Process Control Systems Forum

Technology Roadmap to Secure Control Systems in the Energy Sector

May 17, 2005

Hank Kenchington
US Department of Energy

AGENDA

- Background
- Role of DOE in DCS/SCADA security
- Accomplishments
- Need for a coordinated strategy
- Path forward

Critical Infrastructure Protection:
Federal Policy Development

- National Strategy for Homeland Security (July 2002)
- Homeland Security Act of 2002 (November 2002)
- National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)
- National Strategy to Secure Cyberspace (February 2003)
- Homeland Security Presidential Directive 7 (December 2003)

HSPD 7 Sector-Specific Agencies

President

Secretary of Homeland Security

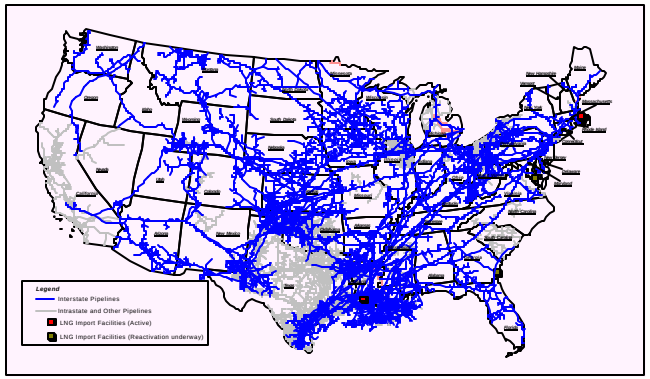
Sector	Lead Agency
Agriculture, Food	**Department of Agriculture**
Water	**EPA**
Public Health	**Health and Human Services**
Energy	**Department of Energy**
Banking and Finance	**Department of Treasury**
National monuments and icons	**Department of Interior**
Defense industrial base	**Department of Defense**

HSPD 7 designates DOE as the Sector-Specific Agency responsible for critical infrastructure protection (physical and cyber) for the energy sector (oil, gas, and electric, not nuclear).

Scale and Complexity of Energy Infrastructure

- 157,810 Miles of Electrical Transmission lines
- 16,756 Generators; 948,446 Megawatts (net summer capacity)
- Over 3,100 Electric Utilities, with 131 million customers

Active Refinery Locations, Crude and Product Pipelines



Source: Energy Information Administration, Office of Oil & Gas

- 2,000,000 Miles of Oil Pipelines
- 1,300,000 Miles of Gas Pipelines
- 2,000 Petroleum Terminals
- ~1,000,000 Wells
- Extensive Ports, Refineries, Transportation, and LNG Facilities

Critical Differences of Today's Energy Infrastructure

Increased threats against critical infrastructure

An aging infrastructure facing increasing demand and operating in new ways

An ever-increasing degree of "interconnectedness" between critical infrastructures

A Shared Responsibility

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

Control System Security is a Priority

Gap Analysis, DOE National Laboratory Task Force on Energy Infrastructure Assurance, February 2002

"SCADA systems . . . employ few modern cyber security technologies and are increasingly prone to malicious activity."

Making the Nation Safer, The Role of Science and Technology in Countering Terrorism, National Research Council, 2002

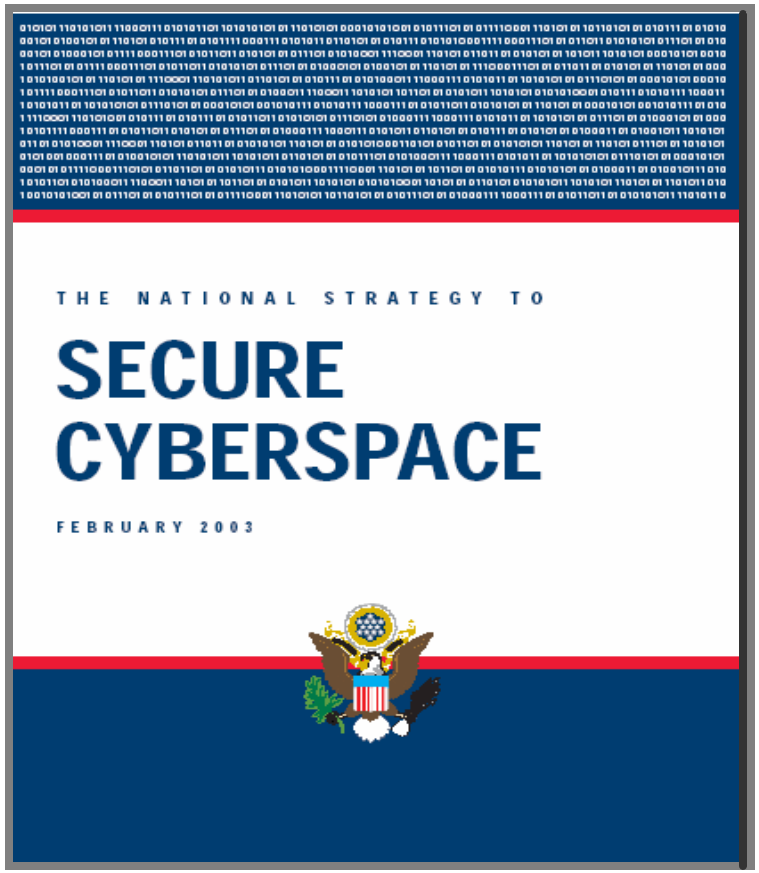
Fourteen of the Most Important Technical Initiatives

