U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

National SCADA Test Bed Program

Multi-Year Plan FY2008–2013

Enhancing Control Systems Security in the Energy Sector

January 2008

Contents

1. Introduction

The National SCADA Test Bed Program is a unique program within the U.S. Department of Energy (DOE) that aims to reduce the risk of energy disruptions due to cyber attacks on energy control systems. The program is integral for achieving a reliable, secure, and robust energy infrastructure that incorporates cyber security as a central design element. The program invests in research and development (R&D) for next generation control systems, vulnerability assessments, and risk analysis to improve cyber security both today and tomorrow.

This document presents the ***National SCADA Test Bed Program Multi-Year Plan***, a coherent strategy for improving the cyber security of control systems in the energy sector. The NSTB Program is conducted within DOE's Office of Electricity Delivery and Energy Reliability (OE), which leads national efforts to modernize the electric grid, enhance the security and reliability of the energy infrastructure, and facilitate recovery from disruptions to the energy supply. The Plan covers the planning period of fiscal year 2008 to 2013.

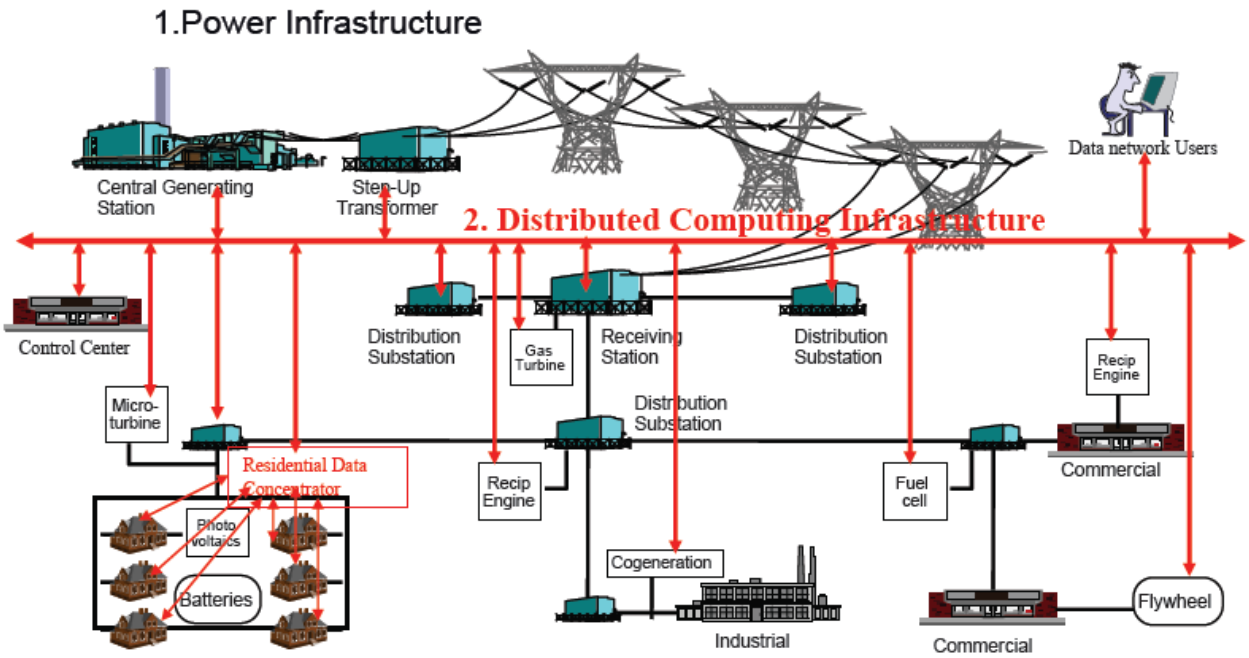
1.1 The Control Systems Security Imperative

An efficient, secure, and reliable energy infrastructure is increasingly important as we face a rapidly expanding digital economy, an increased threat environment, and the convergence of physical and cyber systems. The critical role of the energy sector was underscored during the 2003 Northeast blackout and during Hurricane Katrina in 2005, in which prolonged interruption of basic energy—electricity, natural gas, and petroleum—proved devastating.

As our dependence on uninterrupted energy distribution increases, so does the risk of a major disruption due to cyber attacks on energy control systems (i.e., supervisory control and data acquisition [SCADA] and distributed control systems [DCS]). Control systems are the digital "brains" that monitor, manage, and control the nation's vast interconnected network of electric transmission and distribution lines, electric substations, oil and gas pipelines, petroleum refineries, and natural gas processing plants. The increasingly critical role of control systems in our nation's infrastructures was emphasized in the White House's ***National Strategy to Secure Cyberspace*** and the recent report by the U.S. president's National Infrastructure Advisory Council titled ***Convergence of Physical and Cyber Technologies and Related Security Management Challenges***.

The immense complexity of modern energy systems and the increased need to respond rapidly to systems and market fluctuations have led the energy industry to rely substantially on information technology and the communication infrastructure to operate its physical assets. The reliability of the energy infrastructure is constantly threatened by any problems that the information infrastructure might suffer. This convergence of the physical and cyber realms has, metaphorically, placed an enormous and unprecedented number of eggs in one basket—exposing our vital energy infrastructure to increasing risks from all hazards (Exhibit 1.1).

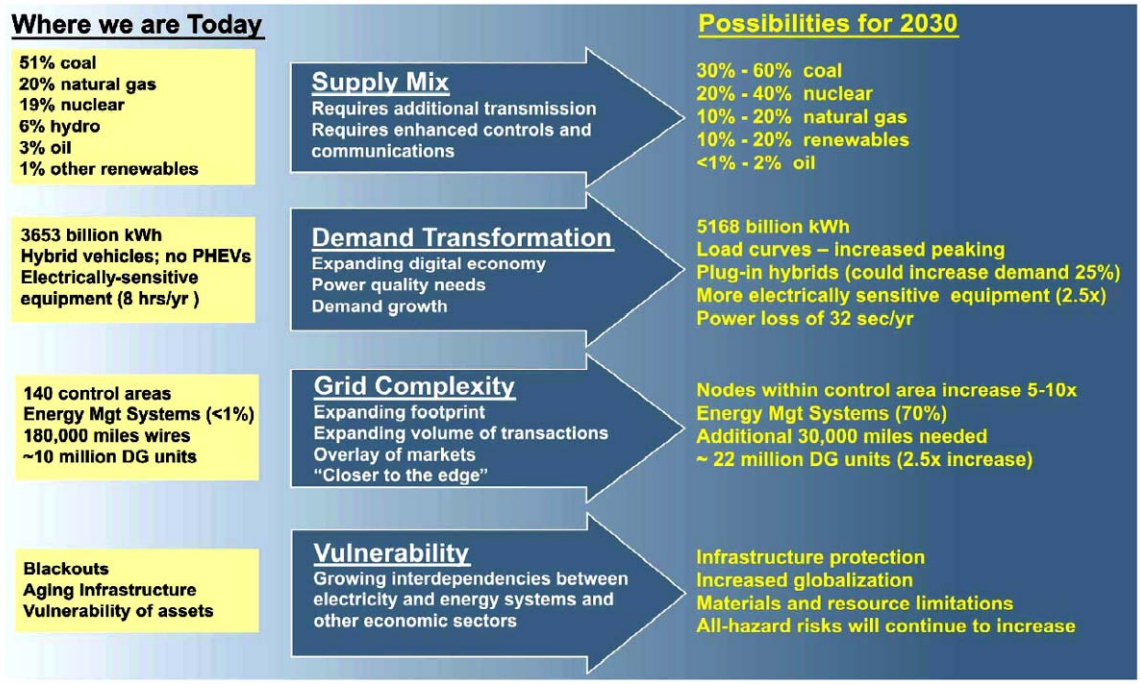
Exhibit 1.1 Two Infrastructures Must be Managed in the Future, Not Just One



Source: Electric Power Resource Institute (EPRI)

Looking forward, the delivery of electricity faces significant challenges (Exhibit 1.2). Electricity delivery systems will need to expand, evolve, and become "smarter" to meet the challenges ahead. A smart grid will grow to rely on control systems to enable two-way communication and digital control throughout the electricity delivery infrastructure. Integrating modern technologies—such as renewable technologies, plug-in hybrid vehicles, automatic metering, and smart appliances—into the electric infrastructure will require significant growth in computing and intelligence capacity, while substantially increasing the complexity of the entire systems. These advances will lead to greater cyber vulnerabilities unless cyber security is incorporated into emerging technologies. Without due consideration for cyber security, a smart, reliable, resilient grid will not be possible.

