: are there beyond-compliance activities? Given that there are very little or no cybersecurity standards specified at this point by State regulatory authorities in regard to the distribution portion of the electrical grid, what are you doing to get in front of this?

17. How do you determine which systems, components and functions get priority in regard to implementation of new cybersecurity measures?

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

18. Is cybersecurity addressed differently for each major electrical component: distribution, transmission, generation, retail customers?

Procurement Practices

While the information of procurement seen upstream to vendors may only be proprietary to the utility, the decisions the vendor makes around procurement may contain key elements for cybersecurity. The questions below cover these aspects of procurement.

19. Has your organization conducted an evaluation of the cybersecurity risks for major systems at each stage of the system deployment lifecycle? What has been done with the results?

20. Are cybersecurity criteria used for vendor and device selection?

21. Have vendors documented & independently verified their cybersecurity controls? Who is the verifier and how are they qualified?

22. Are there third-party providers of services whose cybersecurity controls are beyond the ability of your organization to monitor, understand, or assure? Has your organization explored whether these may create cybersecurity vulnerabilities to your operations?

23. Does your organization perform vulnerability assessment activities as part of the acquisition cycle for products in each of the following areas: cybersecurity, SCADA, smart grid, internet connectivity and Web site hosting?

24. Has the company managed cybersecurity in the replacement and upgrade cycle of its networked equipment? Does this include smart meters?

25. What kind of guidance do you follow to ensure that your procurement language is both specific and comprehensive enough to result in acquiring secure components and systems? (Note: Does your company include Cyber Security Procurement Language for Control Systems within its Procurement Language? Available at http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf IEC 62443)

26. Would the company be willing to provide a presentation to Staff (as a closed, *in-camera* and non-disclosable setting with no documentation or materials coming into possession of the PUC)?

Personnel and Policies

Personnel, the people who run the systems we aim to protect, are key to ensuring cybersecurity. They way employees are hired, trained and separated from operations can make or break cybersecurity.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

27. Is cybersecurity budgeted for? What is the current budget for cybersecurity activities relative to the overall security spending?

28. Are individuals specifically assigned cybersecurity responsibility? Do you have a Chief Security Officer and do they have explicit cybersecurity responsibilities?

29. Does your company employ IT personnel directly, use outsourcing or employ both approaches to address IT issues? For companies that lack a full IT department, explain if one individual in your company is held responsible for IT security. (You may want to ask same questions in regard to Operations Technology (OT) [i.e. energy operations] security; larger companies may have separate staffs.)

30. What training is provided to personnel that are involved with cybersecurity control, implementation and policies?

31. What personnel surety / background checking is performed for those with access to key cyber components? Are vendors and other third parties that have access to key cyber systems screened?

32. For the most critical systems, are multiple operators required to implement changes that risk consequential events? Is a Change Management process in place, especially in regard to systems which could present a risk to electrical reliability?

33. Has business process cybersecurity has been included in continuity of operations plans for areas like customer data, billing, etc.?

34. Describe the company's current practices that are employed to protect proprietary information and customer privacy and personal information. Does the company have an information classification and handling policy?

35. Does the company collect personally identifiable information electronically? What type of information (name, address, social security number etc.) is collected? Is there a policy for the protection of this information? How is your company ensuring that any third parties you deal with are also keeping this information secure?

36. Identify whether the company has identified points of contact for cybersecurity:

    a. Emergency management / law enforcement?

    b. National security? DHS, including protective and cybersecurity advisors?

    c. Fellow utilities, ISO/RTO, NERC CIPC, others?

    d. NESCO, VirtualUSA, Einstein, Fusion centers, Infragard, US-CERT, ICS-CERT, ES-ISAC?

    e. Interdependent system service providers?

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Systems and Operations

Be aware that as the questioning agency, you want to consider carefully whether answers to the below questions are needed and, if so, whether the answers to them could create vulnerabilities to the system. Modify them to your needs accordingly.

37. Is cybersecurity integrated between business systems and control systems? For the existing grid and for the smart grid?

38. Have logical and physical connections to key systems been evaluated and addressed?

39. Does the company maintain standards and expectations for downtime during the upgrade and replacement cycle?

40. Does the company have equipment dependant on remote upgrades to firmware or software, or have plans to implement such systems? Does the company have a plan in place to maintain system cybersecurity during statistically probable upgrade failures? Is there a schedule for required password updates from default vendor or manufacturer passwords?

41. Has cybersecurity been identified in the physical security plans for the assets, reflecting planning for a blended cyber / physical attack?

42. Discuss what the PUC can do to assist your company in the area of cybersecurity.

43. What network protocols (IP, proprietary, etc.) are used in remote communications? Is the potential vulnerability of each protocol considered in deployment?

44. Does the company have a log monitoring capability with analytics and alerting – also known as "continuous monitoring"?

45. Are records kept of cybersecurity access to key systems?

46. Are systems audited to detect cybersecurity intrusions?

47. Are records kept of successful cybersecurity intrusions?

48. What reporting occurs in the event of an attempted cybersecurity breach, successful or not? To whom is this report provided (internal and external)? What reporting is required and what is courtesy reporting?

