Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council,
Oil and Natural Gas Sector Coordinating Council, and
Government Coordinating Council for Energy

Acknowledgements

The Energy Sector Control Systems Working Group (ESCSWG) developed this roadmap in support of the Electricity Sub-sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and the Government Coordinating Council for Energy under the Critical Infrastructure Partnership Advisory Council (CIPAC) Framework; the roadmap has been approved for release by these councils. The ESCSWG members volunteered their time and expertise to this effort and would like to thank the other participants for their valuable perspectives and contributions to this important effort. Special thanks go to the U.S. Department of Energy, which provided the funds and support needed to convene participants and facilitate the discussions necessary to deliver a robust roadmap. Katie Jereza, Melanie Seader, and the Energetics Incorporated team facilitated and prepared the document. Donald Satterlee, California Independent System Operator, provided the Folsom control room photo on the cover.[1]

Message from the Energy Sector Control Systems Working Group

This *Roadmap to Achieve Energy Delivery Systems Cybersecurity* provides a plan to improve the cybersecurity of the energy sector. The strategic framework within presents the vision of industry, vendors, academia, and government stakeholders for energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next decade. It marks a continued effort by public and private stakeholders to identify steps to build, deploy, and manage resilient energy delivery systems for the electric, oil, and natural gas industries.

The roadmap is an update of the 2006 *Roadmap to Secure Control Systems in the Energy Sector,* representing the sector's ongoing commitment to security. North America's water, transportation, communication, and other critical infrastructures increasingly depend on the reliable operation of the energy sector, making it an attractive target for evolving, sophisticated cyber adversaries. As cyber threats are fast moving, multifaceted, well resourced, and persistent, we need to ramp up efforts to effectively prepare and respond to them.

The energy sector is aware of this need—more than 80 stakeholders participated in the roadmap update. We want to thank those participants for not only recognizing the importance of this effort, but also what can be achieved when we work collaboratively toward a common vision.

Roadmap partners contributed their expertise, ideas, and energy into this guiding framework, and now it is time to leverage that momentum and act on it. We strongly encourage every stakeholder to take ownership of the vision and identify a goal or milestone to which they can contribute. Researchers, vendors, academia, policy makers, and owners and operators need to join forces to confront the challenges we collectively face. Your continued support and commitment is critical to fulfilling the vision in the years ahead.

The Energy Sector Control Systems Working Group

Dave Batz
Edison Electric Institute

Jim Brenton
Electric Reliability
Council of Texas

David Dunn
Independent Electricity System
Operator Ontario

Gerard Williams
BP

Page Clark
El Paso Corporation

Steve Elwart
Ergon Refining Inc.

Ed Goff
Progress Energy

Brian Harrell
North American Electric
Reliability Corporation

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

Morgan Henrie
Alyeska Pipeline

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

Doug Maughan
U.S. Department of Homeland
Security Science & Technology
Directorate

Lisa Kaiser
U.S. Department of Homeland
Security National Protection and
Programs Directorate

Dave Norton
Federal Energy Regulatory
Commission
Office of Electric Reliability

Table of Contents

Executive Summary

Energy delivery systems are critical to the effective and reliable operation of North America's energy infrastructure. Our way of life is made possible by a vast network of processes that produce, transfer, and distribute energy as well as the interconnected electronic components, communication devices, and people that monitor and control those processes. Today's highly reliable and flexible energy infrastructure depends on the ability of energy delivery systems to provide timely, accurate information to system operators and automated control over a large, dispersed network of assets and components. This vast and distributed control requires communication among millions of nodes and devices across multiple domains, exposing energy systems and other dependent infrastructures to potential harm from accidental and malevolent cyber attacks.

Cybersecurity is a serious and ongoing challenge for the energy sector. Cyber threats to energy delivery systems can impact national security, public safety, and the national economy. Because the private sector owns and operates most of the energy sector's critical assets and infrastructure, and governments are responsible for national security, securing energy delivery systems against cyber threats is a shared responsibility of both the public and private sectors. A common vision and a framework for achieving that vision are needed to guide the public-private partnerships that will secure energy delivery systems.

> "The public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure."
>
> — *White House Cyberspace Policy Review May 2009*

An Updated Roadmap to Address Progress and Change

Starting in 2005, the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, the U.S. Department of Homeland Security Science and Technology Directorate, and the Energy Infrastructure Protection Division of Natural Resources Canada facilitated the development of the *Roadmap to Secure Control Systems in the Energy Sector* (hereafter referred to as the 2006 Roadmap) to enhance cybersecurity across the energy sector. The 2006 Roadmap established a common vision and strategic framework for industry and government to develop, deploy, and maintain control systems that could survive an intentional cyber assault without loss of critical functions. The 2006 Roadmap was constructed using the collective insights of the control systems community, including owners and operators, commercial vendors, national laboratories, industry associations, academia, government agencies, and members of the international community. As a result, a number of diverse efforts and ideas aligned toward common goals and the knowledge and resources of other sector stakeholders were better leveraged.

The release of the 2006 Roadmap marked the beginning of a national and international collaborative public-private partnership for increased cybersecurity in the energy sector. The sector has made notable progress, as tracked and detailed in Appendix B and the Interactive Energy Roadmap website ([ieRoadmap] *www.controlsystemsroadmap.net*). The *Roadmap to Achieve Energy Delivery Systems Cybersecurity* is an update to the 2006

Roadmap Scope

The scope of the Roadmap encompasses

- Electricity, oil, and natural gas sectors
- Production, transmission, distribution, and delivery of energy to consumers
- 10-year timeframe divided into near-, mid-, and long-term efforts
- Risk as a function of threat, vulnerability, and consequence
- Prevention, detection, response, and recovery efforts
- Cyber disruptions caused by unintentional incidents, intentional cyber attacks, and attacks against the cyber-physical interface

Roadmap; it reflects subsequent cybersecurity and other technology advances and the evolving needs of the sector. The update includes the following:

- **Changing landscape.** The roadmap now has a broader focus on energy delivery systems, including control systems, smart grid technologies, and the interface of cyber and physical security—where physical access to system components can impact cybersecurity. This update recognizes that smart technologies (e.g., smart meters, phasor measurement units), new infrastructure components, the increased use of mobile devices, and new applications are changing the way that energy information is communicated and controlled while introducing new vulnerabilities and creating new needs for the protection of consumer and energy market information.
- **Building on successes and addressing gaps.** The roadmap reflects new priorities identified by roadmap update participants: enhancing vulnerability disclosure between government, researchers, and industry; optimizing the limited time and resources of stakeholders through innovative partnerships; improving the measurement of progress made toward milestones; and addressing gaps to further advance technologies. While the 2006 Roadmap provided a solid foundation that aligned multiple public and private programs, research and development (R&D) investments, interoperability and cybersecurity standards development and adoption, advanced training, and accelerated product development, there is more work to do in tackling persistent and emerging challenges.
- **Advancing threat capabilities.** The roadmap recognizes that cyber threats to energy delivery systems are real and are becoming increasingly innovative, complex, and sophisticated. Adversaries have pursued progressively innovative techniques to exploit flaws in system components, telecommunication methods, and common operating systems found in modern energy delivery systems with the intent to infiltrate and sabotage them. The Stuxnet worm, which was found to have targeted a specific industrial control system, a programmable logic controller, is an example of a threat designed to reprogram and take control of a system component that is also used by critical energy infrastructure.[2]
- **Emphasizing a culture of security.** The roadmap recognizes that achieving resilient energy delivery systems requires more than a focus on compliance; a culture focused on security that permeates the sector is needed. While regulations and standards can be used to raise security baselines, sustaining a secure and resilient energy infrastructure will not be possible without people trained in developing and implementing the best available security policies, procedures, and technologies tailored to the energy delivery systems operational environment.

The Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

The strategies to achieve this vision confront the formidable technical, business, and institutional challenges that lie ahead in protecting critical systems against increasingly sophisticated and persistent cyber attacks. Energy companies have long recognized that it is neither practical nor feasible to fully protect all energy assets from natural, accidental, or intentional damage. However, the sector's track record of excellent reliability reflects an effective protective approach that balances preventive measures with rapid response and recovery. Accordingly, the industry's vision for securing energy delivery systems focuses on critical functions that, if lost, could result in loss of life, public endangerment, environmental damage, loss of public confidence, or severe economic damage. This prioritized approach is a product of risk-management principles in use throughout the energy sector.

Strategic Framework

Five strategies must be pursued to achieve the energy sector's vision:

- **Build a Culture of Security.** In a culture of security, extensive dialogue about the meaning of security and the consequences of operating under certain levels of risk is ongoing, by various means, among citizens and stakeholders. When integrated with reliability practices, a culture of security ensures sound risk management practices are periodically reviewed and challenged to confirm that established security controls remain in place and changes in the energy delivery system or emerging threats do not diminish their effectiveness. Implementing this strategy will help the sector achieve the following goal: Cybersecurity practices are reflexive and expected among all energy sector stakeholders.
- **Assess and Monitor Risk.** Assessing and monitoring risk gives companies a thorough understanding of their current security posture, enabling them to continually assess evolving cyber threats and vulnerabilities, their risks, and responses to those risks. Implementing this strategy will help the sector achieve the following goal: Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators.
- **Develop and Implement New Protective Measures to Reduce Risk.** In this strategy, new protective measures are developed and implemented to reduce system risks to an acceptable level as security risks—including vulnerabilities and emerging threats—are identified or anticipated. These security solutions are built into next-generation energy delivery systems, and appropriate solutions are devised for legacy systems. Implementing this strategy will help the sector achieve the following goal: Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident.
- **Manage Incidents.** Managing incidents is a critical strategy because cyber assaults can be sophisticated and dynamic and any system can become vulnerable to emerging threats as absolute security is not possible. When proactive and protective measures fail to prevent a cyber incident, detection, remediation, recovery, and restoration activities minimize the impact of an incident on an energy delivery system. Post-incident analysis and forensics enable energy sector stakeholders to learn from the incident. Implementing this strategy will help the sector achieve the following goal: Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment.
- **Sustain Security Improvements.** Sustaining aggressive and proactive energy delivery systems security improvements over the long term requires a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders. Energy sector collaboration provides the resources and incentives required for facilitating and increasing sector resilience. Implementing this strategy will help the sector achieve the following goal: Collaboration between industry, academia, and government maintains cybersecurity advances.

The strategies form the core of a strategic framework (Exhibit E.1), tied to distinct milestones and time frames, that will coordinate efforts currently under way in the public and private sectors and help align new projects to advance energy delivery systems security

Key Challenges

The energy sector faces a number of challenges to achieving the milestones. The challenges described below and in Exhibit E.1 are not prioritized; each is key to realizing the sector's vision. However, these are not the only challenges the sector must overcome; further barriers are described in Section 4.

Although the ability of energy companies to assess and monitor cybersecurity posture has improved since the 2006 Roadmap, real-time solutions are needed to keep pace with increasingly sophisticated cyber threats that are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures. The dynamic landscape complicates the creation of consistent metrics and advanced tools for measuring risks. Upgrading legacy systems often requires replacing technology to implement the needed security capabilities due to inherent limitations of existing equipment and architectures or degradation of system performance caused by the security upgrades. New architectures with built-in, end-to-end security require multidisciplinary efforts, significant resources, and years to develop and deploy throughout the energy sector. Information about attacks that occur, consequences, and lessons learned often are not shared beyond the organization experiencing the incident. Outside the energy delivery community, cybersecurity problems, their implications, and the need for solutions tailored to energy delivery systems are still not well understood.

Making a strong business case for cybersecurity investment is complicated by the difficulty of quantifying risk in an environment of rapidly changing, unpredictable threats with consequences that are hard to demonstrate. Regulatory uncertainty caused by changing and new regulations can also introduce risk for private sector cybersecurity investments. As recognized by the U.S. Government Accountability Office (GAO), the "existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity."[3]

Roadmap Implementation

Implementing this roadmap requires the collective commitment of government, industry, academia, researchers, vendors and other solution providers, and asset owners and operators. These stakeholders bring distinct skills and capabilities for improving energy delivery systems security today and in the future. Industry organizations and government agencies can provide the needed coordination, leadership, and investments to address important barriers and gaps. Researchers at government laboratories and universities also play a key role in exploring long-term solutions and developing tools to assist industry. Asset owners and operators bear the chief responsibility for ensuring that systems are secure, investing appropriately, and implementing protective measures. They are supported by the software and hardware vendors, contractors, IT and telecommunications service providers, and technology designers who develop and deliver products and services tailored to energy delivery systems.

Measuring progress is critical to success; however, progress depends on the actions of many stakeholders, dispersed throughout North America, working to achieve a common goal. Manually polling these stakeholders to identify and document advancements is highly time consuming and resource intensive. To address this issue, the Energy Sector Control Systems Working Group (ESCSWG) encourages stakeholders to use the ieRoadmap to record actions they are taking to enhance cybersecurity. Using the ieRoadmap, energy stakeholders can align resources, partner to develop and implement strategic and tactical approaches to achieve roadmap milestones, and evaluate and communicate progress each year. The ESCSWG will help coordinate and measure the sector's progress towards meeting the roadmap vision.

Exhibit E.1 Strategies for Achieving Energy Delivery Systems Cybersecurity

Vision	**By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.**				
Barriers	• **Cyber threats are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures** • **Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures** • **Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations** • **Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry** • **Weak business case for cybersecurity investment by industry** • **Regulatory uncertainty in energy sector cybersecurity**				
Strategies	**1. Build a Culture of Security**	**2. Assess and Monitor Risk**	**3. Develop and Implement New Protective Measures to Reduce Risk**	**4. Manage Incidents**	**5. Sustain Security Improvements**
Near-term Milestones (0–3 years) By 2013	1.1 Executive engagement and support of cyber resilience efforts 1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched	2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available 4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders 5.2 Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems
Mid-term Milestones (4–7 years) By 2017	1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available 1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics	3.2 Scalable access control for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	4.3 Incident reporting guidelines accepted and implemented by each energy subsector 4.4 Real-time forensics capabilities commercially available 4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
Long-term Milestones (8–10 years) By 2020	1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector
Goals	**Cybersecurity practices are reflexive and expected among all energy sector stakeholders**	**Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators**	**Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident**	**Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment**	**Collaboration between industry, academia, and government maintains cybersecurity advances**

1. Introduction

Our finances, transportation, health care, water supply, and emergency services depend on reliable energy. Building and maintaining survivable energy delivery systems that ensure the continuity of energy service in the face of all hazards is critical to the stability of our economy and the safety and well-being of citizens. However, state and non state adversaries are acquiring increasingly sophisticated cyber attack tools and capabilities to exploit and potentially disrupt or destroy critical energy infrastructures.

Enhancing the cybersecurity for energy delivery systems requires an ongoing, coordinated approach between the government, charged with protecting the nation against foreign and domestic threats; and the private sector, responsible for ensuring the continuity of critical energy service and protecting shareholder value. The *Roadmap to Achieve Energy Delivery Systems Cybersecurity* is a high level, sector-supported framework to stimulate public-private coordination and investment over the next ten years to achieve the sector's vision for cybersecurity. Construction of this roadmap was guided by industry, government, vendors and other solution providers, and academic partners that have been working to enhance the cybersecurity of energy delivery systems for more than a decade.

