



Securing Control Systems in the Energy Sector

U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Hank Kenchington
202-586-1878
henry.kenchington@hq.doe.gov



Homeland Security – need for a collaborative approach

Homeland security is a shared responsibility. In addition to a national strategy, **we need compatible, mutually supporting state, local, and private-sector strategies.**

*President George W. Bush
July 16, 2002*

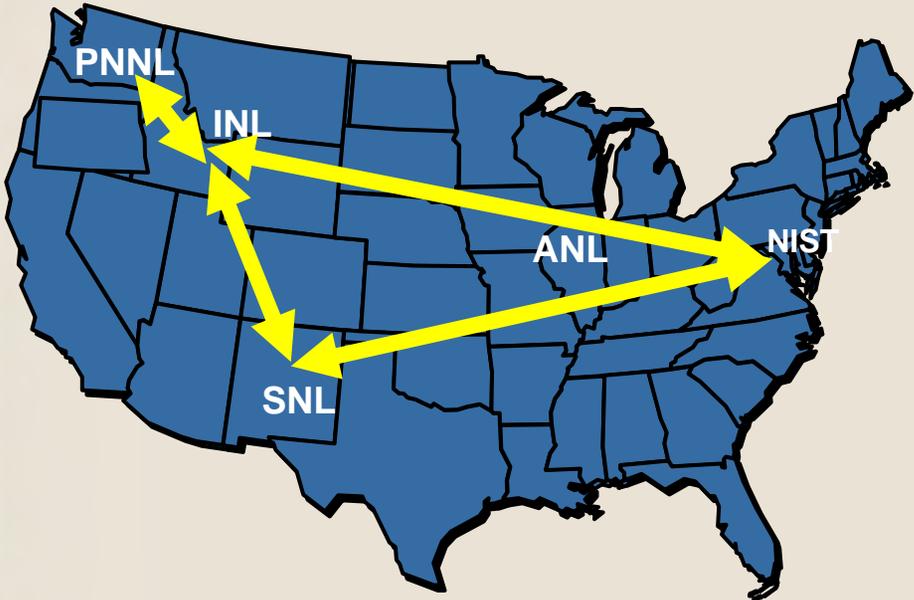
National SCADA Test Bed

OBJECTIVE

Support industry and government efforts to enhance control systems cyber security across the energy infrastructure

Scope

DOE multi-laboratory program jointly managed and executed by Idaho National Laboratory and Sandia National Laboratory



Key program areas

- SCADA system vulnerability assessment/mitigation
- RDT&E of advanced secure control systems technology
- support development of security standards
- outreach and awareness

National SCADA Test Bed

Key accomplishments:

1. SCADA System Assessments - ABB, AREVA, GE, Siemens
2. Provided cyber security training to over 500 end-users
3. Evaluated use of off-the-shelf IT antivirus and firewall tools in control systems
4. Working closely with electricity sector, developed mitigation strategies for “top 10” vulnerabilities
5. Conducting performance testing and cryptographic analysis of AGA 12 serial link encryption technology
6. Developed SCADA Reference Model
7. Developing Virtual Control Systems Environment Tool

Results:

- **New “hardened” SCADA systems now being deployed**
- **Software patches developed by vendors and supplied to end-users to better secure existing systems**