Exhibit 1.2 Electricity Delivery Faces Future Challenges



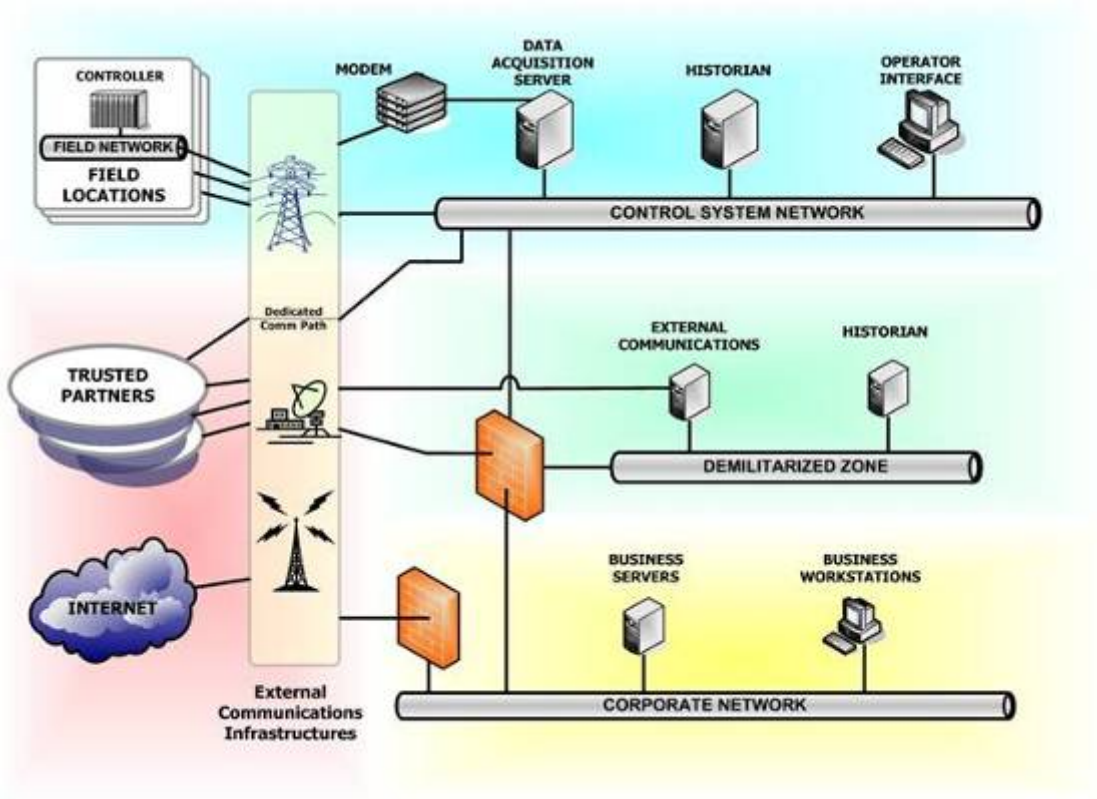
Source: *Office of Electricity Delivery and Energy Reliability Strategic Plan*, September 2007

1.2 Challenges to Secure Control Systems in the Energy Sector

Much of our current energy infrastructure and the control systems that operate it are being used in ways that were never intended in a deregulated energy market and a highly dynamic and expanding digital economy. Many of the control systems were designed decades ago for reliability in vertically integrated utilities with little or no consideration for cyber security. To remain competitive and meet changing energy demand patterns, the energy sector has invested heavily in information, communications, and automation technologies, including commercial-off-the-shelf (COTS) hardware and software. These systems improved productivity and efficiency but are now being connected to business networks, the Internet, and wireless networks—all of which have made energy control systems more vulnerable to cyber attack.

Today's energy control systems include a hierarchy of networked physical and electronic sensing, safety, monitoring, and control devices connected to a central supervisory station or control center. Control systems encompass: SCADA systems used to monitor vast, widely dispersed operations; DCS used for a single facility or small geographical area; and remote components such as remote terminal units (RTU) and programmable logic controllers (PLC) that monitor systems data and initiate programmed control activities in response to input data and alerts. Exhibit 1.3 depicts a control systems architecture commonly used in the energy sector.

Exhibit 1.3 Common Control Systems Architecture



Potential adversaries with malicious intent have developed sophisticated cyber attack tools that exploit flaws in systems components, telecommunication methods, and common operating systems in modern control systems. Effectively enhancing the security of energy sector control systems is a complex task. Exhibit 1.4 summarizes a number of interrelated technological, infrastructure, business, and informational challenges that dictate control systems security needs.

Exhibit 1.4 Challenges in Protecting Control Systems

- Adoption of standardized technologies with known vulnerabilities
- Increasing connectivity with other networks
- Insecure remote connections
- Limited understanding of vulnerabilities and consequences
- Lack of cyber security technologies specific to control systems
- Control systems not designed with cyber security built-in
- Weak business case for private sector investment in security
- Introduction of vulnerabilities via use of new hardware, software, or communication techniques
- Dependence on foreign manufacturers and suppliers

1.3 ROADMAP TO SECURE CONTROL SYSTEMS IN THE ENERGY SECTOR

Many energy companies and government agencies are actively working to assess and reduce the security risks to energy control systems. To define a common strategy for coordinating these diverse activities, control systems security experts developed the industry-driven ***Roadmap to Secure Control Systems in the Energy Sector***. The Roadmap was funded and facilitated by DOE-OE in collaboration with the U.S. Department of Homeland Security's Science and Technology Directorate (DHS S&T) and the Energy Infrastructure Protection Division of Natural Resources Canada. Input from industry experts in the electric, oil, and natural gas industries helped create real, applicable goals.

This landmark Roadmap established the following 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."**

The strategic framework to achieve this vision enables industry and government to align their programs and investments to improve cyber security quickly and efficiently. Exhibit 1.5 lists targets by 2015 for each of the Roadmap's four strategic goals.

Exhibit 1.5 Roadmap Goals

Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion & Implement Response Strategies	Sustain Security Improvements
Goal	**Goal**	**Goal**	**Goal**
By 2015, the sector will help ensure that energy asset owners have the ability and commitment to perform fully automated security state monitoring of their control system networks with real-time remediation capability.	By 2015, next-generation control system components and architectures that offer built-in, end-to-end security will replace many older legacy systems.	By 2015, the energy sector will operate control system networks that automatically provide contingency and remedial actions in response to attempted intrusions into the control systems.	By 2015, energy asset owners and operators are committed to working collaboratively with government and sector stakeholders to accelerate security advances.

With these industry-driven objectives in mind, an Energy Sector Control Systems Working Group of the Critical Infrastructure Partnership Advisory Council will coordinate Roadmap research efforts among the Electric Sector Coordinating Council (SCC), the Oil & Natural Gas SCC, and the Government Coordinating Council (GCC) for Energy (comprised of DOE and DHS members). The Working Group will review the status of Roadmap-related efforts and recommend necessary activities and appropriate roles and responsibilities as they relate to Energy SCC and GCC members. The NSTB Program will use this guidance to help prioritize its future efforts. While these needs will evolve over time, the Roadmap provides a starting point for upcoming research.

1.4 Security Partners

Enhancing control systems security in the energy sector requires the collective commitment of key stakeholders throughout the control systems value chain. Asset owners and operators bear the chief responsibility for ensuring that systems are secure, making appropriate investments, and implementing protective measures. They are supported by the software and hardware vendors, contractors, IT and telecommunications service providers, and technology developers who deliver systems products and services. Researchers at government laboratories and universities also play a key role in exploring long-term solutions and developing tools to assist the industry. Industry organizations and government agencies can provide the needed coordination, leadership, and investments to address important barriers and gaps. Each of these stakeholder groups brings specialized skills and capabilities for improving control systems security.

1.5 Federal Role

Despite increasing awareness among energy asset owners and operators of the need to improve the security of their control systems, little market incentive exists for private sector investment to develop and implement more secure control systems (GAO 2004). Equally significant, the private sector lacks dedicated sector-wide testing facilities and resources to do so in a cost-effective, efficient manner. Fully aware of this dilemma, DOE recognizes the distinct value its National SCADA Test Bed (NSTB) provides to the energy community.

NSTB is a unique federal resource that draws on the extensive assets and expert capabilities of participating national laboratories to accelerate development of a more secure and reliable energy infrastructure. The DOE National SCADA Test Bed Program funds gaps in control systems R&D and partners with industry to leverage the full benefits of NSTB as a shared, singular resource for the energy sector. Extending beyond internal recognition of its responsibility to secure the energy infrastructure, the DOE's role in energy infrastructure assurance has been defined in key policy guidance documents.

In 2003, the ***National Strategy to Secure Cyberspace*** outlined priority strategies to protect against cyber threats and the damage they can cause. It called for the DOE and DHS to work in partnership with industry to

> **"…develop best practices and new technology to increase security of DCS/SCADA, to determine the most critical DCS/SCADA-related sites, and to develop a prioritized plan for short-term cyber security improvements in those sites."**

Federal roles and responsibilities in infrastructure protection are more specifically defined in ***Homeland Security Presidential Directive 7*** and the ***National Infrastructure Protection Plan (NIPP)***. HSPD-7 designated DOE as the sector-specific agency for the energy infrastructure. As such, it is directed to

