SAND2011-3639C

Critical Spares Project Workshop: Prioritizing and Exercising Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies

WRG Oil & Gas Cyber Security Summit Conference
June 2011

Homeland Security

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

National Nuclear Security Administration

Sandia National Laboratories

Agenda

- Goals and Logistics for the Workshop
- Review the Handout Packet
- Overview of DHS Critical Spares Project
- Review Findings
- Systems Architecture Discussion
- Policy and Standards Discussion
- Discussion Session

Goals of this Event

- Discuss the next-generation issues and emerging risks in cyber security for control systems
- Review and discuss common control system architectures
- Discuss the existing findings of the Spares Project
- Discuss the role of policy, standards, and supply chain issues
- Interact on the most pertinent risks and most critical areas of the architecture

Sandia National Labs

In 1949, President Harry S. Truman charged Sandia National Laboratories with the responsibility for performing "…exceptional service in the national interest". Since then, Sandia National Laboratories has developed science-based technologies that support our national security. Today, the 300+ million Americans depend on Sandia's technology solutions to solve national and global threats to peace and freedom.

Through science and technology, people, infrastructure, and partnerships, Sandia's mission is to meet national needs in five key areas:

- **Nuclear Weapons**
  - ensuring the stockpile is safe, secure, reliable, and can support the United States' deterrence policy
- **Energy and Infrastructure Assurance**
  - enhancing the surety of energy and other critical infrastructures
- **Nonproliferation**
  - reducing the proliferation of weapons of mass destruction, the threat of nuclear accidents, and the potential for damage to the environment
- **Defense Systems and Assessments**
  - addressing new threats to national security
- **Homeland Security**
  - helping to protect our nation against terrorism

Emerging Issues in Control System Security

Annie McIntyre
Principal Member of Technical Staff
Energy Systems Analysis Department
Phone: 505-284-0968
Email: amcinty@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Spares Overview

- Prioritize and Exercise Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies – Critical Spares for Transportation, Nuclear, Electric, and Water Sectors

Purpose*: To develop and validate an all hazards methodology for measuring the level of risk to these components and determining the appropriate response*

Spares Overview

- Identify sector-specific threats and resulting impacts to critical components
- Identify critical architecture components, functions and processes
- Evaluate the consequence to sectors resulting from the failure or loss of the components
- Examine risk and cost-benefit trade-offs
- Assess the benefits of potential mitigation strategies
  - Strategic spares for components with long-lead times
  - Development or refinement of contingency plans to include cyber Prioritize and Exercise Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies.
- Build a methodology transferrable to industry

Spares Overview

- Approach: Develop a methodology
  - System definition
  - Component ranking and filtering by consequence and threat
  - Mitigation strategies and cost-benefit tradeoff
- Conduct pilot studies to improve the methodology
  - Engage multiple utilities per sector
  - Use lessons learned to enhance the process

Project Approach

- Engage with industry
- Develop system architecture(s)
- Identify critical components and processes
- Validate findings through on-site assessments
- Determine key decision factors and interdependencies
  - –Policies
  - –Technology drivers
  - –Economic factors
  - –Operational concerns
- Compile sector findings into a final report

Progress to Date

- Industry Partners
- Outreach Events
- Assessments
- Feedback and Analysis
- Trending Analysis

Goals of this Event

1. Discuss the most critical issues in cyber security today
2. Obtain industry feedback on system architecture
3. Discuss decision factors
4. Gather feedback on operational issues from a variety of backgrounds (SCADA, IT, auditors)
5. Boil down the biggest concerns to industry
6. Discuss existing findings

Initial Findings

- Directory Services
- Telecommunication interaction
- Lack of policies
- Lack of coordinated threat information
- Field sites
- Perimeter security implementation and firewalls
- Technology trends

