U.S. Department of Energy

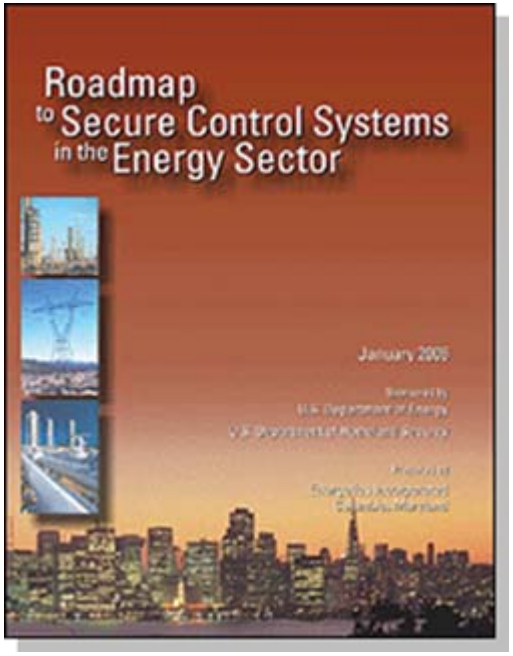
Office of Electricity Delivery and Energy Reliability

Three Years Down Range: Promising Results from the *Roadmap to Secure Control Systems in the Energy Sector*

SANS SCADA Summit
Orlando, FL
February 2, 2009

Thomas R. Flowers, P.E.
US Department of Energy

The Roadmap – Three Years Down Range

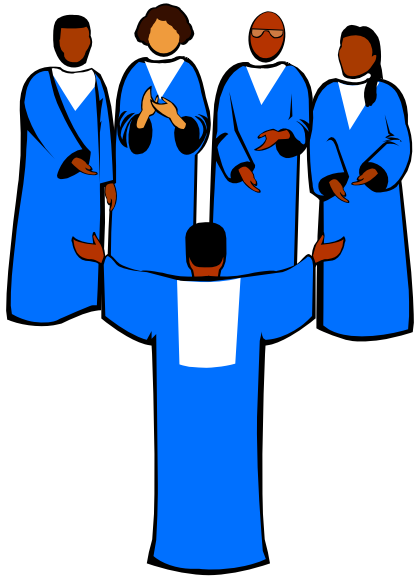


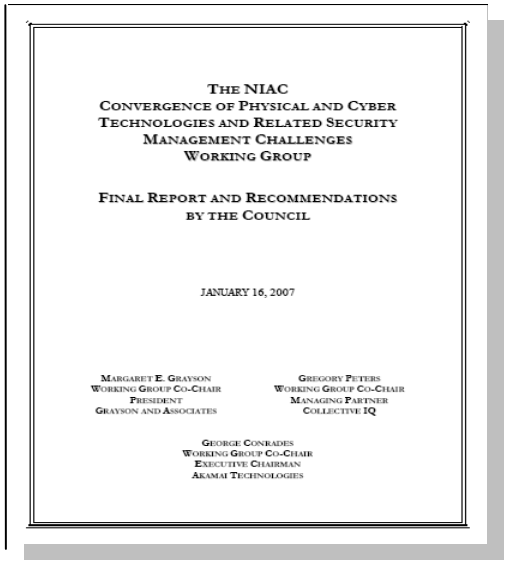
- **Strategic framework to guide public-private collaboration**
- **Industry-driven**
- **Near, mid, and long term**
- **Public-Private Working Group to coordinate implementation**
- ***ieRoadmap - enables implementation***

Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to ***survive*** an intentional cyber assault with no loss of critical function.