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Appendix B

Glossary	
All-Hazards Approach	Comprehensive approach to security that includes intentional, unintentional, man-made and naturally-occurring threats to the electric grid
Attestation[25]	The validation of all aspects of a component that relate to its safe, secure and correct operation
Authentication[26]	Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources
Authorization[27]	Verifying a user's permissions (after the user had been authenticated) for accessing certain resources or functionality
Bandwidth[28]	A communication channel the amount of information that can be passed through a communication channel in a given amount of time, usually expressed in bits per second
Boundary protection[29]	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels)
Bulk Electric System (BES) Cyber Asset[30]	A cyber asset that if rendered unavailable, degraded or misused would, within 15 minutes of its required operation, mis-operation or non-operation, adversely impact facilities, systems or equipment, which, if destroyed, degraded or otherwise rendered unavailable when needed, would affect the reliable operation of the bulk electric system
Connectivity[31]	The minimum number of nodes or links whose removal results in losing all paths that can be used to transfer information from a source to a sink
Confidentiality[32]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Contingency[33]	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element
Control Center[34]	Facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a

[25] Evgeny Lebanidze and Craig Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," *National Rural Electric Cooperative Association Cooperative Research Network* (2011): 113.
[26] *Ibid.*
[27] *Ibid.*
[28] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=5692
[29] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[30] NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012: 9.
[31] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6637
[32] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[33] *Ibid.*
[34] NERC, "Glossary of Terms Used in NERC Reliability Standards," 13.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

	Generation Operator for generation Facilities at two or more locations
Credential[35]	Information passed from one entity to another to establish the sender's access rights or to establish the claimed identity of a security subjective relative to a given security domain
Critical Assets[36]	Facilities, systems and equipment which, if destroyed, degraded or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system
Critical Infrastructure[37]	The assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety or any combination thereof
Cyber Asset[38]	Programmable electronic devices, including the hardware, software and data in those devices
Cybersecurity Incident[39]	A malicious act or suspicious event that: 1) Compromises, or was an attempt to compromise, the ESP or PSP, or 2) disrupts, or was an attempt to disrupt, the operation of a BES cyber system
Denial of Service (DoS) [40]	Unauthorized prevention or (for time-critical operations) delay of any part of an information system (IS) from legitimate access or functioning
Deterrence	Designing a system to that an attack would be unprofitable, limited in scope and easily traceable
Electronic Security Perimeter (ESP)[41]	The logical border surrounding a network to which systems are connected
Energy Assurance	Infrastructure that is robust, secure, provides reliable energy and is able to restore services rapidly in the event of any disaster
Encryption (also encipherment)[42]	The cryptographic transformation of data that produces coded text
Firmware	Embedded software that cannot be modified, but allows reading and executing software
Header[43]	The portion of a message that contains information used to guide the message to the correct destination. *Note:* Examples of items that may be in a header are the addresses of the sender and receiver, precedence level, routing instructions and synchronizing bits
Identity-Based Access Control[44]	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of

[35] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6764
[36] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[37] U.S. Department of Homeland Security, "Critical Infrastructure," (May 23, 2012): http://www.dhs.gov/files/programs/gc_1189168948944.shtm.
[38] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[39] NERC, "Glossary of Terms Used in NERC Reliability Standards," 14.
[40] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[41] NERC, "Glossary of Terms Used in NERC Reliability Standards," 18.
[42] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=8119
[43] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=4731
[44] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

	that user) where access authorizations to specific objects are assigned based on user identity
Impacta[45]	Damage to an organization's mission and goals due to the loss of confidentiality, integrity or availability of system information or operations
Incident[46]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of a system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies
Information Security[47]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability
Information System[48]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information (Note: information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems and environmental control systems.)
Information Technology	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information
Integrity[49]	Guarding against improper information modification or destruction; includes ensuring the non-repudiation and authenticity of information
Internet protocol	A formal set of conventions (both semantic and syntactic) governing the format and control of interaction among parts of the system that communicate with each other
Interoperability[50]	Ability of diverse systems and their components to work together; enables integration, effective cooperation and two-way communication among the many interconnected elements of the electric power grid
Least Privilege	Principle of having access to the least information or fewest resources necessary to complete a legitimate purpose
Latency[51]	Refers to the speed with which network data is transmitted or processed. A system with low latency communicates more quickly, while a high latency connection generally communicates less frequently and has longer delays
Loss Containment	Protecting the overall system, even if some individual components can be compromised

[45] *Ibid.*
[46] *Ibid.*
[47] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[48] *Ibid.*
[49] *Ibid.*
[50] NIST, "NIST & the Smart Grid," (May 23, 2012): http://www.nist.gov/smartgrid/nistandsmartgrid.cfm.
[51] Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," 5.

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Management controls[52]	The security controls (i.e., safeguards or countermeasures) of an information system that focus on the management of risk and of information system security
Need to Know	A practice that restricts information or resources in the execution of a task outside of what is critical in order to complete that task, despite clearance level
Network (Computer Network)[53]	Collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information or receiving a message
Operational controls	The security controls (i.e., safeguards or countermeasures) of an information system that are primarily implemented and executed by people (as opposed to systems)
Packet[54]	The sequence of binary digits transmitted and switched as a composite whole
Physical Security Perimeter (PSP) [55]	The physical border surrounding locations in which cyber assets, systems or electronic access control systems reside and for which access is controlled
Potential impact[56]	The loss of confidentiality, integrity or availability that might be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets or individuals
Privileged user[57]	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform
Programmable logic controller (PLC)[58]	A digital computer used for the automation of electromechanical processes
Resilience	The ability to restore services rapidly in the event of any disaster
Right-to-Know	Legal principle that a citizen has the right to know a piece of information about a potential hazard
Risk[59]	Measure of the extent to which an entity is threatened, typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Security risks related to information security arise from the loss of confidentiality, integrity or availability of information or information systems with potential adverse impacts on operations