Control System Architectures

Morgan Henrie, Ph.D.
MH Services
Phone: 907-229-5469
Email: mhenrie@mhcinc.net

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Outline

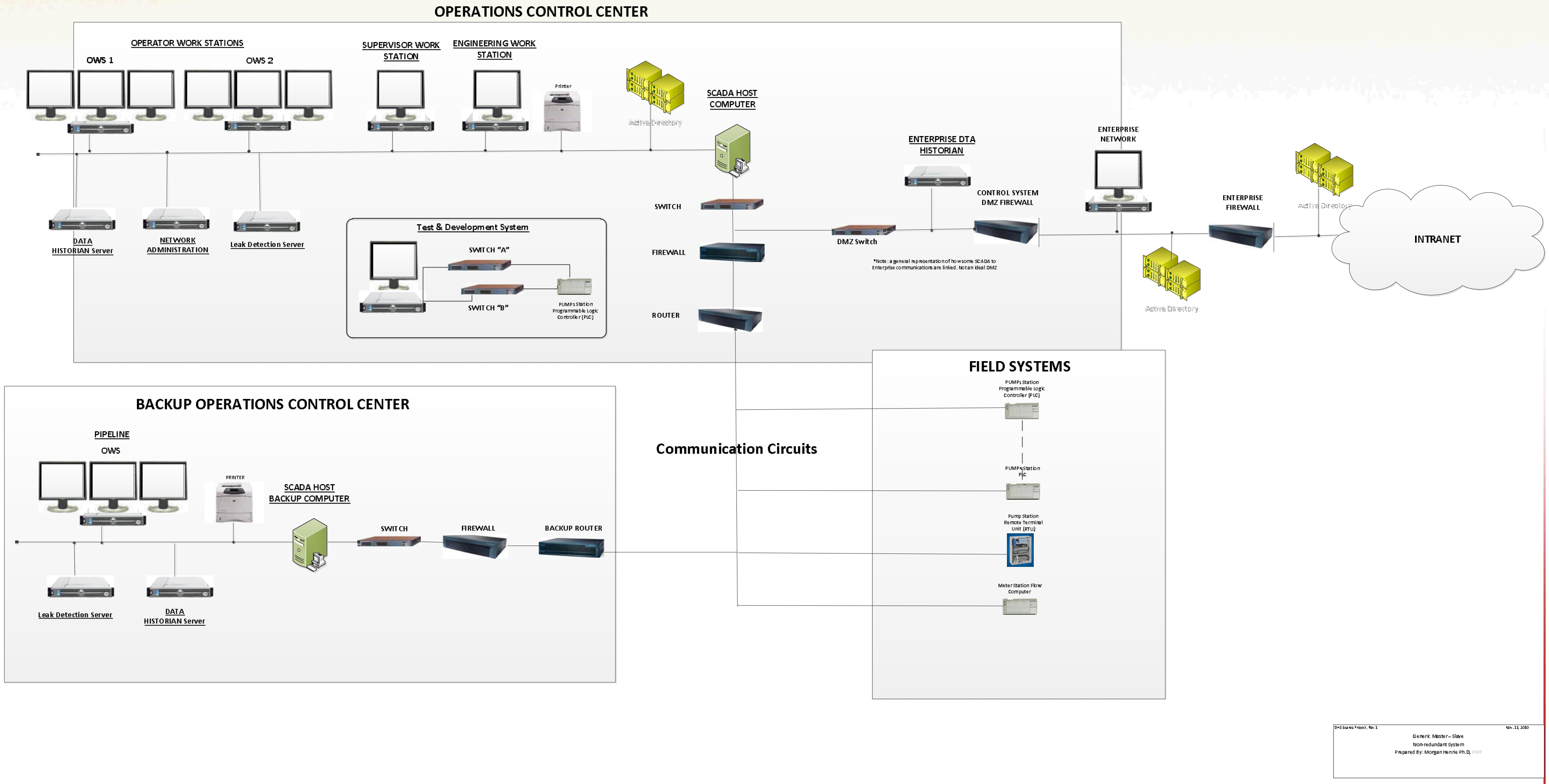
- Why generic diagrams?
- Simple Master – Slave system
- Redundant Master – Slave system
- Distributed control system

Why Generic Diagrams

- **Provide the capability to discuss systems, in general**
- **Is not an end user specific**
- **Does not identify any proprietary information**

- **LIMITATIONS**
  - May include more than an end user actually has
  - May not include as much as an end user utilizes