"Protect energy distribution services by improving security for supervisory control and data acquisition (SCADA) systems . . ."

Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, GAO, March 2004

"Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for the private sector to develop and implement more secure control systems."

National Policy Guidance



"Securing DCS/SCADA is a national priority. Disruption of these systems could have significant consequences for public health and safety."

(pg. 32)

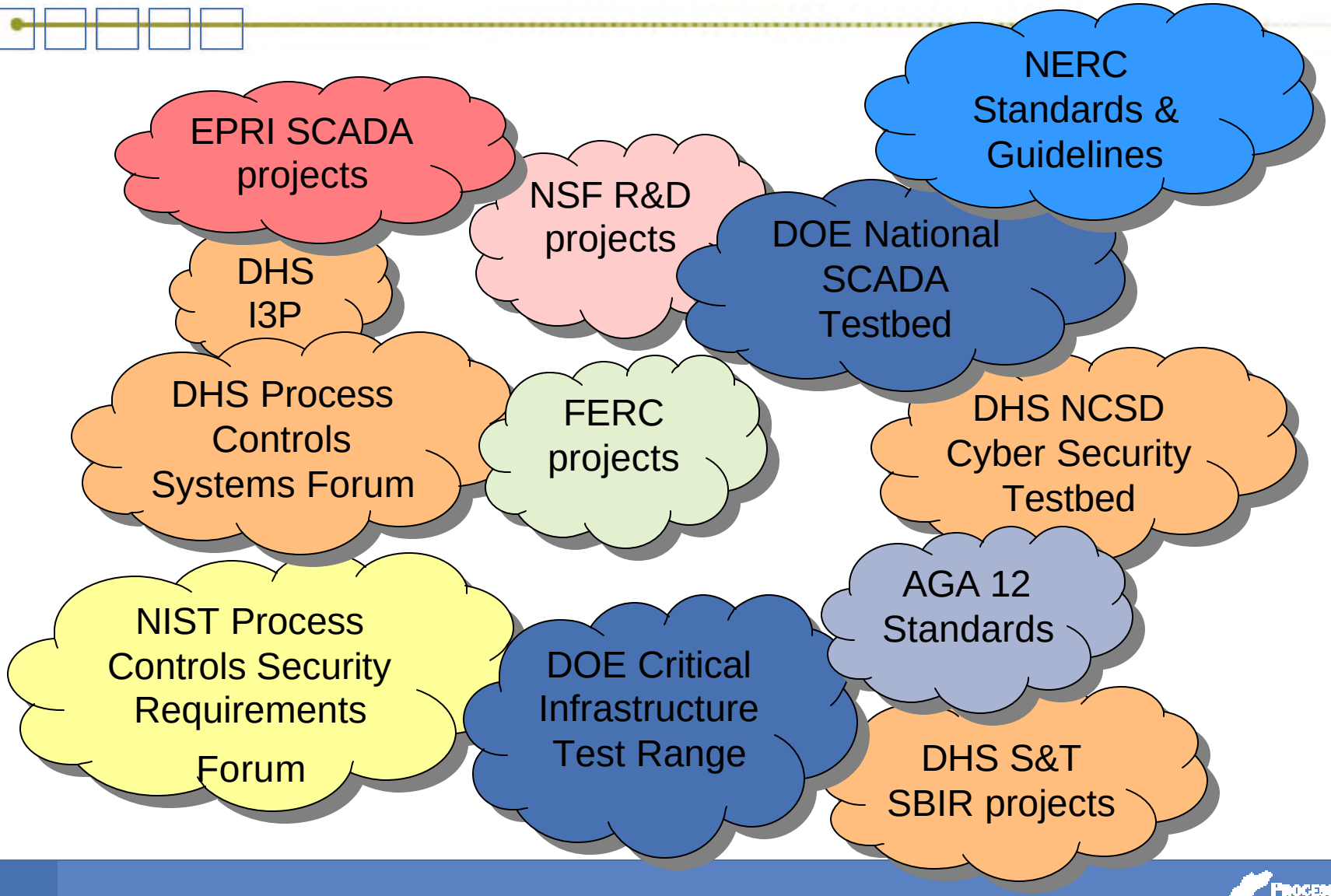
The Security Challenge

- Use of standardized technologies increasing
- Control systems connected to other networks
- Control systems may not have built-in security features
- Increased use of internet as communications channel
- Lack of control system security technologies applicable to control systems

Recommendations for Improved Cyber Security in Energy Sector Control Systems

- *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*, President's Commission on Critical Infrastructure Protection, 1998
- *An Approach to Action for the Electricity Sector*, North American Electric Reliability Council, June 2001
- *Securing Oil and Gas Infrastructures in the New Economy*, National Petroleum Council, June 2001
- *Gap Analysis*, DOE National Laboratory Task Force on Energy Infrastructure Assurance, February 2002
- *The Electricity Sector response to the Critical Infrastructure Protection Challenge*, North American Electric Reliability Council, May 2002
- *Physical Protection Planning Workshops*, Defense Threat Reduction Agency, RAND Corporation, Summer 2002
- *Making the Nation Safer, The Role of Science and Technology in Countering Terrorism*, National Research Council, 2002
- *Natural Gas Infrastructure Surety Workshop*, Gas Technology Institute (GTI), the Interstate Natural Gas Association of America (INGAA) and Sandia National Laboratories, December 5, 2002.
- *National Strategy to Secure Cyberspace*, The White House, February 2003

Coordination?



Why a Technology Roadmap?

- Identify customer needs and priorities
- Improve coordination
- Improve communications
- Align and leverage resources
- Achieve results faster and more efficiently

Control Systems Roadmap

PURPOSE

- Define a strategy that reflects the cyber security needs of private and public owners in the energy sector
- Identify critical needs and priorities for advanced energy sector control systems to improve their security, reliability, and functionality
- Guide resources in industry, academia, and government and define roles and responsibilities for key stakeholders