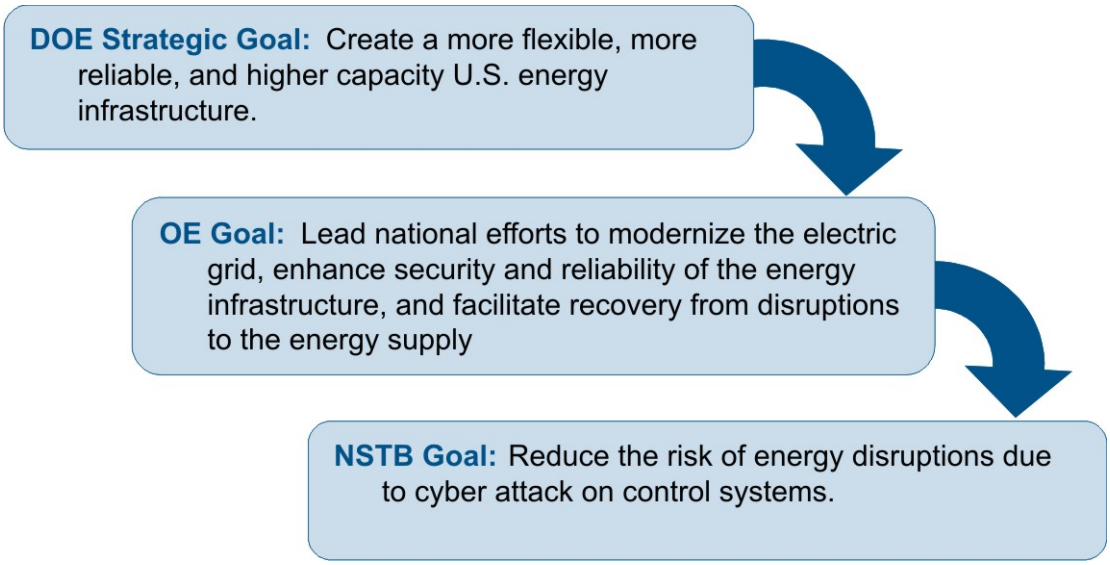
> **"…collaborate with all relevant federal departments and agencies, state and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources."**

2. Goals

2.1 DOE Strategic Plan

The ***U.S. Department of Energy Strategic Plan*** (2006) established 16 strategic goals to achieve its mission and vision in "promoting America's energy security through reliable, clean and affordable energy." These goals are inclusive of energy security, nuclear security, scientific discovery and innovation, environmental responsibility, and management excellence. More specifically Strategic Plan Goal 1.3 targets the creation of a more flexible, more reliable, and higher capacity U.S. energy infrastructure. The connections between this goal and those of OE and the NSTB Program are shown in Exhibit 2.1.

Exhibit 2.1 Relationship of NSTB Program Goal to DOE Strategic Goal



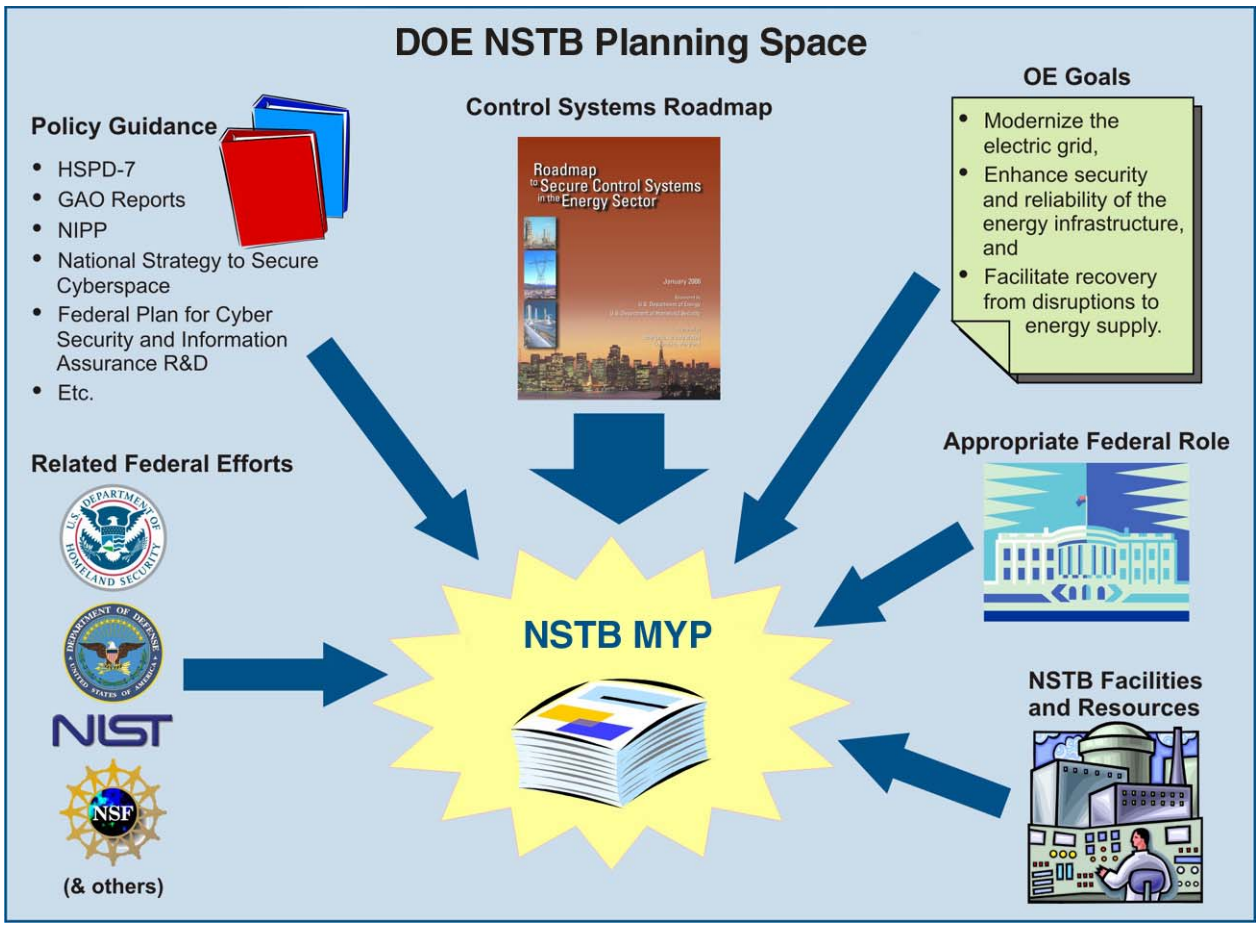
2.2 Office of Electricity Delivery and Energy Reliability

The Office of Electricity Delivery and Energy Reliability is the primary organization in DOE responsible for creating a more modern, resilient, and secure electric delivery infrastructure for America. OE's mission is to advance technology—in partnership with industry, government, academia, and the public—to meet America's need for a reliable, efficient, and resilient electric power grid.

2.3 National SCADA Test Bed Program

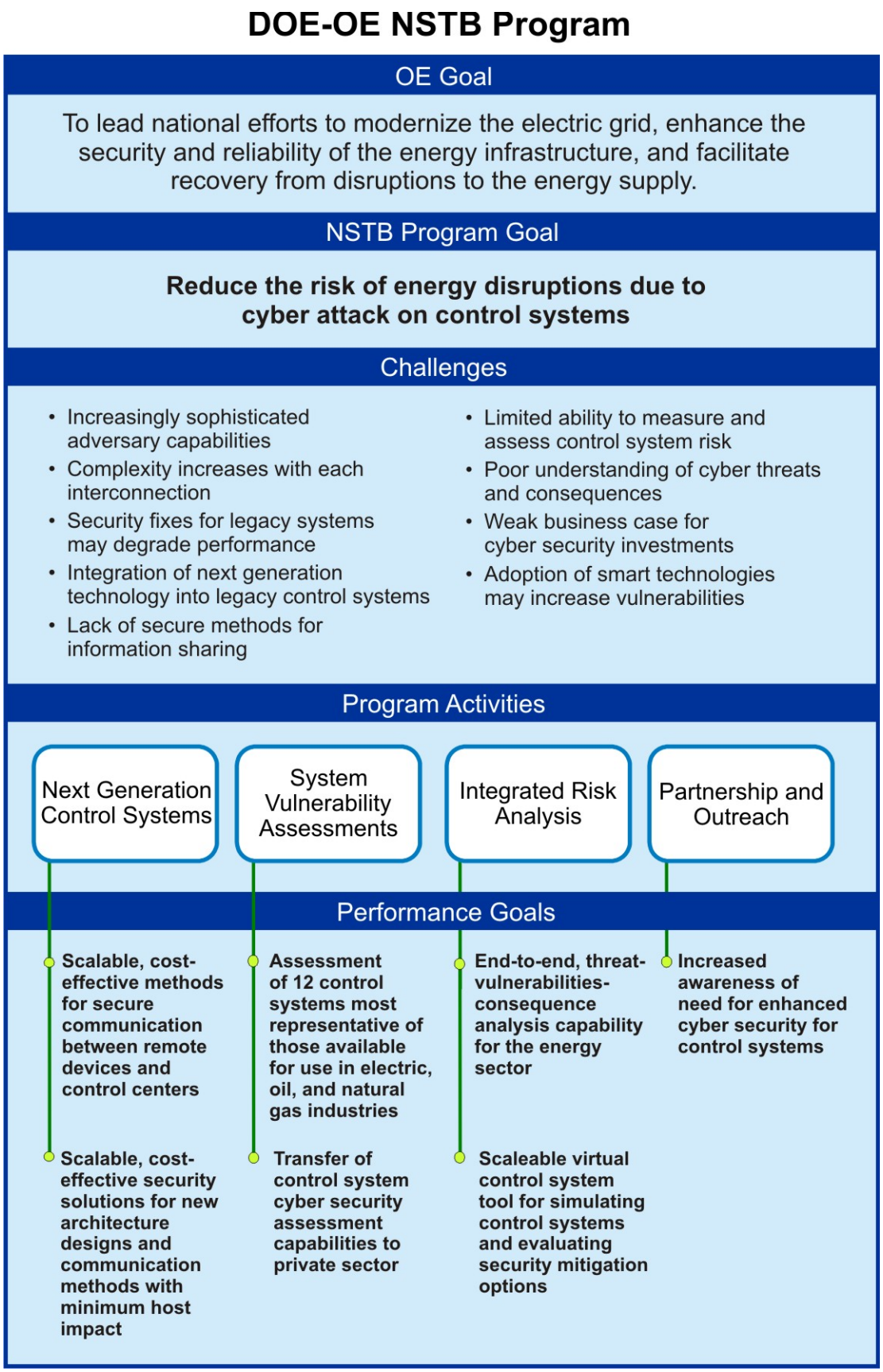
The National SCADA Test Bed (NSTB) Program is critical to achieving the mission and goals of OE. The NSTB Program was created with a clear understanding that improving the security of control systems is integral to protecting the energy infrastructure and the sectors it serves. Although many solutions will originate from the private sector, the transfer of these solutions involves national leadership, effective partnerships, and a shared vision of the future. Accordingly, the NSTB Program aligns its efforts with the industry roadmap, U.S. policy, OE goals, NSTB facilities and resources, the federal role, and related federal efforts. Exhibit 2.2 illustrates the planning space in which the NSTB Program operates.