Simple Master – Slave, minimal redundancy

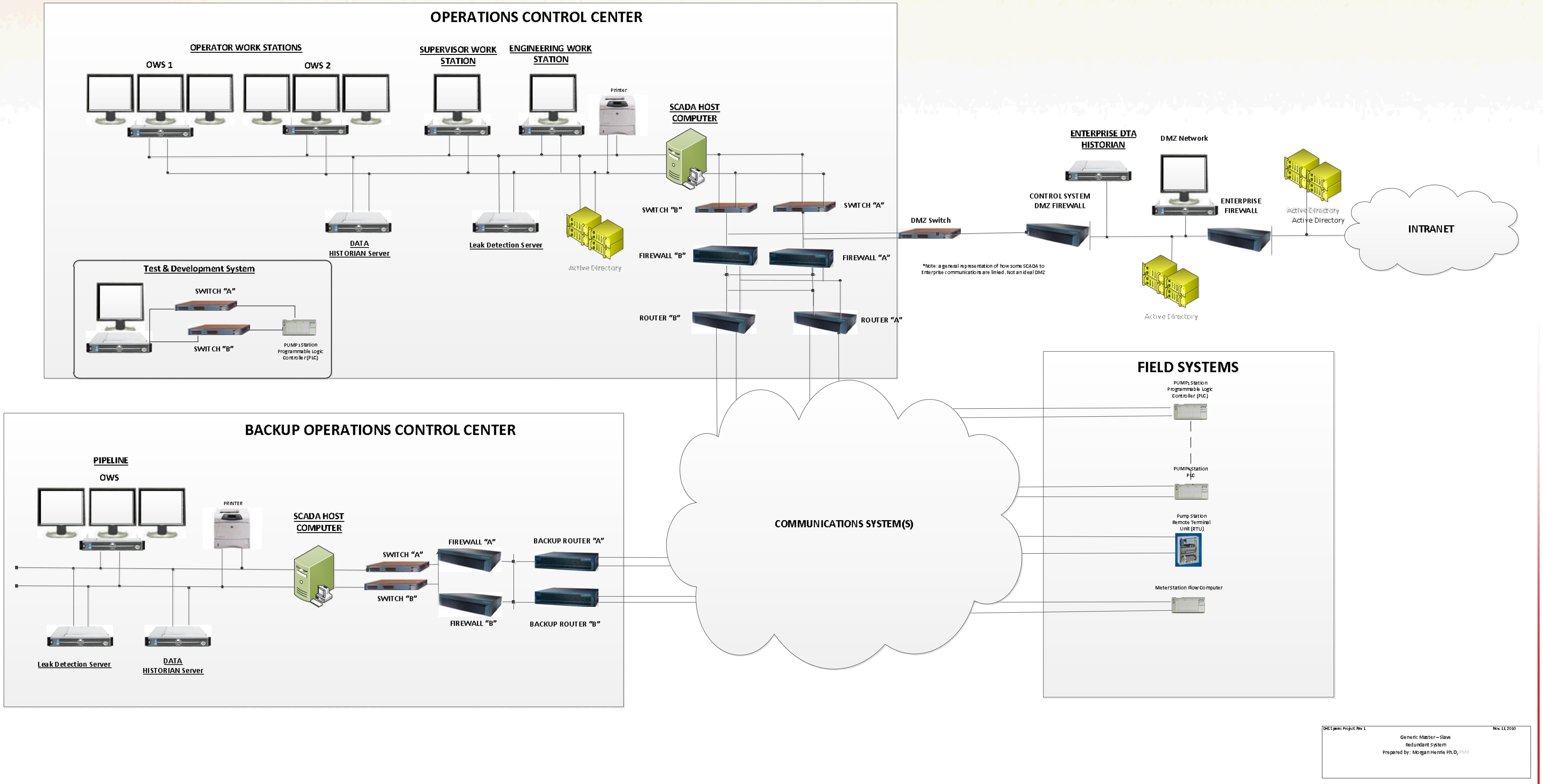


*Note : a general representation of how some SCADA to Enterprise communications are linked. Not an ideal DMZ