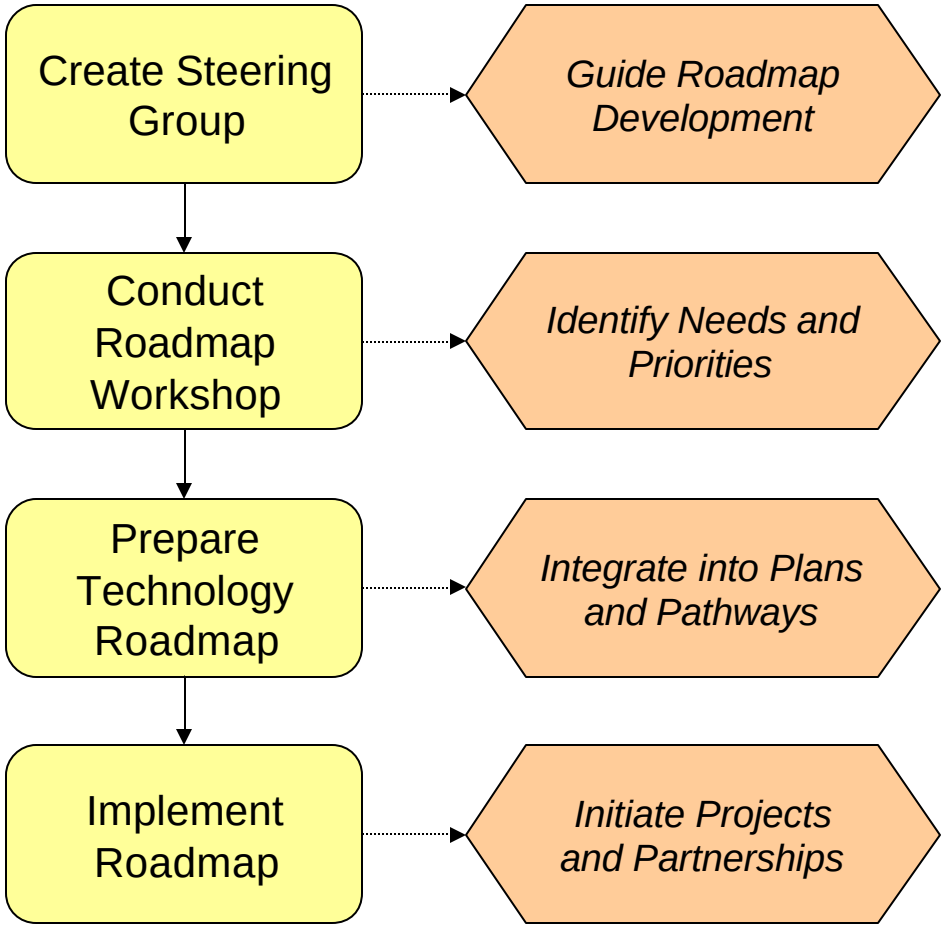
REQUIREMENTS

- Led by energy sector owners and operators
- Reflects control system needs of electricity and oil and gas systems
- Engages a cross-section of stakeholders and experts
- Provides solutions for the near, mid, and long term
- Is actionable

EXPECTED OUTCOMES

- Publish a technology roadmap document that aligns industry and government interests to improve process systems
- Identify gaps in R&D, technology, and other activities
- Form public-private partnerships to pursue roadmap priorities
- Guide federal research agendas
- Improve the security of existing and future control systems

Roadmap Development Steps



Steering Committee

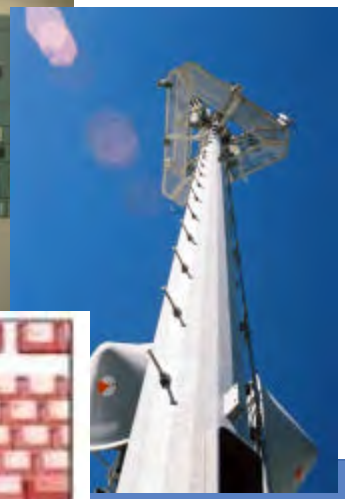
- Electricity Sector Asset Owners (2)
- Oil and Gas Asset Owners (3)
- Gas Technology Institute
- American Petroleum Institute
- DHS/S&T
- Institute for Information Infrastructure Protection
- Public Safety and Emergency Preparedness Canada
- Natural Resources Canada
- International Energy Infrastructure Assurance Forum
- DOE National Laboratories (3)

National SCADA Test Bed

RDT&E Assets

Idaho National Laboratory / Sandia National Laboratory

- ***SCADA / Process Control Systems Test Bed***
- ***Wireless Test Bed***
  - *3G/4G testing*
  - *Local area network and 802.11 testing*
- ***Power Grid Test Bed***
