



Cyber Summit 2011

Critical Infrastructure Protection

Cyber Security & State Energy Assurance Plans



Michigan Cyber Summit 2011

Friday, October 7, 2011

Jeffrey R. Pillon, Director of Energy Assurance
National Association of State Energy Officials

What is Energy Assurance

- Response: It's about responding to any hazard that disrupts energy supply and assuring a rapid return to normal conditions.
- Prevent and Protect: Its about mitigating the risk in the long run by making investments that provide for a more secure, reliable, and resilient energy infrastructure.
- This is a coordinate effort involving the private energy sector, working with local, State & federal governments.
- Cyber security is an integral element of Energy Assurance.



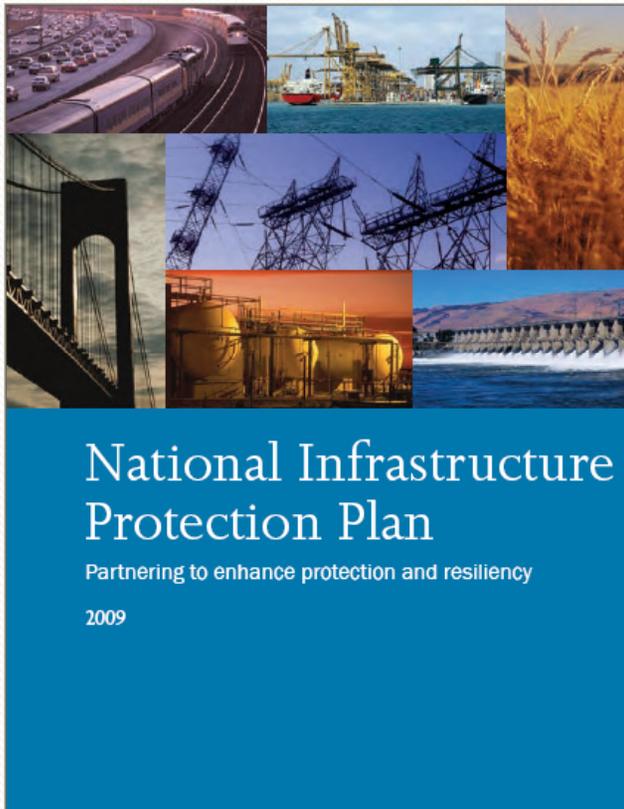


State Energy Assurance Program

- With funding from the U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability, States have been working over the last two years to:
 - update their energy emergency response plans, and assure they are coordinated with the federal and local plans and the plans of the private sector;
 - protect and enhance the resiliency of critical energy Infrastructure through a public/private partnership;
 - develop systems to track energy supply disruptions and assess their consequences; and
 - provides for staff training and conduct In-State and Multi-State exercises, and revise plans as needed.