Enhanced SCADA systems in market TODAY

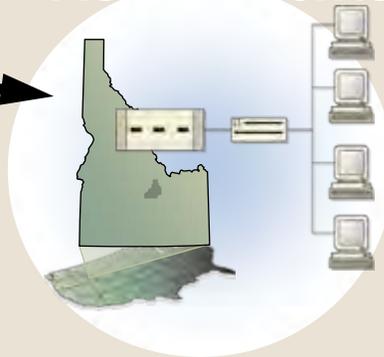
Vendor



**“Proprietary”
Assessment
Results**

**DCS/SCADA
Systems**

**NSTB
Assessments**



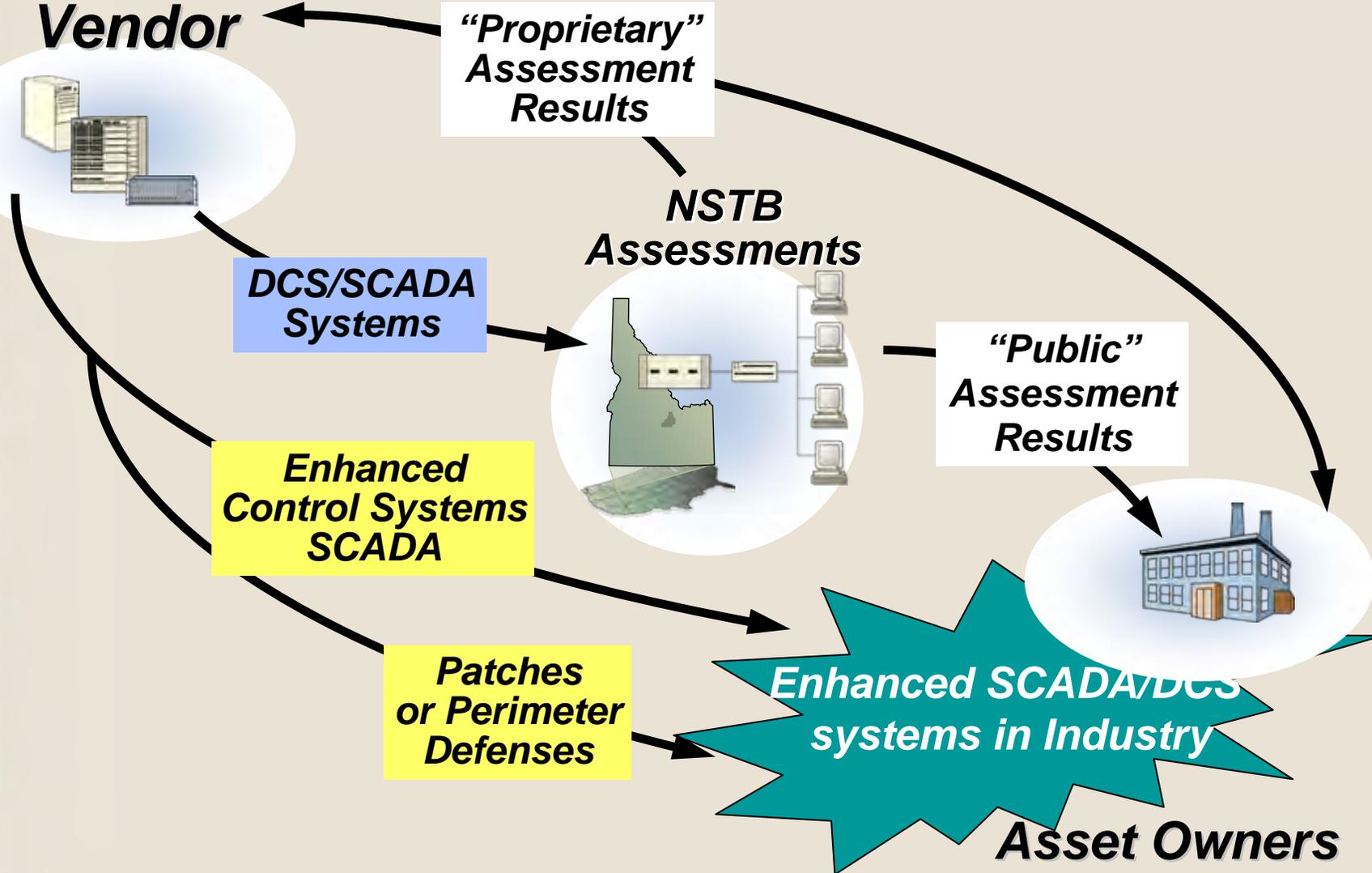
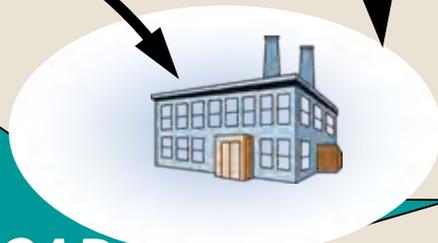
**“Public”
Assessment
Results**

