Cybersecurity for State Energy Planning

A Presentation at the NCSL Legislative Summit
August 5, 2012

Christina A Cody
Program Officer,
National Association of Regulatory Utility Commissioners

With support from the Department of Homeland Security Office of Infrastructure Protection

Cybersecurity is one element of all-hazards preparedness

© Reuters

Why Cyber? (cont'd.)

- Ubiquity of networks and dependency on them
- A network is cheaper, faster, more effective, and ultimately enhances reliability
- Ease of launching a sophisticated attack
- Tools are freely available on the Internet (e.g. Metasploit)
- Industry reliance on commercial software
- Evolution toward distributed networks
- Interdependencies between sectors

Why Cyber?

- In a 2011 Symantec survey, 71% of the organizations polled had come under deliberate cyber-attack in the last 12 months.

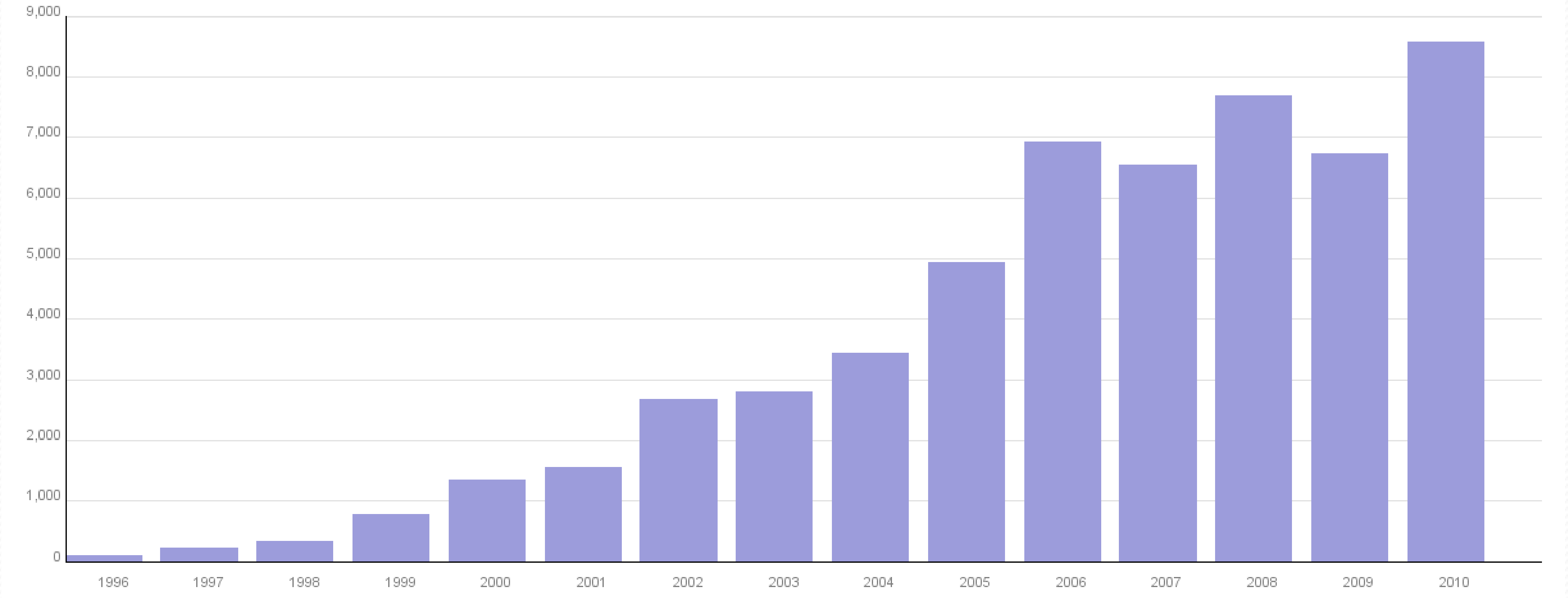
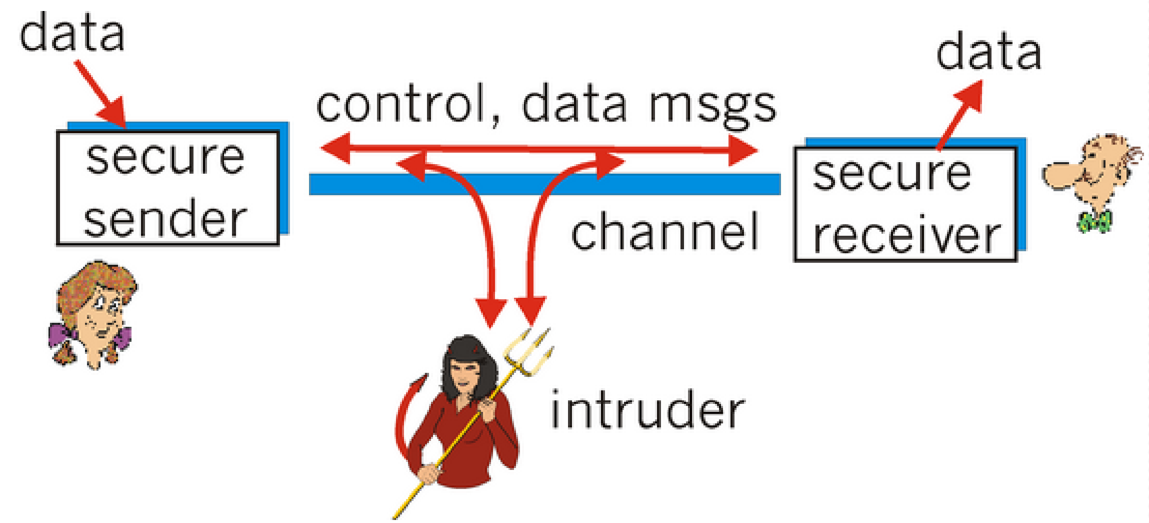