What Changed – Increasing Awareness and Collaboration





THE NIAC
CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES WORKING GROUP

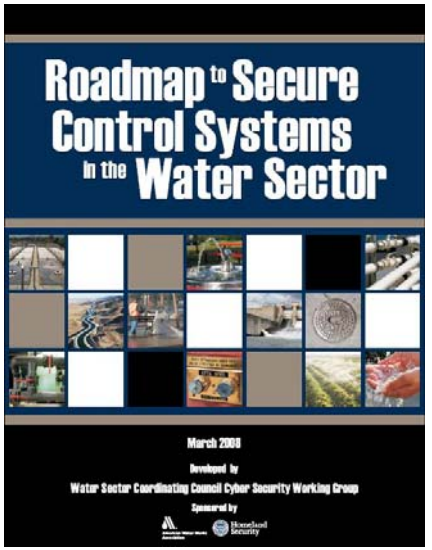
FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

JANUARY 16, 2007

MARGARET E. GRAYSON
WORKING GROUP CO-CHAIR
PRESIDENT
GRAYSON AND ASSOCIATES

GREGORY PETERS
WORKING GROUP CO-CHAIR
MANAGING PARTNER
COLLECTIVE IQ

GEORGE CONRADES
WORKING GROUP CO-CHAIR
EXECUTIVE CHAIRMAN
AKAMAI TECHNOLOGIES



2006

Preaching to the choir: Former NERC president and CEO Michehl Gent says at a Roadmap meeting industry must deal “with issues both *privately and publicly*.”

2007

Others take notice: The president’s National Infrastructure Advisory Council recommends other sectors “develop sector-specific roadmaps, *using the Energy Sector Roadmap as a model*.”

2008

Embracing the model: The water sector works with public and private stakeholders to develop their own roadmap with a similar vision and goals.

Support Increases from All Sides

2006: The business case challenge

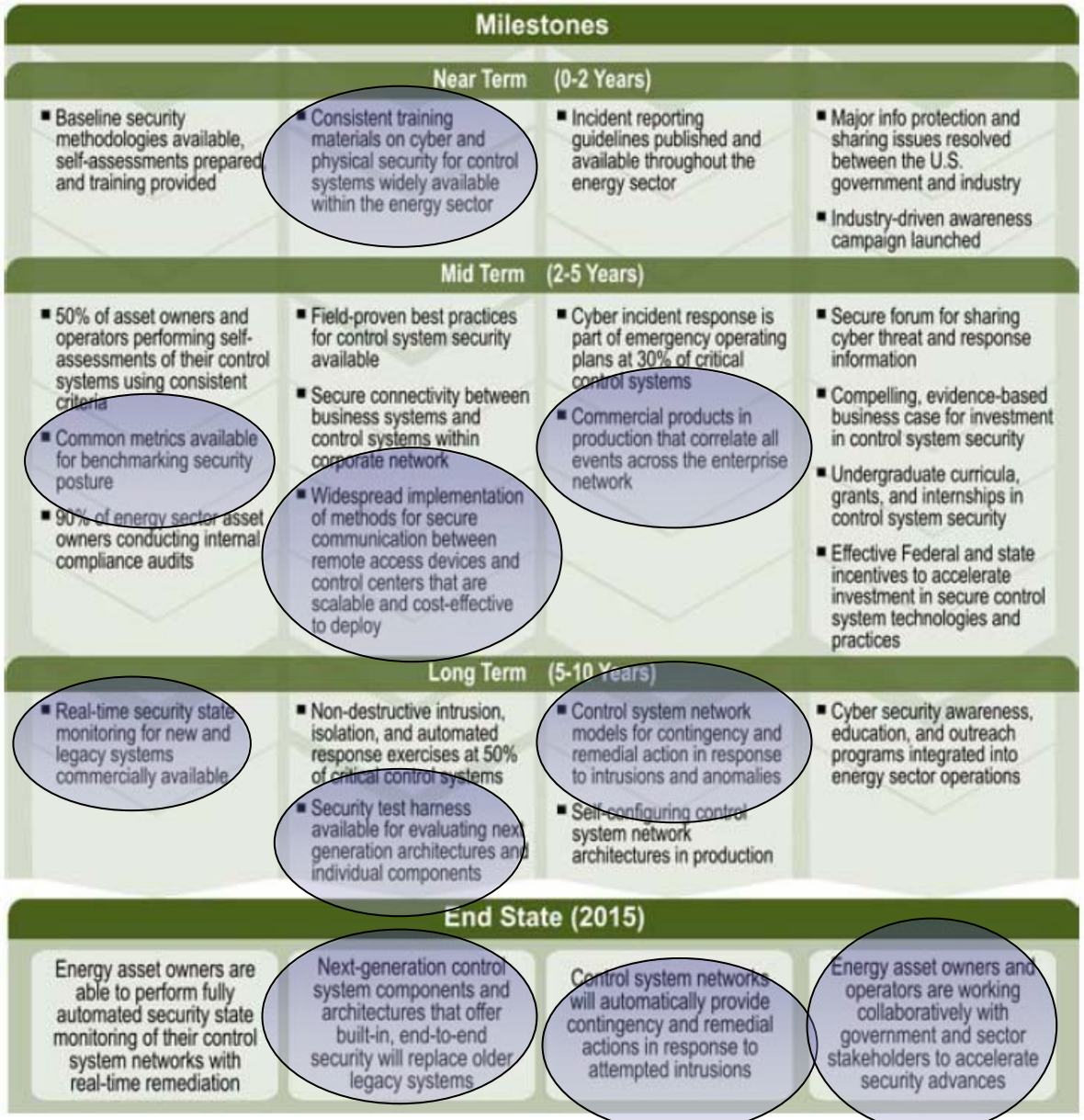
Roadmap identifies the weak business case for cyber security investments as a key challenge to industry collaboration and reaching Roadmap goals.