**Enhanced
Control Systems
SCADA**

**Patches
or Perimeter
Defenses**

**Enhanced SCADA/DCS
systems in Industry**

Asset Owners



NSTB Assessment Findings

	Completed	In Process	Planned
Systems In House	6	1	5*
Components	1		
On-Site	3	1	7

* 3 out of the 5 are in the 2nd or 3rd iteration

Assessments have helped develop more secure SCADA systems:

3	Enhanced Systems
1	Enhanced System in development
1	Patch (addressing 2 issues)
2	New Perimeter Architectures
6	Repeat Assessments

Example Vulnerability: Clear Text Communications

	Skill	Severity
5/6 – Enumeration of Accounts and Passwords	 Moderate	 High
6/6 – Possible Replay Attack	 Low	 High
6/6 – Possible Reverse Engineer Protocol (3 completed)	 Low	 High

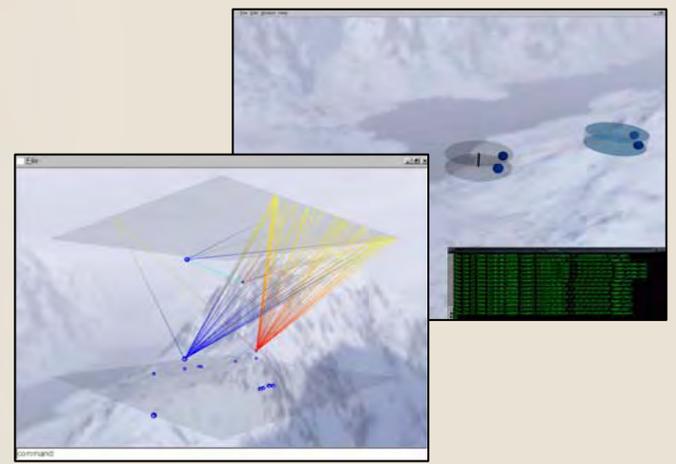
Mitigations: Encrypt where feasible — requires vendor modifications and support. New applications can/should use available secure protocols

Virtual Control System Environment Tool (VCSE)



Description:

Modeling and simulation tool to analyze and assess control systems without risking disruption to critical operations. Simulate control system devices and network communications and enable real-time, hardware-in-the-loop (HITL) emulation.