[52] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[53] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6555
[54] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=30770
[55] NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012:36.
[56] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[57] *Ibid.*
[58] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 115.
[59] *Ibid.*

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Risk management	The process conducting a risk assessment, implementing a risk mitigation strategy and employing of techniques and procedures for the continuous monitoring of the security state of the information system. Risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place – synonymous with risk analysis
Risk severity[60]	A combination of the likelihood of a damaging event actually occurring and the assessed potential impact on the organization's mission and goals if it does occur
Role-based access control[61]	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals
Sensitive information[62]	Information of which the loss, misuse, unauthorized access or modification could adversely affect the organization, its employees or its customers
Smart Grid	Modernization of electricity infrastructure through added technology, allowing the grid to gather and store data, to create a "dialogue" between all components of the grid, and allowing for automatic command and response within the function of the grid
Supervisory Control and Data Acquisition (SCADA)	Systems that monitor and control industrial, infrastructure or facility-based processes, such as automatic (and often remote) control devices. They include simple functions such as "on/off" and sensor capability, communications capability and the human-machine interface (HMI) that connects them to people operating the system
Threat	The potential for an actor, circumstance or event to adversely affect assets, people or organizational operations of the system
Traffic[63]	The information moved over a communication channel, including the quantitative measurement of the total messages and their length, expressed in CCS or other units, during a specified period of time
Virus	An unwanted computer program that replicates itself and spread from one computer to another. "Virus" is often incorrectly used to refer to malware, including adware and spyware programs, which do not have a reproductive ability
Vulnerability	A specific weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source

[60] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 115.
[61] *Ibid.*
[62] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 116.
[63] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=649

This research document is presented for consideration by the membership of the National Association of Regulatory Utility Commissioners (NARUC). This document does not represent any NARUC policy nor those of any of its members.

Attachment 2

State of Florida

Public Service Commission

CAPITAL CIRCLE OFFICE CENTER • 2540 SHUMARD OAK BOULEVARD
TALLAHASSEE, FLORIDA 32399-0850

-M-E-M-O-R-A-N-D-U-M-

DATE: July 29, 2016

TO: Braulio L. Baez, Executive Director

FROM: Benjamin Crawford, Public Utilities Supervisor, Office of Industry Development and Market Analysis
James E. Breman, Senior Analyst, Office of Industry Development and Market Analysis
Cayce H. Hinton, Director, Office of Industry Development and Market Analysis
Kathryn Gale Winter Cowdery, Senior Attorney, Office of the General Counsel

RE: Briefing on the U.S. Environmental Protection Agency's Proposed Rule Addressing The Clean Energy Incentive Program

CRITICAL INFORMATION: Please place on the August 9, 2016 Internal Affairs. **Direction sought.**

On June 30, 2016, the U.S. Environmental Protection Agency (EPA) published in the *Federal Register* a proposed rule addressing design details of the Clean Energy Incentive Program (CEIP).[1] Comments on the proposed rule are due to the EPA by September 2, 2016. The CEIP is a voluntary program established by the rules on Carbon Pollution Emission Guidelines for Existing Stationary Sources: Electric Generating Units (Clean Power Plan). Attachment A provides a summary of the proposed rule. Attachment B is a draft comments should the Commission decide to file comments on the proposed rule. Staff seeks direction on whether to file comments regarding the proposed CEIP rule.

Attachments

cc: Keith Hetrick, General Counsel
Mark Futrell, Deputy Executive Director, Technical
Apryl Lynn, Deputy Executive Director, Administrative

[1] https://www.gpo.gov/fdsys/pkg/FR-2016-06-30/pdf/2016-15000.pdf

Clean Energy Incentive Program Design Details [Docket ID: EPA–HQ–OAR–2016–0033]

Background

As first introduced in the final Clean Power Plan (CPP), the EPA provided a broad outline of a new program entitled the Clean Energy Incentive Program (CEIP). The CEIP was described as providing to states and tribes the option to adopt or include in CPP State Implementation Plans (SIP) both demand-side energy efficiency programs in low-income communities, and certain renewable energy projects. The intent of the CEIP was to encourage early emission reduction during the two-year period immediately prior to the beginning of the CPP compliance period.

The CEIP creates an incentive through the issuance of pollution trading instruments during 2020 and 2021. In the CPP, EPA established two types of pollution trading instruments, allowances and emission rate credits (ERC). An allowance authorizes the holder to emit one ton of carbon dioxide. An ERC certifies that the holder generated or avoided one MWh with zero emissions of carbon dioxide. The trading of allowances is associated with a mass-based compliance strategy while ERC trading is associated with a rate-based compliance approach. All allowances or ERCs issued under the CEIP can be used for CPP compliance purposes after 2021.

In the CPP, the CEIP renewable energy projects were limited to solar and wind technology projects that commenced construction on or after September 6, 2018. Demand-side energy efficiency programs in low-income communities that commenced on or after September 6, 2018, could qualify for the CEIP if they are included in the state's CPP compliance filing and are in operation during 2020 and 2021. Qualifying energy efficiency programs would receive twice the allowances or ECRs that renewable energy projects would receive.

Additionally in the CPP, EPA established a set-aside reserve of 300 million allowances for the CEIP. The set-aside reserve is part of the total 5.9 billion allowances that were authorized for the 2022-2024 CPP compliance period. Separate from the set-aside reserve, an additional 300 million matching or bonus allowances would also be available during the 2020-2021 period for qualified CEIP programs. This would potentially double the number of total early reduction allowances available to states under the CEIP.