> "…that's why we're going to need all of you to keep coming together—government, industry, academia, think tanks, media and privacy and civil liberties groups—to work together, to develop the solutions we need to keep America safe and prosperous in cyberspace."
>
> — *President Barack Obama*
> *White House Event on*
> *Cybersecurity Progress*
> *July 2010* [4]

Updating the Roadmap

This roadmap is an update of the 2006 *Roadmap to Secure Control Systems in the Energy Sector* (2006 Roadmap). Since 2006 the sector has made notable progress, as detailed in Appendix B and the interactive Energy Roadmap website (ieRoadmap, *www.controlsystemsroadmap.net*). The roadmap builds on the framework established by the 2006 Roadmap and addresses the changes in the energy delivery systems landscape since 2006, including cybersecurity and other technology advances, the evolving needs of the sector, and lessons learned. The key changes this roadmap update addresses include:

- **Changing landscape**. Smart technologies (e.g., smart meters and phasor measurement units) are introducing millions of new intelligent components to the energy infrastructure that communicate and control energy delivery in much more advanced ways than in the past. New infrastructure components and the increased use of mobile devices in energy infrastructure environments introduce new digital vulnerabilities and additional physical access points. New applications, such as managing energy consumption, involve new stakeholders (e.g., retail service providers, energy and financial market traders, industrial, commercial, and residential consumers) and require protection of private customer and energy market information. Because of the changing landscape, the roadmap now has a broader focus on energy delivery systems, which include control systems, smart grid technologies, and the interface of cyber and physical security—where physical access to system components can impact cybersecurity.
- **Building on successes and addressing gaps.** The 2006 Roadmap provided a solid foundation that aligned multiple public and private programs, research and development (R&D) investments, interoperability and cybersecurity standards development and adoption, advanced training, and accelerated product development. These research and product development efforts introduced new cybersecurity products that are commercially available today. While much progress has been made, there is more work to do in tackling persistent and emerging challenges. Roadmap update

participants identified the following new priorities: enhancing vulnerability disclosure between government, researchers, and industry; optimizing the limited time and resources of stakeholders through innovative partnerships; improving the measuring of progress made toward achieving milestones; and addressing gaps to further advance cybersecurity technologies.

- **Advancing threat capabilities.** Energy delivery systems are vulnerable to cyber attack and the threat is real. Adversaries have pursued progressively destructive means to exploit flaws in system components, telecommunication methods, and common operating systems found in modern energy delivery systems with the intent to infiltrate and sabotage them. The Stuxnet worm, which was found to have targeted a specific industrial control system, a programmable logic controller, is an example of a threat designed to reprogram and take control of a system component that is also used by critical infrastructure.[5]
- **Emphasizing a culture of security.** While regulations or standards can be used to raise security baselines, a focus on compliance alone will not produce resilient energy delivery systems. A culture focused on security that permeates the sector is needed. Social and human factors are particularly important because cybersecurity is a sensitive issue in which trust and careful stewardship are paramount. Sustaining a secure and resilient energy infrastructure will not be possible without people trained in developing and implementing the best available security policies, procedures, and technologies tailored to the energy delivery systems operational environment.

For more information on revisions to the 2006 Roadmap, please refer to Appendix A.

Energy Stakeholder Input to the Roadmap

The roadmap updating effort was designed and directed by the Energy Sector Control Systems Working Group (ESCSWG). The ESCSWG consists of 14 energy sector security experts supporting the Electricity and Oil & Natural Gas Sector Coordinating Councils and the Government Coordinating Council for Energy (see Appendix C). The roadmap content is based on expert input collected from a broad cross-section of energy delivery system stakeholders during four phases:

- **Over-the-Horizon Analysis**: On July 7, 2009, nearly 20 asset owners, government leaders, vendors, and researchers convened to examine the solid foundation of the 2006 Roadmap and provide recommendations to better align the framework with the wide range of complex energy delivery systems security needs the sector will have to address today and in the future.
- **Roadmap Update Workshop**: On September 2 and 3, 2009, more than 80 asset owners and operators, chief information officers (CIOs), researchers, technology developers, security specialists, and vendors focused on addressing the most persistent challenges: vulnerability disclosure, measuring progress, innovative partnerships, and technology gaps and advancements. Participants defined the issues and identified a set of prioritized solutions to address these concerns.
- **Roadmap Technical Review Workshop**: On November 18, 2009, 12 subject matter experts convened to clarify the technical challenges and recommend additional milestones to ensure that the sector has a clear path to achieving roadmap goals. For workshop results, please review the Roadmap Update Workshop Summaries found on the ieRoadmap.
- **Roadmap Review**: The ESCSWG synthesized the results of the above efforts to update the 2006 Roadmap and create a draft roadmap. The draft was circulated among Roadmap Workshop participants, energy delivery system experts, and on the ieRoadmap for comment and was revised for clarity and added insight.

Roadmap Purpose

The roadmap strategies and priorities help inform and strengthen government, industry, vendor, and academic programs designed to improve protection of energy delivery systems across North America. The roadmap was designed to achieve the following:

- Define a framework that articulates the cybersecurity needs of asset owners and operators in the energy sector and high-level strategies for increasing the resilience of energy delivery systems—including next-generation, current day, and legacy components—over the next 10 years.
- Guide industry, government, and academic efforts to meet a common vision and create a permanent culture of security to sustain that vision.
- Encourage collaboration among all stakeholders to strengthen public-private partnerships and leverage expertise and capabilities across each stakeholder group.
- Encourage each stakeholder to plan and engage in efforts that directly align with one or more of the roadmap priorities.

Roadmap Scope

The scope of the Roadmap encompasses:

- Electricity, oil, and natural gas sectors
- Production, transmission, distribution, and delivery of energy to consumers
- 10-year timeframe divided into near-, mid-, and long-term efforts
- Risk as a function of threat, vulnerability, and consequence
- Prevention, detection, response, and recovery efforts
- Cyber disruptions caused by unintentional incidents, intentional cyber attacks, and attacks against the cyber-physical interface

Infrastructure Protection and Policy Influences

Energy sector partners from industry, government, and academia are collaborating to improve critical infrastructure protection—part of the large and growing public-private effort to strengthen and protect the critical infrastructure sectors in North America. The efforts within the energy sector as well as those among interdependent critical infrastructures have influenced the development of this roadmap and will affect its implementation. Since the publication of the 2006 Roadmap, several new public and private critical infrastructure protection efforts have focused on cybersecurity, including the following:

- In November 2010, the North American Electric Reliability Corporation (NERC) Board of Trustees approved the Electricity Sub-sector Coordinating Council's (ESCC) **Critical Infrastructure Strategic Roadmap**,[6] which provides a framework to identify risks, including severe-impact cyber risks, that have the potential to seriously disrupt the supply of electricity to customers, and promotes the actions necessary to enhance reliability and resilience.
- In June 2010, the jointly commissioned NERC and U.S. Department of Energy (DOE) **High-Impact, Low-Frequency Event Risk to the North American Bulk Power System** report[7] described the risk of a coordinated cyber, physical, or blended attack and recommended nine proposals for action to the electric industry, including more direct information sharing, robust system modeling tools, and operator training.
- In November 2009, DOE announced a commitment of $18.8 million in project funding provided by DOE, the U.S. Department of Homeland Security (DHS), and five universities—Cornell University, Dartmouth College, University of California at Davis, University of Illinois at Urbana-Champaign, and Washington State University—to leverage and expand upon previous work funded primarily by

the National Science Foundation. This new project, **TCIPG (Trustworthy Cyber Infrastructure for the Power Grid)** is a university led public-private research partnership supported by DHS, DOE, and industry for resilient and secure smart grid systems.

- In November 2009, a total public-private investment worth more than $9.6 billion spurred the transition to a smarter, stronger, more efficient and reliable electric system. The $4.5 billion in DOE funds from the **American Recovery and Reinvestment Act (ARRA)** was leveraged with $5.1 billion in funds from the private sector to support 131 smart grid investment and demonstration projects across the country. Project awardees committed to developing and implementing a cybersecurity plan that includes an evaluation of cyber risks and planned mitigations, cybersecurity criteria for device and vendor selection, and relevant standards or best practices that the project will follow.[8]
- In March 2008, the **Roadmap to Secure Control Systems in the Water Sector**[9] outlined strategic industry-driven guidance for the Water Sector. In September 2009, the **Roadmap to Secure Control Systems in the Chemical Sector**[10] outlined strategic industry-driven guidance for the Chemical Sector. Many small municipalities are responsible for both water and electric service, and some oil and natural gas facilities produce and deliver chemicals.
- In May 2007, the Energy Government Coordinating Council worked with the Electricity and Oil and Natural Gas Sector Coordinating Councils (SCCs) to develop the **Energy Sector-Specific Plan**[11] (SSP) as input to the National Infrastructure Protection Plan. The Energy SSP adopted the roadmap vision and framework. A revised SSP was released in 2010.

Since 2006, cybersecurity has gained high visibility in the White House, Congress, industry, and the general public. U.S. legislators have proposed a number of bills to enhance cybersecurity, and the Administration designated cybersecurity as a top national priority. In addition, NERC has also listed cybersecurity as one of the top emerging reliability issues facing the electric industry today.[12] Examples of recent documents providing Federal policy guidance on cybersecurity include the following:

- In October 2010, the U.S. president's National Infrastructure Advisory Council released **A Framework for Establishing Critical Infrastructure Resilience Goals,**[13] which examined resilience practices and needs in the electricity sector and offered recommendations to the White House to improve resilience and cybersecurity, including initiating an executive-level, public-private dialogue to address high-impact risks; enhancing private sector information sharing; and encouraging industry self-governance.
- In May 2010, the **National Security Strategy** identified cybersecurity threats as a serious challenge and protecting the nation's digital infrastructure as a national security priority. To "deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks," the strategy focuses on investing in people and technology as well as strengthening partnerships.
- In October 2009, the DHS document **A Roadmap for Cybersecurity Research**[14] outlined R&D agendas for the future relating to 11 hard problem areas in cybersecurity. It is intended for use by agencies of the U.S. Government and other potential R&D funding sources.
- In October 2009, the DHS **Strategy for Securing Control Systems: Coordinating and Guiding Federal, State, and Private Sector Initiatives**[15] provided a framework for coordinating control systems security efforts across all critical infrastructures.
- In May 2009, the **White House Cyberspace Policy Review**[16] recognized the 2006 Roadmap's vision for control systems security. It calls for the federal government and the private sector to work closely on near-term efforts to secure the nation's communications infrastructure, including developing a framework for R&D strategies that focus on game-changing technologies.

2. Energy Sector Progress

The 2006 Roadmap provided the first comprehensive strategy to organize industry's existing and future control systems needs and focus cybersecurity priorities throughout the public and private sectors. Although the 2006 Roadmap has been widely acknowledged,[17] its true value is in providing a sector-supported basis that enables coordination and stimulates investment within the sector toward achieving common goals. As a result, more secure control systems are now available and being developed by the sector. The energy sector is better prepared to face emerging cyber risks.

The 2006 Roadmap started dozens of collaborative initiatives across industry, national laboratories, universities, and government. Many important efforts are still under way and are mapped to specific 2006 Roadmap milestones on the ieRoadmap. Moreover, several 2006 Roadmap initiatives have produced tangible near-term improvements that have reduced cyber risks in today's energy systems. An extensive list of achievements and ongoing efforts, which contribute to each of the four strategic goals contained in the 2006 Roadmap, are included in Appendix B. Exhibit 2.1 shows a visual representation of the range of public and private projects supporting 2006 Roadmap milestones. The achievements listed below are a handful of the many efforts and help to highlight progress in making electricity, oil, and natural gas infrastructures more secure against cyber incidents.

Bandolier and the Roadmap

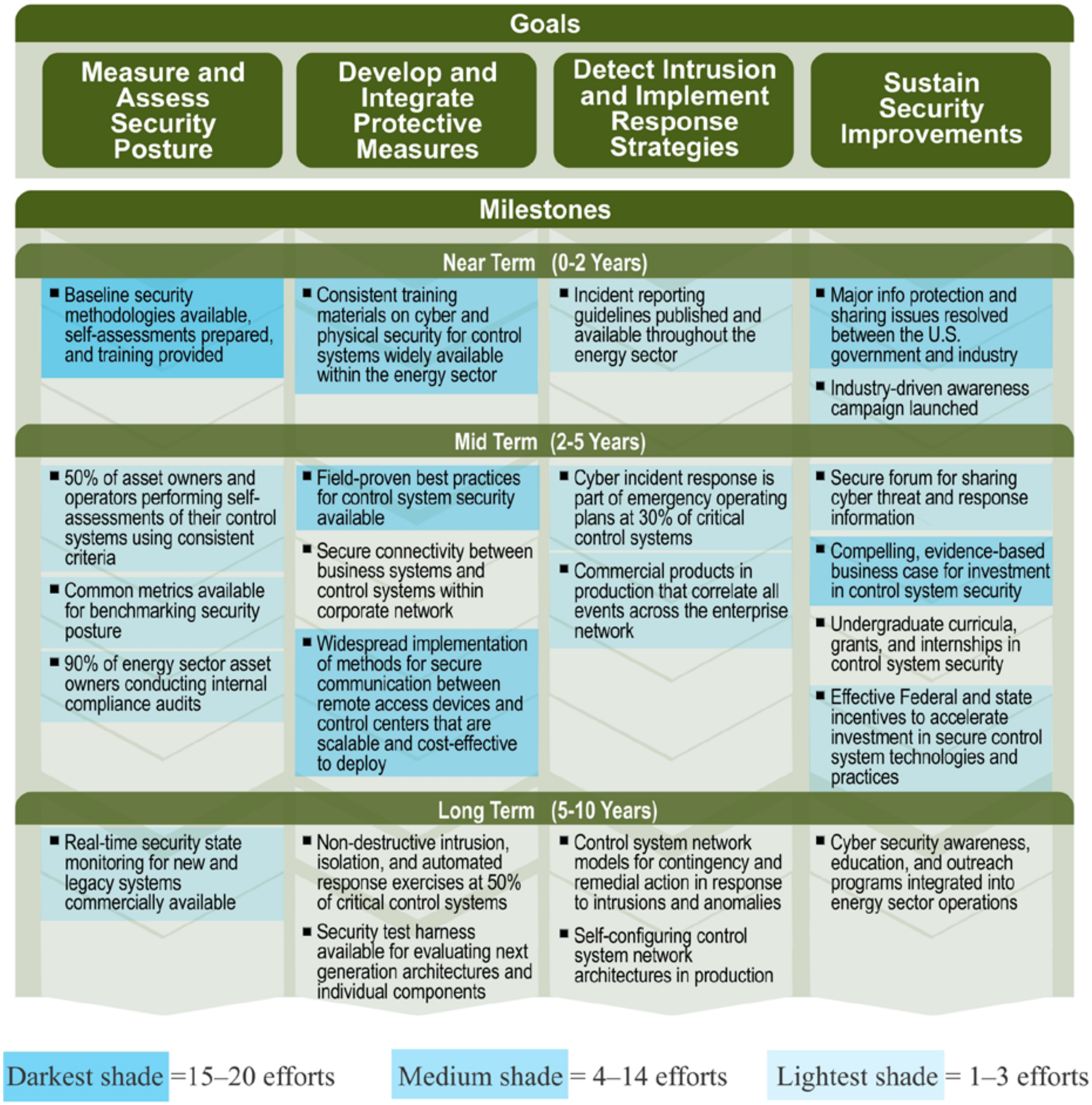
In 2006, Digital Bond partnered with Tenable Network Security to enhance an existing risk assessment tool for control systems applications. However, the costs of developing and deploying this technology were too high for this small business. Through DOE's competitive solicitation process, which funds projects that address Roadmap priorities, such as "efforts to develop [a] tool set for owners and operators to conduct-self assessments," Digital Bond was able to obtain the funding required to bring the first release of this tool to the energy sector. Digital Bond now partners with leading control system vendors who continue to provide funding for new versions of the tool and additional products.