There is a specific requirement to consider cyber security in these plans

Base Plan June 2006 , Updated First Qtr 2009

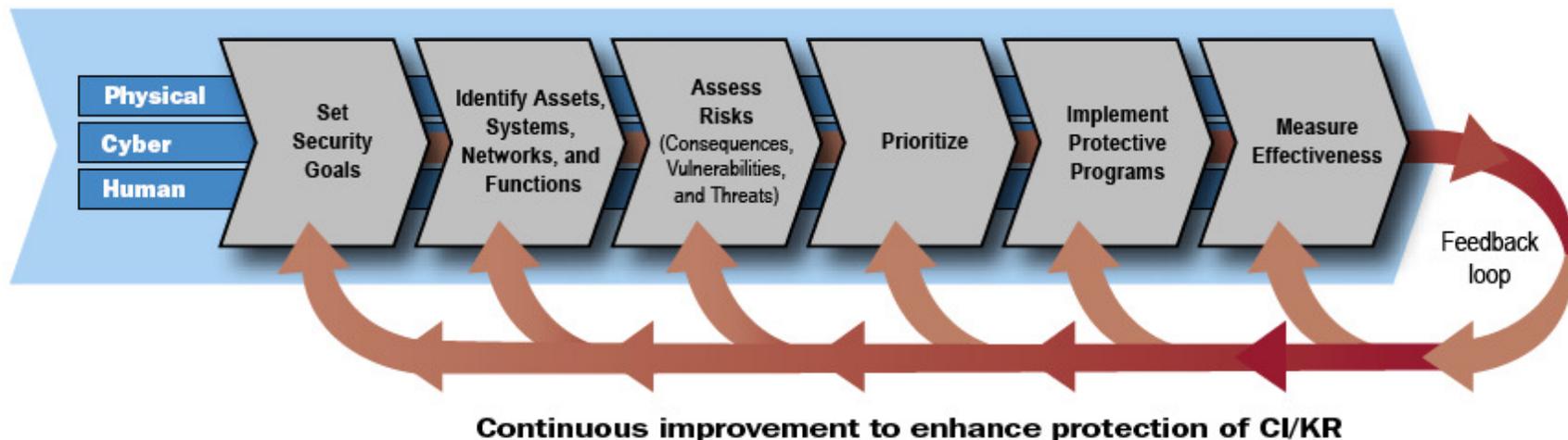


www.dhs.gov/nipp

- Incorporates extensive State, local, and private sector input
- Expands risk management framework:
 - Risk framework is based on threat, vulnerability, and consequences
 - Focuses on assets, systems, networks, and functions
- Strengthens information sharing and protection to include the “information sharing life-cycle”
- Establishes a “steady-state” of security across critical infrastructure/key resource (CI/KR) sectors

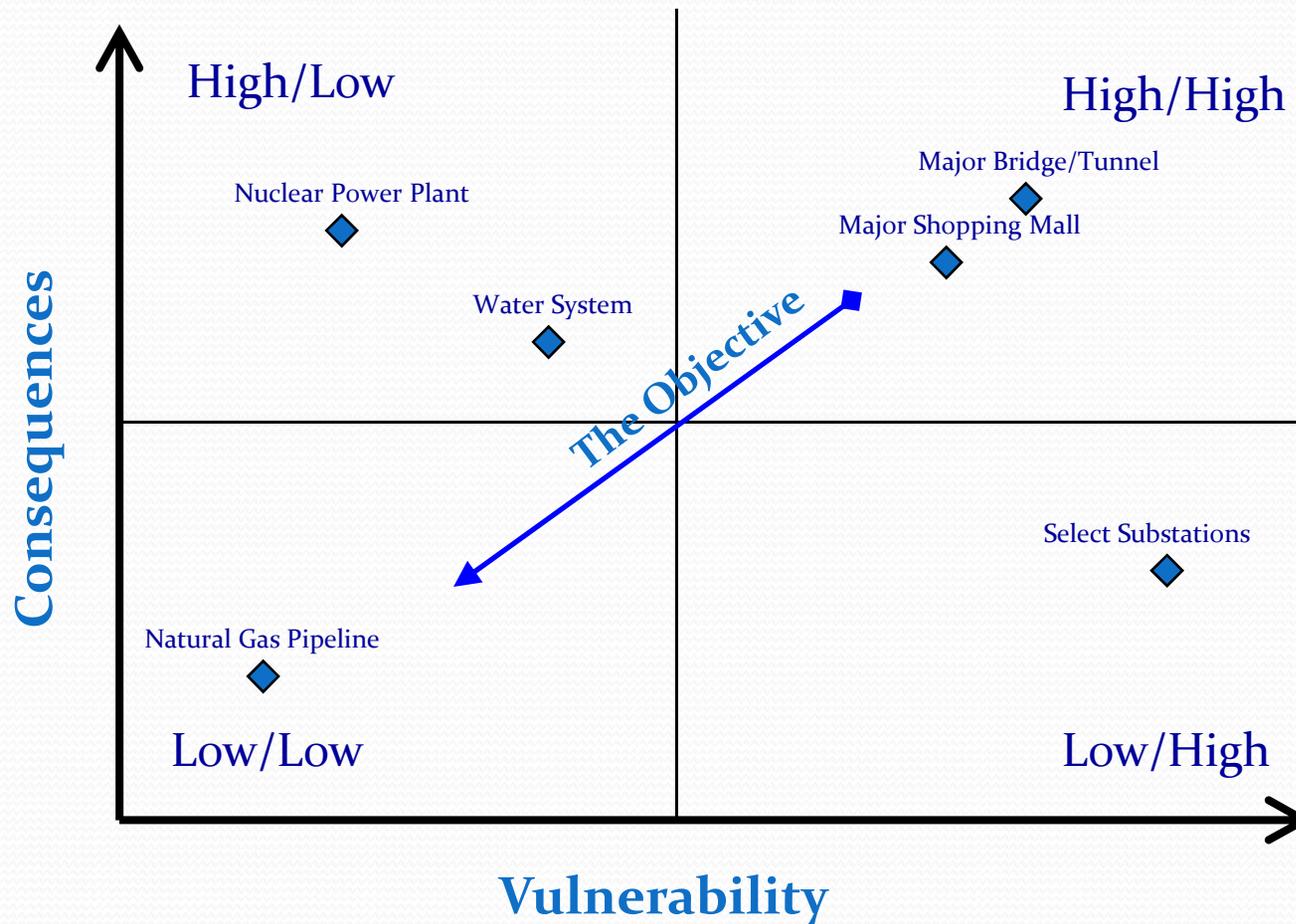
The NIPP and supporting Sector-Specific Plans (SSPs) describe the processes to:

- Set Security Goals
- Identify Assets, Systems, Networks, and Functions
- Assess Risk (Consequences, Vulnerabilities, and Threats)
- Prioritize
- Implement Protective Programs
- Measure Effectiveness



Determining Criticality

Illustrative Examples Only



How should "Threat" be factored in using an "All Hazards Approach"?

Risk Assessment

Risk is a function of

[Consequence x Threat x Vulnerability]

- Loss of revenue
- Economic losses
- Public safety
- Physical damage
- Cost of recovery & remediation
- Loss of confidence
- Decline in Stock value
- Interdependencies
- Cascading interdependencies
- Modification of data in transit
- Denial of service attacks
- Theft of information
- Spoofing
- Sniffing
- Viruses/worms
- Human engineering
- User Errors
- Equipment Failure
- Inadequate physical security
- Natural hazards
 - Flood
 - Storms
 - Earthquakes
 - Pandemics



Cyber Security Threats

- In 2001, hackers penetrated the California Independent System Operator which oversees most of the state's electricity transmission grid; attacks were routed through California, Oklahoma, and China.
- Ohio Davis-Besse nuclear power plant safety monitoring system was offline for 5 hours due to Slammer worm in January 2003.
- In 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. In a few cases, these intrusions had “caused an impact.”
- Associated Press on August 4, 2010 reported “Hackers Try to Take Over Power Plants” Last month, cyber experts discovered for the first time a malicious computer code, called a worm, specifically created to take over systems that control the inner workings of industrial plants.
- Stuxnet is a computer worm designed to attack industrial system using a “zero-day” exploit which are software vulnerabilities yet unknown to the software maker or antivirus vendors. Stuxnet is believe to be responsible for destroying 20% of Iran's Uranium centrifuges.

Motivation for Cyber Intrusions

Low
↑
Frequency
↓
High

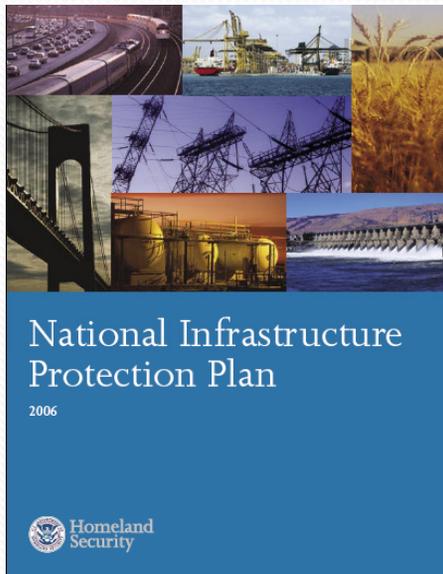
- Gain System Control -- ability to remotely modify and operate the system as a vehicle for attack.
- Extortion – criminal motivation to make money.
- Attacks -- Terrorism and Nation State attacks – objective to disrupt, destroy, frighten. Disgruntled current or former employees.
- Theft – organized crime, US, International and individuals. Objective to make money and often do not want the theft to be discovered -- stealth.
- Intrusion -- unauthorized access to information and the potential to use information to do harm.