EPA noted at the time of the release of the final CPP rule that further program design details would be developed through other rules. Notably, the CPP did not provide detailed guidance on the distribution of trading instruments to demand-side energy efficiency programs in low-income communities and renewable energy projects. There was no description of the set-aside reserve in terms of ERCs. Also, the proposed Model Trading rules provided no guidance regarding the tracking of early-issued ERCs for states considering a rate-based compliance strategy.[2]

The proposed CEIP rule released on June 30, 2016, formalizes and further clarifies the CEIP program in these areas. Comments to the EPA on this proposed rule are due September 2, 2016.

[2] The Model Trading rules, proposed October 3, 2015, addressed general oversight and tracking of allowances and ERCs for CPP compliance purposes. https://www.gpo.gov/fdsys/pkg/FR-2015-10-23/pdf/2015-22848.pdf

Summary of Changes

The proposed CEIP rule incorporates many program features first identified in the CPP rule as well as revisions included in the Model Trading rules. The proposed CEIP rule also includes additional program clarifications and new provisions. Major revisions and additional provisions include:

- Additional qualifying renewable energy programs – Geothermal and hydropower programs were added to the renewable program list that previously allowed only solar and wind projects.
- Additional qualifying low-income programs – Solar projects that directly benefit a low-income community were added to the list that allowed energy efficiency programs.
- Revised definition of when a renewable energy project can become eligible – The phrase "commence construction" was replaced with "commence commercial operation."
  - Projects that commence commercial operation by beginning to sell or provide usable electricity on or after January 1, 2020.
- Clarification of definition of "commence construction" for demand-side energy efficiency projects.
  - Projects located in or providing usable electricity to the benefit of low-income communities that commence operation by delivering quantifiable and verifiable electricity savings on or after September 6, 2018.
- Total CEIP set-aside reserve – EPA reaffirmed the cap of 300 million allowances. The associated cap of ERCs is 375 million.
  - Un-awarded CEIP set-aside reserve allowances or ERCs will be retained by the state for issuance under the CPP during 2022-2024.
- Total matching EPA reserve – The cap is the same as for the CEIP set-aside reserve. The matching EPA reserve must be divided equally between demand-side energy efficiency programs in low-income communities and renewable energy projects.
  - Un-awarded matching allowances or ERCs will be retired by January 1, 2023.
- CEIP programs must meet the same evaluation, measurement, verification and reporting requirements as any other CPP programs.
- Definition of "low-income community" – EPA will allow states and tribes to use one or more existing definitions of low-income communities as long as the definitions existed prior to October 23, 2015.
- Example approaches for implementing a CEIP program – EPA supplied optional regulatory CEIP program text for either a mass-based or rate-based emission reduction plan that a state may use in the CEIP portion of its SIP.

Estimated Allocations to Florida

Under a mass-based compliance strategy, Florida's CPP 2022-2024 allowance allocation, including the CEIP set-aside reserve, is 358,141,341 allowances. The Florida CEIP set-aside reserve is capped at 9,690,744 allowances for issuance to qualifying demand-side energy efficiency programs in low-income areas and renewable energy projects. Unissued Florida CEIP set-aside reserve allowances will be retained by Florida for purposes of the 2022-2024 CPP compliance period.

EPA determined the equivalent ECRs for a rate-based compliance strategy using 2012 actual data. Florida's CEIP set-aside reserve of ERCs is 12,113,430. The ERC set-aside reserve is otherwise administered similar to the allowance set-aside reserve. However, to account for issued CEIP ERCs that are drawn from the 2022-2024 CPP compliance period, the 2022-2024 issued ERCs are reduced on a prorated basis.

Tables 1 and 2 below, provide examples showing Florida's CEIP set-aside reserve allowances and ERCs under a mass-based and a rate-based CPP compliance strategy, respectively. Additionally, as previously discussed, EPA has proposed to authorize matching allowances or ERCs on a one-to-one basis. Thus, each issued CEIP set-aside reserve allowance or ERC will be doubled. The EPA matching allowances or ERCs will double the amounts indicated in Tables 1 and 2 without changing any other aspects of the CEIP allocations or CPP performance requirements.

Table 1

Florida's CEIP Mass-Based Allowance Set-Aside Reserve (Allowance = Emit 1 ton of CO_2)			
Allowances are issued on a project basis using MWHs provided or avoided during the Pre-CPP period of 2020 and 2021	Issued During Pre-CPP Period 2020-2021		
	Renewables	EE & Solar to Low-Income	Total Set-Aside Reserve
Each category receives 50% of total set-aside reserve	4,845,372	4,845,372	9,690,744
Allowances/year	2,422,686	2,422,686	
EPA issuance factors (tons/2 MWh)	80%	160%	
Maximum annual MWhs	6,056,715	3,028,358	
CEIP 2020-2021 Total MWhs	12,113,430	6,056,715	18,170,145

Source: Based on proposed CEIP Rule

Table 2

Florida's CEIP Rate-Based Emission Rate Credit (ERC) Set-Aside Reserve (ERC = zero emitting MWH or exceeding CO_2 rate standard)			
ERCs are issued on a project basis using MWHs provided or avoided during the Pre-CPP period of 2020 and 2021	Issued During Pre-CPP Period 2020-2021		
	Renewables	EE & Solar to Low-Income	Total Set-Aside Reserve
Each category receives 50% of total set-aside reserve	6,056,715	6,056,715	12,113,430
Annual ERCs/year	3,028,358	3,028,358	
EPA issuance factors (ERC/2 MWh)	100%	200%	
Maximum annual MWhs	6,056,715	3,028,358	
CEIP 2020-2021 Total MWhs	12,113,430	6,056,715	18,170,145