Exhibit 2.2 DOE NSTB Planning Space



The NSTB Program goal is to reduce the risk of energy disruptions due to cyber attacks on energy control systems. To achieve this goal, the NSTB Program has organized its activities into the strategic framework shown in Exhibit 2.3. This risk-based approach will enable both the NSTB Program and the energy community it serves to rapidly and effectively develop, integrate, and sustain security improvements. The NSTB Program invests in R&D for next-generation control systems, vulnerability assessments, and risk analysis to improve cyber security both today and tomorrow.

Exhibit 2.3 Strategic Framework for NSTB Program



3. Technical Plan

NSTB Program activities focus on developing next-generation control systems technology, conducting systems vulnerability assessments, developing end-to-end risk modeling and simulation capability, and partnering with public and private energy sector stakeholders to raise security awareness and leverage resources. All NSTB Program efforts also align with key challenges and priorities identified by industry in the ***Roadmap to Secure Control Systems in the Energy Sector***. A strategic framework consisting of these four program activity areas, shown earlier in Exhibit 2.3 and described below, provides a sound foundation for collectively enhancing the security and reliability of the energy infrastructure by reducing the risk of energy disruptions due to cyber attack on control systems:

- **Next-Generation Control Systems.** Efforts to accelerate the deployment of hardened next-generation control systems with built-in security will concentrate on developing cross-cutting security solutions for new control systems components, novel architecture designs, and secure communication technologies. Next-generation R&D successes over the next five years will culminate in the demonstration of scaleable, cost-effective security solutions for new architecture designs employing secure communication methods between remote devices and control centers with minimum host impact.
- **Systems Vulnerability Assessments.** Assessments of supervisory control and data acquisition (SCADA)/energy management systems (EMS) vulnerabilities reveal exploitable cyber security gaps that could permit unauthorized access to, and subsequent manipulation of, critical data functions. Assessments of 12 control systems most representative of those available for use in the electric, oil, and natural gas industries during the next five years will facilitate the development of hardened next-generation control systems, encourage rapid deployment of security fixes in operational settings, and inform future systems design and coding. DOE assessment experts will team closely with systems developers and operators throughout to fully transfer control systems assessment capabilities to the private sector.
- **Integrated Risk Analysis.** Energy sector stakeholders require a thorough understanding of their existing cyber security posture to determine where control systems vulnerabilities exist and what actions may be required to address them. Accordingly, end-to-end, cyber threat-vulnerabilities-consequence analysis capability will be developed in five years time. Development of a scaleable virtual control systems tool will complement risk analysis by enabling simulation of control systems environments and evaluation of security mitigation options.
- **Partnership and Outreach.** Engaging the public and private energy sector stakeholders in program activities is critical to evaluate real-world applicability, increase security awareness, coordinate public-private sector roles, maximize program resources, and prioritize industry needs. Through active partnership with the control systems community—asset owners and operators, control systems developers, vendors, researchers, industry associations, government agencies, and others—the NSTB Program will increase awareness of energy sector control systems security. This will be achieved through outreach avenues such as: technical reports, publications, industry news, and additional information posted on the NSTB Program website; promotion of public-private participation in the online interactive energy Roadmap (ieRoadmap); instruction of cyber security awareness training sessions; participation in industry conferences and workshops; and membership in public-private energy sector control systems security and critical infrastructure working groups.

To be successful in meeting NSTB Program goals, specific milestones and deliverables must be accomplished in the FY 2008–2013 period. Projects, activities, and initiatives for each program activity area are discussed in Sections 3.1–3.4.

3.1 NEXT-GENERATION CONTROL SYSTEMS

As cyber threats to control systems continue to evolve, so must the energy sector's ability to protect and defend against them. Effectively securing energy control systems over the long term requires next-generation control systems technologies such as: intelligent, inherently secure, and dependable control system architectures, software, and hardware; advanced device-to-device authentication; comprehensive intrusion detection, event correlation, and response capability; and secure communication protocols. These solutions will reduce the risk of energy disruption by better securing communications between remote devices and control centers, and between enterprise and control networks. Security improvements must be compatible with legacy systems, address potential threats that have not yet surfaced, and accommodate the increasing number of nodes and access points utilized in modern energy systems.

3.1.1 Performance Goals

The Next-Generation Control Systems program activity supports research focused on achieving the following performance goals by FY 2013:

- **Scalable, cost-effective methods to secure communication between remote devices and control centers.** Activities focus on developing and accelerating the adoption of innovative solutions to protect and transfer data securely across electronic security perimeters, including those of legacy systems.
- **Scalable, cost-effective security solutions for new architecture designs and communication methods with minimum host impact.** Activities target accelerating the transfer of technologies that significantly raise situational cyber security awareness for energy control systems, including: the development of real time integrated intrusion detection, prevention, and event correlation capabilities; open, interoperable security architecture designs; protocol authentication devices; middleware for secure information sharing framework; security auditing and vulnerability scanning tools; and intelligent distributed power grid technology.

3.1.2 Technical Challenges & Needs

Poorly designed connections between control systems networks, remote devices, and business networks can introduce numerous cyber vulnerabilities. Every new connection point increases infrastructure complexity and can create a new attack vector. These cyber risks are intensified by the energy sector's growing use of commercial-off-the-shelf (COTS) technologies, standardized operating systems, and reliance on open-communication protocols in the operation of their control networks. The addition of new security technologies to address these cyber security issues, particularly to legacy systems, may degrade systems performance and slow response times during security events. Accordingly, industry has emphasized the need for security solutions, including the following:

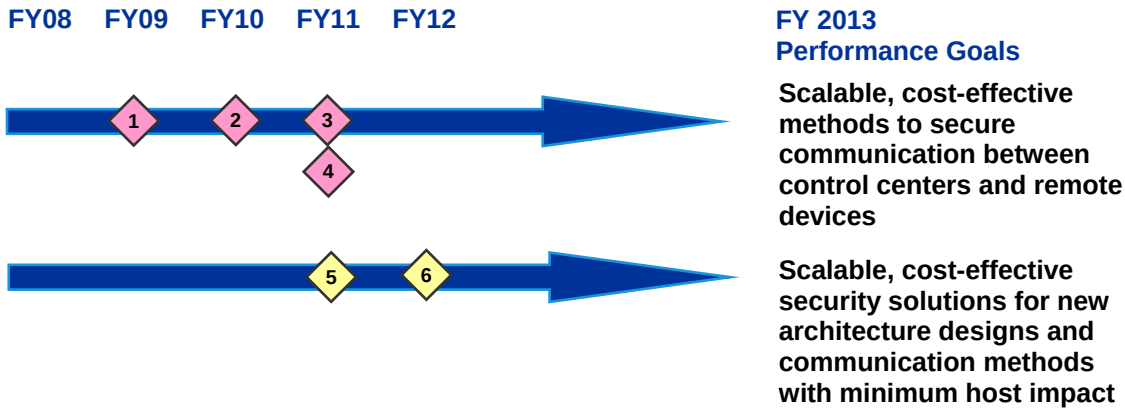
- Development of non-intrusive, cost-effective, and robust SCADA encryption devices
- Development of secure plug-and-play control systems components
- Development of cost-effective gateway security technologies that integrate firewalls, intrusion detection, and anti-virus protection with minimum host impact
- Development of intrusion detection and prevention technologies with automated reporting
- Development of security event management and forensic tools
- Development of automated security state and response support systems
- Improvement of system communication performance to enable the application of advanced security solutions without compromising system performance

3.1.3 Milestones

Progress toward the achievement of these performance goals will be measured by the milestones identified in Exhibit 3.1

Exhibit 3.1 Next Generation Control Systems Milestones and Performance Goals

.



Milestones

1. Field test serial protocol authenticator technology with industry vendors.
2. Transfer serial protocol authenticator technology to commercial vendor.
3. Field test interoperable control systems security architecture with industry partners.
4. Transfer interoperable control systems security architecture to commercial vendor.
5. Demonstrate capability for integrated intrusion detection, prevention, and event correlation designed specifically for control systems applications.
6. Transfer technology for integrated intrusion detection, prevention, and event correlation to commercial vendor.