As a result, asset owners and operators can now audit and optimize the security configurations of their control system workstations and servers against vendor supported security configurations using the Bandolier Security Audit Files. Vendors are using Bandolier for delivering hardened systems, acceptance testing, and routine security validation testing during patching and updating. In addition, Bandolier can help validate compliance with standards, such as NERC CIP. The Audit Files leverage the compliance plug-in of the widely used Nessus scanner to enable auditing without additional software and are available for over twenty control system components from nine vendors.

Measure and Assess Security Posture

- DOE's National SCADA Test Bed (NSTB) has completed 37 cyber vulnerability assessments of control systems and components. These NSTB assessments, performed by Idaho National Laboratory (INL), have enabled vendors to identify problems, deliver patches to existing customers, and integrate stronger security into next-generation systems. The assessments conducted to date include laboratory assessments of 14 vendor components and 15 vendor systems, and 8 onsite assessments of asset owner systems. The NSTB was formed in 2003 to provide a fail-safe environment to rigorously examine commercially available systems and validate security enhancements based on extensive cybersecurity research at the national laboratories. Onsite assessments with asset owners enable researchers to evaluate vulnerabilities in an operational environment and can validate fixes made after test bed assessments. As a result of this work, more secure next-generation control systems and security patches are now available and in use by the energy sector.

Exhibit 2.1 Energy Sector Efforts Supporting 2006 Roadmap Milestones



Goals

Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion and Implement Response Strategies	Sustain Security Improvements
Milestones			
Near Term (0-2 Years)			
▪ Baseline security methodologies available, self-assessments prepared, and training provided	▪ Consistent training materials on cyber and physical security for control systems widely available within the energy sector	▪ Incident reporting guidelines published and available throughout the energy sector	▪ Major info protection and sharing issues resolved between the U.S. government and industry ▪ Industry-driven awareness campaign launched
Mid Term (2-5 Years)			
▪ 50% of asset owners and operators performing self-assessments of their control systems using consistent criteria ▪ Common metrics available for benchmarking security posture ▪ 90% of energy sector asset owners conducting internal compliance audits	▪ Field-proven best practices for control system security available ▪ Secure connectivity between business systems and control systems within corporate network ▪ Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy	▪ Cyber incident response is part of emergency operating plans at 30% of critical control systems ▪ Commercial products in production that correlate all events across the enterprise network	▪ Secure forum for sharing cyber threat and response information ▪ Compelling, evidence-based business case for investment in control system security ▪ Undergraduate curricula, grants, and internships in control system security ▪ Effective Federal and state incentives to accelerate investment in secure control system technologies and practices
Long Term (5-10 Years)			
▪ Real-time security state monitoring for new and legacy systems commercially available	▪ Non-destructive intrusion, isolation, and automated response exercises at 50% of critical control systems ▪ Security test harness available for evaluating next generation architectures and individual components	▪ Control system network models for contingency and remedial action in response to intrusions and anomalies ▪ Self-configuring control system network architectures in production	▪ Cyber security awareness, education, and outreach programs integrated into energy sector operations

Darkest shade =15–20 efforts   Medium shade = 4–14 efforts   Lightest shade = 1–3 efforts

- Two utility consortia pooled resources to fund vulnerability assessments for the control systems they employ. Twelve utilities using ABB systems, including Austin Energy, Detroit Edison, Indianapolis Power & Light Company, ITC Transmission, Kansas City Power & Light Company, Lower Colorado River Authority (LCRA), New York Independent System Operator, Snowy Hydro Limited, and Tri-State Generation and Transmission Association, Inc. from the United States and Australia formed a consortium to privately fund user-driven ABB system vulnerability assessments at INL. Utilities using AREVA systems have followed suit, forming their own consortium to leverage funding for follow-on testing of AREVA systems.

- The LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) program was formed to facilitate cooperative R&D, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems. LOGIIC is an ongoing collaboration of oil and natural gas companies and the DHS Science and Technology Directorate. The first LOGIIC project was a technology integration and demonstration effort that demonstrated an opportunity to reduce vulnerabilities of oil and gas process control environments by sensing, correlating, and analyzing abnormal events to identify and prevent cyber security threats.

Develop and Integrate Protective Measures

- The Lemnos Interoperable Security project, a DOE cost-shared project, developed and demonstrated an interoperability configuration profile for creating a secure communications channel between two control system networks operated by different vendors. Vendors including GarretCom, Industrial Defender, N-dimension, Phoenix Contact, RuggedCom, Schweitzer Engineering Laboratories, and Siemens have tested and publicly demonstrated the interoperability using the Lemnos profile. The profile, built on Sandia National Laboratories' Open PCS Architecture for Interoperable Design (OPSAID) project, has been accepted as the basis for an OpenSmartGrid (OpenSG) Security Working Group Task Force under the UCA International Users Group (UCAIug).

- INL has trained more than 2,300 operators and other stakeholders in introductory, intermediate, and advanced security courses, including two NERC-certified courses, conducted by DOE and DHS. These courses raise awareness of vulnerabilities, attack mechanisms, and operational issues. More than 224 energy company representatives from the electric, oil, and natural gas subsectors have engaged in weeklong classroom courses and a full-day red/blue/white team exercise during advanced training, designed to leave participants with security techniques they can take back and use in their facility.

- The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), a public-private project between North American utilities and DOE, released two security profiles, one for advanced metering infrastructure (AMI) and another for third-party data access. The AMI profile provides guidance and security controls to organizations developing and implementing AMI solutions. This profile was adopted and ratified in December 2009 by the AMI Security (AMI-SEC) Task Force within UCAIug, and AMI-SEC released version 2.0 in June 2010. ASAP-SG's AMI profile accelerated the work of AMI-SEC, enabling the document to go from inception through ratification to version 2.0 in less than a year. The AMI profile also served as a reference to the National Institute of Standards and Technology (NIST) Cyber Security Working Group's development of the NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*.

Detect Intrusion and Implement Response Strategies

- The Portaledge release package from Digital Bond was developed in a DOE cost-shared project. Portaledge allows asset owners to aggregate control system security events and correlate those events to help detect cyber attacks. Portaledge includes templates that aid an owner/operator in leveraging the installed base and capabilities of OSISoft's PI Server to collect, analyze, and report control system data that potentially signify an attack. User customized event sequences will alert an operator to a potential attack, and operators can use the chain of individual events to respond to or analyze an incident. Version 1 is available to more than 200 Digital Bond subscribers.

- The *NERC Security Guideline for the Electricity Sector: Threat and Incident Reporting* was developed to enable electric sector entities to satisfy mandatory incident reporting requirements or participate in voluntary reporting. Designed to provide different information requirements for three different incident stages, it facilitates timely reporting of cyber and physical threats or incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and NERC Reliability Coordinator Information System. It can also be used for voluntary DHS and Public Safety Canada/Royal Canadian Mounted Police reporting.

Sustain Security Improvements

- In January 2010, the Federal Bureau of Investigation (FBI) and DOE identified a virtual private network (VPN) vulnerability. Within 90 days of this discovery, an awareness bulletin was provided to industry that included the details of the vulnerability and recommendations to mitigate risk. This actionable security product was a result of a joint collaboration between ES-ISAC, the sector lead agency (DOE), the FBI, and the Control System Security Program (CSSP) at DHS. The U.S. Government supplied technical and actionable information regarding observed cyber incidents. The

ES-ISAC formed a team of network security experts from industry and worked with government partners to develop the bulletin.

- The Energy Sector Security Consortium, Inc. (EnergySec) online forum (*www.energysec.org*) was established to enable energy sector asset owners, government representatives, and product vendors to share threat and incident information, communicate, and coordinate confidentially with a network of peers. This enables the exchange of actionable information directly among staff-level individuals.
- In 2010, DOE announced an investment of $16.5 million by DOE, EnergySec, and the Electric Power Research Institute (EPRI) to form two electric sector cybersecurity organizations, NESCO and NESCOR. NESCO (the National Electric Sector Cybersecurity Organization) led by EnergySec, works to improve electric system reliability by supplying data analysis and forensics capabilities for cyber-related threat. It also assists in creating a framework to identify and prepare for challenges to grid reliability; share information, best practices, resources, and solutions to and from domestic and international electric sector participants; and encourage key electric sector supplier and vendor support and interaction. NESCOR (the National Electric Sector Cybersecurity Organization Resource) led by EPRI, conducts assessment and analysis of cybersecurity requirements, results, and standards in addition to testing security technologies in laboratories and pilot projects in support of NESCO.

The Path Forward

This roadmap presents a high-level strategy addressing these needs, but it does not prescribe a single path forward. Federal and private organizations and public-private collaborations continue to produce unique cybersecurity solutions that meet the roadmap's defined needs and align with goals. Agencies and organizations are encouraged to participate in cybersecurity efforts that will best capitalize on their distinct skills, capabilities, and resources while meeting their mission and needs. The following strategies and guidelines are examples that can provide more detailed and tactical guidance on how to achieve the roadmap goals and vision:

- The **National Strategy for Trusted Identities in Cyberspace (NSTIC)**[18] was released by the White House on April 15, 2011. The Department of Commerce will coordinate the federal government and private sector in implementing this effort to raise the level of trust associated with the online identities of individuals, organizations, services, and devices. The guidance calls for private sector entities to focus first on implementing two-factor authentication for individuals for operational and, in time, business networks; and to seek to improve the authentication of devices. Both efforts should comply with and be interoperable with the broader NSTIC effort.
- In August 2010, the NIST Smart Grid Interoperability Panel's **Guidelines for Smart Grid Cyber Security (NISTIR 7628)**[19] detailed a strategy that included smart grid use cases, high-level smart grid security requirements, a risk-assessment framework, a high-level security architecture, and assessment of smart grid standards. It also identified high-level areas where "approaches to secure [smart grid] technologies and to protect privacy must be designed and implemented early in the transition to the Smart Grid." Cybersecurity requirements will be critical in all of the priority action plans included in the corresponding *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*.

As the energy sector pursues the roadmap strategies, it will continue to review, assess, and adjust the mix of efforts that will improve energy delivery systems security for today and tomorrow. Section 5, Implementation, provides an industry-managed process currently in place for launching and managing essential energy delivery system projects.

Standards Establish Baseline Security

Since the 2006 Roadmap's publication, cybersecurity has moved to the forefront of national security as a focus for policy initiatives, long-term planning, and best practices and standards, both within the energy sector and in other interdependent critical infrastructures. There are now numerous energy sector standards, best practices, and guidelines focused on cybersecurity, and the list is growing. Standards development and implementation reinforces the technological and operational enhancements the sector has made over the last four years and elevates cybersecurity across the sector.

Specific to the electricity subsector, the Energy Policy Act of 2005 (EPACT) made cybersecurity standards mandatory for the bulk electric system. The Federal Energy Regulatory Commission (FERC) selected the North American Electric Reliability Corporation (NERC) as the Electricity Reliability Organization (ERO) to develop the standards. NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009 became mandatory in 2008. The NERC CIP standards require utilities in the bulk electric system to do the following:

- Identify critical cyber assets (002)
- Develop security management controls to protect these critical cyber assets (003)
- Implement personnel risk assessment, training, and security awareness (004)
- Identify and implement electronic perimeter security for critical cyber assets (005)
- Implement a physical security program to protect critical cyber assets (006)
- Protect assets and information within the electronic security perimeter (007)
- Conduct incident response reporting and response planning (008)
- Implement recovery plans for critical cyber assets (009)

These standards are the baseline required by FERC to support the reliability of the bulk power system and include complex reporting and auditing requirements. Other voluntary interoperable and cybersecurity standards developed by NIST, International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), and International Society of Automation (ISA) address cybersecurity and are also applicable to the electricity sector.

The American Petroleum Institute (API) standard, *API 1164 Pipeline SCADA Security Version 2*, released in 2009, is a voluntary industry standard specific to supervisory control and data acquisition (SCADA) for the petroleum pipeline industry. The standard provides SCADA security best practices to guide liquid pipeline operators on risk assessments, system design, and establishment and review of company policies. API 1164 addresses access control, communication security, information distribution classification, physical issues including disaster recovery and business continuity plans, operating systems, network design, data interchange between enterprise and third-party support/customers, management systems, and field devices configuration and local access.

Although standards may elevate cybersecurity across the energy sector, they do so by requiring the implementation of minimum security measures that set a baseline for cybersecurity across an industry. These minimum security levels may not be sufficient to secure the sector against new and quickly evolving risks. Asset owners compliant with standards may still be vulnerable to cyber intrusion. For example, the CIP standards require risk assessment, security controls, and monitoring; these efforts, each documented extensively, do not verify that the documents represent the actual state of the utility's security. Verified and dynamic security is required to identify and respond to new and quickly evolving risks. New, more resilient capabilities for continuous security monitoring, risk assessment, protection, and response are needed along with a security culture that drives and sustains these security enhancements.

Achieving and maintaining acceptable levels of security will require energy sector asset owners to adopt a risk management approach to ensure that the appropriate investments in security are made. For example, ratepayers and utilities face financial pressure such that any new costs must be justified by reasonable assessments of risks. A risk-based approach will enable asset owners and operators to apply the most appropriate level of risk mitigation to adequately protect the critical missions and business functions of their organizations. Risk management requires continuous monitoring and improvement in the security state of the energy delivery system as well as the overall resilience of the energy sector organization. This approach enables asset owners to quickly apply the proper level of risk mitigation measures to the most appropriate energy delivery systems to adequately protect the critical missions and business functions of the energy sector organization.

3. Energy Delivery Systems Landscape

The 2006 Roadmap focused on enhancing the cybersecurity of energy sector control systems. Control systems are the electronic, computer-based facilities, systems, and equipment used to remotely monitor and control sensitive processes and physical functions. Energy control systems encompass SCADA systems used to monitor and control vast, widely dispersed operations; energy management systems (EMS) used with SCADA systems to optimize energy delivery system performance; distributed control systems (DCS) used for a single facility or small geographical area; and remote components such as remote terminal units (RTU), programmable logic controllers (PLC), and intelligent electronic devices (IED) that monitor system data and initiate programmed control activities in response to input data and alerts.

As national policies and economics have changed over the past five years, two-way communications and intelligent communicating devices have become more important in increasing the efficiency of the energy sector. In particular, the electricity subsector is integrating new technologies, services, and entities across the existing complex and reliable electricity infrastructure to enable two-way capabilities for communicating information, controlling equipment, and distributing energy. This "smart" electric power grid is central to increasing energy efficiency, reliability, and security; to transitioning to renewable sources of energy; to reducing greenhouse gas emissions; and to building a sustainable economy that ensures future prosperity. The gas subsector has also begun deploying similar smart technologies. Although these technologies bring benefits to the energy sector, they also introduce new vulnerabilities and additional physical access points. Therefore securing energy delivery requires securing these new, smarter technologies and the interface between cyber and physical security—where physical access to system components can impact cybersecurity. See Appendix D for more information on the energy delivery systems for the electricity, oil, and natural gas subsectors.