Source: Based on proposed CEIP Rule

Internal Affairs Memorandum
July 29, 2016

Attachment B

STATE OF FLORIDA

JULIE I. BROWN
CHAIRMAN

Capital Circle Office Center
2540 Shumard Oak Boulevard
Tallahassee, FL 32399-0850
(850) 413-6042

Public Service Commission

September 2, 2016
DRAFT LETTER

Administrator Gina McCarthy
Air and Radiation Docket and Information Center
Environmental Protection Agency
Mailcode 28221T
1200 Pennsylvania Avenue NW
Washington, DC 20460

RE: Florida Public Service Commission Comments on the Clean Energy Incentive Program Rule for the Clean Power Plan (Docket ID: EPA-HQ-OAR-2016-0033)

Dear Administrator McCarthy:

The Florida Public Service Commission (FPSC or Commission) respectfully requests the consideration of comments as provided herein on the proposed rule addressing the Clean Energy Incentive Program design details. The FPSC recognizes the necessity and role of the Environmental Protection Agency (EPA) in addressing public health and environmental issues. Section 366.105, Florida Statutes, encourages the FPSC to participate in federal proceedings that impact the utilities we regulate. The FPSC submitted comments on December 1, 2014, regarding the Clean Power Plan.[3] A portion of those comments expressed the FPSC's concerns regarding the Clean Power Plan's effects on Florida's generating fuel diversity and the impacts that implementation of the Clean Power Plan may have on reliability and cost to Florida's electric customers. The Commission renewed its concerns in its January 21, 2016 comments regarding the proposed Federal Plan and Model Rules.[4]

Electric usage in Florida is impacted by the state's unique weather, customer base, and high reliance on electricity for cooling and heating. Florida stands out as having the highest number of cooling degree days of any state in the continental U.S. This indicates the greatest use for air conditioning in the summer months compared with other states. Florida's electricity customers are almost 89 percent residential. Over 80 percent of these residential customers have energy requirements that are met with electricity, rather than the direct use of natural gas or other fuels for cooling and heating. This makes Florida's customers particularly sensitive to electric rate

[3] http://www.floridapsc.com//Files/PDF/Dockets/Federal/Comments_EPA_12_1_2014.pdf
[4] http://www.floridapsc.com//Files/PDF/Dockets/Federal/FPSC%20comments%201.21.16%20Dkt%20EPA-HQ-OAR-2015-0199.pdf

increases and reliability of service fluctuations. This sensitivity, combined with Florida's geography and climate, requires the FPSC to carefully examine all factors related to electric generation and energy efficiency programs to ensure cost-effective, reliable electricity for all Floridians.

In 2015, Florida utilities had a net summer generating capacity of 58,421 MW.[5] Electric transmission capacity to import energy into peninsular Florida from other states is approximately 3,600 MW, some of which is already committed to the import of out-of-state generation to meet the state's current and future power needs. The Florida Legislature has enacted policies that establish electric generation fuel diversity as a consideration in the review of utility resource plans and in the approval of new generation, and has emphasized fuel diversity in policies that address renewable resources.[6] Currently, approximately 60 percent of the electric power in Florida is generated from natural gas.

Florida law requires the FPSC to determine the need for new generating facilities, and specifically to consider the need for electric system reliability and integrity. This process involves ensuring adequate electricity at a reasonable cost and assessing the need for fuel diversity and supply reliability.[7] It is important for Florida to maintain a diversified generation fuel source mix when seeking to comply with relevant CO_2 standards. This diversified fuel supply can enhance system reliability and significantly mitigate the effects of volatile fuel price fluctuations, extreme weather events, and unplanned plant outages. One of Florida's primary supply pipelines crosses the Gulf of Mexico and is subject to the risk of hurricanes, which adds to the concerns from diminished fuel diversity.

Florida law also gives the FPSC exclusive jurisdiction to implement the Florida Energy Efficiency and Conservation Act (FEECA).[8] FEECA emphasizes reducing the growth rates of weather-sensitive peak demand, electricity consumption, and consumption of expensive resources, such as petroleum fuels. Pursuant to FEECA, the FPSC has authority to adopt goals for increasing the efficiency of energy consumption and increasing the development of demand-side renewable energy systems.[9] Importantly, in adopting these goals, the FPSC evaluates the full Florida-specific technical potential of all available demand-side conservation and efficiency measures, and takes into consideration the costs and benefits to participating customers and ratepayers as a whole, and the costs imposed by state and federal regulations on greenhouse gas emissions.[10] Once goals are established by the FPSC, the utilities must submit cost-effective demand-side management (DSM) plans, which contain the DSM programs designed to meet the approved goals. Among its powers, the FPSC may modify or deny demand-side management plans or programs that would have an undue rate impact from the costs passed on to customers.[11]

---

[5] Florida Reliability Coordinating Council (Regional Load and Resource Plan) (May 2016) p. S-7. http://www.floridapsc.com/Files/PDF/Utilities/Electricgas/TenYearSitePlans/2016/FRCC.pdf
[6] Sections 186.801, 366.91, and 403.519, Florida Statutes.
[7] Section 403.519(3), Florida Statutes.
[8] Sections 366.80-366.82, Florida Statutes
[9] Section 366.81, Florida Statutes
[10] Section 366.82(3), Florida Statutes
[11] Section 366.91(5) and (6), Florida Statutes

The Clean Energy Incentive Program is intended to promote energy efficiency in low income communities through the early issuance of allowances or emission rate credits. In the most recent FEECA DSM goal-setting proceeding, the Commission ordered the utilities to educate low-income communities on energy efficiency opportunities.[12] Each utility presented programs within its DSM plan that addressed low-income conservation efforts. For each company, these programs mainly focused on efforts to provide weatherization opportunities to residential homes for purpose of conserving energy. In many cases, the utilities have established partnerships with government and non-profit agencies to develop programs that educate low-income customers on conservation and the financial benefits of using less energy.