Figure 1 Data source: IBM X-Force 2010 Trend and Risk Report (for the IT and Telecom sectors).
http://www-958.ibm.com/software/data/cognos/manyeyes/visualizations/vulerabilities-per-year

Threats and Vulnerabilities

- Threat: The potential for an actor, circumstance or event to adversely affect assets, people or organizational operations of the system.
- 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.



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:

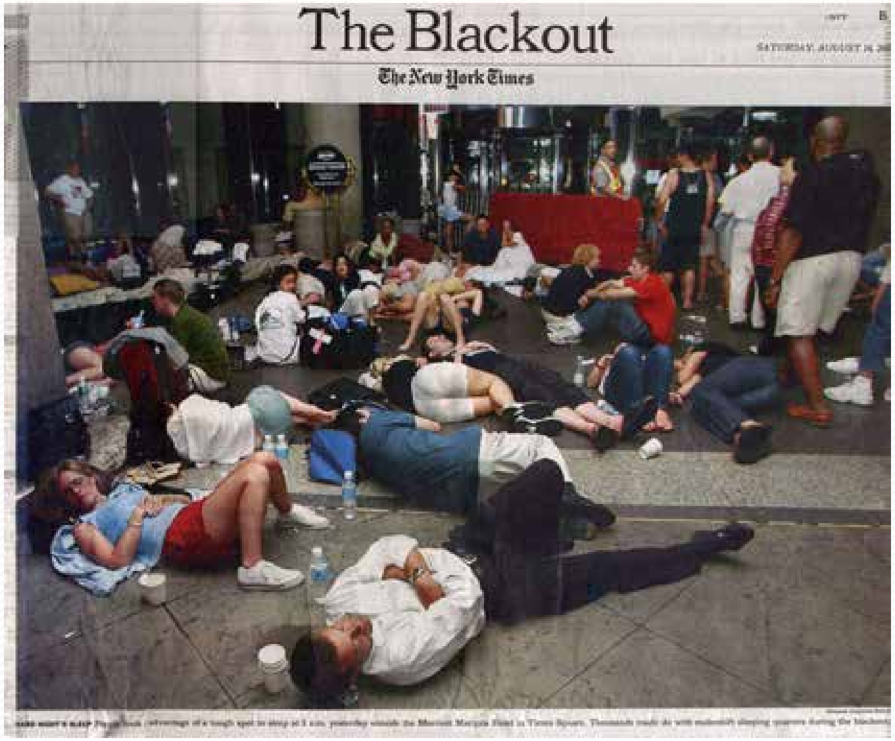
- *Directed against multiple assets designed to disable the system*
- *Highly-coordinated, well-planned*
- *Advanced Persistent Threat*