2008: Private sector utilities form cyber security consortiums

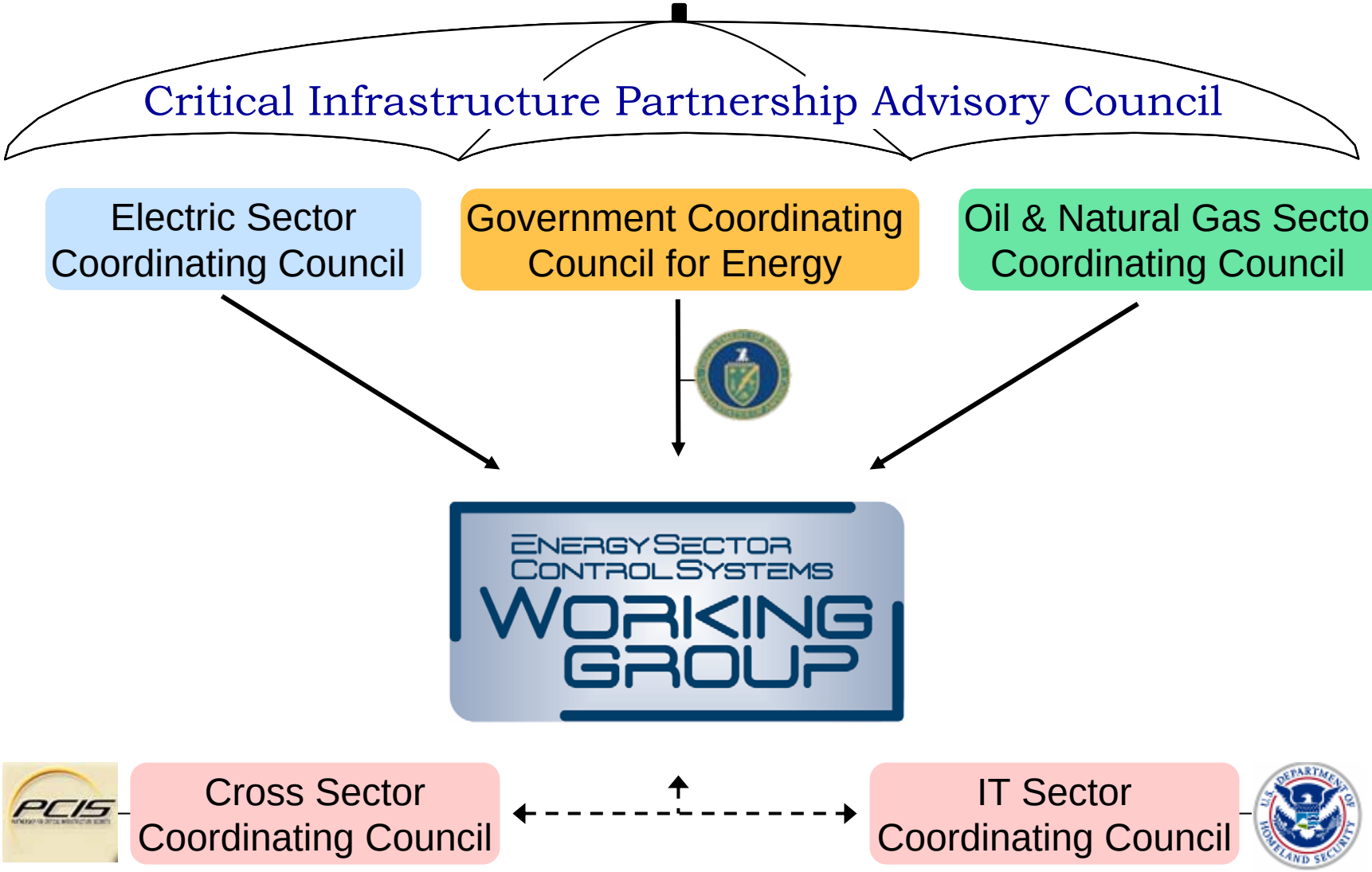
- Utilities who use ABB and AREVA systems join together to jointly fund vulnerability assessments at the National SCADA Test Bed on the control systems they use
- Leverages utility, vendor, and government funding to identify vulnerabilities