The CEIP is also intended to promote renewable resources through early issuance of tradeable instruments. Though not opposed to the promotion of renewable energy, the FPSC is concerned about the impact of additional intermittent resources on service reliability requirements. Due to the state's unique characteristics described herein, Florida requires a robust, diverse, and dispatchable baseload generating fleet. However, many zero-carbon technologies that can be deployed in Florida are intermittent, non-dispatchable, non-baseload technologies. For example, in 2013, the monthly capacity factor for solar photovoltaics in the U.S. ranged from 13 to 22 percent.[13] Due to operational constraints from the availability of sunshine, there is no currently demonstrated baseload solar option. These low capacity factors mean that the requirement for reliable backup energy generation is not removed and each utility must continue to ensure it can economically fulfill its obligation to provide service (inclusive of the intermittent resources). Consequently, the need for existing power plants and transmission systems remains and reliability requirements may necessitate new natural gas fired facilities to address increased reliance on intermittent resources.[14]

The FPSC continues to support the general principles for federal environmental regulations as established in the National Association of Regulatory Utility Commissioners' (NARUC) resolution, entitled "Resolution on Increased Flexibility with Regard to the EPA's Regulation of Greenhouse Gas Emissions from Existing Power Plants."[15] The resolution was approved by the Board of Directors of NARUC at its 2013 Annual Meeting in November 2013. NARUC resolved that "the guidelines should provide sufficiently flexible compliance pathways or mechanisms that recognize State and regional variations."

The FPSC takes no position on certain aspects of the form and specificity of EPA's Clean Energy Incentive Program. However, EPA's rule should recognize that businesses involved in renewable energy projects will economically optimize the timing of projects and programs when clear performance requirements are expressed. Presently, there is uncertainty regarding the compliance timelines of the Clean Power Plan due to ongoing litigation. Since the Clean Energy Incentive Program is voluntary, EPA should allow all projects that commence construction after October 23, 2015, (publication date of the Clean Power Plan Rule) to qualify for inclusion in the

[12] Order No. PSC-14-0696-FOF-EU, Docket Nos. 130199-EI through 130205-EI, In re: Commission review of numeric conservation goals, issued December 16, 2014.
[13] U.S. Energy Information Agency, Electric Power Monthly (February 2014), Table 6.7.B.
[14] http://www.brattle.com/system/publications/pdfs/000/005/060/original/Solar_Energy_Support_in_Germany_-_A_Closer_Look.pdf?1406753962
[15] http://pubs.naruc.org/pub/53A0C721-2354-D714-5119-A6E9EFD6F5BE

Clean Energy Incentive Program. This flexibility promotes smooth phasing into commercial service while avoiding accumulation of projects and programs targeting a startup date of January 1, 2020. The FPSC respectfully submits that the Clean Energy Incentive Program Rule must allow states the opportunity to provide electric utilities the flexibility to choose the most efficient, least-cost compliance option to meet public health and environmental requirements.

Thank you for your consideration of the foregoing comments. Please let me know if you have any questions or concerns.

Sincerely,

Julie I. Brown, Chairman
Florida Public Service Commission

JB:jb

cc: Commissioner Lisa Polak Edgar
Commissioner Art Graham
Commissioner Ronald A. Brisé
Commissioner Jimmy Patronis
Jonathan P. Steverson, Secretary, Florida Department of Environmental Protection

II. Outside Persons Who Wish to Address the Commission at Internal Affairs

Note: The records reflect that no outside persons addressed the Commission at this Internal Affairs meeting.

III. Supplemental Materials for Internal Affairs

Note: The records reflect that there were no supplemental materials provided to the Commission during this Internal Affairs meeting.

IV. Transcript

BEFORE THE
FLORIDA PUBLIC SERVICE COMMISSION

PROCEEDINGS:	INTERNAL AFFAIRS
COMMISSIONERS PARTICIPATING:	COMMISIONER JULIE I. BROWN COMMISSIONER LISA POLAK EDGAR COMMISSIONER ART GRAHAM COMMISSIONER RONALD A. BRISÉ COMMISSIONER JIMMY PATRONIS
DATE:	Tuesday, August 9, 2016
TIME:	Commenced: 1:30 p.m. Concluded: 1:42 p.m.
PLACE:	Gerald L. Gunter Building Room 105 2540 Shumard Oak Boulevard Tallahassee, Florida
REPORTED BY:	Andrea Komaridis Court Reporter and Notary Public in and for the State of Florida at Large

PREMIER REPORTING
114 W. 5TH AVENUE
TALLAHASSEE, FLORIDA
(850) 894-0828

P R O C E E D I N G S

CHAIRMAN BROWN: Today is Tuesday, August 9th. This is the internal affairs agenda. The time is 1:30.

I do want to just point out that I was very excited about our program today. We had Miles Keogh from NARUC coming in to give us a wonderful presentation in kind of a roundtable discussion with our staff, too, on cyber-security issues.