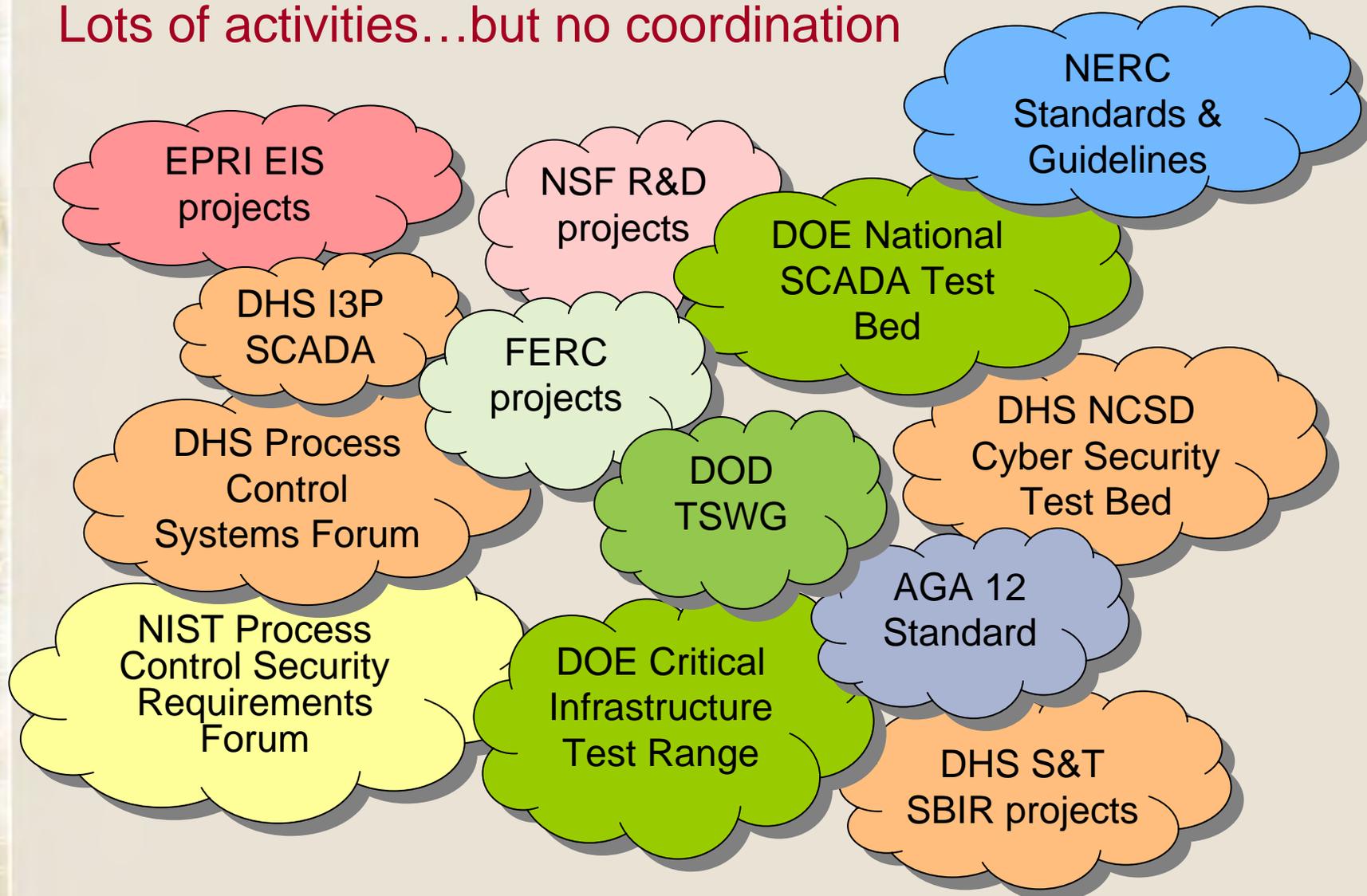


Benefits:

Tool for industry to analyze impacts of system vulnerabilities, estimate failure consequences, and assess performance impacts of alternative security approaches.

Why a Roadmap?

Lots of activities...but no coordination



Roadmap Steering Committee

Asset Owners and Operators

- Tom Flowers, CenterPoint Energy (electricity)
- Linda Nappier, Ameren(electricity)
- Al Rivero, formerly w/Chevron (oil and gas)
- David Poczynek, Williams Co. (oil and gas)
- Tom Frobase – TEPPCO (oil and gas)
- Michael Assante – formerly w/AEP and IEIA Forum

Industry Organizations

- Bill Rush, GTI
- Lisa Soda, API
- Kimberly Denbow, AGA
- Gary Gardner, AGA
- Tom Kropp, EPRI

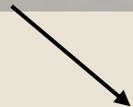
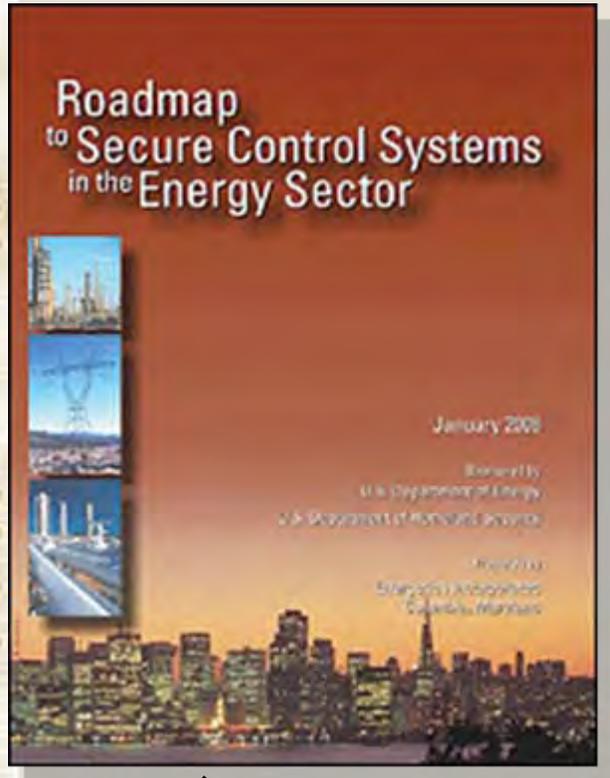
Government