The energy sector is also becoming more reliant on other sectors such as the telecommunications sector. The source of energy for electricity generation is also changing, increasing the electricity industry's reliance on the delivery of energy from other energy sectors such as natural gas.

New Smart Grid Efforts

With the ongoing effort to modernize the energy delivery infrastructure, several public and private partnerships have been working to address emerging risks. The Smart Grid Interoperability Panel-Cyber Security Working Group (SGIP-CSWG)—established in March 2009 and led by NIST, with more than 475 participants from the private sector (including vendors and services providers), manufacturers, various standards organizations, academia, regulatory organizations, and federal agencies—has developed NISTIR 7628: *Guidelines for Smart Grid Cyber Security*.[20] NISTIR 7628 defines cybersecurity for the power industry as:

> All issues involving automation and communications that affect the operation of electric power systems and the function of the utilities that manage them and the business processes that support the customer base. . . . Cybersecurity for the Smart Grid supports both the reliability of the grid and the confidentiality (and privacy) of the information that is transmitted.

Exhibit 3.1 describes the cybersecurity considerations for Smart Grid as identified by the NIST SGIP-CSWG.

Exhibit 3.1 Cybersecurity Considerations for Energy Delivery Systems[21]

Availability for energy system delivery has various time latency needs:

- ≤ 4 milliseconds (ms) for protective relaying
- Subseconds for transmission wide-area situational awareness monitoring
- Seconds for substation and feeder supervisory control and data acquisition (SCADA) data\
- Minutes for monitoring noncritical equipment and some market pricing information
- Hours for meter reading and longer term market pricing information
- Days/weeks/months for collecting long-term data, such as power quality information

Integrity for energy system operations includes the following assurance:

- Data has not been modified without authorization
- Source of data is authenticated
- Timestamp associated with the data is known and authenticated
- Quality of data is known and authenticated

Confidentiality is becoming more important with the increasing availability of customer information online. Confidentiality needs include the following:

- Privacy of customer information
- Electric market information
- General corporate information, such as payroll, internal strategic planning, etc.

Escalating Threats and New Vulnerabilities

The energy sector faces an increasingly sophisticated and aggressive threat environment. Intelligence reports indicate that cyber adversaries are more persistent and better financed, and their ability to develop and launch new attack tools and techniques could outpace the sector's ability to develop and deploy new countermeasures. Stuxnet—discovered in 2010—was the first known computer worm to target and reprogram an industrial control system, a programmable logic controller, while hiding the changes from system operators.[22]

In addition to an evolving threat environment, new vulnerabilities are also increasing as North America transitions to a cleaner, more efficient energy economy. Smarter technologies will significantly increase the number and availability of digital access points to energy communication networks. For example, smart grid technologies such as automated metering and control equipment, if not designed with adequate security built in, could be vulnerable to cyber attacks. Secure, interoperable smart grid technologies will make grid modernization possible.

Both the cyber and energy environments are constantly changing. New threats, business practices, market trends, regulations, and technologies will challenge the North American security posture and reshape the energy delivery systems security landscape (see Exhibit 3.2 and 3.3) over the next 10 years.

Exhibit 3.2 Trends and Drivers Affecting Future Energy Delivery Systems Security

Business Practices

- Aging workforce and staff turnover
- Increasing need for new skills to address both operations and business information technology
- Increasing use of corporate resources for regulation compliance activities reduces the resources available for security enhancement
- Growing reliance on commercial off-the-shelf technologies
- Increasing attention to consumer confidence and privacy concerns created by smarter technologies
- Increasing reliance on external providers for business solutions and services, which introduces additional cyber and physical reliability challenges

Energy Markets and Operations

- Increasing interconnection of business and control system networks
- Further growth in dynamic, market-based system control
- Increasing need for real-time business information
- Increasing use of distributed and alternative energy sources
- Increasing reliance on the telecommunications industry and the Internet for communications
- Increasing reliance on natural gas for electricity generation
- Increasing interdependencies with other critical infrastructure (e.g., transportation systems and water)

Regulations and Standards

- Increasing regulations and mandatory standards
- Evolving regulations and standards

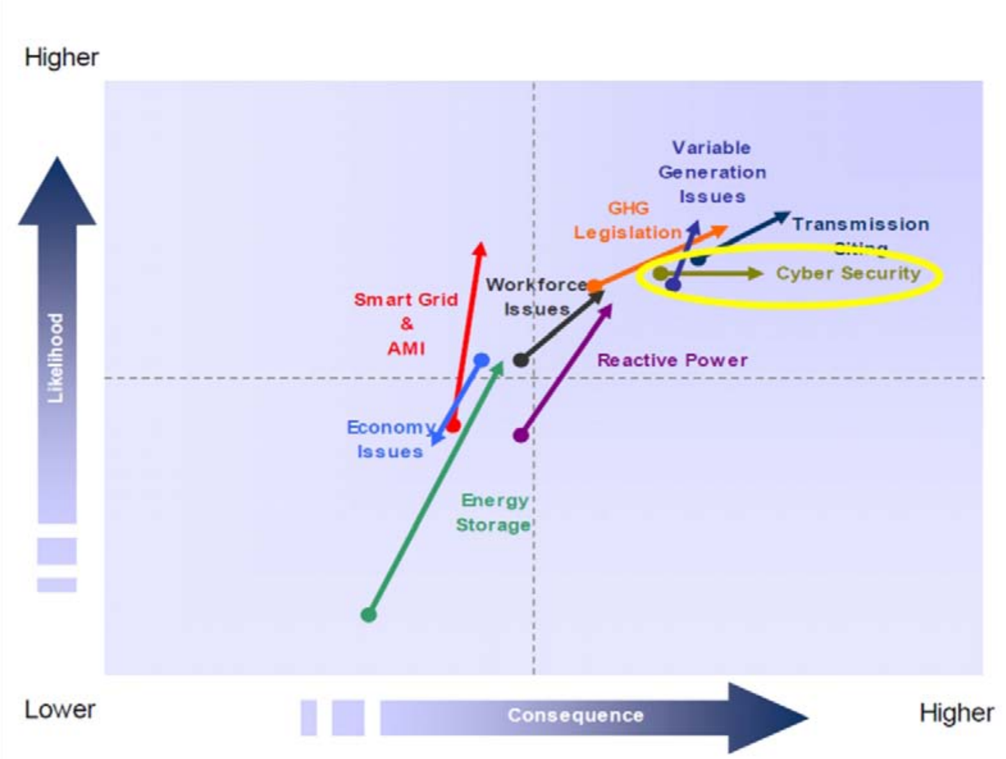
Technology and Telecommunications

- Increasing convergence of information technology and telecommunications functions
- Increasing use of commercial off-the-shelf technologies
- Increasing system interconnectivity
- Increasing use of Internet Protocol (IP)-based communications
- Increasing reliance on wireless communications
- Increasing use of distributed intelligent devices and controls
- Increasing number of digital access points in energy delivery communication networks
- Continuing need for remote access
- Increasing adoption of authentication and encryption techniques
- Increasingly sophisticated detection and alarming mechanisms
- Increasing use of mobile devices in energy infrastructure environments

Threats

- Increasing advanced cyber attack capabilities
- Escalating criminal enterprise, terrorist, and nation-state threats

Exhibit 3.3 Cybersecurity is One of the Top Emerging and Standing Issues Facing the Electric Sector over the Next 10 Years



Source: 2009 NERC Long Term Reliability Assessment, October 2009[23]

4. Framework for Achieving Energy Delivery Systems Cybersecurity

The energy sector's vision of resilient energy delivery systems guides decision making about policies, standards, research, market development, and procurement required to minimize energy disruptions due to a cyber incident. When it was first developed in 2006, the sector's shared vision affirmed the urgent need to protect energy delivery systems from cyber assault and aligned sector-wide resources to meet that need. It recognized that protecting against every potential intrusion is impossible and focused on building an infrastructure able to continue critical operations in the face of a cyber incident.

The Vision

Through the roadmap development and implementation process, the energy sector developed a strategic framework to addresses the urgent security concerns of today's systems while preparing for the needs of tomorrow. The sector's vision is as follows:

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

What has changed? After examining their efforts and lessons learned, energy sector partners updated the sector's vision of the future. Updates to the 2006 vision are identified in ***bold italics*** and include the following:

- ***Resilient energy delivery systems*** encompass more than securing control systems; they also include ***securing smart technologies*** (e.g., smart meters) and impact physical security at the ***cyber-physical interface***. By adding "resilient" to the vision, the sector emphasizes the need for survivability and continuity of critical services.
- ***Sustaining critical functions*** supports a risk management approach for operational reliability and national security. Critical functions include any energy delivery system operation, task, or service that, were it to fail or be compromised, would produce major safety, health, operational, or economic consequences. The criticality of a function is determined by the severity of consequences resulting from its failure or compromise. Such functions may include controlling operating circuit breakers, managing pipeline pressure, or ***managing energy consumption***. Also, the use of smart meters that interface with consumer electricity use makes the ***protection of private consumer information*** increasingly important in an organization's risk management approach. A risk management approach allows each organization to customize the prioritization of the risk of losing a critical function to the potential consequences specific to that organization's energy delivery systems. Risk management will enable industry and government partners to prioritize their investment toward efforts that effectively protect the public, customers, corporate assets, and shareholders.
- Energy delivery systems must survive a ***cyber incident***, not just an ***intentional cyber assault***. ***Manmade unintentional cyber incidents*** can be caused by inattentive or untrained employees, software upgrades, maintenance procedures, and equipment failures that inadvertently disrupt systems or corrupt data. Intentional threats include both targeted and untargeted attacks.[24] A ***manmade deliberate threat*** occurs when a group or individual with malicious intent

(e.g., disgruntled employees, hackers, nation-states, or organized crime) attacks a specific system or cyber-based critical infrastructure.[25] An ***untargeted attack*** occurs when the intended target of the attack is uncertain, such as when a virus, worm, or other malicious software is released on the Internet with no specific target.[26]

- Energy sector stakeholders expect to ***realize their vision by 2020***. The timeframe has been extended from 2015 to ***2020*** because the energy delivery systems threat and technology environment will continue to be dynamic and uncertain, requiring a long term view of the future.

What has not changed? The updated vision continues to emphasize critical functions, as it is neither practical nor feasible to protect all energy assets from a hazardous incident. The roadmap provides a strategy that articulates the essential goals needed to improve energy sector cybersecurity. It will enable industry, vendors, and government partners to prioritize investments toward efforts that effectively protect the public, customers, corporate assets, and shareholders. However, due to the dynamic, uncertain future of energy delivery systems, it is likely that the time frames, strategies, goals, milestones, and priorities will require updates in the future to evolve with the growing needs of the energy sector.

Energy Delivery Systems Security Goals

Achieving the vision is a sizable challenge. As the understanding of energy delivery system risks has evolved, so too have the methods used to measure, assess, and manage risk. Building on the solid foundation of the 2006 framework, this roadmap recognizes the need for establishing a culture of security, assessing and monitoring risk, developing and implementing new protective measures to reduce risk, managing incidents, and providing resources necessary to continuously sustain security improvements as new threats emerge and operating environments advance. While the culture of security strategy has been added to focus resources on the human element, the other strategies are similar in scope to the 2006 Roadmap but have been revised for clarity. Each of these strategies is focused on a specific goal, shown in Exhibit 4.1.1 and described below. This framework provides a logical path forward for industry, government, and academia to realize and sustain the vision.

- **Build a Culture of Security.** *Cybersecurity practices are reflexive and expected among all energy sector stakeholders.* Extensive dialogue about the meaning of security and the consequences of operating under certain levels of risk is ongoing, by various means, among citizens and stakeholders. A culture of security, integrated with reliability practices, ensures that sound risk management practices are periodically reviewed and challenged to confirm that established security controls remain in place and that changes in the energy delivery system or emerging threats do not diminish their effectiveness.

- **Assess and Monitor Risk.** *Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators.* Companies have a thorough understanding of their current security posture, enabling them to continually assess evolving cyber threats and vulnerabilities, their risks, and responses to those risks.

- **Develop and Implement New Protective Measures to Reduce Risk.** *Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident.* As security risks—including emerging threats—are identified or anticipated, protective measures are developed and applied to reduce system vulnerabilities and their consequences. These security solutions are built into next-generation energy delivery systems, and appropriate solutions are devised for legacy systems.

- **Manage Incidents.** *Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment.* Intentional cyber assaults can be sophisticated and dynamic, and any system can become vulnerable to emerging threats as absolute security is not possible. When proactive and protective measures fail to prevent a cyber incident, detection, remediation, recovery, and restoration activities minimize the impact of an incident on an energy delivery system and post incident analysis/forensics enable energy sector stakeholders to learn from the incident.
- **Sustain Security Improvements.** *Collaboration between industry, academia, and government maintains cybersecurity advances.* Maintaining aggressive and proactive energy delivery systems security over the long term requires a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders. Energy sector collaboration provides the resources and incentives required for facilitating and increasing resilience throughout the sector.

Projects, efforts, and initiatives that result from this roadmap should be tied to the milestones shown in Exhibit 4.1.1. In the years ahead, the sector must step up collaboration to enhance learning and technology development across roadmap efforts and optimize the use of all available resources. Exhibit 4.1.2 offers an example of the achievements that can be made by national laboratories, asset owners, and vendors as they collaboratively pursue roadmap goals.

Exhibit 4.1.1 Strategies for Achieving Energy Delivery Systems Cybersecurity

Vision	**By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.**				
Barriers	• **Cyber threats are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures** • **Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures** • **Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations** • **Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry** • **Weak business case for cybersecurity investment by industry** • **Regulatory uncertainty in energy sector cybersecurity**				
Strategies	**1. Build a Culture of Security**	**2. Assess and Monitor Risk**	**3. Develop and Implement New Protective Measures to Reduce Risk**	**4. Manage Incidents**	**5. Sustain Security Improvements**
Near-term Milestones (0–3 years) By 2013	1.1 Executive engagement and support of cyber resilience efforts 1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched	2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available 4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders 5.2 Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems
Mid-term Milestones (4–7 years) By 2017	1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available 1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics	3.2 Scalable access control for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	4.3 Incident reporting guidelines accepted and implemented by each energy subsector 4.4 Real-time forensics capabilities commercially available 4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
Long-term Milestones (8–10 years) By 2020	1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector
Goals	**Cybersecurity practices are reflexive and expected among all energy sector stakeholders**	**Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators**	**Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident**	**Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment**	**Collaboration between industry, academia, and government maintains cybersecurity advances**

Exhibit 4.1.2 Hallmark Cryptographic Serial Communication

By uniting a national laboratory, asset owner, vendor, and industry advisory board to pursue a Roadmap goal, the Hallmark project team brought the Secure SCADA Communications Protocol (SSCP) from a research idea to a commercialized product for electric and oil/natural gas customers, the SEL-3025. The commercial product was immediately successful, and the first lot scheduled for manufacturing sold out.