3.1.4 Current Activities

Aligned with both program goals and Roadmap priorities, the following projects are being funded as part of the NSTB Program's FY07 efforts in this area (project partners listed in alphabetical order):

- Lemnos Interoperable Security Program

  (*Project Partners*: Sandia National Laboratories [SNL], Schweitzer Engineering Laboratories Inc. [SEL], Tennessee Valley Authority [TVA])

  A key goal of the Lemnos project is to accelerate the development and use of cost-effective, interoperable, IP-based secure communication methods between and among remote devices and control centers, and to increase the availability and accessibility of interoperable security solutions for energy sector control systems. The project team will determine key security functionality and interoperability specifications, and subsequently develop testing procedures for evaluating interoperable technologies against those criteria. An open-source reference design and a commercial prototype security gateway will be independently built and tested to these specifications in isolation, followed by tests to validate interoperability between the two devices. The Lemnos team will engage industry through a workshop demonstration of its completed interoperable security devices. Final functionality, interoperability, and performance requirements will be published and testing tools and methods will also be made available to industry.

This project will leverage ongoing development of the Open PCS Security Architecture for Interoperable Design (OPSAID) led by SNL. OPSAID's open architecture incorporates a series of modules to provide encryption, authentication, secure remote management, logging, intrusion detection, firewalls, and state-of-health monitoring capability. OPSAID is being designed for broad-application ranging and mainframe-based systems to more modern platforms, as well as yet-to-be installed systems that may benefit from ongoing but nascent automation security efforts.

- Secure SCADA Communications Protocol

  (*Project Partners*: Pacific Northwest National Laboratory [PNNL], SEL, Siemens)

  The SCADA communications protocol technology "wraps" original, serial SCADA communication traffic with a unique identifier and an authenticator. A remote device receiving the message then uses the unique identifier in the wrapper to ensure the communication is valid, allowing it to detect and prevent various attack scenarios—including man-in-the-middle, injected traffic, or message replay. The protocol authenticator has achieved system prototype demonstration in an operational environment. The ultimate goal is to prove the technology will work in its final form and under expected conditions, upon which the technology will be transferred to an industry vendor for commercialization.

- Hallmark Project

  (*Project Partners*: CenterPoint Energy Inc., PNNL, SEL)

  The Hallmark Project will develop the Secure SCADA Communications Protocol into a commercialized form that any vendor or energy sector asset owner can easily integrate with legacy, existing, and future control systems equipment in a manner that does not adversely impact reliable control systems operation. The technology will be made available in three formats: a software solution that runs on an industrial PC, a software solution that runs on a proof-of-concept micro-controller platform, and an embedded solution that resides between the I/O server and its communication ports. The Hallmark Project will provide end-users with a cost-effective, low-maintenance method to improve the reliability, security, and robustness of their control systems.

- Cyber Security Evaluation of GridStat Technology

  (*Project Partners*: Avista Utilities, Idaho National Laboratory [INL], PNNL, Washington State University [WSU])

  GridStat is an information sharing framework that facilitates communication between SCADA devices and adds additional capabilities to improve the Quality of Service (QoS) of inter-device communications. It belongs in a class of software called "middleware," which functions between the operating systems and application software. GridStat's increased communication speed and flexibility could support improved situational awareness for systems operators in the power transmission and generation network. A regional demonstration of GridStat will be conducted to analyze its potential cyber security advantages relative to traditional communication means. This project also seeks to establish a technology transfer path for eventual adoption of GridStat by the electric power industry. Other industry sectors that require wide area control may also benefit from the approaches demonstrated through this project.

- Detection and Analysis of Threats to the Energy Sector (DATES)

  (*Project Partners*: ArcSight, Invensys Process Systems, SNL, SRI International)

  The DATES project is a groundbreaking effort to develop capabilities for the energy sector including integrated intrusion detection, security incident event monitoring, and large-scale threat analysis. Advances in existing intrusion detection systems (IDS) technologies at the device, network, and host level will be developed and paired with complementary detection techniques to

achieve wide-ranging coverage. DATES will incorporate newly developed security incident management techniques to correlate IDS alerts with control systems events, in turn providing owners and operators with an accurate, high-level view of their security posture. DATES will also feature a new sector-wide threat analytics tool, implemented in a manner to protect privacy and preserve anonymity, that will collect security incidents submitted by energy owners and operators. This security information repository will enable users to query databases and analyze security events, thus facilitating correlation of security event data to better identify and anticipate emerging threats, assess relative security posture, and improve security event management.

- Cyber Security Audit and Attack Detection Toolkit

  (*Project Partners*: Constellation Energy, Digital Bond Inc., PacifiCorp, TVA)

  The Toolkit will extend popular vulnerability scanning and audit tools to test the configuration of 20 popular energy sector SCADA systems, distributed control systems (DCS), and energy management systems (EMS) in a safe and efficient manner. This capability will be used to determine if these control systems are configured securely and to expose existing security vulnerabilities. Security events from existing servers and data historians deployed in the electric, oil, and gas sectors will also be aggregated to pinpoint attack attempts on energy control systems. The results from these two exercises will be correlated to identify control systems meta events which will then be programmed into an enterprise security event management (SEM) device. Once tested and validated, a release package of software and documentation will be developed and made available to all project participants at no cost and to the energy control systems community on Digital Bond's website as subscriber content.

- Protecting Intelligent Distributed Power Grids Against Cyber Attacks

  (*Project Partners*: INL, Rutgers University, Siemens)

  This project will focus on the design and development of distributed technology to ensure security and survivability of intelligent power grid systems against cyber attacks. The technology will consist of three components: (1) a risk-based critical asset identification system that provides probabilistic risk measures on the various intelligent grid infrastructure assets, (2) an integrated and distributed security layer spanning across the intelligent power grid network in a hierarchical manner, and (3) an optimization technique to establish the best topology for networking the security components according to security metrics and economical measures defined as part of the task. Upon completion of the project, software and firmware prototypes will be available and general guidelines will be established for future product development and commercialization.

- Trustworthy Cyber Infrastructure for the Power Grid (TCIP)

  (*Project Partners*: Cornell University, Dartmouth College, DHS, DOE, National Science Foundation [NSF], University of Illinois–Urbana-Champaign, WSU)

  TCIP, initiated by the NSF Cyber Trust Center, is a long-term effort to protect the nation's power grid by providing the fundamental science and technology needed to create an intelligent, adaptive power grid that can survive cyber attacks from malicious adversaries, provide continuous delivery of power, and support dynamically varying trust requirements. The center will significantly improve the way the power grid's cyber infrastructure is built, making it more secure, reliable, and safe.

3.2 System Vulnerability Assessments

Through successive system vulnerability assessments, energy sector partners will expand their understanding of potential control systems weaknesses and the most effective security practices to mitigate them. Assessments will examine system architecture design and configuration, communication paths and protocols, and control systems hardware. Participants will leverage this knowledge to resolve existing vulnerabilities, develop self-assessment capabilities, and inform the design and operation of more secure, more resilient, next-generation control systems.

3.2.1 Performance Goals

System Vulnerability Assessment program activities target accomplishing the following performance goals by FY 2013:

- **Assessment of 12 control systems most representative of those available for use in the electric, oil, and natural gas industries.** Activities include partnering with industry to conduct three systems vulnerability assessments each year. Each assessment will rigorously examine a range of potential vulnerabilities that might be exploited in an energy sector cyber attack. Assessments will be conducted at National SCADA Test Bed (NSTB) facilities and on-site at field installations. Once completed, confidential assessment reports are provided to participating vendors. Vendors use this information to prepare and deliver patches and upgraded or hardened systems to their users. Vendors also leverage this information to inform more secure designs in future systems.
- **Transfer of control systems cyber security assessment capabilities to private sector.** Activities include the gradual movement of system vulnerability assessment activities to the private sector. Industry assessment participants will be familiarized with proven assessment techniques and given access, on a cost-recovered basis, to the unique assessment resources in place at NSTB facilities.

3.2.2 Technical Challenges & Needs

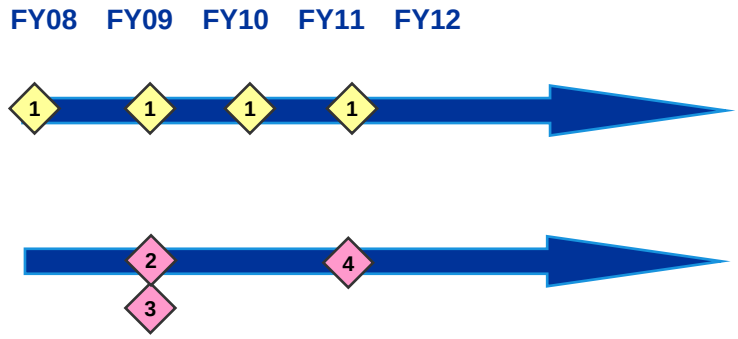
A lack of industry methods and resources to effectively test for and identify cyber vulnerabilities is a significant dilemma facing the energy sector. No standards exist to assess cyber vulnerabilities, and standardized test plans and upgrades for new technology are not widely available. Increasing connectivity between business networks and control system networks can also introduce new vulnerabilities outside the scope of what vendors and operators can influence. Rapid discovery of control systems vulnerabilities and subsequent deployment of associated security fixes are vital to securing energy sector control systems. This knowledge also provides vendors with specific security requirements for future systems or those currently in development. To address these challenges, energy sector stakeholders have identified the following priorities:

- Development of vulnerability assessment methodologies
- Identification of best practices for mitigating control systems vulnerabilities (inclusive of substations)
- Development of patching technologies that do not impact operating systems
- Maintaining the NSTB to work with vendors and asset owners to test equipment, architectures, and processes for cyber security vulnerabilities

3.2.3 Milestones

Progress toward the achievement of these performance goals will be measured by the milestones identified in Exhibit 3.2.