And he spent a great deal of time preparing for that. And really want to thank Mark Futrell for the work that you've done along with other staffers who really put a lot of effort into it.

But you know, Delta -- it's challenging on a good day to get into Tallahassee. So, he had -- he had some problems. But we will be rescheduling that. So, I hope it will be a very fruitful, productive discussion in the near future.

So, we're going to have a very brief internal affairs today. We have one major item here. And we have staff who is here to give us an overview. So, with that, good morning -- afternoon.

MR. CRAWFORD: Good afternoon, Commissioners. I am Ben Crawford with the Office of Industry Development and Market Analysis.

On June 30th, 2016, the U.S. Environmental Protection Agency published in the Federal Register a proposed rule addressing design details of the Clean Energy Incentive Program or CEIP.

I'm here to provide you with the briefing on the CEIP and to get direction from the Commission on whether to file comments with the EPA regarding the proposed rule. Comments are due on September 2nd, 2016. And staff has provided a draft letter, if the Commission would like us to submit it to the EPA.

The CEIP is a voluntary program established by the Carbon Pollution Emission Guidelines for existing stationary sources and electric-generating units, better know as the Clean Power Plan or CPP.

The CEIP provides a means of recognizing early CPP compliance actions for projects located in low-income areas, as well as new renewable-energy projects prior to the official commencement of the CPP in 2022.

Numerous provisions have been changed from the version of the CEIP introduced in the Clean Power Plan. Additional technologies, specifically geothermal and hydropower, were added to the renewable-energy list, and solar was added to the

low-income projects list.

The day the project became eligible was changed from commencement of construction to the commencement of commercial operations. These changes, as well as others, are all detailed as part of Attachment A.

Renewable energy can consist of solar, wind, geothermal, or hydropower, and must begin commercial operation on or after January 1st, 2020, to be eligible for the CEIP. Energy efficiency or solar programs in low-income communities must lower electric bills for people in the low- -- in these low-income communities and must begin commercial operation -- commercial service -- I'm sorry -- on or after September 6th, 2018. States can also receive matching allowances from the EPA.

Depending on a state's CPP appliance -- compliance approach, these projects generate either allowances or Emission Rate Credits, known as ERCs. Each allowance authorizes the holder to emit one ton of carbon dioxide. And the ERC certifies that the holder either generated one megawatt hour with zero emissions of carbon dioxide or avoided generating one megawatt hour entirely.

Allowances for states that use a mass base

compliance strategy, which is states that have a total emissions goal they are trying to reach -- and ERCs are for states that have rate-base compliance goals; states that are trying to reach an average emissions per megawatt hour generated.

We have one late development that Kathryn was going to address.

MS. COWDERY: It has to do with the request for extension of time that was filed by 27 states, including the state of Florida. These are the same states that are challenging the Clean Power Plan.

They've requested EPA, by letter, to extend the time for filing comments until -- basically until the end of litigation on the Clean Power Plan, which we would anticipate sometime in 2017, 2018. But at this time, September 2 remains the deadline for filing comments.

MR. CRAWFORD: Staff also has an oral modification. It's just a typo. On Page 3 of part of Attachment A, the fourth bullet point, it reads "commence construction"; it's meant to say "commence operations."

Staff is seeking guidance on whether or not the Commission wishes to file comments with the EPA regarding the CEIP. Staff has provided draft

comments as Attachment B. Comments are due to the EPA, as said, on September 2nd. And the next internal affairs is currently scheduled for September 13th.

Staff is available to answer any questions you may have.

CHAIRMAN BROWN: Excellent. And thank you for preparing this --

MR. CRAWFORD: You're welcome.

CHAIRMAN BROWN: -- this letter in advance for our review and -- and some updates. And thank you, Kathryn, as well, for keeping us informed via e-mail on all updates with regard to the litigation. So, thank you for all of that.

Before I turn to the other Commissioners, I do want to turn to Commissioner Edgar, since this is very near and dear to her expertise level, and find some input and -- on the approach and any additional comments you may have.

COMMISSIONER EDGAR: Sure. Thank you, Madam Chair.

I also am appreciative to the staff for preparing this information, keeping us all up to current as things are moving, even though they are moving a little slower than they were at one point

in time, but continuing to stay on top of it and to coordinate with other agencies, of course, that we work with on these sorts of issues.

When the Supreme Court first issued its stay, one of the earliest things EPA did was try to assess from their legal perspective what, if any, pieces of their overall proposal they could continue to work on, and what things were -- were completely put on hold due to the stay.

This very small piece of their larger-umbrella plan, the CEIP, is one that they've said from the get-go, after the stay, was something that they were going to continue to work on, felt very strongly that they had that legal authority, and wanted to be in the position to give states who might want to participate legal direction so that they could move forward.

So, from the comments that -- the draft comments for us that -- well, I -- let me back up. So, to see that they are moving forward on this very small, very narrow piece is certainly not a surprise. They've been very clear about their intention on that from the beginning.

The comments that the staff have prepared are good. They are very, you know -- very much a

repeat of the messages that we have -- have sent during other comment windows.

I think that the paragraph at the bottom of Page 8 is really kind of the key, the meat of it, so to speak, which basically just asks for flexibility to states and recommends setting the time frame to participate for projects that -- that would be -- that it could apply to as slightly earlier than what they have -- are saying, which I -- I think is -- is very reasonable -- is a very reasonable approach.