The SSCP safeguards serial supervisory control and data acquisition (SCADA) communications between remote devices and the control center and engineering dial-up access through message authentication and optional encryption. It encapsulates original messages with a unique header and authenticator that is cryptographically validated by the receiving device to ensure the message comes from a trusted source and is not altered in transit.

R&D in a National Laboratory

The concept of the SSCP was born in DOE's Pacific Northwest National Laboratory (PNNL), initially under funding from the Office of Naval Research, followed by DOE funding. The Roadmap's release in 2006 with the milestone of "widespread implementation of methods for secure communication between remote access devices and control centers" confirmed the industry need for the technology.

Collaboration Drives Commercialization

In 2007, DOE issued a competitive industry solicitation to develop and commercialize solutions aligned with the Roadmap through a three-year industry cost share. DOE and industry ultimately committed more than $10 million across five collaborative projects, including Schweitzer Engineering Laboratory's (SEL) Hallmark Project. For this effort, SEL teamed with PNNL to build the SSCP into commercial products, brought in CenterPoint Energy for field testing and validation, and convened an advisory board of industry experts to ensure relevance to end users.

The Hallmark Project work continues today, and the project team has grown to include a new vendor, Siemens Energy, and asset owner, ONCOR Electric Delivery. The current work focuses on development of centralized key management and using SSCP for user-based access control and accountability logging for dial-up serial access.

Industry Deployment

The project team built the SSCP into two solutions, released in June 2010:

- **Cryptographic Card**—SEL-3045, an electronic Federal Information Processing Standard (FIPS) 140-2 level 2 validated (pending as of January 2011) hardware card that runs the SSCP, designed for original equipment manufacturers to accelerate integration of the SSCP technology into new products.
- **Bump-in-the-Wire Link Module**—SEL-3025, a hardware and firmware platform (integrating the Cryptographic Card) that secures existing serial communication links.

The Hallmark team is also working to integrate the SSCP specification into IEEE Standard P1711 for cybersecurity of serial communication links.

Strategies for accomplishing the five goals presented in Exhibit 4.1.1 are detailed in Exhibits 4.2.1, 4.3.1, 4.4.1, 4.5.2, and 4.6.1. Each strategy presents challenges that must be overcome, requires completion of milestones on an established timetable, and prompts a set of priorities toward meeting the goal for each strategy. These priorities represent examples of potential projects, initiatives, and efforts that were identified by energy delivery system experts (see Appendix C) and are not intended to be exhaustive.

Strategy: Build a Culture of Security

People are vital to sustaining critical functions in large technical systems, particularly in the face of system volatility or stress.[27] A culture of security promotes working in a secure manner, rewards sharing of security risk information, and encourages a sustained level of attentiveness at the individual, small group, and organizational levels, and across many organizations. Extensive dialogue should be ongoing, by various means and with sufficient breadth and depth of reach to affect the attitudes and behaviors of citizens, policymakers, and stakeholders about the meaning of energy delivery systems security and the consequences of operating under certain levels of risk. Sound risk management practices should be periodically reviewed and tested to confirm that established security controls remain in place and changes in the energy delivery system or emerging threats do not diminish their effectiveness. A culture of security will ensure that sound security practices permeate among all stakeholders and become reflexive and expected.[28] An overview of the milestones, barriers, and priorities to meet the milestones for building a culture of security is shown in Exhibit 4.2.1.

Barriers to Achieving the Goal

Over the next five years, energy companies will face a critical shortage of engineers and skilled craft workers. For example, about 45% of engineers—7,000 in electric utilities alone—are predicted to retire or leave for other reasons. Compounding that, two to three times more power engineers may be needed to satisfy the needs of the entire economy,[29] and future operations will require broader skill sets than those prevalent today.

Limited knowledge, understanding, and appreciation of energy delivery systems security risks inhibits security actions within the energy sector. There is also an incomplete understanding of the cost of decisions and system resilience in terms of failure modes and vulnerabilities. Current risk assessment capabilities fall short of determining the effects of each cost decision on system resilience in terms of failure modes and vulnerabilities.

While standards have helped to raise security to a baseline level across the sector, some standards remain unclear or too broad, or may have prompted utilities to use less advanced security measures to meet requirements. In addition, a rapidly changing risk environment means standards compliance today may not be sufficient tomorrow.

Exhibit 4.2.1 Building a Culture of Security

STRATEGY: Build a Culture of Security
GOAL: Cybersecurity practices are reflexive and expected among all energy sector stakeholders

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
1.1 Executive engagement and support of cyber resilience efforts 1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched	1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available 1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry

Barriers

- Lack of highly educated staff with broad skill sets to manage future operations
- Insufficient training of vendor staff in the techniques of designing and programming secure systems/applications
- Limited knowledge, understanding, and appreciation of energy delivery systems security risks inhibits action
- Belief that security standard compliance is sufficient for cybersecurity of energy delivery systems inhibits adoption of additional security measures
- Secure coding practices are not uniformly enforced
- Incomplete understanding of the cost of decisions and system resilience in terms of failure modes and vulnerabilities
- Patching/fixing vulnerabilities in energy delivery systems can create new cyber risks

Priorities

Support

- **Create high-level meetings with DOE and DHS secretaries and C-level executives to gain support from the top**
- **Develop a roadmap to address legal aspects of collaboration, leveraging existing and forthcoming agreements**
- Develop and launch a roadmap outreach plan to increase awareness and garner support for roadmap implementation efforts
- Conduct analysis of the incentives and benefits of implementing security beyond mandatory standards to help fortify the business case
- Leverage information from 2009 American Recovery & Reinvestment Act projects to accelerate progress in developing cybersecurity solutions

Best Practices

- Identify and disseminate best practices for connecting secure and resilient energy delivery systems and business networks (e.g., deploy and properly configure firewalls, intrusion detection systems, and antivirus solutions at all appropriate locations)
- Identify and implement best practices for managing the risk at the cyber-physical interface of field equipment and control center risk
- Develop best practice periodicals that focus on techniques, practices, procedures, and polices for energy sector operators, engineers, and technical staff to encourage widespread adoption of best practices
- Develop a program to independently validate that components and systems conform to best practices

Progress

- **Establish methodology for quantifying roadmap participation, including total number engaged and percentages by group**
- **Develop a voluntarily populated matrix of vendors and asset owners conducting vulnerability assessments and applying best practices**
- Measure progress of adopting certain standards and measure performance of those standards
- Develop, publish, and provide training on a roadmap report card
- Create a dashboard for presenting progress
- Measure awareness including people, processes, systems, and solutions
- Measure the number of professionals trained in security and whether the training was effective
- Track outcomes of public-private partnerships, (e.g., products created and deployed)

Vulnerability Management

- Establish and implement vulnerability and patch management programs and policies (e.g., workarounds, defense in depth, and monitoring)

Education

- **Increase executive understanding of energy delivery system cybersecurity issues and risks**
- Create a culture of responsible vulnerability disclosure; exchange an “access to” kit with an agreement to disclose
- Expand offering of undergraduate curriculums in academic institutions in energy delivery systems security, including scholarships, internships, and research grants
- Significantly increase the number of graduate students in energy and information systems engineering
- Integrate cybersecurity awareness, education, and outreach programs into energy sector and vendor operations
- Incorporate cybersecurity into personnel performance evaluations
- Empower the future workforce to adopt good cybersecurity security habits at an early age
- Promote the benefits of a career in cybersecurity for energy delivery systems

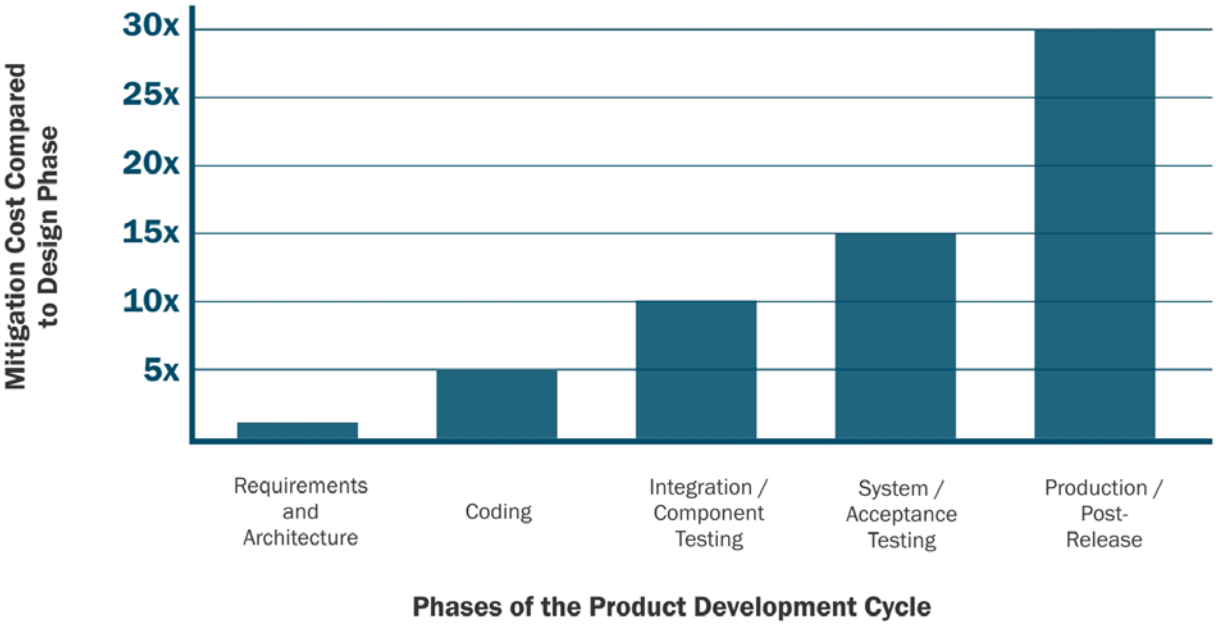
Certification

- Develop an operational security readiness certification program
- Develop a smart grid security professional certification program
- Develop a professional certification program on cybersecurity for energy delivery systems for vendors and other solution providers
- Develop a certification program that shows results of vulnerability testing and secure coding practices employed

Bolded text indicates the top priority efforts identified by participants at the September 2009 Roadmap Update Workshop

Many vendors have insufficient training programs for their staff in the techniques of designing and programming secure energy delivery systems and applications. Secure coding practices are not uniformly enforced. As shown in Exhibit 4.2.2, a study by NIST[30] estimated that the cost of fixing a software vulnerability discovered during acceptance testing is about 15 times greater than the cost of fixing it during the design phase. For example, a vendor that reacts to problems discovered by late-cycle vulnerability assessments or incident reports consumes significant resources to quickly mitigate them or suffers delays in releasing the new product. Experience has also shown that patching a newly integrated system takes time, because users must be notified and patches must be tested to prove that they will not compromise normal energy delivery systems functionality prior to implementation.

Exhibit 4.2.2 Costs Significantly Increase when Security Vulnerability is Discovered and Mitigated Late in the Security Design Cycle



Source: Microsoft SDL: Return On Investment, September 2009

Priorities to Overcome Barriers and Achieve Milestones

Building a culture of security requires security to be cost effectively built into the design, installation, operation, and maintenance of energy delivery systems. Increased executive engagement is needed to help decision makers better understand energy delivery systems security issues. This knowledge will enable government and industry decision makers to make resource investment decisions for resilience that are appropriate to their organization. A high-level meeting among the appropriate Federal Agency Secretaries (e.g., DOE, DHS) and senior executives is a possible first step to gaining support from the top.

Best practices in safe code development and integration can be promoted by the energy sector. Vendors can employ best product development practices. Although these practices may not eliminate all software vulnerabilities, promoting a security culture has shown to make a difference in the security levels of products. Companies—both vendors and owners—who have embraced a culture of security have found the cost of code audits and associated code changes to be very cost effective versus fixing single vulnerabilities as they are discovered externally. In addition, fewer security patches for deployed systems will enhance customer service and loyalty. Asset owners can actively inquire about and monitor security notices and implement security patches or compensatory requirements as quickly as possible.

As many of the most experienced power systems operators begin to retire, the energy sector needs dedicated knowledge and skill transfer programs to retain the centuries of experience that these workers possess. As the energy infrastructure becomes increasingly automated and complex, information technology and security will become valuable backgrounds for system operators and engineers. Industry can work directly with universities to develop curricula that channel skilled workers into promising career paths and build a strong pipeline of energy delivery system workers knowledgeable in cybersecurity that significantly increases in the next five years.

Select universities are now expanding their power system curricula to address cybersecurity. Until now, undergraduate and graduate programs focused strictly on the technical aspects of power generation and delivery. The advent of the smart grid is changing those requirements. Studies in power system analysis and design are beginning to merge with cybersecurity to stay on pace with grid modernization and other infrastructure advancements in the oil and natural gas sectors.

Strategy: Assess and Monitor Risk

Understanding the full depth and breadth of the security posture of energy delivery systems allows operators to determine and prioritize appropriate corrective actions quickly and effectively. To gain this understanding, reliable and widely accepted security metrics are needed, as well as tools and methodologies for measuring and assessing both static and real-time security states to support risk management decision making. Because of the unique configurations of many control systems, owners need the tools to conduct self-assessments. The industry eventually needs security state monitoring tools that trigger autonomic (i.e., quick device response) and/or dynamic (i.e., can evolve) corrective actions within the control system, while allowing operators to override them, if necessary. A vigilant culture of security will motivate the stakeholder base to continually assess evolving cyber threats, their risks, and responses to those risks.[31] An overview of the milestones, barriers, and priorities to meet the milestones for assessing and monitoring risk is shown in Exhibit 4.3.1.

Barriers to Achieving the Goal

While many asset owners and operators are performing self-assessments of their control systems, the methods and metrics they use continue to vary across the sector. Without consistent criteria or metrics, benchmarking and comparing energy delivery systems risk and evaluating the impact of security efforts is difficult. However, gaining broad agreement among stakeholders continues to be a significant challenge. Quantifying risk is also problematic when the energy sector faces rapidly changing threats that are difficult to predict and have consequences that are hard to demonstrate. Also, the increasing complexity of and interconnections with enterprise, telecommunications, environmental, safety, and smart networks can introduce new vulnerabilities.

An ambiguous and uncertain threat is difficult, if not impossible, to quantify. While research is under way to develop advanced tools and methodologies to provide a deep analysis of malevolent attack vectors and resulting consequences, commonly used risk analysis capabilities are limited to the survey and analysis of critical assets and evaluation of the impact of their compromise or loss of availability. Understanding and properly categorizing the threat is a major challenge. In addition, the ability to assess the extent to which a risk has been mitigated remains a difficult task.

Processing vast quantities of disparate data from a variety of sources (e.g., business, information, production, delivery, consumer, market, and other energy systems) and levels of granularity (e.g., subseconds to months) into actionable and timely knowledge that provides situational awareness of cybersecurity posture is a significant challenge. As more intelligent energy delivery systems control capabilities are extended across North America, the increasing complexity of the interfaces between these sources will further compound the problem. Increasing interconnections with enterprise, telecommunications, environmental, safety, and smart networks can introduce vulnerabilities that can propagate across multiple domains.