Exhibit 3.2 System Vulnerability Assessments: Milestones and Performance Goals



FY 2013 Performance Goals

Assessment of 12 control systems most representative of those available for use in electric, oil, and natural gas industries

Transfer of control systems cyber security assessment capabilities to private sector

Milestones

1. Assess 3 control systems most representative of those available for use in electric, oil, and natural gas industries (including electric substations).
2. Initiate transfer of systems vulnerability assessment capability to private sector.
3. Support industry to lead two systems vulnerability assessments with NSTB resources.
4. Make portion of National SCADA Test Bed resources available (cost recovered) to researchers, vendors, and users.

3.2.4 Current Activities

Aligned with both program goals and Roadmap priorities, the following project is being funded as part of the NSTB Program's FY07 efforts in this area (project partners listed alphabetically):

- System Vulnerability Test Bed and On-Site Assessments

  (*Project Partners*: ABB, American Gas Association [AGA], American Petroleum Institute [API], American Transmission Company, AREVA, Argonne National Laboratory [ANL], Detroit Edison, General Electric [GE], INL, Interstate Natural Gas Association of America [INGAA], Open Systems International [OSI], PacifiCorp, Siemens, SNL, Telvent)

  A critical need to understand specific cyber vulnerabilities and corresponding mitigation strategies is being addressed by system vulnerability assessments conducted at the NSTB facilities and on-site at field installations of control systems. The systems assessed are typically new products on the market most representative of those used by the electric, oil, and natural gas industries, since these are the products for which vendors can best justify business expenditures for enhanced security.

  Test bed assessments include the key equipment and characteristics of an actual installation and use typical data flow and component response. Subsequent on-site assessments help to determine whether vulnerabilities identified in a laboratory setting are relevant in actual installations. Control systems vendors and operators collaborate with NSTB staff throughout the assessments. Over time, NSTB seeks to transfer its control systems assessment expertise to the private sector and provide cost-recovered user facilities to enable vendors, owners, and operators to lead assessments.

  Upon completion, assessment results are documented and provided to the system developers. Findings from each assessment are also added to an annually updated "Lessons Learned" document that compiles findings across system types. Control system developers can use this information to harden their next-generation systems and to develop patches applicable to legacy systems. Through presentations at vendor user group meetings and selective sharing of assessment reports, results and mitigation strategies are also provided to vendor customers.

3.3 INTEGRATED RISK ANALYSIS

As defined for the NSTB Program, integrated risk analysis is the process through which the three components of energy control system risk—threat, vulnerability, and consequence—will be collectively analyzed to determine the energy sector's cyber security posture. An accurate risk assessment of critical cyber assets enables energy sector stakeholders to prioritize security needs and focus limited resources on the most pressing security issues. Risk assessment data are also necessary to build a sound business case for investment in creating, procuring, and implementing control systems cyber security measures. Conducting these assessments for energy systems requires an integrated set of analysis and modeling tools that are currently limited in scope and scale.

3.3.1 Performance Goals

Integrated Risk Analysis program activities are directed at achieving the following performance goals by FY 2013:

- **End-to-end, threat-vulnerabilities-consequence analysis capability for the energy sector.** Research focuses on identifying and demonstrating integrated cyber threat scenarios for small-, moderate-, and large-scale systems. These scenarios must include end-to-end capabilities (i.e. systems approach) to improve the characterization of risk and determine the most appropriate action for mitigating that risk.
- **Scalable virtual control systems tool for simulating control systems and evaluating security mitigation options.** Research efforts include developing a cost-effective and practical tool for predicting the robustness of a system's security posture and the impact of implementing security measures on systems operation without introducing unacceptable risk to an online system in operation.

3.3.2 Technical Challenges & Needs

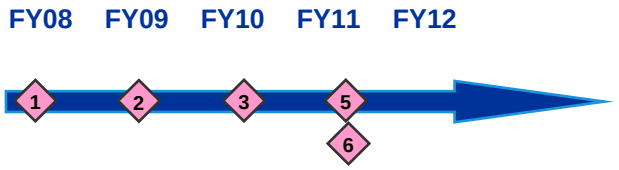
Cyber risk factors for control systems are not widely understood. Threat, vulnerability, and consequence analysis will be critical to establish a baseline risk profile from which progress can be measured, defensible business cases for cyber security investment can be made, and appropriate security action can be taken. Risk remains difficult to quantify and demonstrate due to a lack of sufficient tools to measure risk. Risk simulation and modeling tools would assist in evaluating real-world energy sector cyber attack scenarios to determine potential consequences and cascading effects on other sectors. Such tools could also help determine the effectiveness of new security technologies at mitigating those effects. To address these challenges, participants recommended implementing the following initiatives:

- Creation of a risk matrix that balances threat, vulnerability, and consequence for realistic attack scenarios
- Development of risk assessment tools including frameworks for prioritizing control measures and cost justification tools
- Development of cyber attack and response simulators
- Establishment of a baseline security posture for energy sector control systems
- Development of a security test harness with built-in testing architectures and guidelines

3.3.3 Milestones

Progress toward achieving these performance goals will be measured by the milestones identified in Exhibit 3.3.

Exhibit 3.3 Integrated Risk Analysis Milestones and Performance Goals



FY 2013 Performance Goals

End-to-end, threat-vulnerabilities-consequence analysis capability for the energy sector

Scalable virtual control systems environment tool for simulating control systems and evaluating security mitigation options

Milestones

1. Identify plausible control systems cyber threat scenarios for energy sector.
2. Demonstrate the end-to-end risk analysis capability in a small scale scenario.
3. Demonstrate the end-to-end risk analysis capability in a moderate scale scenario.
4. Demonstrate the initial operating capability of the security evaluation tool - virtual control systems environment (VCSE).
5. Demonstrate the end-to-end risk analysis capability in a large scale scenario.
6. Offer a fully integrated end-to-end risk analysis capability to the energy sector stakeholders.
7. Offer the use of a fully capable VCSE tool to the energy sector stakeholders.

3.3.4 Current Activities

Aligned with both program goals and Roadmap priorities, the following projects are being funded as part of the NSTB Program's FY07 efforts in this area (partners listed in alphabetical order):

- Plausible Threat Characterization

  (*Project Partners*: Detroit Edison, Georgia Systems Operations Corporation, SNL)

  Models to characterize cyber threats and plausible attack scenarios specific to energy sector control systems will be developed to provide control system owners and operators with more concrete information concerning the cyber attack abilities of adversaries and the likelihood that the adversary is capable and willing to attack energy sector resources. A greater understanding of the potential attackers and their intent will enable utility owners and operators and other key stakeholders to better design, develop, and deploy appropriate defenses against sophisticated cyber threats. Efforts will also include exploring the extent to which the threat discovery process previously developed for counter-proliferation (CP) applications can be adapted for use in the energy infrastructure protection domain.

- Consequence Modeling

  (*Project Partners*: PNM, SNL)

  Consequence models will be developed to measure both physical and market consequences resulting from successful cyber attacks on energy sector control systems. Power system simulators will be used to link predicted physical infrastructure end-states with specific types of

cyber attack. For each attack scenario, the consequence data will be used to estimate the overall physical health (resiliency) of the affected infrastructure and how quickly damaged elements can recover from the attack. Additional analysis will determine how cyber attacks can cause power markets to deviate from normal operation and to what extent market influences drive physical infrastructures to a "crippled" state. Findings will be analyzed to identify the most critical energy infrastructure assets which, if compromised by a cyber attack, could lead to the most severe consequences and cascading effects.

- Impact Analysis of Cyber Attacks on Control Systems

  (*Project Partners*: SNL, TBD industry partners)

  Impact modeling and simulation activities will build on previous critical outage evaluation efforts by analyzing malevolent threat capabilities and rigorously evaluating myriad possibilities concerning potential faults in electric power grid elements due to cyber attacks. Outage evaluation capabilities will be improved through dynamic simulations of electrical grids to better identify effects of perturbations involving multiple faulted grid elements. The project will support the development of an improved capability to evaluate the range of potential impacts to the U.S. electrical infrastructure due to cyber attack.

- Virtual Control System Environment (VCSE)

  (*Project Partners*: SNL, TBD industry partners)

  The Virtual Control System Environment (VCSE) tool will simulate control system devices and network communications to enable real-time, hardware-in-the-loop (HITL) emulation. VCSE will incorporate data from threat, consequence, and impact modeling activities to support the design, integration, and evaluation of security solutions. The tool focuses on (a) the rapid development of new models for the control systems element; (b) easy federation of existing simulation, visualization, and analytic tools; and (c) evaluation of cyber security postures in large infrastructures. VCSE will help asset owners select appropriate security solutions for their control systems and effectively manage the technological complexities associated with simultaneously securing both legacy and emerging system components and architectures.