So, I would be in favor of us supporting these comments, again, recognizing that it is a very narrow piece of the overall program that will be moving forward. And I think it's good for Florida to weigh in when we can.

CHAIRMAN BROWN: Excellent. Thank you, Commissioner Edgar, for those points and feedback.

Do you have any suggestions of any kind of modifications to the letter?

COMMISSIONER EDGAR: I do not. It is a staff product and -- but I certainly would be open to any, if the others do.

CHAIRMAN BROWN: Thank you.

Commissioners, any thoughts, comments,

agreement?

Commissioner Graham?

COMMISSIONER GRAHAM: I don't have any changes I want to propose to the letter, but I -- I guess I would propose that staff would hold on to the letter until just before this September 2nd date just in case we get notification that they've pushed all this stuff back and held it back.

MR. CRAWFORD: Yeah, we can -- we can definitely do that. We usually, you know, wait until the submittal date or --

COMMISSIONER GRAHAM: Yeah, let's just make sure that we get it there, but --

COMMISSIONER PATRONIS: Definitely.

MR. CRAWFORD: Yeah. Yeah.

COMMISSIONER GRAHAM: -- there is no need to send it out tomorrow.

MR. CRAWFORD: And -- and if -- if --

COMMISSIONER PATRONIS: Good point.

MR. CRAWFORD: In the event that there is some sort of extension on time or if -- if EPA elects to delay or there is a court issue, we would hold off and seek additional direction from the Commission, definitely.

COMMISSIONER GRAHAM: Thank you.

COMMISSIONER EDGAR: I'm very comfortable with that.

CHAIRMAN BROWN: Sounds like a good suggestion.

Any other comments or feedback?

Can I get a motion to approve the letter submitting these comments and letter to EPA?

COMMISSIONER PATRONIS: So moved.

COMMISSIONER EDGAR: Move approval. Second.

COMMISSIONER PATRONIS: Second.

CHAIRMAN BROWN: All those in favor, say aye.

(Aye, in unison.)

CHAIRMAN BROWN: All right. Thank you.

Thank you for your work on this. Greatly appreciated.

Moving along to our general counsel's report, who has been busy --

MR. HETRICK: Yes. Thank you, Madam Chair. Obviously, we're in deep preparation for the FP&L rate case coming up. I would like to congratulate Bart Fletcher and Suzanne Brownless for all the effort and time they've put in -- and not just them, but all of the staff that's working around the clock, weekly and on weekends. We do have AC on weekends for them to -- all of us to bring

together and get this case in proper order for you and for you, Ms. Pre-hearing Officer.

So, thank you very much.

COMMISSIONER EDGAR: I'll just chime in, if I may, and say, ditto, ditto, ditto. I know that our legal staff and our technical staff are working very hard on this. In fact, Suzanne brought me five draft orders today, so -- which we are turning around and getting out. So, everything is very much in process. Pre-hearing is scheduled for Friday.

CHAIRMAN BROWN: We will all be tuning in. Thank you. Thank you.

And executive directors' report?

MR. BAEZ: No specific items, Madam Chair. Your next IA is on September 13th. You all know we closed our fiscal year at the end of June 30th, and we're busy closing our books.

And we will most likely probably do a walk-around to -- to fill you in on the tale of the tape for the last fiscal year with the details. So, we'll be checking with each of your offices individually for a visit.

CHAIRMAN BROWN: Thank you.

Any questions for the executive director?

Okay. Thank you for your report.

MR. BAEZ: Thank you.

CHAIRMAN BROWN: Moving on to other matters. Are there any other matters that the Commissioners have?

I do. I just wanted to recognize our resident creative expert here. I think she's in the room. Ms. Laura, please come up to the table, if you could. She has helped almost every single person in this room.

Laura is -- we are very lucky to have Laura back here. She's been with the Commission since 1989 and is truly the artistic maestro of the group, comes up with things that people get paid, oh, gosh, so much money. And we're just so lucky to have you here as a state employee with your skill set.

And we've all recognized you. Your fellow colleagues here have recognized you. And you're very dedicated. And your sweet, kind spirit is always a joy to be around. So, thank you so much for being the employee of the month for August. And I wanted to give you this.

And we'll take a selfie after (laughter).

(Applause.)

CHAIRMAN BROWN: So, if there are no other matters or if anybody has any further comments --

COMMISSIONER EDGAR: Did anybody have a birthday recently?

CHAIRMAN BROWN: We have a few people -- where is Bruce Ritchie?

(Laughter.)

CHAIRMAN BROWN: Internal joke in the internal affairs room. No.

Thank you very much, you all, for coming. And this is a very short, brief internal affairs. And it is adjourned. Thank you.

(Whereupon, the proceedings were concluded at 1:42 p.m.)

CERTIFICATE OF REPORTER

STATE OF FLORIDA)
COUNTY OF LEON)

I, ANDREA KOMARIDIS, Court Reporter, do hereby certify that the foregoing proceeding was heard at the time and place herein stated.

IT IS FURTHER CERTIFIED that I stenographically reported the said proceedings; that the same has been transcribed under my direct supervision; and that this transcript constitutes a true transcription of my notes of said proceedings.

I FURTHER CERTIFY that I am not a relative, employee, attorney or counsel of any of the parties, nor am I a relative or employee of any of the parties' attorney or counsel connected with the action, nor am I financially interested in the action.

DATED THIS 17th day of August, 2016.

ANDREA KOMARIDIS
NOTARY PUBLIC
COMMISSION #EE866180
EXPIRES FEBRUARY 09, 2017