Priorities to Overcome Barriers and Achieve Milestones

To achieve real-time situational awareness and inform appropriate response, advanced technologies are needed that identify, acquire, correlate, analyze, and display cyber and physical security-related data from all levels of the energy delivery systems architecture (device, system, and network) and across the cyber-physical domains. A real-time, visually intuitive display of the results of security-related data correlation and analyses is needed to maintain situational awareness of the system's real-time energy delivery systems cyber and physical security posture and enable human operators to prioritize mitigation options.

These capabilities can lead to techniques that show the impact of communication failures on energy delivery, the potential effects of energy disruptions on digital communications, and how a simultaneous combination of failures in each of the systems might impact the system as a whole. A rigorous approach is needed to identify and highlight these key interdependencies across all critical common infrastructure elements.[32] Error-filtering techniques that prioritize error reporting can enhance situational awareness by selecting those errors that convey actionable information and suppressing those errors that have limited or no operational value.

New methods are needed to measure and identify the scope of a cyber attack and the available dynamic cyber threat response options in a way that can serve as a decision support tool for human operators. Provable methodologies are needed to quantify trustworthiness and risk within a component, within systems, and within a "system of systems." Advanced tools and technologies based on quantitative risk notions can provide deeper insights to determine the appropriate level of security. Additionally, new techniques and tools are needed to evaluate the impact of proposed technologies, security measures, and network topologies prior to implementation in an operational environment.

Exhibit 4.3.1 Assessing and Monitoring Risk

STRATEGY: Assess and Monitor Risk

GOAL: Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	2.2 Majority of asset owners baselining their security posture using subsector specific metrics	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available

Barriers

- Risk factors (threat, vulnerability, and consequence) are not consistent and widely accepted by all energy sector stakeholders
- Baseline security postures of energy delivery systems in operational settings are not consistent and widely accepted by all energy sector stakeholders
- Threats, vulnerabilities, and consequences are uncertain and ambiguous factors of risk, which need to be addressed to manage risk

- Threats change with time and are hard to quantify, making it difficult to understand and properly categorize threat actors and timing of potential attacks
- Difficult to provide actionable and timely information and visualizations of security posture from vast quantities of disparate data from a variety of sources and levels of granularity
- Increasing complexity and interconnections with enterprise, telecommunications, environmental, safety, and smart networks can introduce the vulnerabilities of these systems to energy delivery systems

Priorities

Risk Factors and Levels

- **Develop key metrics to describe relative security posture before and after deployment of security solution**
- **Develop and achieve a consensus on scientifically defensible terms and measures for testing and baselining energy delivery systems security**
- Describe energy delivery system cyber risk levels according to current mitigation need
- Establish levels of risk for energy asset owners and develop a strategic implementation plan to gain widespread adoption
- Quantify trustworthiness and risk within a component, system, and "system of systems"
- Develop methods to better identify and characterize threats
- Develop appropriate threat actor models (expertise/motivation/attack vector)
- Develop deceptive reasoning algorithm(s) to counter plausibility, assertions, and threat hypotheses
- Characterize a set of threat scenarios and metrics for assessing energy delivery systems risk
- Develop industry attack surface metrics released annually with industry agreed upon parameters
- Define security and results in terms of prevent, detect, and respond

Risk Methodologies and Tools

- Employ resources for assessing energy delivery systems risk using consistent criteria within the context of each energy subsector
- Assess energy delivery systems risk using consistent criteria for the energy sector as a whole to help the sector and individual entities baseline their security posture
- Develop risk assessment tools that include methodologies for assessing vulnerabilities, frameworks for prioritizing control measures, and means for justifying costs
- Develop tool sets for asset owners to assess and benchmark energy delivery systems risk
- Develop methods to measure risk based on uncertain threats
- Create a risk-level matrix that balances threat, vulnerability, and consequence
- Develop engineering decision making tools for optimizing security
- Develop a distributed security state estimator that is tailored to multiple users and used by autonomous agents
- Develop time-to-deploy models for risk mitigations based on asset inventory
- Develop data driven ability to determine how and which vulnerabilities and threats should be addressed; track financial losses resulting from cyber incidents; and develop ability to trace vulnerabilities to financial losses

Security State Monitoring

- **Develop real-time security status visualization tools to baseline security states and compare security posture after implementation of new solutions**
- **Develop modeling and simulation tools that have dynamic automated capabilities to discover implication of complexities and inform risk management decisions**
- Develop real-time security state monitoring of energy delivery network support systems (uninterruptable power supply, environmental, emergency power, safety, and telecommunication systems)
- Develop real-time security state monitoring of new and legacy system applications
- Develop visualization technologies that integrate and correlate multiple data streams
- Create an upgradable dashboard for presenting security posture benchmarks of asset owner energy delivery system applications
- Develop methods to reduce data quantities to actionable levels
- Develop modeling and simulation tools for device management and control
- Develop network management/control at mesh-network (smart grid) scale (millions of devices)
- Develop tools for visualizing smart grid functions at transmission control centers
- Develop large-scale, high-resolution, multi-infrastructure modeling and simulation tools

Bolded text indicates the top priority efforts identified by participants at the September 2009 Roadmap Update Workshop

Strategy: Develop and Implement New Protective Measures to Reduce Risk

As security problems are identified, known protective measures can be applied and new solutions developed to make legacy and next-generation energy delivery systems more resilient to a cyber incident.[33] A resilient energy delivery system will continue to perform critical functions from the start of an incident, while under duress, and as it quickly returns to normal operations after the incident. A resilient energy delivery system inherently requires security against all reasonable hazards when it is first designed, and ensures an integrated and balanced security approach spanning the entire life cycle of the system.

To harden energy delivery systems, security tools, procedures, and patches for fixing known security flaws and retrofit security technologies must be added on over time and in a way that does not degrade system performance. A wide variety of communication media—ranging from leased lines, wireless, and power line communication to the Internet—is used to transfer data between remote devices and control centers and across many domains, such as corporate, market, service provider, customer, transmission, pipeline, refining, and generation networks. Such communication media should incorporate various security measures, including device and application authentication, access control, redundancy and fail over for continued operation, and encryption for privacy and leakage of sensitive information.

The most comprehensive security improvements are realized with the development and adoption of next-generation energy delivery system architectures that incorporate advanced interoperable components, which are inherently secure and offer enhanced functionality and performance. By 2020, these systems will provide “defense in depth” with built-in, end-to-end, interoperable, and upgradable security and continue operating in a degraded condition during a cyber attack. An overview of the milestones, barriers, and priorities to meet the milestones for developing and implementing new protective measures to reduce risk is shown in Exhibit 4.4.1.

Barriers to Achieving the Goal

System architectures are widely distributed and incredibly complex[34] (see Exhibit 4.4.2). It is challenging to secure tens of millions of credentials and keys used to secure cryptographic information across the millions of remote field devices, substations, and meters, especially with current processing capabilities that have limited space and computational power. In addition, embedded electronics in the components are sometimes manufactured by untrusted entities. Cybersecurity for home area networks (HAN) and AMI components are located in areas that are readily accessible and vulnerable to physical tampering or misuse. These systems must be designed and constructed to be cost-competitive yet secure, which requires an appropriate balance between costs and security.

Some security solutions have the potential to introduce serious operational issues. Traditional information technology solutions can disable or shut down energy delivery systems because the operating performance requirements are very different. Poorly configured security tools have slowed critical data communications to the point where energy delivery systems become inoperable. It is difficult to deploy technologies that are both scalable and interoperable and can provide secure interorganizational interaction in real energy environments. New technologies must respect the real-time operation imperative of the energy delivery system, and must not introduce unacceptable latency or degrade or disrupt service. In addition, false-positive and false-negative error reports impede situational awareness and must be aggressively eliminated.

Exhibit 4.4.1 Developing and Implementing New Protective Measures to Reduce Risk

STRATEGY: Develop and Implement New Protective Measures to Reduce Risk

GOAL: Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	3.2 Scalable access control solutions for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented

Barriers

- Difficult to provide quality data and robustness without introducing latency issues
- Performance/acceptance testing of energy delivery systems, networks, architectures, and components without disrupting real-time operations is difficult
- System architectures are widely distributed and complex
- Complexity of energy delivery systems increases exponentially with an increase in number of nodes
- Protective systems are not as fast as attack systems
- Security upgrades hard to retrofit to legacy systems, may be costly, and may degrade system performance

Priorities

Resilience Testing and Validation

- Develop security acceptance testing capability for evaluating security robustness of next-generation energy delivery systems, networks, architectures, and components; including architectures and guidelines for the capability
- Develop tools for automated code review in both static and runtime environments
- Develop a real-time adaptive security infrastructure that makes authorization and policy management an on-demand service for all systems and devices
- Develop tools to evaluate candidate architectures, concepts, and protocols before devices are built
- Develop security validation test beds

Systems

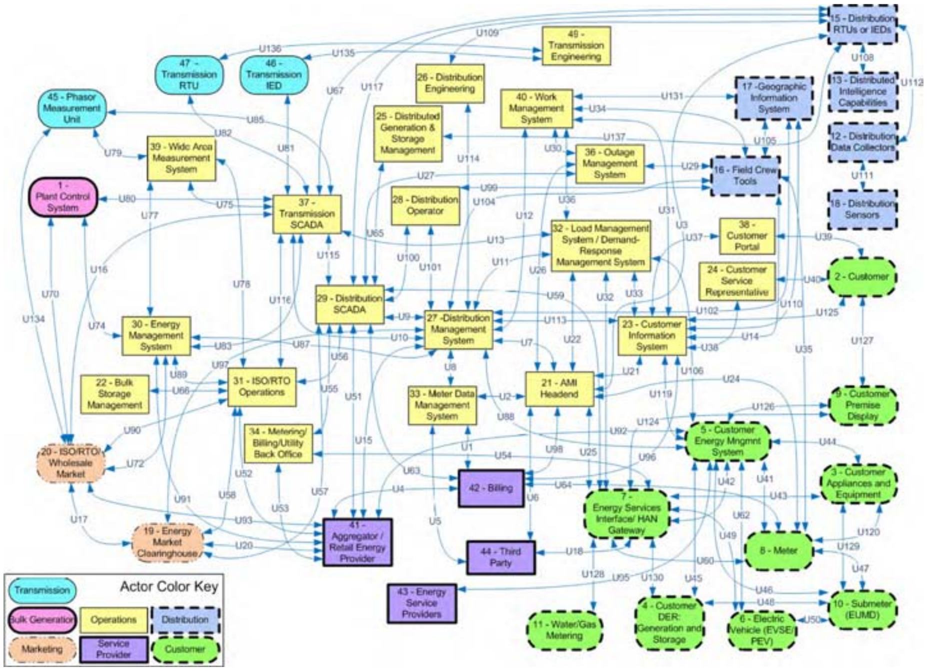
- **Developers and operators implement a systems approach to building, integrating, and operating resilient energy delivery systems**
- **Develop a nonbootable patching (hot patching) capability for the overall system**
- **Leverage existing robust platform-level solutions, such as those used in military applications**
- Develop safe harbor designs to prevent cascading failures
- Develop provisioning guidance to managing change in the configuration of energy delivery system environments
- Develop tools for secure change management across widely distributed systems
- Future-proof security capabilities
- Develop methods to streamline security administration
- Define security life cycle procurement specifications to guide vendor product development
- Improve understanding of interoperability requirements and needs

Access and Communications

- **Adopt agreed upon, available intrinsic data and source integrity in SCADA/EMS protocols to develop control systems that will inherently respond to and defend themselves against internal and external threats**
- **Develop techniques to provide explicit, managed communications trust**
- Develop software architectures that can isolate the impact of exploited vulnerabilities
- Develop adaptive assured quality of service protocols to support real-time data delivery
- Develop advanced cryptographic key management methods for securing millions of devices
- Develop trusted platform modules and trusted network connections for real-time communications that are nonproprietary
- Develop technology for one-over-one configuration changes by network administration (2-key rule) for insider assurance
- Develop end point security to protect against insider threat
- Develop scalable built-in security for embedded operating systems
- Develop capability to integrate new security technologies at the micro-level
- Develop white list capabilities for applications and communications
- Improve understanding of interoperability requirements and needs
- Develop cybersecurity solutions for the cyber-physical interface
- Continue to develop emerging technologies that meet security and privacy requirements

Bolded text indicates the top priority efforts identified by participants at the September 2009 Roadmap Update Workshop

Exhibit 4.4.2 Architectures Such as the Smart Grid Example Shown Here, are Increasingly Complex and Interconnected across Multiple Domains


15 - Distribution RTUs or IEDs
49 - Transmission Engineering
47 - Transmission RTU
46 - Transmission IED
26 - Distribution Engineering
40 - Work Management System
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
45 - Phasor Measurement Unit
25 - Distributed Generation & Storage Management
12 - Distribution Data Collectors
39 - Wide Area Measurement System
36 - Outage Management System
16 - Field Crew Tools
1 - Plant Control System
28 - Distribution Operator
37 - Transmission SCADA
18 - Distribution Sensors
32 - Load Management System / Demand-Response Management System
38 - Customer Portal
24 - Customer Service Representative
2 - Customer
29 - Distribution SCADA
27 -Distribution Management System
30 - Energy Management System
23 - Customer Information System
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
9 - Customer Premise Display
34 - Metering/ Billing/Utility Back Office
5 - Customer Energy Mngmnt System
20 - ISO/RTO/ Wholesale Market
42 - Billing
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
19 - Energy Market Clearinghouse
41 - Aggregator / Retail Energy Provider
8 - Meter
44 - Third Party
43 - Energy Service Providers
4 - Customer DER: Generation and Storage
11 - Water/Gas Metering
6 - Electric Vehicle (EVSE/ PEV)
10 - Submeter (EUMD)
U109
U136
U135
U67
U117
U85
U82
U79
U81
U114
U27
U99
U104
U80
U75
U77
U65
U100
U101
U115
U16
U78
U116
U70
U134
U74
U9
U10
U83
U87
U56
U97
U89
U66
U8
U55
U51
U90
U15
U1
U72
U52
U63
U4
U91
U58
U57
U53
U93
U17
U20
U5
U131
U34
U137
U30
U105
U108
U112
U111
U29
U36
U31
U12
U3
U37
U39
U13
U11
U26
U40
U59
U32
U33
U110
U102
U125
U113
U7
U22
U14
U38
U35
U127
U21
U106
U24
U2
U119
U88
U126
U124
U92
U44
U98
U25
U54
U96
U42
U41
U64
U6
U43
U62
U49
U120
U129
U18
U60
U47
U128
U95
U130
U45
U46
U48
U50
Actor Color Key
Transmission
Bulk Generation
Operations
Distribution
Marketing
Service Provider
Customer

Priorities to Overcome Barriers and Achieve Milestones

To support resilient and robust architectures, attack-resistant platforms, including field equipment, front-end processors, real-time operating systems, and other systems are needed. Technology advancements can include the development of hardened field devices, such as programmable logic controllers and remote terminal units, or security appliances that can be installed with each critical asset/field device to protect it from malicious attack, offering another layer of defense. While energy delivery systems deployed across the electricity and oil and natural gas sectors have similar features, each application has unique characteristics that require fine-tuning and careful configuration. As such, secure communication architectures are needed within the context of each subsector, and they must be hardened against cyber attack and able to continue operating in a degraded condition during a cyber attack. Innovative, graded security architectures comprising built-in security techniques and methodologies are needed to ensure long-term security while keeping up with a highly dynamic and fast-paced technology environment.