Three Flavors

Conventional IT Systems + **Control Systems** + **Electrical Infrastructure** = **“Smart Grid”**

Interdependencies

- A pretty bad hypothetical scenario…

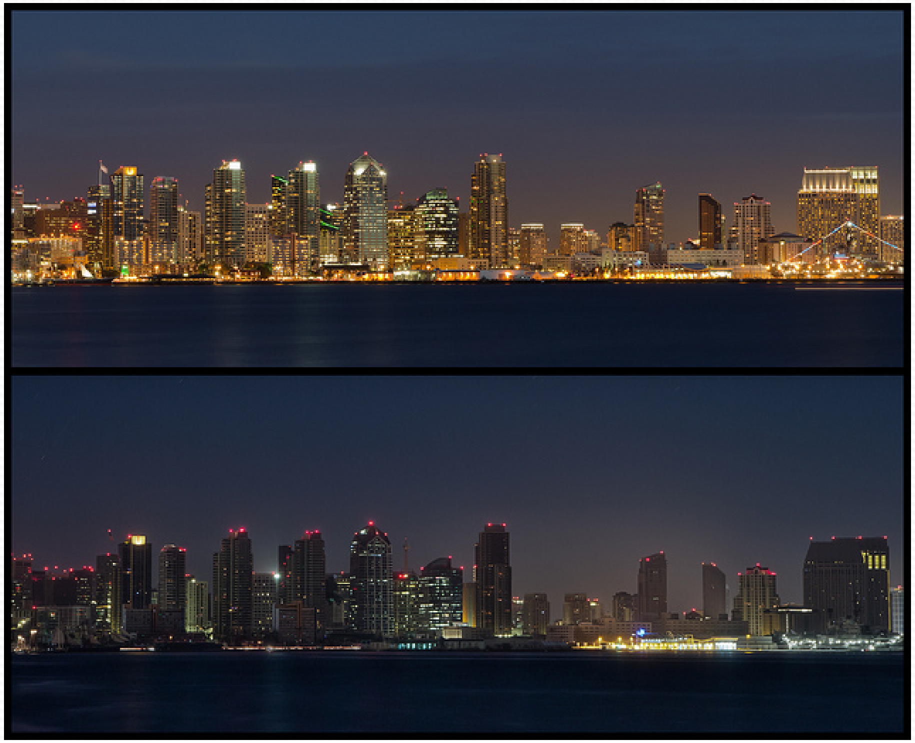


The Blackout

The New York Times

SATURDAY, AUGUST 16, 2003

[illegible] advantage of a tough spot to sleep at 3 a.m. yesterday outside the Marriott Marquis Hotel in Times Square. Thousands made do with makeshift sleeping quarters during the blackout.



A very real threat

- April / May 2007: Estonian economy largely 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 comments
- Aurora: an experiment to hack control systems and destroy a generator staged by the DOE and DHS; revealed by CNN
- STUXNET: computer worm created to attack Iran's nuclear infrastructure – only attacked designated targets
- Flame: out since at least 2010, discovered 2012, the most sophisticated of its kind
- March 2012 cyber attack targeted US and Canadian natural gas pipelines' computer systems
- **In 2011 a malfunctioning water pump in Illinois was accessed from Russia, prompting cyber attack fears (since discredited)***

* Note: even attacks that have been discredited do not mean that the vulnerability did not exist there: the attacks were credible enough to be reported.