Consequence of Cyber Intrusions

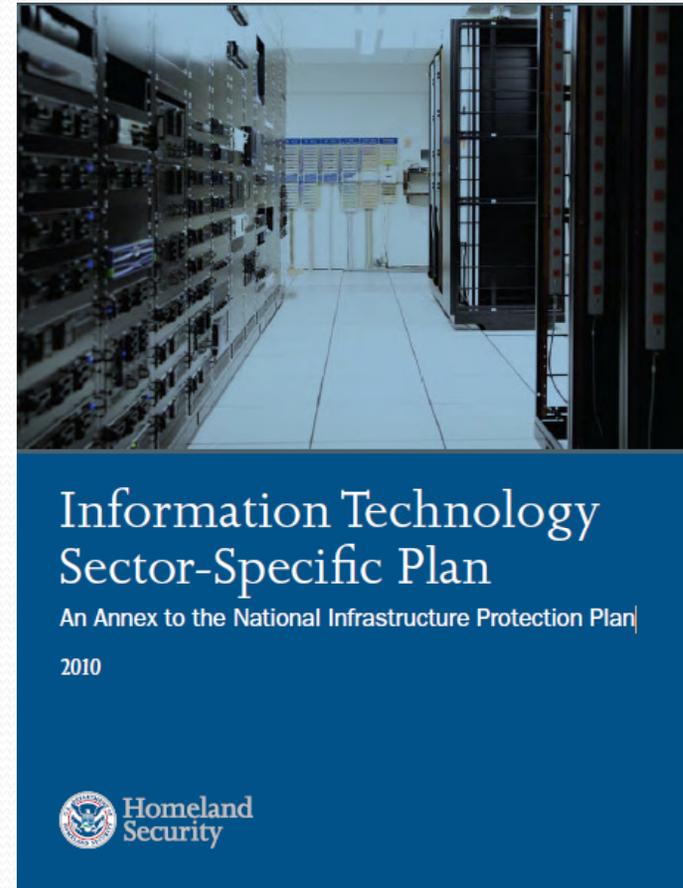
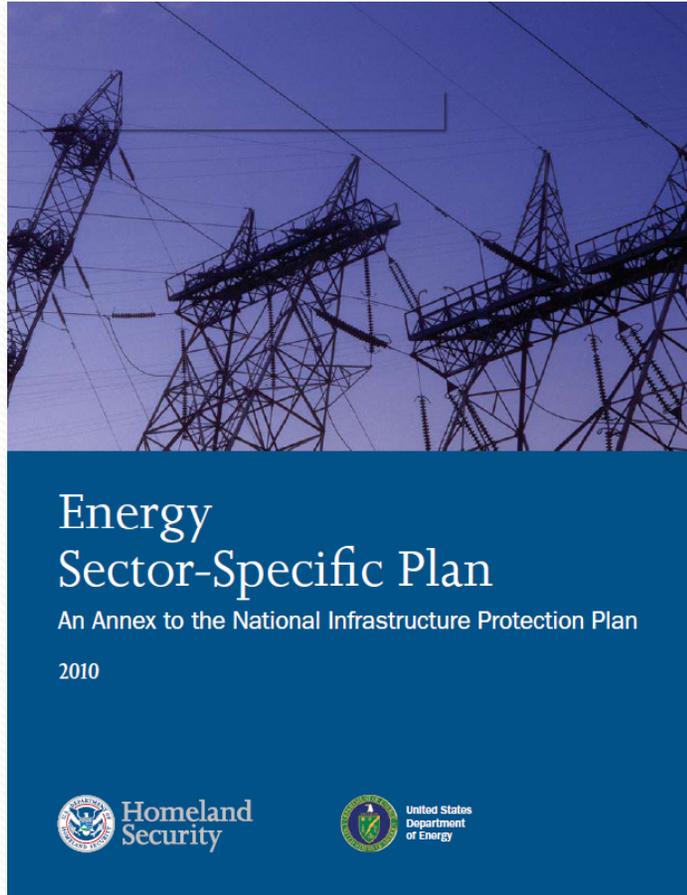
- Power outage only no control systems affected or infected. The response may be similar to any of the “All hazards” type of events.
 - The attack causes physical damage to equipment. This would be like an “All Hazards” event, but depending on the scope of the damage may take longer to repair and if repaired could it be damaged again if the perpetrators are not caught?
-
- Access to information, such as system maps or customer information that facilitates other types of attacks, physical or cyber.
 - Control systems affected within or without a power outage. This may require a different response than those commonly used in an “All Hazards” plans. It may take longer to find and remove the problems.