Hardening legacy systems requires the implementation of a patch management program to mitigate the risk of known vulnerabilities. To shorten the time between discovery and patching, a nonbootable patching (hot patching) capability for the overall system should be developed. While some hot patching capabilities currently exist, they cannot be applied system wide. To realize the full potential of this capability, hot patching techniques must be deployable throughout the system without harming operations.

It is important to have secure operating systems (OS) as part of a robust real-time platform. Prior to deployment, these systems must be trusted to perform as intended. Existing platform-level solutions, such as those used in military applications, can be leveraged for potential use in the energy sector.

Also, it is important to consider needs prompted by smart grid technologies. Risk assessment, modeling, and simulation tools that have dynamic automated capabilities are needed to discover the implication of new complexities, design and implement a smart grid with built-in security, and inform engineering decisions to optimize security.

Advancements in secure communications, such as perimeter security technology that can implement rules to enforce the behavior of energy delivery system traffic, examine the details of energy delivery system packets at the application level, and/or offer proxy services for these protocols are needed to secure communications between devices across all domains and at all levels of energy delivery systems. A major challenge is ensuring that these solutions respect the real-time operation imperative of the energy delivery system and do not introduce unacceptable latency or degrade reliability.

Secure remote access control is becoming increasingly important. Technologies are needed to eliminate unauthorized attempts to access resources within the energy delivery systems environment, including remote field devices. For example, technologies can be focused on authenticating users and processes and detecting and preventing unauthorized actors from controlling the system. Another viable approach is to investigate role-based access control and secure entitlement management schemes that enforce least-privilege access to energy delivery system resources.

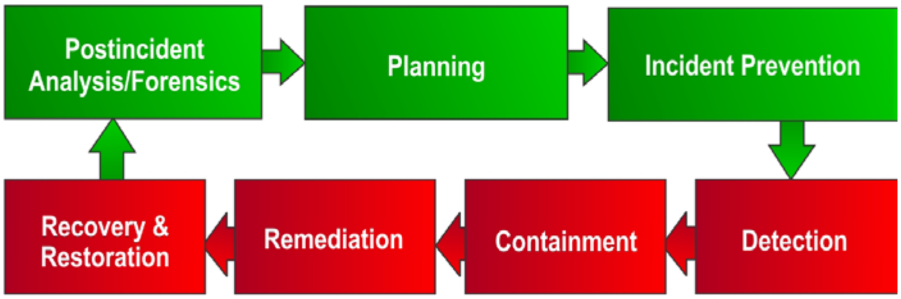
To meet the real-time requirements of energy systems, strategies can be developed to minimize and make predictable the impacts that security solutions such as encryption, authentication, and re-keying will have on the timing of system communications. Hardened platforms, including field equipment, front-end processors, real-time operating systems, and other systems that support resilient and robust energy delivery system architectures are needed. In addition, advanced capabilities are needed to quantify the robustness and survivability of advanced platforms, systems, and networks and the effectiveness of various architectures, policies, or changes.

A means to securely exchange cryptographic keys is needed that does not hinder existing power system information and communication systems monitoring for reliability and security requirements. Technologies that are scalable and can effectively manage large sets of cryptographic keys for large, geographically dispersed, complex systems of heterogeneous devices and communications media are needed. Likewise, techniques for restoring trust after a cyber intrusion while maintaining functionality will be increasingly important as more and more components are built from untrusted sources. Additionally, consumer privacy and the confidentiality of individual participants in smart grid technologies is a new and growing concern for the industry.

Strategy: Manage Incidents

Managing cyber incidents should include several elements that are both proactive and reactive in nature to ensure that the organization is prepared to respond and can act swiftly and effectively when an incident occurs.[35] Proactive elements include planning, incident prevention, and lessons learned from post-incident analysis/forensics, as shown in green in Exhibit 4.5.1. Reactive elements center on detecting and managing an incident once it occurs. These elements, shown in red in Exhibit 4.5.1, are typically carried out under severe time constraints and high visibility.

Exhibit 4.5.1 Key Elements of Effective Incident Management



Source: DHS Control Systems Security Program

Detection, containment, remediation, recovery and restoration, and post incident analysis/forensics are the focus of the managing incidents strategy. Planning and incident prevention are covered by the other roadmap strategies.

Cyber intrusion tools are sophisticated and dynamic, and any system can become vulnerable to emerging threats. Despite the sector's best efforts, cyber intrusions will occur. To successfully limit the magnitude and duration of a potential crisis and do it in a competitive market environment, energy sector stakeholders need to embrace strategies that not only make energy delivery systems more resilient, but also allow humans to operate with resilience during a cyber incident. For example, today's power systems have carefully planned and thoroughly evaluated responses to N-1 physical contingencies, such as the loss of a generator or transmission component, so that the power grid remains resilient and continues to operate in a degraded state when the function of a physical component has been compromised. Similar response processes, organizational structures, and supporting advanced technologies must be in place so that the energy infrastructures remain resilient and continue to operate in a degraded state when cyber components have been compromised. By 2020, energy sector stakeholders will have the ability to mitigate a cyber incident as it unfolds, have resources in place to get back to normal as quickly as possible, and have the means to adapt according to lessons learned from the incident. An overview of the milestones, barriers, and priorities to meet the milestones for managing incidents is shown in Exhibit 4.5.2.

Barriers to Achieving the Goal

The sector's protection and forensic systems cannot adapt and respond as quickly as the attack tools that hackers have access to today. For example, the nature of attacks, the number of attempts, and the around-the-clock timing of the attempts create an environment where manual observation is very difficult, if not impossible. In addition, there are no easy methods available today to log and preserve the state of a real-time operating system's kernel at the time of an attack. At the same time, some attempts to log and preserve too much data have resulted in overwriting or destroying useful information. The destruction of information and unclear roles and responsibilities among stakeholders limits lessons learned after a cyber incident.

The increasing sophistication of cyber intrusion tools and complexity of energy delivery systems makes it difficult for asset owners and operators to recognize an incident once it is under way. The use of automated intrusion detection systems (IDS) and applications have the potential to introduce serious operational issues. Traditional information technology solutions can disable or shut down energy delivery systems because the operating performance requirements are very different. Poorly configured IDS and antivirus tools have slowed critical data communications to the point to where energy delivery systems become inoperable.

Priorities to Overcome Barriers and Achieve Milestones

While automated methods of incident detection can be extremely valuable in preventing exploits to energy delivery systems, it is essential that a proper balance of automation for the application be configured properly, work as intended, and include the appropriate human review and interaction. For some cyber contingencies, an automated contingency response would be appropriate, while in other cases an automated response could be unsafe, making manual intervention imperative. New research is needed to measure and identify the scope and extent of the impact of a threat that supports cyber attack decision making for the human operator. And new capabilities are needed to establish contingency techniques that contain the attack before it can further propagate.

Given the vast numbers of automation components in a smart grid and a modern oil and natural gas infrastructure, providing actionable information will become more important in understanding the overall health of the energy system. Innovations in distributed decision making approaches will play a more prevalent role than hierarchical command-and-control approaches to ensure that the system behaves much like an ecosystem, in which some portions may be impacted by varying degrees, but the remainder of the system reacts to contain the damage and continue operating the critical functions until the incident has passed and the system is returned to normal service.

Every cyber incident provides an opportunity to examine weaknesses in the system and also in the way the organization handles its response. Advanced tools that enable extensive review of the logging functions of firewalls, routers, switches, servers, and workstations will help determine a baseline of normal activity and enable a comparison of how the unauthorized access is attempted or successfully completed. New capabilities that enable real-time forensics will help operators understand the nature of the attack and collect essential evidence for prosecution. Tools that identify attack access paths will enable operators to close these avenues and prevent a repeated attack. A clear and public process for vulnerability and incident reporting that establishes roles and responsibilities for each party is also needed. To receive the desired response from asset owners and vendors, vulnerability disclosure can be tied to specific mitigation activities.

Exhibit 4.5.2 Managing Incidents

STRATEGY: Manage Incidents

GOAL: Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available 4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	4.3 Incident reporting guidelines accepted and implemented by each energy subsector 4.4 Real-time forensics capabilities commercially available 4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available

Barriers

- Forensic systems are not as fast as attack systems
- Value proposition (and time function) of data as it relates to decision process is not well understood
- Difficult to recognize an incident once it is under way
- Traditional information technology solutions can disable or shut down energy delivery systems
- Unclear roles and responsibilities among stakeholders limits lessons learned after a cyber incident

Priorities

Intrusion Detection, Response, and Recovery Tools and Techniques

- **Develop real-time assisted detection, containment, remediation, and recover/restoration actions in response to a cyber incident**
- Develop ability to contain attack while response and recovery measures are under way
- Develop ability to contain successful intrusions by establishing electronic security perimeter (ESP) compartmentalization techniques
- Use both cyber- and physical- state information in developing automated and assisted response capabilities
- Adapt intrusion prevention system for more robust application to network and application
- Develop and deploy sensor systems with mechanisms to detect and report anomalous activity
- Develop intrusion detection systems that incorporate chaos theory
- Develop methods to identify whether an incident will escalate to a national-scale incident
- Develop capabilities to measure the degree of resilience, including the cyber/physical impacts of a cyber incident

Lessons Learned

- Use existing Federal and private sector resources to identify existing incident reporting guidelines (both mandatory and voluntary) and best practices
- Use existing public-private partnerships to establish an easy to follow approach to incident reporting for the entire energy sector
- Develop capabilities that enable automated collection of security information, including incident reports and visualization tools for correlation
- Develop ability to conduct real-time forensics
- Develop audit trail capability for intrusion detection systems to enable automated reporting
- Develop a common system for reporting incidents by sector

Incident Management Training

- Provide operational energy delivery systems security training using a common and comprehensive set of simulation tools
- Train staff on enterprise security protocol compartmentalization techniques to effectively prevent and delay propagation in response to a cyber incident
- Set up and evaluate cyber incident and response simulators

Bolded text indicates the top priority efforts identified by participants at the September 2009 Roadmap Update Workshop

Strategy: Sustain Security Improvements

Energy delivery systems security will be a continued imperative within the energy sector as technology advances and modernization continues. A sustained effort that combines the expertise and perspectives of all stakeholders ensures that security needs are being met and anticipated from every angle. Forming innovative and productive partnerships with national laboratories, academia, vendors, and asset owners and operators is essential to provide the resources, incentives, and collaboration required for facilitating and increasing security improvements. Additionally, information and cost sharing minimizes the duplication of technology development efforts and maximizes resources to efficiently achieve effective solutions.

While public and private partners are still clarifying their respective roles and responsibilities, multiple efforts are under way to improve energy delivery systems. Leadership and commitment are needed to remove barriers, facilitate information exchange, and support R&D for technology improvements that are hard to justify within the sector's current business model. Ongoing engagement allows stakeholders to provide input from the field to help guide future technology development. Moving forward, energy asset owners will be working collaboratively with government and sector stakeholders to accelerate security and resilience advances. An overview of the milestones, barriers, and priorities to meet the milestones for sustaining security improvements is shown in Exhibit 4.6.1.

Barriers to Achieving the Goal

Although regulations may raise the overall baseline of security, they may lead to unintended consequences. For example, as a result of the NERC CIP standards, some utilities are now focused on meeting regulatory requirements rather than achieving "comprehensive and effective cybersecurity."[36]

Executives, the public, and even organizations within the utility still lack a full understanding of energy delivery system vulnerabilities and the potential consequences of an incident. The limited exchange of threat and incident information prevents the sector from compiling the evidence it needs to build a compelling business case to increase private investment in energy delivery systems security. Credible, actionable, and timely information is also essential to ensuring that the energy sector can adequately mitigate energy delivery system vulnerabilities before adversaries can exploit them. Current efforts to report vulnerabilities or share information are often ineffective or stall because each party in the chain of disclosure lacks an understanding of what they must (or can) do when they receive vulnerability information. Regulatory, privacy, proprietary, and pricing sensitivity issues often create disincentives for, or legal barriers to, disclosing vulnerabilities.

The pace of technology change in the cyber realm is significantly faster than the traditional technology life cycle in the energy sector. The urgent need to test any security solution prior to implementation not only creates resource challenges, but also requires expert input from industry asset owners who are already in short supply. Experience has shown that researchers who work with asset owners early in the development process produce more applicable and useful products than those who do not.

Improving security comes at a cost, and demonstrating direct line benefits to an energy organization is difficult. Without the occurrence of a catastrophic cyber incident or a strong business case, public and private partners will continue to have limited time and/or resources to invest in partnership efforts. Many of these partners volunteer their time and ideas in addition to handling their regular workload. And a shortage of industry partners causes researchers to ask the same volunteers to help again and again. In addition, technology change is inhibited by a lack of multidisciplinary expertise, high costs, and fragmented government and industry programs.

Exhibit 4.6.1 Sustaining Security Improvements

STRATEGY: Sustain Security Improvements
GOAL: Collaboration between industry, academia, and government maintains cybersecurity advances

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders 5.2 Federal and state incentives are available to accelerate investment in and adoption of resilient energy delivery systems	5.3 Collaborative environments, mechanisms, and resources are available for connecting security and operations researchers, vendors, and asset owners 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector

Barriers

- Bridging the technology transfer gap and accelerating progress, while addressing technology obsolescence
- Technology change is inhibited by lack of multi-disciplinary expertise, high costs, and fragmented government and industry programs
- Cybersecurity is a difficult business case
- Raising security levels is slow due to unclear roles and responsibilities among all stakeholders
- Limited understanding of how to share and what to do with vulnerability information
- Private sector partners have limited time and/or resources to invest in partnership efforts that do not provide meaningful and clear benefits to the company; government demands on their time appear to be growing while the workforce is being streamlined
- New regulations may impose requirements with unintended consequences
- Insufficient sharing of threat and incident information among government and industry entities

Priorities

Innovative Partnerships

- **Develop a forum and/or clear process for bringing the right people to the table for vulnerability reporting, analysis, and response information**
- **Develop a matchmaking forum to connect researchers, vendors, and asset owners to accelerate research from concept to commercialization**
- **Develop mechanisms for utility and vendor engagement for pilot research studies to address the business case up front**
- **Create a forum for industry to detail and request R&D topics**
- **Require diverse (academic, lab, industry) participation to receive funding**
- Provide dedicated resources and long-term commitments to address the most serious and complex issues that require longer term resource investment to bring solutions to market
- Create a protocol for working with partners including suppliers, law enforcement, etc.
- Initiate policy and collaboration mechanisms to accelerate the availability of cybersecurity solutions for the energy sector

Investment

- Implement effective incentives through federal and state governments to accelerate investment in secure energy delivery system technologies and practices
- Create appropriate incentives to invest in energy delivery systems security and resilience improvements
- Conduct analysis of incentives and benefits of implementing security to help fortify the business case
- Develop cost/benefit case studies and a mechanism to share them across the sector

Vulnerability Disclosure

- **Create a matrix of three critical vulnerability disclosure factors: who found the vulnerability, the interface list, and the degree of risk**
- **Adopt a vulnerability disclosure "Bill of Rights," which establishes roles and responsibilities of each party and communicates impacts**
- **Develop a clear, public, and industry-accepted vulnerability disclosure process**
- Support legislation that protects entities who disclose vulnerabilities in good faith to the appropriate parties

Information Sharing

- **Develop an asset inventory/configuration database to determine who has a need to know and to track configuration changes, regulatory compliance, and vulnerabilities**
- Develop standards, regulations, and/or tools for secure data exchange and communications
- Facilitate information sharing by guaranteeing protection of industry critical infrastructure protection information through legislation and other means (e.g., expedite security clearances)
- Enhance environments for securely sharing collected government information on threats and real-world attacks with asset owners and vendors
- Establish legal framework to enable effective information sharing between industry, government, and academia

Bolded text indicates the top priority efforts identified by participants at the September 2009 Roadmap Update Workshop

Priorities to Overcome Barriers and Achieve Milestones

To improve technology transfer, new initiatives are needed that accelerate technology transfer by effectively matching researchers with asset owners to assist in the development of new security products. Innovative ways to facilitate collaboration among multidisciplinary experts who are geographically dispersed are needed to solve complex problems. Policy and collaboration mechanisms may also be needed to accelerate the availability of cybersecurity solutions for the energy sector

Researchers and other appropriate stakeholders need controlled but efficient access to real operating data. Access to this data would dramatically advance the ability of vendors and researchers to design and validate technical, operational, and business-model feasibility of emerging technologies. Bridging this information-sharing gap between asset owners and solution providers will accelerate the cybersecurity product development process, increase confidence in new security capabilities, and encourage widespread adoption.