- Control Systems Risk Analysis Workshop

  (*Project Partners*: SNL, TBD industry partners)

  The NSTB Program will sponsor an end-of-year workshop to increase energy sector awareness of its cyber risk analysis and reduction products. An attack scenario co-developed by the NSTB Program and industry partners will be used to showcase numerous program tools and capabilities including: threat characterization, impact analysis, consequence modeling, VCSE, open control system security architecture designs, and other NSTB resources. The workshop will also facilitate discussion between asset owners, vendors, government agencies, national laboratories, and policy makers in the oil, gas, and electric sectors. Providing this conduit between stakeholders and the NSTB Program will help ensure relevance and applicability of program activities to critical cyber security needs.

3.4 PARTNERSHIP & OUTREACH

Forming partnerships with national laboratories, vendors, and asset owners and operators is essential to securing the energy infrastructure. Combining the expertise and perspectives of all facets of the sector ensures that security needs are being met and anticipated from every angle. Additionally, information and cost sharing minimizes the duplication of technology development efforts and maximizes resources to efficiently achieve effective solutions.

Outreach and educational activities are equally important, as they keep industry groups across the nation informed and up-to-date regarding effective strategies and technologies to enhance infrastructure security. Journal articles, published reports, internet presence, recommended security practices, and training courses increase industry members' awareness of security risks to their own systems. Engaging these groups through outreach encourages them to quickly implement new security measures and provide input from the field to help guide future technology development.

3.4.1 Performance Goals

Continuously working to expand the energy sector's knowledge, methodologies, and technologies for protecting control systems in today's evolving threat environment, Partnership & Outreach program activities focus on achieving the following performance goal:

- **Increased awareness of need for enhanced cyber security for control systems**. Combines NSTB Program investments with the resources and expertise of the national laboratories, industry organizations, and other public and private sector partners to perform information sharing and technology transfer activities, such as conducting workshops and training sessions, developing and implementing security guidelines, and creating and distributing awareness materials.

3.4.2 Technical Challenges & Needs

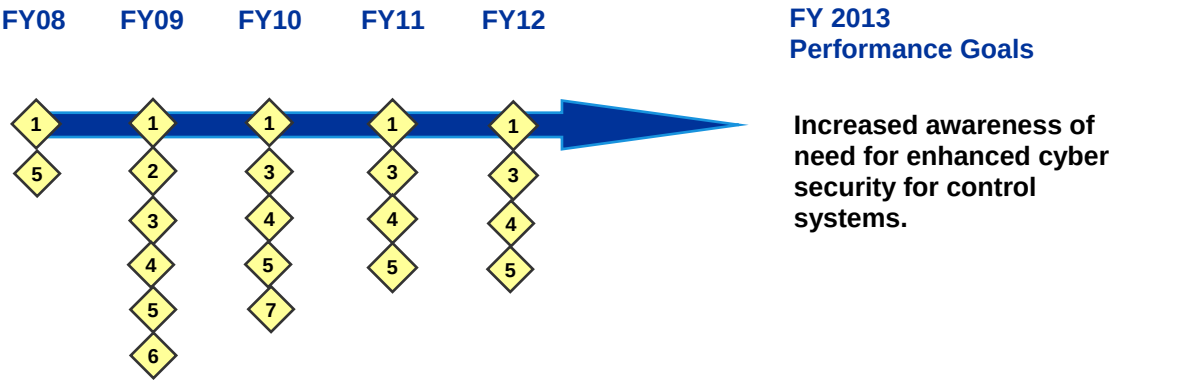
A lack of cyber security awareness and information sharing across the industry limits the sector's ability to initiate and sustain security improvements. Insufficient knowledge, understanding, and appreciation of control systems security make justifying investment in cyber security a difficult business case for asset owners and operators. To date, effective security-oriented partnerships have been difficult to establish, and poor coordination and insufficient information sharing among stakeholders has created confusion. To effectively address these concerns with the limited resources available for funding cyber security initiatives, workshop participants identified pursuing the following activities as a sector priority:

- Development of standards and/or regulations for secure data exchange and communication
- Creation of a secure forum for sharing cyber threat and response information throughout the energy sector
- Analysis of incentives and benefits of implementing cyber security solutions to develop a compelling, evidence-based business case for investment in control systems security
- Make available and disseminate field-proven best practices for control systems security
- Publication of consistent cyber security training materials for energy sector control systems
- Development and implementation of security and awareness training
- Launch of an industry-driven awareness campaign

3.4.3 Milestones

Progress toward achieving these performance goals will be measured by the milestones identified in Exhibit 3.4.

Exhibit 3.4 Partnership and Outreach Milestones and Performance Goals



Milestones

1. Work with North American Electric Reliability Corporation (NERC) to develop recommended mitigations for annual "Top Ten Vulnerabilities of Control Systems and Their Associated Mitigations" report.
2. Establish Critical Infrastructure Partnership Advisory Council (CIPAC) Energy Sector Control Systems Working Group.
3. Conduct three NSTB SCADA security awareness sessions.
4. Update "Lessons Learned" report on common control systems vulnerabilities and associated mitigation techniques.
5. Conduct an annual workshop to engage energy sector stakeholders and demonstrate NSTB capabilities.
6. Implement marketing strategy for interactive *Roadmap to Secure Control Systems in the Energy Sector* (ieRoadmap) tool.
7. Work with ISA to develop guidelines for the secure use of wireless technologies in the energy sector.

3.4.4 Current Activities

Aligned with both program goals and Roadmap priorities, the following projects are being funded as part of the NSTB Program's FY07 efforts in this area:

- Industry Outreach & Awareness

  Outreach and awareness is essential to establishing and reinforcing strong working relationships with all organizations involved in control systems security. Activities support two-way communication and partnership with energy sector stakeholders participating in the national effort to improve security in energy infrastructure control systems. Program efforts will include: (1) preparing journal articles, technical reports, project fact sheets, press releases, and other materials to share information gained through program activities and successes and to enhance visibility of the program with the intent of increasing awareness of security issues and solutions; (2) responding to industry inquiries and developing collaborative opportunities; (3) supporting industry efforts in enhancing awareness of security best practices, technology developments, and mitigation approaches to common vulnerabilities; (4) participating in control systems vendor user group, standards, and industry association meetings and workshops to share information gained via vulnerability assessments and technical analyses and to engage industry for input on security-related interests and needs, and (5) maintaining a program website to host technical reports, publications, industry news, and additional information on current program activities and resources.

  Current DOE energy sector cyber security colleagues include: NERC Critical Infrastructure Protection Committee (CIPC) and Control Systems Security Working Group (CSSWG), American Petroleum Institute (API), Instrumentation Systems & Automation Society (ISA), Process Control Systems Forum (PCSF), Institute for Information Infrastructure Protection (I3P), Department of

Homeland Security (DHS), National Institute of Standards & Technology (NIST), Electric Power Research Institute (EPRI), Federal Energy Regulatory Commission (FERC), National Science Foundation (NSF), American Gas Association (AGA), Interstate Natural Gas Association of America (INGAA), International Electricity Infrastructure Assurance Forum (IEIAF), and others.

- Control Systems Security Training

  Training leverages unique lessons learned generated over time at NSTB via completion of multiple system vulnerability assessments. Sessions are conducted primarily for control system vendors and their user groups in direct association with those assessments to help improve their understanding of potential vulnerabilities in specific systems and to inform them of good practices that can help address those vulnerabilities. Currently a series of two workshops, "Introduction to SCADA Security for Managers and Operators" and "Intermediate SCADA Security," are conducted by the program. To date, more than 1,200 energy sector stakeholders have participated in these training sessions. Instruction of SCADA security workshops will continue following each assessment in an effort to foster increased cyber security awareness and to educate energy sector control system operators and asset owners on best practices for sustainable control systems security.

- Critical Infrastructure Protection Advisory Committee (CIPAC) Energy Sector Control Systems Working Group (ESCSWG)

  (*Working Group Members*: DOE, DHS, industry participants TBD)

  The ***Roadmap to Secure Control Systems in the Energy Sector*** is the result of an unprecedented collaboration between the energy sector and government to identify concrete steps to secure control systems in the electricity, oil, and natural gas infrastructures over the next ten years. The Roadmap presents a vision and framework of goals and milestones for protecting all control systems from intentional cyber assault within the next ten years and organizes them into four key strategies: (1) measure and assess security posture, (2) develop and integrate protective measures, (3) detect intrusion and implement response strategies, and (4) sustain security improvements. The proposed Energy Sector Control Systems Working Group (ESCSWG) will provide advice, guidance, and recommendations to help implement the Roadmap**.**

  The efforts of the ESCSWG are designed to foster private and public collaboration to improve control systems security in the energy sector. The ESCSWG will have these key functions:

  - Provide advice and guidance for Roadmap implementation
  - Identify critical gaps and overlaps in research, training, practices, etc.
  - Ensure roadmap milestones and priorities are accurate and relevant
  - Help measure progress toward Roadmap goals and milestones
  - Harmonize Roadmap with other industry initiatives; revise as required
  - Help identify and map existing projects and activities using the online interactive energy Roadmap tool (ieRoadmap)
  - Recommend and/or help launch specific projects or activities
  - Increase awareness of control systems security issues within the energy sector
  - Help establish the business case for investment in cyber security

  The ESCSWG will consist of senior representatives from the electric, oil, gas, and government sectors, as designated by the Electric and Oil & Natural Gas Sector Coordinating Councils and the Government Coordinating Council for Energy. In addition, members may be invited as appropriate from other sector councils, such as Communications and Information Technology SCCs.