2009: Those same utilities are now chipping in additional funding for follow-on testing

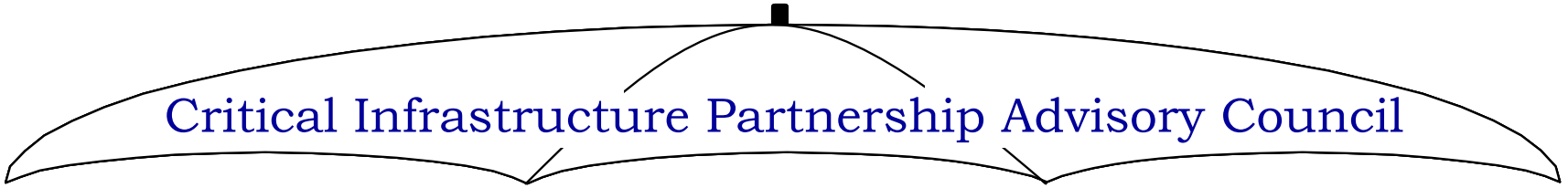
NSTB Activities Directly Support the *Roadmap*



Working Group Oversees Roadmap Implementation



Working Group Oversees Roadmap Implementation



Electric Sector Coordinating Council

- Alliant Energy
- IESO Ontario
- Progress Energy
- Entergy Corporation

Government Coordinating Council for Energy

- DOE National SCADA Test Bed Program
- DHS Science & Technology Directorate
- DHS National Cyber Security Division

Oil & Natural Gas Sector Coordinating Council

- NiSource
- El Paso Corporation
- BP
- Ergon Refining Inc.
- Alyeska Pipeline

2008 Workshops – A Closer Look at ieRoadmap Progress

Projects Assessed for Roadmap Alignment by Working Group Industry Members

Reviewed 42 of 102 total projects on ieRoadmap

mapped by 21 organizations

	16 projects	Measure and Assess Security Posture
	22 projects	Develop and Integrate Protective Measures
	13 projects	Detect Intrusion and Implement Response Strategies
	5 projects	Sustain Security Improvements

ieRoadmap – *We've Moved!*

Find us at our new address:

www.controlsystemsroadmap.net

We've reorganized, added links to important industry documents and information, made it easier to add and edit project details, and added new site content:

Promote your participation by linking to the site or putting the logo on project materials

See upcoming events on the industry calendar – and add your own events!

Read the Working Group's quarterly newsletter or sign up to receive it monthly – and stop by the NSTB booth to pick up this quarter's edition today!

The 2009 Initiatives

- **Impacts Report –** What are the Roadmap deliverables over the last three years?
- **Gap Analysis –** Refresh and sharpen the Goals, Milestones, and Projects for the 2009 – 2018 timeframe
- **ESCSWG Matchmaker Initiative –** Put processes and communication links in place to bring together asset owners and NSTB researchers
- **Issue the 2009 Roadmap to Secure Control Systems in the Energy Sector**

For more info, contact:

Thomas R. Flowers, P.E.