DHS Scada Project, Rev 1 Nov. 11, 2010

Generic Master – Slave
Non-redundant System
Prepared By: Morgan Henrie Ph.D, PMP

Redundant Master - Slave



Role of Policies and Standards in Cyber Security Decisions

Jacquelynne Hernández
Member of Technical Staff
Energy Systems Analysis Department
Phone: 505-844-6576
Email: jhernan@sandia.gov

National Nuclear Security Administration

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Sandia National Laboratories

Outline Presentation

- **Energy Policy – The Basics**
- **The Energy Policy Framework**
  - Definition
  - Objectives
- **Standards – Integrated Policy Instruments**
- **Challenges, Opportunities, and Gaps**
  - Workshop Teaser
  - Post Event Participant Input Follow-up Website

Policies & Standards Outline

- **Energy Policy – The Basics**
- **The Energy Policy Framework**
  - Definition
  - Objectives
- **Standards – Integrated Policy Instruments**
- **Challenges, Opportunities, and Gaps**
  - Workshop Teaser
  - Post Event Participant Input Follow-up Website

Simple Definition of Energy Policy

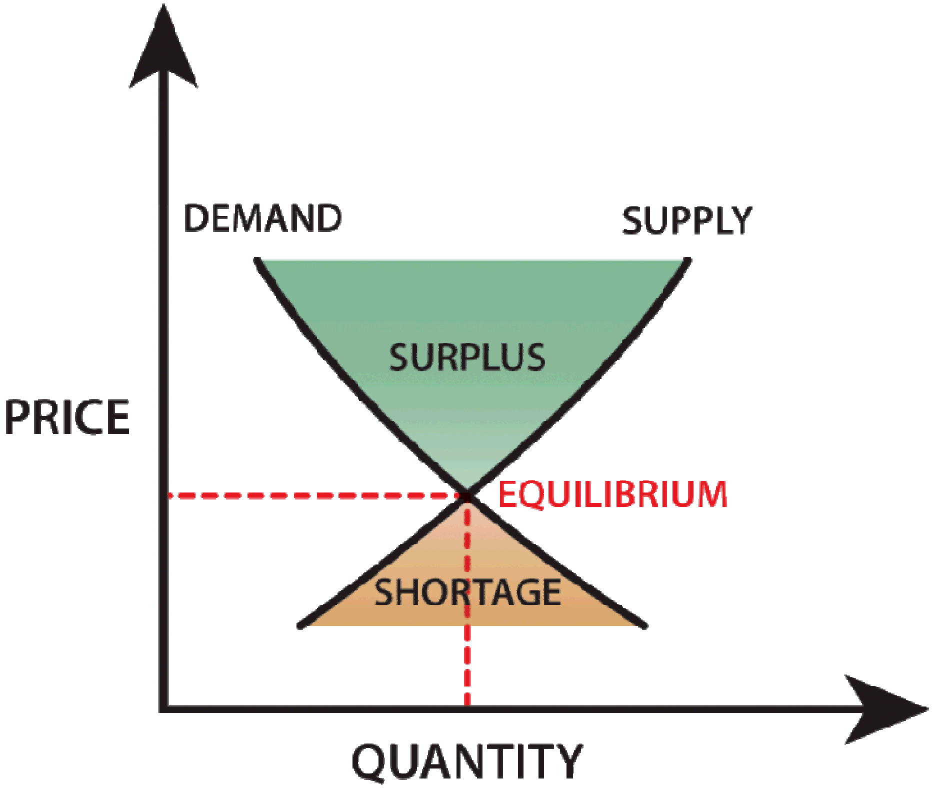
Energy policy is –

How a given entity ***(usually a government)***
Has determined to address
Energy Development issues (in particular):

- Energy Consumption
- Energy Production
- Energy Distribution

Energy Policy – The Basics

Energy Policy & Analysis, when aligned with Technology is a multifaceted area affecting the supply and demand balance.



The fundamentals do not change over time

Policies & Standards Outline

- Energy Policy – The Basics
- **The Energy Policy Framework**
  - Definition
  - Objectives
- Standards – Integrated Policy Instruments
- Challenges, Opportunities, and Gaps
  - Workshop Teaser
  - Post Event Participant Input Follow-up Website

What is a Framework?