  - *61 miles of 138 kV transmission*
  - *7 substations*
- ***Cyber Security Test Bed***
  - *Vulnerability assessments*
  - *Intrusion detection expertise*
- ***Control Center Lab***
- ***Remote Substation Lab***
- ***Attack Resource Center***
- ***Center for Cyber Defenders***
- ***Network Research Lab***
- ***Cryptography Lab***
- ***Electric Power Test Labs***
- ***Center for SCADA Security***



Recent Accomplishments

- Established Critical Infrastructure Test Range
- Established multi-laboratory National SCADA Test Bed team
- Completed vulnerability testing of SCADA systems manufactured by major suppliers
- New “hardened” systems are now being deployed and supplier is upgrading installed systems
- Developed SCADA Reference Model
- Cataloged existing applicable SCADA Standards

National SCADA Test Bed

Recent Accomplishments and Pathway Forward:

FY 03

$3 million (INL)

- *Critical Infrastructure Test Range*

FY 04

$2 million (INL/SNL)

- *Secure ICCP, TCP/IP testing, Scada reference model, Standards catalogue*
- *Completed ABB Scada testing*

FY 05

$5 million (INL/SNL/PNNL/ANL)

- *Scada vulnerability testing (Areva, GE)*
- *AGA 12 crypto module testing*
- *Virtual SCADA environment*

FY06

Adjust plan to meet needs identified in Technology Roadmap to Secure Control Systems in the Energy Sector

END