- Doug Maughan, U.S. DHS (HSARPA)
- Hank Kenchington, U.S. DOE
- David Darling, Natural Resources Canada

Researchers (National Labs)

- Tommy Cabe, Sandia National Laboratories
- Jeff Dagle, Pacific Northwest National Laboratory
- Bob Hill, Idaho National Laboratory

Roadmap Scope

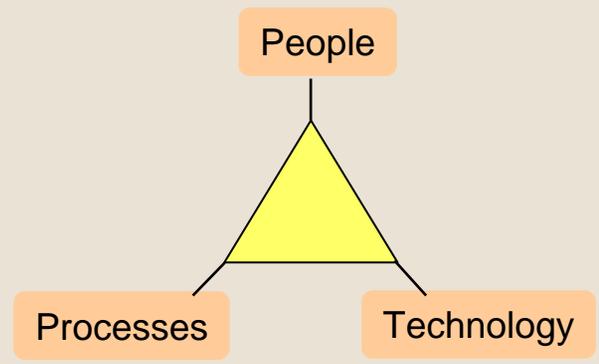


See: www.controlsroadmap.net

Sectors

Electricity Oil Gas Telecom (supporting)

Potential Solutions



Time Frames

- Near: 0-2 yrs.
- Mid: 2-5 yrs.
- Long: 5-10 yrs.

Roadmap Framework

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.

Key Strategies

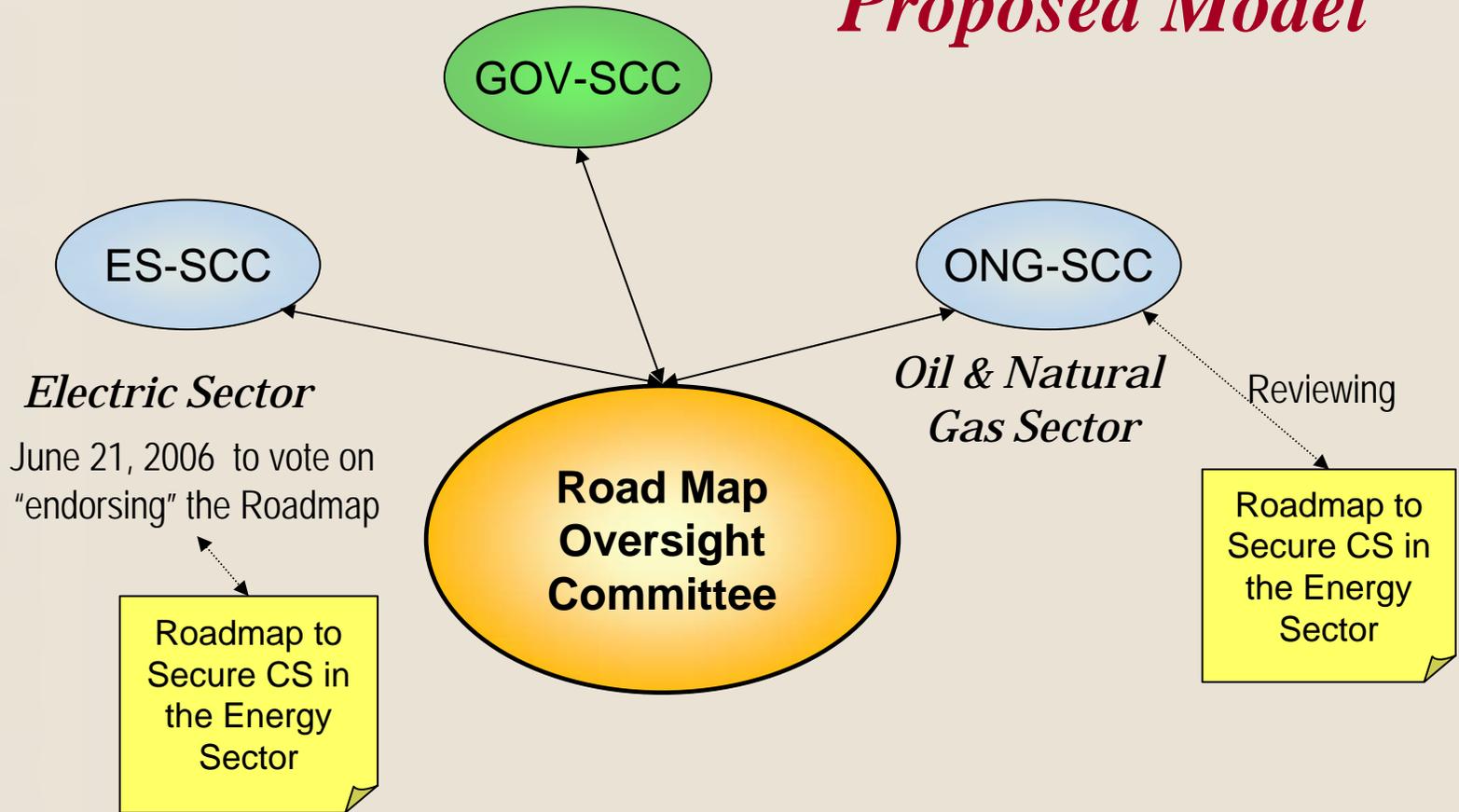
1. Measure and assess security posture
2. Develop and integrate protective measures
3. Detect intrusion and implement response strategies
4. Sustain security improvements