Flowers Control Center Solutions, LLC

flowersccs@att.net

936-894-3649

Hank Kenchington

US Department of Energy

henry.kenchington@hq.doe.gov

202-586-1878

ie Roadmap

interactive energy Roadmap to secure control systems

www.controlsystemsroadmap.net

Promising Results toward Roadmap Goals

Ant Farm

- Uses passive techniques to remotely map a utility's electronic security perimeter
- In 5-10 years, real-time security state monitoring for new and legacy systems commercially available
- Audits control systems against an optimal security configuration
- Brings security event manager capabilities to existing scanning tools

- BACKUP SLIDES

The Public-Private Partnership Projects

1. **Hallmark Project** - commercialize Secure SCADA Communications Protocol (SSCP) - **Schweitzer Engineering Laboratories, Pacific Northwest National Laboratories, CenterPoint Energy**

2. **Detection and Analysis of Threats to the Energy Sector (DATES)** – IDS (network, host, and device level), event correlation framework, and a sector-wide, distributed, privacy-preserving repository of security events for participants to automatically contribute *without attribution* - **SRI International, ArcSight, Sandia National Laboratory, end-user** (tbd)

3. **Audit and Attack Detection Toolkit -** extend capability of existing vulnerability scanning tools (e.g., Nessus et al) to evaluate SCADA security configuration (supports compliance with NERC CIP-005 and CIP-007) and develop templates for a security event monitoring system by mining data in PI Systems - **Digital Bond, Tenable Network Security, OSIsoft, Constellation Energy, PacifiCorp, TVA**

4. **Lemnos Interoperable Security Program -** conduct testing, validation, and outreach to increase the availability of cost-effective, interoperable security solutions for IP-based communications; foster development and acceptance of standards - **EnerNex Corp., Schweitzer Engineering Laboratories TVA, Sandia National Laboratory**

5. **Protecting Intelligent Distributed Power Grids against Cyber Attacks -** develop risk-based critical asset identification system; an integrated and distributed security layer including security agents, distributed security switched managers, and security managers and an optimization technique to establish the best topology for networking the security components -**Siemens Corporate Research, Idaho National Laboratory, Rutgers Center for Advanced Energy Systems**

Roadmap-Centric NSTB Reports

- Measure and Assess Security Posture
  - ***Categorizing Threat: Building and Using a Generic Threat Matrix*** **(SNL)**
  - ***Threat Analysis Framework*** **(SNL)**
  - ***Security Metrics for Process Control Systems*** **(SNL)**
- Develop and Integrate Protective Measures
  - ***Secure SCADA Communication Protocol Performance Test Results*** **(PNNL)**
  - ***AGA 12, Part 2 Performance Test Results*** **(PNNL)**
  - ***Secure ICCP Integration Considerations and Recommendations*** **(SNL)**
  - ***NERC 2007 Top 10 Vulnerabilities/Mitigations*** **(NSTB)**
  - ***Security Framework for Control System Data Classification and Protection*** **(SNL)**
- Detect Intrusion and Implement Response Strategies
  - ***OPSAID Initial Design and Testing Report*** **(SNL)**
- Sustain Security Improvements
  - ***Framework for SCADA Security Policy*** **(SNL)**
  - ***Impacts of IPv6 on Infrastructrure Control Systems*** **(SNL)**

Selected NSTB FY08 Activities

1. System Vulnerability Assessments and Mitigation

- Test bed and On-site SCADA/EMS Vulnerability Assessments:
  Completed: ABB, AREVA, GE, Siemens
  In process/planned: Telvent, OSI, Siemens, ABB Consortium, Teltone Gauntlet Dial-up Gateway

2. Public-Private Partnership, Outreach, and Awareness

- Vendor User Groups, training courses - over 1,700 end-users trained to date
- Red/Blue Team Training
- Coordinate with Industry groups (electric, oil, and gas)

3. Integrated Risk Analysis

- Modelling/simulation capability to better evaluate RISK of various cyber threats

4. Next Generation Technology Development

- Secure SCADA Communications Protocol for serial-based data communications
- Open architecture for secure, interoperable IP-based communications
- Advanced Network Toolkit for Advanced Remote Mapping (ANTFARM)
- 5 new industry-led projects – over $8MM in federal funding plus private cost-share

Enhanced SCADA Systems in Market TODAY!