- Interactive *Roadmap to Secure Control Systems in the Energy Sector* (ieRoadmap)

  The ieRoadmap is an innovative, web-based tool designed to accelerate collaboration in securing control systems in the energy sector and currently delivers the most comprehensive list to date of projects throughout the energy control systems community. The tool organizes ongoing projects across the public and private sectors according to the key challenges within each of four goals defined in the ***Roadmap to Secure Control Systems in the Energy Sector***. By matching current activities to priority needs, this tool will enable the energy sector to measure its progress in meeting its defined Roadmap goals and milestones. The tool also facilitates identifying both gaps in coverage and opportunities for leveraging resources through partnership. To date, public and private sector organizations have posted more than 70 ongoing projects in ieRoadmap and aligned them with Roadmap challenges and strategies. Outreach efforts will continue to increase industry awareness and use of the tool.

  The DOE NSTB Program has partnered with the Process Control Systems Forum (PCSF) to host this user-friendly tool at www.pcsforum.org/roadmap.

- Recommended mitigations for NERC "Top 10" list

  Annually, NERC's Control Systems Security Working Group (CSSWG) publishes the "**Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations**." The NSTB develops the foundational, intermediate, and advanced mitigations for each identified "Top 10" vulnerability. NERC CSSWG and NSTB will continue this partnership to provide industry with best practices to help reduce potential risks to energy control systems.

Appendix A – National SCADA Test Bed Resources

National SCADA Test Bed

The DOE Office of Electricity Delivery and Energy Reliability (OE) established the National SCADA Test Bed (NSTB) as a national resource to help the energy sector and equipment vendors assess control system vulnerabilities and test the security of control system hardware and software. To support the development of a more secure and reliable energy infrastructure, the test bed offers a full-scale infrastructure suite of facilities for testing and validating control systems. Funded by the NSTB Program and jointly run by Idaho National Laboratory (INL) and Sandia National Laboratories (SNL), the NSTB offers the integrated expertise and resources of multiple national laboratories, including Argonne National Laboratory (oil and gas infrastructure), Pacific Northwest National Laboratory (electricity infrastructure), and Oak Ridge National Laboratory.

By 2010, the NSTB Program plans to designate new cost-recovered NSTB user facilities for use by energy sector control system vendors and asset owners and operators to conduct system vulnerability assessments.

Benefits

Working in partnership with the energy sector, the NSTB Program leverages NSTB resources to:

- Identify and mitigate existing vulnerabilities
- Facilitate development of security standards
- Serve as an independent facility to test SCADA equipment and control systems
- Identify and promote best cyber security practices
- Increase awareness of control systems security within the energy sector
- Accelerate development of more secure and robust advanced control systems architectures and technologies

Facilities and Capabilities

The NSTB comprises a national network of assets and capabilities, including:

- Critical Infrastructure Test Range
- Center for SCADA Security
- Supervisory Control and Data Acquisition/Energy Management Systems (SCADA/EMS) Test Bed
- Next-Generation Wireless Test Bed (3G/4G testing; local area network and 802.11 testing)
- Power Grid Test Bed (61 miles of 138 kV transmission loop; 7 substations)
- Cyber Security Test Bed (vulnerability assessments; intrusion detection expertise)
- Control systems security training courses (best practice course; assessment course)
- Virtual Control System Environment (VSCE)
- Control Center Laboratory

- Remote Substation Laboratory
- Attack Resource Center
- Center for Cyber Defenders
- Network Research Laboratory
- Cryptography Laboratory
- Electric Power Test Laboratories
- Red Teaming Laboratory
- Extreme Measurement Communications Center (wireless technology modeling, simulation, and characterization support)
- Secure virtual private network (VPN) connections between partner national laboratory facilities and other external sites

Publications

Selected Technical Reports

- 21 Steps to Improve Cyber Security of SCADA Networks (September 2002)
- ABB SCADA/EMS INEEL Baseline Summary Test Report (November 2004)
- Project Completion Report - Critical Infrastructure Test Range Program At INL (March 2005)
- Recommendations for Secure ICCP Version 1.0 (March 2005)
- Cyber Assessment Methods for SCADA Security (June 2005)
- Reference Model for Control and Automation Systems in Electric Power Report v1.2 (October 2005)
- Network Security Infrastructure Testing Report v1.2 (October 2005)
- A Summary of Control Systems Security Standards Activities in the Energy Sector (October 2005)
- Mitigation strategies for “NERC Top 10 Vulnerabilities and Their Associated Mitigations” (March 2006)
- AGA 12, Part 2 Cryptographic Security Analysis (May 2006)
- SCADA Cryptographic Security Test Plan: General Guidance (May 2006)
- Secure ICCP Configuration and Performance Test Plan (June 2006)
- The Automation Systems Reference Model: An Introduction to Its Uses (July 2006)
- National SCADA Test Bed: FY05 Virtual Control System Environment Progress Report (July 2006)
- Using Host-Based Anti-Virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts v1.0 (September 2006)
- Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems (September 2006)
- AGA 12, Part 2 Performance Test Plan (November 2006)
- Summary of Ongoing Metrics Projects (April 2007)
- Secure ICCP Integration Considerations and Recommendations (June 2007)

- Descriptive Model of a Generic WAMS (June 2007)
- Securing Wide Area Measurement Systems (July 2007)
- Security Framework for Control System Data Classification (July 2007)
- AGA 12, Part 2 Performance Test Results (August 2007)
- Secure SCADA Communication Protocol Performance Test Results (August 2007)
- Impacts of IPv6 on Infrastructure Control Systems (September 2007)
- Categorizing Threat: Building and Defining a Generic Threat Matrix (September 2007)
- Threat Analysis Framework (September 2007)

Energy Control Systems Roadmap Publications & Products

- Roadmap to Secure Control Systems in the Energy Sector: Workshop Summary Results (August 2005)
- Roadmap to Secure Control Systems in the Energy Sector (January 2006)
- Executive Summary: Roadmap to Secure Control Systems in the Energy Sector (January 2006)
- Interactive Roadmap to Secure Control Systems in the Energy Sector (ieRoadmap) Web-based Tool (March 2007)
- 75 projects have been posted by 13 organizations in the ieRoadmap online tool.

Industry Journal Articles

- "SCADA Gets Tough" in February 2007 *Pipeline & Gas Journal* (February 2007)
- "Partnering for Cyber Security at DOE's National SCADA Test Bed" in March 2007 *Transmission & Distribution World* (March 2007)

Appendix B – References

Bush, President George W. 2003. *Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection*. Office of the Press Secretary. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

Energetics Incorporated. 2006. *Roadmap to Secure Control Systems in the Energy Sector*. Prepared for the U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. http://www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf

GAO. 2004. Government Accountability Office. Critical infrastructure protection: *Challenges and efforts to secure control systems* (GAO-04-354). Washington, DC. www.gao.gov/new.items/d04354.pdf

U.S. Department of Energy. 2006. *U.S. Department of Energy Strategic Plan*. http://www.energy.gov/media/2006_DOE_Strategic_Plan.pdf

U.S. Department of Energy. 2006. *National SCADA Test Bed Fact Sheet*. http://www.oe.energy.gov/DocumentsandMedia/NSTB_Fact_Sheet_09-27-06-1.pdf

U.S. Department of Energy. 2007. *Five-Year Program Plan for Fiscal Years 2008 to 2013 for Electric Transmission and Distribution Programs.* Prepared for the U.S. Congress Pursuant to Section 925 of the Energy Policy Act of 2005. http://www.oe.energy.gov/DocumentsandMedia/Section_925_Final.pdf

U.S. Department of Homeland Security. 2006. *National Infrastructure Protection Plan*. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

White House. 2003. *The National Strategy to Secure Cyberspace*. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Appendix C – For More Information

DOE Contact:

Hank Kenchington
Program Manager, NSTB Program
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
1000 Independence Ave., SW
Washington, DC 20585
202-586-1878
henry.kenchington@hq.doe.gov

National Laboratory Contacts:

Jeff Dagle
Pacific Northwest National Laboratory
jeff.dagle@pnl.gov
509-375-3629

Wayne Manges
Oak Ridge National Laboratory
mangesww@ornl.gov
865-574-8529

Shabbir Shamsuddin
Argonne National Laboratory
shamsuddin@anl.gov
630-252-6273

Dave Kuipers
Idaho National Laboratory
david.kuipers@inl.gov
208-526-4038

Bob Pollock
Sandia National Laboratories
rdpollo@sandia.gov
505-844-4442

Useful Links:

- DOE NSTB Program (www.oe.energy.gov/controlsecurity.htm)
- Roadmap to Secure Control Systems in the Energy Sector (www.controlsystemsroadmap.net)
- Interactive Control Systems Roadmap (ieRoadmap) (www.pcsforum.org/roadmap)
- Argonne National Laboratory (www.iac.anl.gov)
- Idaho National Laboratory (www.inl.gov/scada)
- Oak Ridge National Laboratory (http://www.ioc.ornl.gov/welcome.shtml)
- Pacific Northwest National Laboratory (homeland-security.pnl.gov/cip.stm)
- Sandia National Laboratories (www.sandia.gov/scada)
- DHS National Cyber Security Division (http://www.dhs.gov/xabout/structure/editorial_0839.shtm)
- Process Control Systems Forum (www.pcsforum.org)
- U.S. Computer Emergency Readiness Team (U.S.-CERT) (www.us-cert.gov)