Roadmap-Related Activities

1. **NERC** - Cyber Security Standards, Control Systems Security Working Group
2. **EPRI Energy Information Security** – Improve security of communications and control technologies
3. **DHS/NCSD Control Systems Security Program** – Framework for self-assessments, US-CERT for control systems, standards, outreach
4. **Process Control Systems Forum** – Open forum to accelerate secure controls systems. Funded by DHS
5. **DHS/S&T** – Several R&D projects on advanced intrusion detection systems
6. **NIST** – Process Controls Systems Requirements Forum (PCSRF), standards
7. **DOD/TSWG** – SCADA Pocket Guide, AGA 12
8. **I3P (DHS)** – Research consortium focusing metrics, business case, interdependencies, technology transfer
9. **Trustworthy Cyber Infrastructure for the Power Grid (TCIP)** – Fundamental science for a secure, adaptive power grid with varying trust environments. Funded by NSF, DOE, DHS

Public-Private Partnership to Implement Roadmap

Proposed Model



Implementation: NSTB FY06 Work Plan

.....activities aligned to support Roadmap goals

Goal 1. Measure and Assess Security Posture

- Conduct cyber assessments of 6 SCADA systems in test bed
- Conduct assessments of 4 operational systems (pilot DHS Framework Tool)

Goal 2. Develop and Integrate Protective Measures

- SCADA Protocol Authentication
- Evaluate trends in IT that impact control systems security (e.g., IPv6, wireless, Advanced Metering Infrastructure)
- Develop/demonstrate Virtual Control Systems Environment Tool
- Support Trustworthy Cyber Infrastructure for the Power Grid program (NSF)

Goal 3. Detect Intrusion and Implement Response Strategies

- Work with DHS to advance Security Event Correlation technology

Goal 4. Sustain Security

- Conduct 5 workshops on SCADA systems vulnerabilities and mitigation techniques
- Co-host control systems security conference
- Continue to work with PCSF and others (e.g., NERC/CSSWG, AGA, API Cybernetics Committee)

Implementation: Mapping Activities

Roadmap to Secure Control Systems in the Energy Sector Goal 2 - Develop and Integrate Protective Measures