National Attention / State Responsibility

- What's missing?
  - Enforceable Cybersecurity Rules for Distribution (though some States have led in this area)
  - Metrics for cybersecurity
  - PUC/PSC cybersecurity expertise (emerging)
  - Legislation
- It may fall to State Commissions to ask questions and require performance

States’ Planning

- Cyber attack has physical consequences
- Where do state legislators come in?
  - Executive branch oversight responsibility
    - Talk to state agencies – and who else? Know the players
    - Internal networks vs. Industry sectors
    - Public/Private partnership perspective
    - Working relationship with enterprise security side of operations
  - Understand the lay of the land – what’s the reality in your state?
  - Appropriations
  - “Cybersecurity at home”
- State energy assurance plans

What State Regulators Are Doing

- These are increasingly drivers for cost recovery consideration and other contexts in cases
  - NERC CIP compliance is driving new expenditures by utilities, but it is not exhaustive
  - Regulators are filling needed roles where NERC CIP does not cover, such as in the area of distribution
  - The deployment of smart grid increases instances
- California
  - Approved Smart Grid metrics (including cybersecurity)
- Ohio
  - Heavily involved in NIST SGIP Cyber Security Working Group activities
  - Chair NARUC Staff Subcommittee on Critical Infrastructure
- Texas
  - Staff dedicated almost solely to cybersecurity
  - Participation in various energy sector cybersecurity initiatives

Asking Questions

- The questions are only as good as your ability to understand the answers and take intelligent action
- Sample Approaches to Information Protection
  - "We can't protect it so don't share it"
  - "We can't protect it onsite but can see it at your site"
  - "We can protect it in a special case"
  - "We can protect it within a standard case with a secure hearing"
  - "We can protect it as a matter of course"

Department of Hurricanes

- Cyber secure utility operations is the domain of utilities
- Defending against nation-state cyber attacks and cyber terrorism are national defense and law enforcement matters
- Effective cyber security takes utility/regulator / federal agency (DHS, etc.) partnership
- Agencies like DOE (OE) and DHS are working on this issue,
- But, we don't have a Department of Hurricanes…

Compliance to Standards vs. Risk-Based Assessment

- Prevention - Protection – Recovery
- Mature security practices; highly refined
  - Defense in Depth
  - Principle of Least Privilege
  - Segregation of Duties
  - Need to Know
  - Maintain Confidentiality, Integrity, Availability
- No such thing as 100% Total Security, nor is there a silver bullet
- Strong protection has never been easy, inexpensive or quick to implement
- There may be a tradeoff between functionality and security

Dynamic Defense

- Evolving threat, evolving defense
  - Defense in Depth
  - Principle of Least Privilege
  - Segregation of Duties
  - Need to Know
  - Maintain Confidentiality, Integrity, Availability
- No golden shield, no silver bullet
- Strong protection has never been easy, inexpensive or quick to implement
- There may be a tradeoff between functionality and security

Dynamic Defense (cont'd.)

- If defensive measures can be beaten, the system should ensure the results of the attack are:
  - Limited in consequence - protect the network if a component is lost
  - Unprofitable for attacker
  - Hard enough to make the "juice" not worth the "squeeze"
  - Difficult to replicate
  - Quickly and easily recoverable
  - Traceable and easy to detect
  - Otherwise unappealing

What States Can Do

- Understand the State’s internal cybersecurity profile
- Understand the current cybersecurity requirements for the energy sector
- Determine whether there are cyber security plans in place, and whether they are driven by State regulatory or Federal grants compliance.
- Consider and address the human element
- Understand future guidelines and standards under consideration and how they affect the grid’s futures plans

Step One – Understand the State's internal cybersecurity profile.

1. Understand cybersecurity risks at work and at home. Many States have guidance available. For an example see: http://www.michigan.gov/cybersecurity.
2. Identify the cybersecurity roles and responsibilities of individuals and organizations in State government.
3. Determine which State agency, if any, has lead and/or supporting roles and responsibilities in cybersecurity for smart grid implementation.
4. Know what the State's Continuity of Operations Plans (COOP) and disaster recovery strategies are for essential IT systems.
5. Determine if it may be helpful to become a member of the FBI's InfraGard Program: http://www.infragard.net/.
6. Become familiar with the U. S. Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber attacks for the Federal Civil Executive Branch, as well as information sharing and collaboration http://www.fema.gov/government/coop/index.shtm
7. The SANS (SysAdmin, Audit, Network, Security) Institute is a good resource see: http://www.sans.org/reading_room/whitepapers/recovery/

Step Two – Understand current cybersecurity for the energy sector.