Sector-Specific Plans (SSPs)



- SSPs detail the application of the NIPP risk management framework in each of the 19 Critical Infrastructure Sectors
- Sector-Specific Agencies partner with their sector to develop the individual SSP
- SSPs are annexes to the NIPP Base Plan
- SSPs are updated to be submitted to DHS within 180 days after the NIPP is issued by the Secretary of Homeland Security

**Sector-Specific
Plans (17)**



- Approved May 2007 updated 2010; Sector Annual Report are also available.
- Collaborative effort between the SCC and GCC and DOE (Federal, state, local government and energy sector participants)

http://www.dhs.gov/files/programs/gc_1179866197607.shtm

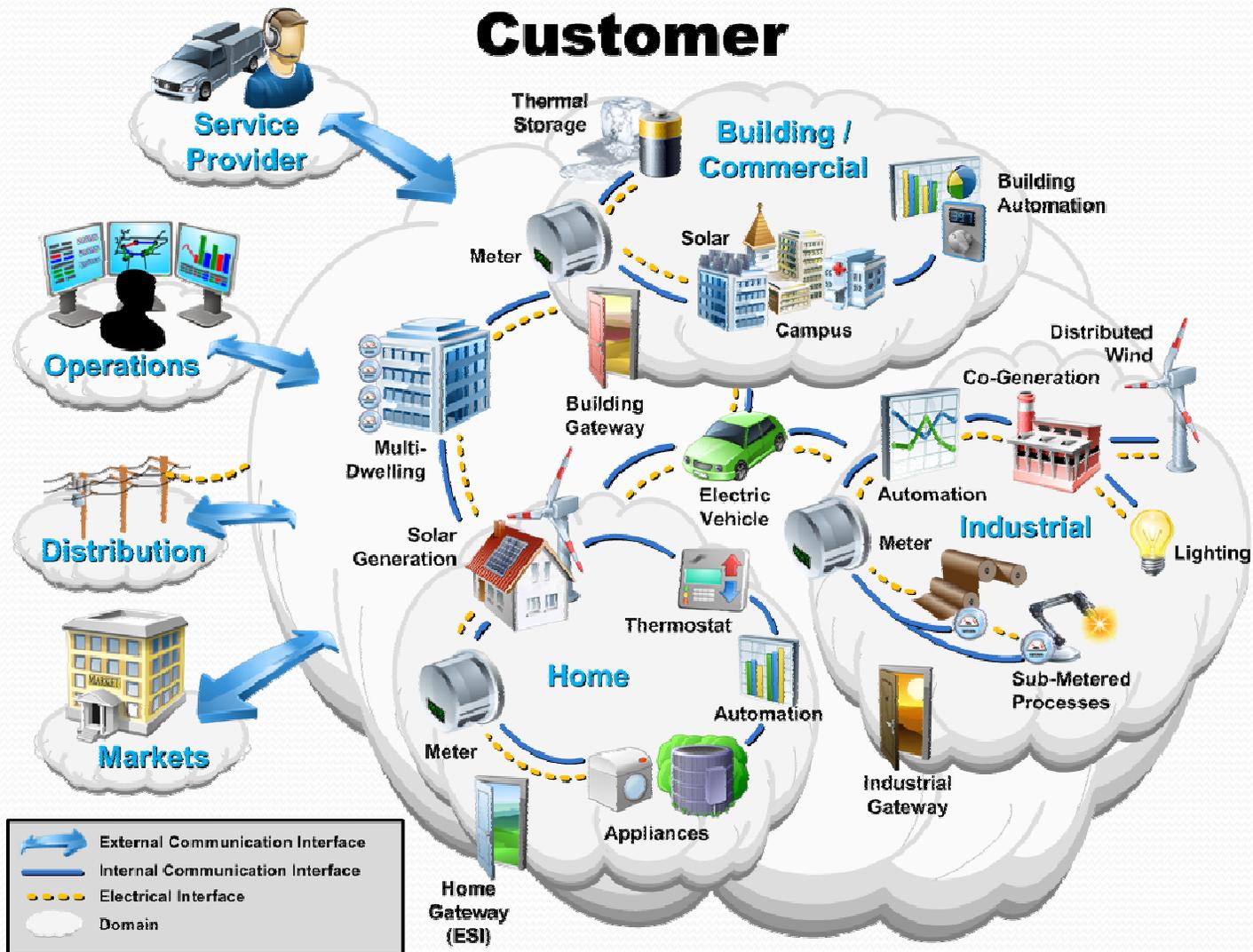


Continuity of Operation Plans (COOP)

An important element of emergency preparedness

- Internal contingency plans of government and business to assure the rapid resumption of essential functions as soon as possible if they are disrupted for any reason: e.g., fire, tornado, hurricanes, wildfires, earthquakes, terrorism, pandemics, etc. – Self-reliance
- Helps assure that critical infrastructure and essential functions can quickly resume operations
- Addresses key or essential employees, required facilities, computer system records and back-up data systems, etc.
- Minimize damage & losses
- Management succession & emergency powers

Smart Grid Customer



A more secure and reliable power grid. Some risk are reduced and new risk from cyber result.