CHALLENGES	INL NSTB/NCSD Projects	SNL NSTB Projects	TSWG Projects	I3P Projects	TCIP Projects	NIST Projects	DHS/HSARPA SBIR Projects	MS-ISAC Projects
Open and flexible control leads to increased risks	SCADA/EEMS Assessments		SCADA Security Packet Guide SCADA Security Guide Training Support Program (TSP) AGA 12 Part 1 SCADA Encryption Module Open Source Security Toolkit SCADA Protocol Vulnerability SCADA Cyber Attack Alert Tool (prepared) Transmission Tower and Line Security Monitor (prepared) Hart-based IIDS/IPS for Control Systems (prepared)	Process Control Systems Security Project: Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency	Secure and Reliable Computing Base Trustworthy Data Collection and Control Infrastructure	PCSRF Central Systems Security Protection Framework Requirements Review SCADA Protection Profile SP 800-53 Baseline Security Controls for SCADA and DCS ISA-SP 99	Secure SCADA Toolkit Secure Source Security Information Management Secure Cryptographic Management System Ariet 12	SCADA Procurement Project
Poorly designed connection to SCADA and business networks can dramatically increase vulnerabilities of control systems	SCADA/EEMS Assessments Recommended Practicer (WP Item 3.6.3)	SCADA Reference Model - Fundamental Security Practicer Virtual Control System Environment	SCADA Security Packet Guide SCADA Security Guide Training Support Program (TSP) AGA 12 Part 1 Open Source Security Toolkit SCADA Protocol Vulnerability SCADA Cyber Attack Alert Tool (prepared) Hart-based IIDS/IPS for Control Systems (prepared)	Process Control Systems Security Project: Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency	Secure and Reliable Computing Base Trustworthy Data Collection and Control Infrastructure	PCSRF Central Systems Security Protection Framework Requirements Review SCADA Protection Profile SP 800-53 Baseline Security Controls for SCADA and DCS ISA-SP 99	Secure SCADA Toolkit Secure Source Security Information Management Secure Cryptographic Management System Ariet 12	SCADA Procurement Project
Security upgrades hard to retrofit to legacy systems, may be costly, and may degrade system performance	SCADA Security Training Report: Cyber Security Assessments of SCADA and Energy Management Systems (to be issued)	Anti-Virus SLAP AGA 12 Secure IOPP IPv6 Network Security Infrastructure Testing	AGA 12 Part 1 SCADA Encryption Module			PCSRF Central Systems Security Protection Framework Requirements Review SCADA Protection Profile SP 800-53 Baseline Security Controls for SCADA and DCS ISA-SP 99 ICS Vendor Security Checklist Program	Ariet 12	SCADA Procurement Project
Known technical risks can migrate from non-vendor supporting hardware and software			SCADA Security Packet Guide SCADA Security Guide Training Support Program (TSP) Open Source Security Toolkit SCADA Protocol Vulnerability Hart-based IIDS/IPS for Control Systems (prepared)	Process Control Systems Security Project: Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency	Secure and Reliable Computing Base Trustworthy Data Collection and Control Infrastructure	PCSRF Central Systems Security Protection Framework Requirements Review SCADA Protection Profile SP 800-53 Baseline Security Controls for SCADA and DCS ISA-SP 99 ICS Vendor Security Checklist Program	Secure SCADA Toolkit	SCADA Procurement Project

Goal 1 Measure and Assess Security Posture

Challenges

- Risk factors are not widely understood or accepted by technologists/managers
- Insufficient security metrics limit risk analysis capability
- Insufficient tools and techniques exist to measure risk
- No standard metrics for cyber

Understanding and Quantifying the Economic Impact of Security Failures and Defense Strategies

Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency

Threat and Intelligence owned

- DOE/NSTB
- DHS/CSSP
- TSWG
- I3P
- TCIP

cyber
state
asset

WIIFM

(What's in it for me?)

- SCADA/DCS vendors are engaged and developing more secure systems
- Risk of adopting new, more secure technologies is being reduced
- Tools/technologies to help you better secure your systems
- Developing awareness of “threat” to support business case
- Opportunities to participate in pilot demonstrations and technology development

For more info...

- www.controlsystemsroadmap.net
- www.sandia.gov/scada
- www.inl.gov/scada
- www.iac.anl.gov
- <http://homeland-security.pnl.gov/cip.stm>

END

US Department of Energy
Office of Electricity Delivery and Energy Reliability

Hank Kenchington
henry.kenchington@hq.doe.gov
202-586-1878