1. Electricity and smart grid:
   - NERC -- Standards CIP-002 through CIP-009 (the Critical Cyber Asset Identification portion of the Critical Infrastructure Protection Standards
   - Section 1305 of Energy Independence and Security Act (EISA) 2007 defines the roles of both Federal Energy Regulatory Commission and NIST as they relate to the development and adoption of smart grid standards. The Act defines the Commission's role as: "At any time after the Institute's work has led to sufficient consensus in the Commission's judgment, the Commission shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."
2. Understand the cybersecurity requirement for other parts of the energy sector including natural gas (pipeline safety standards) and the petroleum sector, because of the interdependency effects that need to be considered.
3. Under EISA 2007, NIST has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…"
   - One of the primary documents was issued in January 2010 and titled *Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0 (Framework)."
   - The Framework identified 75 interoperability standards that are applicable, or are likely applicable, to the ongoing development of smart grid technologies and applications.
   - NIST developed *Guidelines for Smart Grid Cyber Security.*

Step Three – Understand future standards and guidelines currently under discussion and development

1. The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) is a utility-driven, public-private collaborative among DOE, EPRI, and a large group of leading North American utilities. ASAP-SG is developing system-level security requirements for smart grid applications, such as advanced metering, third party access for customer usage data, distribution automation, home area networks, and synchrophasors.
2. Over the next three years, the National Electric Sector Cyber Security Organization (NESCO) will be working with the National Electric Sector Cyber Security Organization Resources (NESCOR) to lead a broad-based, public-private partnership to improve electric sector energy systems cybersecurity

Step Four – Are there cybersecurity plans in place currently? Are they driven by State regulation, Federal grants compliance or other mechanisms?

1. Which requirements are Standards-driven? Which are not?
2. Are there regulatory efforts underway at a State public utility commission to create audit, reporting and compliance obligations on cybersecurity for the utilities?
3. Are there State policies and programs that address cybersecurity?
4. How is your State approaching the public private partnerships as provided for in the National Infrastructure Protection Plan (DHS) and the Energy Sector Specific Plan (DHS and DOE)
5. The ARRA Smart Grid Investment Grants program requires utilities to develop cyber security plans. These Grants require:
   - A description of the cybersecurity risks at each stage of the system deployment lifecycle.
   - Cybersecurity criteria used for vendor and device selection.
   - Cybersecurity control strategies.
   - Descriptions of residual cybersecurity risks.
   - Relevant cybersecurity standards and best practices.
   - Descriptions of how the projects will support/adopt/implement emerging smart grid security standards.

Step Five – Consider and address the human element of cyber security

1. Understand what the insider threat is and what policies and procedures are in place to prevent intrusion and manipulation.
2. Understand what social engineering is and how it can be used to access systems
3. Understand that technical solutions to security should account for human behavior, which can be driven by both cultural and psychological factors.
4. Understand the nature of the threat from employees, contractors, consultants, or anyone with short or long term access to IT systems, and know about system vulnerabilities.
5. Once this information has been developed it can be included in either: (1) the States emergency electrical response plans as it relates to how the private and public sector would respond to a cyber attack. (2) Longer term infrastructure assurance plans (policy and programs) for reducing risks and vulnerabilities to cyber attack on the Energy Sector.

Personnel

- Deliberate vs. Inadvertent Breach
  - Software Bugs; User Errors; Power System Equipment Malfunctions; Communications Equipment Failure
  - Deliberate Intrusions and Sabotage
- Committing staff as a resource
- Training
- State Regulators don't need to be cyber experts, but:
  - They must know what questions to ask a utility (they will return with answers!)
  - Security theater is a waste of money
  - Technology alone won't solve the problem – people are integral to security

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
- **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.)

- NASEO Smart Grid Report
- NARUC Primer
- 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 Spot*. 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

Thank you!

Questions?

Christina Cody
Program Officer, Grants and Research
NARUC
ccody@naruc.org
(202) 898-2200, ext. 1002

U. S. Department of Homeland Security Office of Infrastructure Protection

Homeland Security