Framework Definition

A framework is a model. It is a hypothetical description of a complex entity or process. The description includes the **underlying structure for a group of components or elements that work interactively** to support an issue or concept such that one responding to questions or problems delivers **consistent output, answers,** or potential solutions.

Developing a Framework : How to Reach Energy Policy Goals

QUESTIONS must GENERATE more QUESTIONS to

- **Develop an integrated framework**

  to assess the interaction of energy supply and infrastructure alternatives

- **Provide perspective**

  on a broad range of energy policy questions

- **Understand how to ask** an energy policy question
- **Have confidence in the approach** for how one begins to respond to energy policy questions

Policies & Standards Outline

- **Energy Policy – The Basics**
- **The Energy Policy Framework**
  - Definition
  - Objectives
- **Standards – Integrated Policy Instruments**
- **Challenges, Opportunities, and Gaps**
  - Workshop Teaser
  - Post Event Participant Input Follow-up Website

An Integrated Policy Model : Putting the pieces together

Industry requires an integrated model when energy policy is mandated.

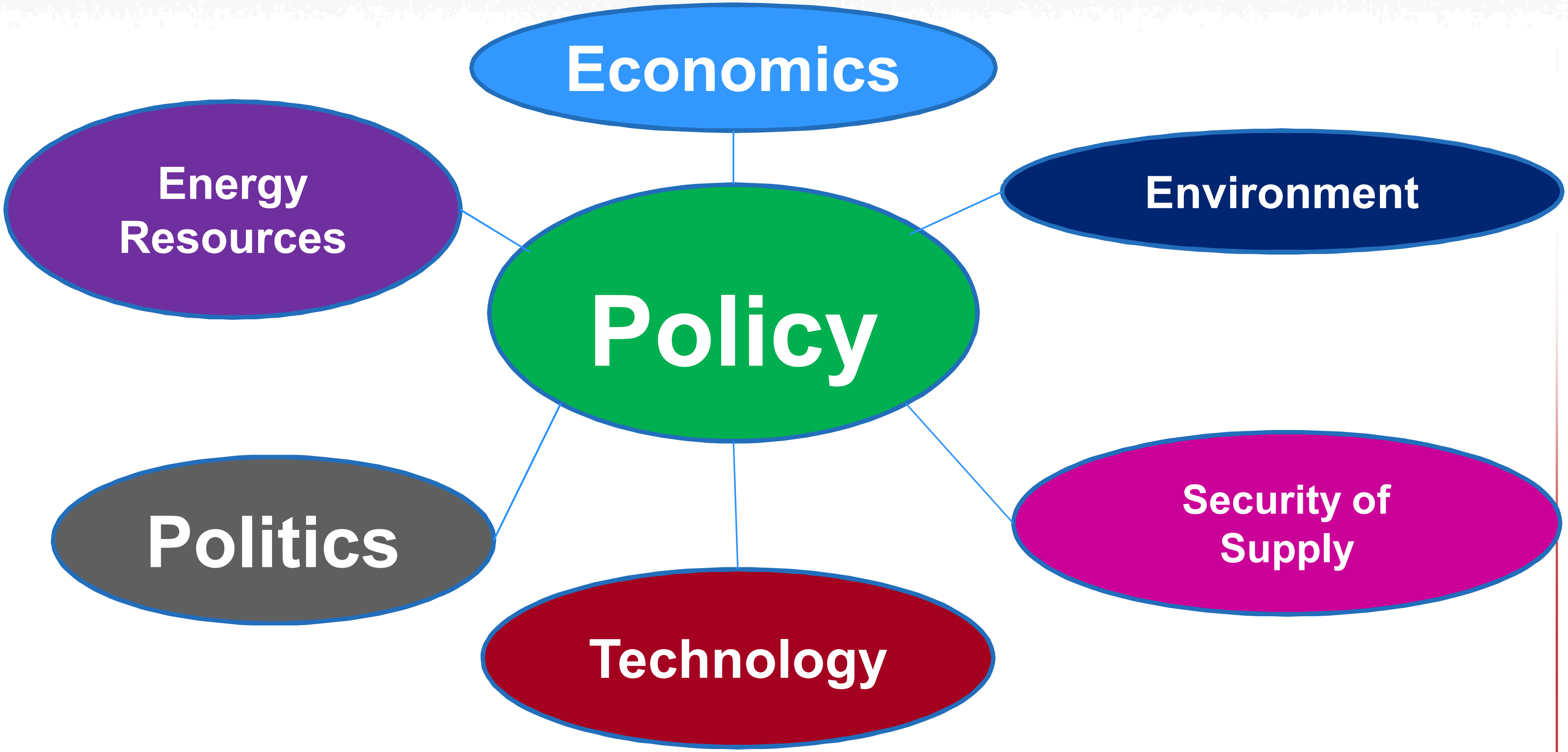
Six underlying structures in any energy policy model:

- Energy resources
- Economics
- Environment
- Technology
- Politics
- Security of supply

ALL PROPPED UP BY APPLIED STANDARDS

Integrated Energy Policy and Standards Complexities (Current Examples)

Based on work by Hong Jian Yang, Feb 2006



Sandia National Laboratories

Integral Policy Framework Elements Explained

- **Economics** – *open to all private participants; investors require the right signal for guarantee of ROI*
- **Energy resources** – *movement toward use of clean (er) energy sources*
- **Environment & Technology** – *Individuals make choices consistent with society's best interests*
- **Security of Supply** – *Dependence on the network infrastructure that MUST be maintained with system coordination*
- **Politics** – *to work, this framework element requires impartial evaluation and frequent monitoring of market performance & incorporation of competitive markets*

List of Policy & Standards Identifying Potential Gaps, Opportunities

- **POLITICS Example:** ***Government Convergence in Cyberspace***
  Title 6
  - Homeland Security
  - Critical Infrastructure
- **Title 10**
  - Defense Critical Infrastructure
  - Defense Industrial Base
  - Military Operations
- **Title 18** Domestic Threat
- **Title 44** National Security Systems
- **Title 50 (Intelligence)**
  - Counterintelligence
  - Intelligence Networks

Policies & Standards Outline

- **Energy Policy – The Basics**
- **The Energy Policy Framework**
  - Definition
  - Objectives
- **Standards – Integrated Policy Instruments**
- **Challenges, Opportunities, and Gaps**
  - Workshop Teaser
  - Post Event Participant Input & Follow-up

Policy Framework: Putting the Puzzle Together/ DHS, TSA, DoD

In accordance with the Homeland Security Act of 2003, Pub. L.. No. 107-296, 116 Stat.2135 (Homeland Security Act) and Homeland Security Presidential Directive No. 7, December 17, 2003 (HSPD-7), Department of Homeland Security (DHS) holds lead authority, primary responsibility, and dedicated resources for security activities in all modes of transportation, to include pipeline security. Pursuant to the Aviation and Transportation Security Act (ATSA) (Pub L. 107-71) and specific delegation by the Secretary of Homeland Security, Transportation Security Administration (TSA) acts as the lead Federal entity for transportation security, including hazardous materials and **pipeline security**.

TSA Requirement

A risk-based Corporate Security Program (CSP) should be established and implemented

by each pipeline industry operator

to address and document the organization's security policies and procedures for managing security related Threats, incidents, and responses

Ref: Order Code RL33347/Pipeline Safety and Security: Federal Programs; Updated February 29, 2008
CRS Author Paul W. Parfomak, Specialist in Energy and Infrastructure Policy Resources, Science, and Industry Division

TSA Pipeline Security Guidelines

- **Every pipeline operator should develop a CSP plan for their organization**
- Every pipeline operator should adopt baseline security measures
- Every pipeline operator should conduct a criticality assessment:
- If it is not a critical facility, then consider conducting a Security Vulnerability Assessment
- If it is a critical facility, then conduct an SVA for each critical facility
- If it is a critical facility, after the SVA, then adopt enhanced security measures at each facility
- Every pipeline operator should monitor HSAS threat levels and implement corresponding HSAS threat level protective measures.