Smart Grid Interoperability Standards

- **NIST Interagency Report 7628 (NISTIR 7628)**
- Collaborative effort between federal agencies, regulators, private sector and academics
- To be used as a “guideline” to evaluate overall Smart Grid cyber risks during implementation and maintenance
- It is not mandatory



NESCO/NESCOR

- **National Electric Sector Cyber Security Organization (NESCO)**
 - First public-private partnership in the electric sector
 - Brings together utilities, federal agencies, regulators, researchers, and academics.
 - Purpose is to “establish a National Electric Sector Cyber Security Organization that has the knowledge, capabilities, and experience to protect the electric grid and enhance integration of smart grid technologies that are adequately protected against cyber attacks.”
- **National Electric Sector Cyber Security Organization Resource (NESCOR)**
 - EnergySec was tasked with forming the NESCO organization and EPRI was selected to serve as a research and analysis resource to the NESCO program.



Why The State Public Utility Commission (PUC) Role is Increasing

- Increased attacks to business processes and losses.
- NERC CIPC compliance is driving new expenditures by utilities that may require cost recovery.
- The deployment of smart grid and cyber security requirements of federal grants.
- These are increasingly drivers for cost recovery consideration and other contexts in current and future rate cases.



PUC's Are Going To Have To Rule On Prudent Security Expenses

- PUCs don't need to become cyber experts, but they do need to be able to ask the right questions.
- Security has never been inexpensive.
- Security theater is a waste of money.
- Information management and risk perception remains an unsolved issue.
- Fines and legal fees are liabilities and real costs.
- People are needed for security, not just technology.



Building a Cyber Security Capability

For State Energy Agencies

- Cyber security is not a one-time activity, like building a fence for protection. Because smart grid will be built over time, cyber security must also grow and evolve over time to address threats and vulnerabilities.
- A critical prerequisite to this is for State energy offices and public utility commissions to assign staff resources to cyber security on an ongoing basis. This might also be done using a team or taskforce approach.
- The National Association of Regulatory Commissioners also adopted a *Resolution Regarding Cyber Security* in February 2010 that states in part:
 - “That NARUC supports member commissions in becoming and remaining knowledgeable about these threats, and ensuring that their own staffs have the capability, training, and access to resources to adequately review and understand cyber security issues that enhances expertise in the review of cyber security aspects of filings by their jurisdictional utilities...”

Building a Cyber Security Capability

For State Energy Agencies

- **Step One** -- Understand the State's internal cyber security profile.
 - Understand cyber security risks at work and at home.
 - Know who in the State government has primary roles for addressing cyber security, and their roles and responsibilities.
- **Step Two** – Understand current cyber security for the energy sector.
 - Electricity and smart grid: NERC -- Standards CIP-002 through CIP-009 (the Critical Cyber Asset Identification and Protection Standards).
 - Section 1305 of Energy Independence and Security Act 2007 defines the roles of both Federal Energy Regulatory Commission and NIST as they relate to the development and adoption of smart grid standards.
- **Step Three** – Understand standards and guidelines currently under development.
- **Step Four** – Understand utility cyber security plans and State regulatory or Federal grants compliance or other policies and programs.
- **Step Five** – Consider and address the human element of cyber security.

http://www.naseo.org/energyassurance/Smart_Grid_and_Cyber_Security_for_Energy_Assurance-NASEO_December_2010.pdf



Next Steps -- Work remains

- Federal roles & responsibilities are evolving and need better definition as to their relationships electric utilities, and State and local governments.
- State energy agencies need to build the capability to address cyber security within their scope of work and regulatory authority as a regular part of their duties.
- Care needs to be exercised to assure that Smart Grid investments by utilities are made assuring an appropriate level of cyber security to address existing and future threats and to realize the benefits for a more secure and reliable power supply.

Questions?

Jeffrey R. Pillon,
Director of Energy Assurance
National Association of State
Energy Officials
517-580-7626
jpillon@naseo.org



For more information on Energy Assurance see: www.naseo.org/energyassurance