- NOTE: Homeland Security Advisory System

TSA Corporate Security Program Plan

3 CORPORATE SECURITY PROGRAM PLAN

Operators should develop and employ a CSP plan. The CSP plan should be customized to the needs and scope of the company

CSP Plan Elements

1. **Security Administration and Management Structure**
2. **Risk Analysis and Assessments**
3. **Physical Security and Access Control Measures**

This section of the CSP plan should include the policies, practices, and procedures necessary to *implement the CSP plan. It should reflect, but not be limited to: physical* barriers, perimeter security,

4. **Personnel Security**
5. **Intrusion Detection**
6. **Equipment Maintenance and Testing**
7. **Design and Construction Security Measures**
8. **Communications**
9. **Personnel Training**

TSA Corporate Security Program Plan (cont)

10. Drills and Exercises

11. Security Incident Procedures

12. HSAS Response Procedures

13. Compliance Reviews

14. Record Keeping

15. Cyber/ SCADA System Security Measures

This section of the CSP plan should include the policies, practices, and procedures necessary to *implement the CSP plan. It should reflect, but not be limited to: access* determination and granting, server and system protection, system penetration, malicious code detection, business resumption and disaster recovery, etc.

16. Critical Contact Listings

*** The CSP plan is subject to review by TSA upon request.**

What puts an operator in play for critical system per HSPD-7?

4.2 System Criticality

In evaluating the U.S. national pipeline network, TSA seeks to identify those pipeline systems that may be considered of the highest consequence based on either the product carried or the amount of energy transported. For the purpose of its analysis, TSA considers a pipeline system to consist of all parts of an interconnected and continuous network operated by one firm through which natural gas or hazardous liquid is transported or distributed. Pipeline systems carrying products that pose a toxic inhalation hazard or that meet the criteria below are considered critical by TSA:

- Crude oil and product pipelines with a throughput in excess of 200,000 barrels per day; or

- Natural gas pipelines with a throughput in excess of 300 million cubic feet per day.

Numbers & Players

TSA 2008 position and stats about the pipeline system landscape in the U.S.:

The **national pipeline system is an extensive model of transportation with unique infrastructure security characteristics and requirements**. A risk-based approach to security acknowledges that there is no uniform security management program that would apply to the entire petroleum and natural gas industry, and that resources are best applied to mitigate high risk situations. Virtually the entire critical pipeline infrastructure is owned and operated by private entities. In particular, there are:

- 161,189 miles of hazardous liquid pipelines; 200 operators
- 309,503 miles of natural gas transmission pipelines, 700 operators
- 1,900,000 miles of natural gas distribution pipelines, 1300 operators

Challenges, Gaps, Trends, Updates

Filling in the Gap for Policy & Cyber Security

- Basic Principle/Strategy
- What we have done in Cyber Security from a Position of Leadership
- Who’s following?
- What’s next in the Real World?

Basic Principle/Strategy

- ***Congress and government agencies to continue working to develop policies and strategies to protect national security and commercial interests.***

Posture from National Leadership

- The current administration developed chose a cyberspace policy that included appointing a “Cyber Czar, Howard A. Schmidt, whose leading policy objectives is the development of "National Strategy for Trusted Identities in Cyberspace"
- Result? Three Competing Senate Bills during the last session to achieve this goal.

What’s the Plan? – *Cyber Space Policy Review*

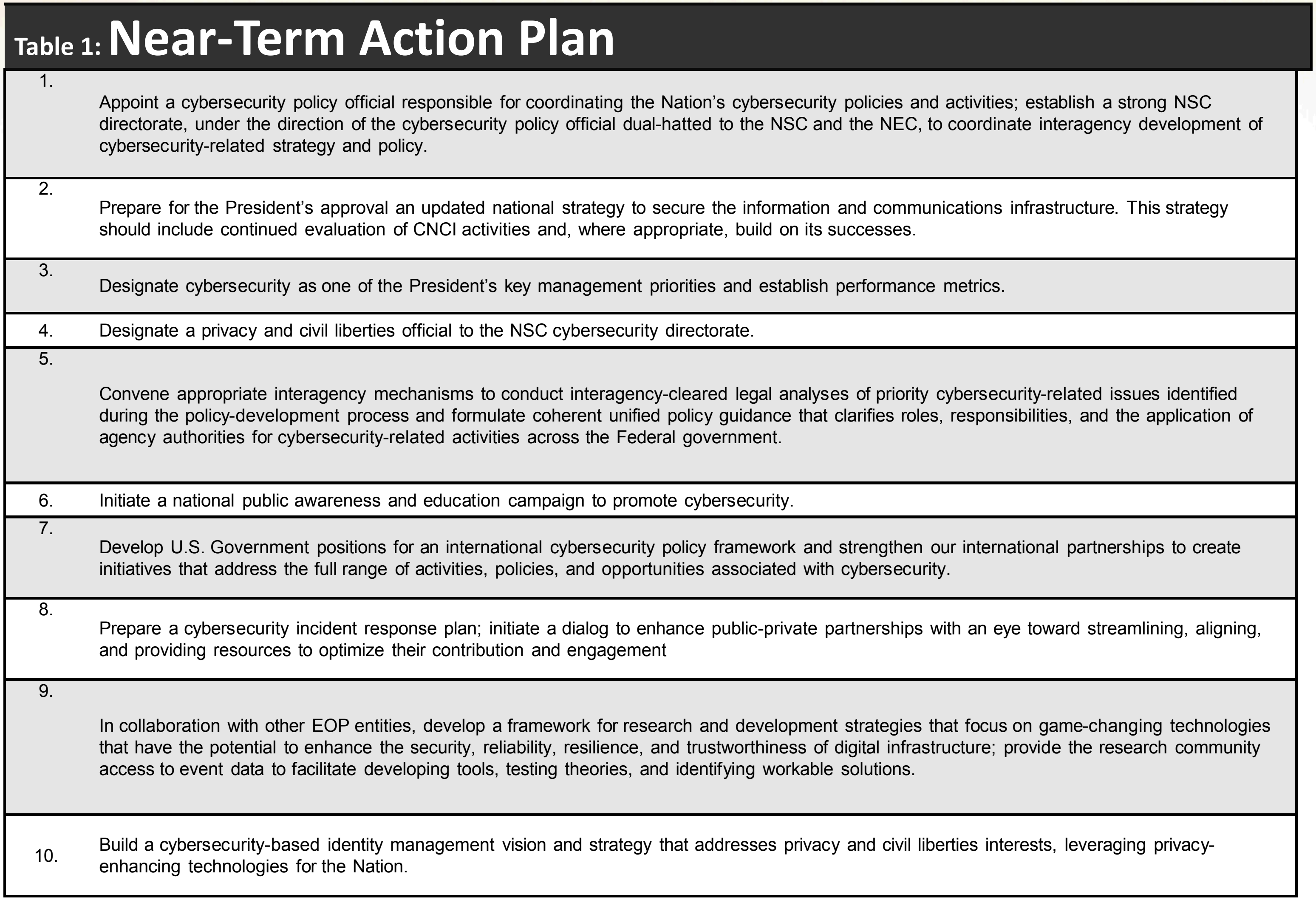


Table 1: **Near-Term Action Plan**

1.	Appoint a cybersecurity policy official responsible for coordinating the Nation’s cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2.	Prepare for the President’s approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3.	Designate cybersecurity as one of the President’s key management priorities and establish performance metrics.
4.	Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5.	Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6.	Initiate a national public awareness and education campaign to promote cybersecurity.
7.	Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8.	Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9.	In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10.	Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (January 14, 2011).

What’s NEXT?

- **Policymakers must deal with the world as it is, not as they wish it were. Any legislation must deal with the Cyber Security issues, architecture, functions as they exist TODAY, not as the U.S. hopes it will be in the future. With the following issues clearly in mind when developing policy:**
  1. Cyberspace is EVERYWHERE
  2. Limited geo-political boundaries in the Cyber world
  3. Anonymity is an inherent feature
  4. The amount of U.S. Government traffic on non-government networks
  5. How much hardware is NOT produced in the U.S.

Closing the Loop on Policy, Cyber Processes & IT Issues

Policy is a many splendored thing…

The answer is:

Policy is complex, but it still is an important aspect of how this industry does work, establishes processes, and serves the public.

The question is: How do energy policies affect your cyber security decisions?

Discussion

- **Cyber Policy Issues raised during November workshop:**