In addition, a strategy to address the legal aspects of collaboration and develop a legal agreement could be developed in collaboration with the major industry organizations (e.g., ISA). To be successful, the highest level of sector engagement is needed.

To sustain technology transfer, security investment, and information sharing, new partnership mechanisms can be developed to provide executive leadership to facilitate research, development, and deployment priorities; identify and disseminate best cybersecurity practices; organize the collection, analysis, monitoring, and dissemination of infrastructure vulnerabilities and threats; and work cooperatively with DOE and other federal agencies.

Also, the government can synthesize classified threat and vulnerability information so that industry organizations can effectively apply the information. A clear process and/or forum for bringing the right people (e.g., subject matter experts to vet and share information with appropriate stakeholders) to the table is needed for timely and effective exchange of vulnerability reporting, analysis, and response information to assist in planning for a cyber incident.

5. Implementation

Implementing this roadmap requires the collective commitment of government, industry, researchers, commercial entities, vendors, asset owners, and operators. Asset owners and operators bear the chief responsibility for ensuring that systems are secure, investing appropriately, and implementing protective measures. However, they rely on the software and hardware vendors, contractors, information technology (IT) and telecommunications service providers, and technology designers who develop, deliver, and integrate system products and services. Researchers at government laboratories and universities play a key role in exploring long-term solutions and developing tools to assist industry. Industry organizations and government agencies can provide additional coordination, leadership, and investments to address important barriers and gaps. Each of these stakeholder groups brings distinct skills and capabilities for improving energy delivery systems security today and in the future.

> "I am here today to stress that, acting independently, neither the U.S. government nor the private sector can fully control or protect the country's information infrastructure. Yet, with increased national attention and investment in cybersecurity initiatives, I am confident the United States can implement measures to mitigate this negative situation."
>
> — *Dennis C. Blair*
> *Former Director of*
> *National Intelligence*
> *February 2, 2010* [37]

Energy Stakeholders

The roadmap presents a high-level strategy for securing energy delivery systems and therefore does not prescribe a single path forward. Voluntary energy sector efforts are the primary driving force promoted by this roadmap to meet the vision. Energy sector stakeholders can use the roadmap in a variety of ways:

- Asset owners and operators can use the roadmap to gain executive support for investment in cybersecurity efforts and encourage vendors and other suppliers to help enhance the cybersecurity of their energy delivery systems.
- Vendors and other suppliers can use the roadmap as guide to improve overall product development and to help validate and promote product marketability.
- Researchers and academia can use the roadmap to focus research on areas that are prioritized by the sector and collaborate with sector stakeholders.
- Government can use the roadmap to guide technology research, development, and deployment funding in critical areas that offer limited incentives for business investment.
- Regulators and standards development organizations can consider the roadmap priorities and ongoing sector activities when developing regulations and standards to help accelerate the sector's progress and address any gaps in existing activities.

Energy Sector Control Systems Working Group

The ESCSWG will launch an awareness campaign to inform and educate energy sector stakeholders, gathering vested interest in reaching the goals and vision set forth in this roadmap. Working group members will encourage public and private partners to step forward to organize, plan, resource, and implement activities focused on the roadmap milestones.

The ESCSWG will update the ieRoadmap to align it with this roadmap and encourage stakeholders to share efforts that they are undertaking to enhance cybersecurity. This will help inform the rest of the sector about new and ongoing work, stimulate collaboration, and minimize any unnecessary, overlapping, or redundant efforts. In addition, the ieRoadmap will help align energy stakeholder resources and collaboration to develop and implement the strategic and tactical approaches needed to achieve the roadmap milestones.

Measuring the sector's progress toward meeting the roadmap vision is critical, but progress depends on the actions of sector stakeholders. Because securing energy delivery systems requires an ongoing, collective, multigroup effort, the challenge will be coordinating and measuring the progress of these efforts over time. Conducting stakeholder polls to identify progress is highly time consuming and resource intensive. Instead, the ESCSWG will use the ieRoadmap to help communicate, coordinate, and measure the progress of the roadmap milestones.

Also, to facilitate collaboration and measure the sector's progress, the ESCSWG will participate in peer reviews and hold workshops that engage energy sector stakeholders in the presentation and review of roadmap activities. These workshops will help stakeholders to better align their activities with the roadmap and improve their collaboration, increasing the likelihood of each activity's adoption into the energy sector. The workshops will allow the ESCSWG to gauge the sector's progress, determine where more focus is needed, encourage further activity, and assess changes in the energy delivery systems landscape. Because this landscape will evolve over time as new technologies are developed and threats emerge, the ESCSWG will update the roadmap as appropriate to keep the sector focused on cybersecurity.

Appendix A: Roadmap Revisions

Revision Number	Roadmap Section	Description
1	Title	The term "energy delivery systems" is used because cybersecurity for the energy sector now goes beyond the control system space to smart grid technologies and the cyber-physical interface.
2	Executive Summary: Roadmap Scope	Scope updated for clarity.
3	Executive Summary, Section 4: Vision	Vision updated to emphasize resilience, extended to 2020, broadened from surviving an intentional cyber assault to a cyber incident, and "with no loss of critical function" changed to "while sustaining critical functions" in recognition that there is no absolute security an in support of a risk management approach for operational reliability and national security.
4	Executive Summary, Section 4: Strategic Framework	Added build culture of security strategy. Revised existing strategies, goals, milestones, and priorities for clarity and based on sector progress made and lessons learned. Added numbers to the strategies and milestones. Added more details to enhance understanding, included new barriers and priorities to achieving the milestones to address smart grid, vulnerability disclosure, innovative partnerships, measuring progress, R&D gaps, and workforce issues. Updated time frames according to the change in the landscape, evolving needs of the sector, and lessons learned in launching and implementing efforts; near-term (0–3 years), mid-term (4–7 years), long-term (8–10 years).
5	Executive Summary: Key Challenges	Focused on key challenges.
6	Executive Summary, Section 5: Roadmap Implementation	Implementation updated to focus on how the various energy stakeholders can implement and use the roadmap, and added the role of the Energy Sector Control Systems Working Group in the roadmap implementation. In the Executive Summary, Roadmap Implementation replaced the Call to Action subsection.
7	Section 1: Introduction	Subsections added on updating the roadmap and stakeholder input to the roadmap. Infrastructure protection and policy influences subsection replaced national context.
8	Section 2: Energy Sector Progress	Added Energy Sector Progress section, which includes the subsection "The Path Forward," which was in the Introduction of the 2006 Roadmap. This new section provides examples of energy sector achievements and a subsection on standards.
9	Section 3: Energy Delivery Systems Landscape	Updated to include new smart grid cybersecurity efforts, increasing attack envelope, and escalating threat.
10	Appendix B: Energy Sector Achievements and Ongoing Efforts	New appendix to illustrate numerous public and private efforts supporting milestones and brief summaries of those efforts.

Appendix B: Energy Sector Achievements and Ongoing Efforts

The following is an extensive, but not all-inclusive list of energy sector achievements and ongoing efforts. Ongoing efforts are *italicized in blue font*.

Measure and Assess Security Posture

Near-term

Baseline security methodologies available, self assessments prepared, and training provided

- Control Systems Vulnerability Assessments—The U.S. Department of Energy (DOE) National SCADA Test Bed (NSTB) conducted 37 assessments of control systems and components, which have enabled vendors to identify problems, deliver patches to existing customers, and integrate stronger security into next-generation systems. These assessments, performed by the Idaho National Laboratory (INL), included laboratory assessments of 14 vendor components and 15 vendor systems, and 8 onsite assessments of asset owner systems. The laboratory test bed provides a fail-safe environment to rigorously examine commercially available systems and validate security enhancements based on extensive cybersecurity research at the national laboratories. Onsite assessments with asset owners enable researchers to evaluate vulnerabilities in an operational environment and can validate fixes made after test bed assessments.
- Inter-Control Center Communications Protocol (ICCP) Security Assessment—A DOE-funded project performed by INL to identify vulnerabilities in the protocol stacks of the two primary ICCP stack providers—SISCO and LiveData—and test the products of supervisory control and data acquisition (SCADA) vendors.
- Advanced Network Toolkit for Assessments and Remote Mapping (ANTFARM)—a free, open-source tool that enables asset owners to map and visualize their control systems networks. This software, developed by Sandia National Laboratories (SNL), remotely and passively queries multiple sources of existing network information, including output from other network analysis tools, network device configuration files, firewall configuration files, and traffic logs. ANTFARM compiles and correlates this data into a database and allows users to create a visual representation of their network components, which aids systems owners and operators in assessing their network security posture and meeting North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standard 005 (NERC CIP-005). ANTFARM has been downloaded more than 100 times.
- Bandolier Security Audit Files—Asset owners are using the Nessus Vulnerability Scanner and Bandolier Security Audit Files to optimize the security configuration of their control systems. In a DOE-supported project, Digital Bond leveraged the compliance plug-in and developed Bandolier Security Audit Files to turn Nessus into a tool that can audit the security configurations of control system workstations and servers without installing any software on the system or negatively impacting the system. Digital Bond has worked with ABB, AREVA, Emerson, Matrikon, OSIsoft, SNC, and Telvent to develop and test Bandolier Security Audit files. Most of these vendors distribute the audit files to their customers, and Digital Bond makes all of the files available as subscriber content on its website for a nominal fee. More than 200 organizations are subscribing. Vendors are also including the Bandolier Security Audit Files in acceptance testing of upgrades and new systems. According to Digital Bond, "Bandolier, in conjunction with the Nessus compliance plug-ins, is the most widely used security tool in industrial control systems."[38]

- Control System Cyber Security Self-Assessment Tool (CS2SAT)—A tool that guides users through a step-by-step process to collect facility-specific control system component information and makes appropriate recommendations for improving the system's cybersecurity posture. Developed by the U.S. Department of Homeland Security (DHS) National Cyber Security Division with assistance from INL, the tool provides a systematic and repeatable approach for assessing many programmatic and other aspects of the cybersecurity posture of industrial control system networks. It is available from the International Society of Automation (ISA) and as part of a tool set from Lofty Perch.
- *Recommended Practice for Securing Control System Modems*—A report providing guidance on the analysis of methodologies for evaluating security risks associated with control system modems and their use in an organization. This report, produced the DHS National Cyber Security Division with subject matter expertise from INL in 2008, discusses methods for assessing modem security and provides options for implementing modem security based on the types of connections and devices being used.
- *Cyber Assessment Methods for SCADA Security*—An INL report released in 2005 that outlines the SCADA vulnerability assessment methodologies used by INL.
- *ABB SCADA/EMS System INEEL Baseline Summary Test Report*—A baseline report released in 2004 by INL (formerly the Idaho National Engineering and Environmental Laboratory, or INEEL) that served as a starting point for subsequent vulnerability assessments.
- Holistic Lifecycle Model—A model developed by CIDG that helps owners and operators determine which security standards apply to their operations and how to address all cyber, physical, operational, management, and legal requirements.
- National Institute of Standards and Technology (NIST) Special Publication 800-82: *Guide to Industrial Control Systems (ICS) Security*—A report released in 2008 that provides typical system topologies, identifies typical threats and vulnerabilities to ICS systems, and recommends security countermeasures to mitigate the associated risks.
- NIST Special Publication 800-53: *Recommended Security Controls for Federal Information Systems and Organizations*—A third revision of SP 800-53, released in 2009, including best practices in information security with updates to security control baselines based on current threat information and cyber attacks. The document includes an appendix specifically for industrial control systems with tailoring guidance for the security controls and specific supplements to the security control baselines.
- *Twenty Critical Controls for Effective Cyber Defense*—A document released in 2009 by a consortium of federal agencies and private organizations that identifies a subset of security control efforts that chief information security officers (CISOs) and chief information officers (CIOs) can focus on as their top, shared priority for cybersecurity based on attacks occurring today and those anticipated in the near future. The 20 Critical Controls only address principally technical control areas; however, the controls map directly to about one-third of the 145 controls identified in NIST Special Publication 800-53.
- *Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment*—A 2007 SNL publication that covers the planning, execution, and reporting process for cyber vulnerability assessments in compliance with the NERC Critical Infrastructure Protection (CIP) standards.
- *Security Framework for Control System Data Classification and Protection*—A framework released by SNL in 2007 that provides methods to classify and secure control systems data.
- *Security Metrics for Process Control Systems*—A 2007 SNL document recommending the use of a metrics taxonomy to assist asset owners in tailoring and applying metrics for control systems security planning.

- *Wireless System Considerations When Implementing NERC Critical Infrastructure Protection Standards*—A paper that examines the risks of wireless use within a utility's Electronic Security Perimeter, presents a defense-in-depth model to monitor and control wireless and technical solutions for each defensive layer to assist with CIP-005 compliance, and offers methods to reduce risk from a number of wireless threat scenarios. The paper was coauthored by experts from Oak Ridge National Laboratory (ORNL), Pacific Northwest National Laboratory (PNNL), and the Energy Sector Control Systems Working Group (ESCSWG) and published in 2009.
- *American Petroleum Institute (API) Standard 1164, Pipeline SCADA Security*—A second edition standard, released in June 2009, that provides holistic SCADA security best practices to liquid pipeline system operators that included guidance on risk assessments, system design, and establishment and review of company policies.
- *Institute of Electrical and Electronics Engineers (IEEE) 1686, Security for Intelligent Electronic Devices*—Established in 2009, the standard sets minimum requirements for substation intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs, such as NERC CIP, and address security regarding the access, operation, configuration, firmware revision, and data retrieval from an IED.
- *International Electrochemical Commission (IEC) 62351, Information Security for Power System Control Operations*—Established in May 2007, the International Electrotechnical Commission (IEC) established a series of standards which defined security requirements for power system management and information exchange. The standards apply to the communication protocols most commonly used in industry, such as IEC 61870, IEC 61950 and Distributed Network Protocol (DNP3).
- *Threat Characterization—A DOE-funded SNL project to provide a framework and tool for leveraging open- and closed-source data to better quantify the level of threat in terms that are meaningful to asset owners.*
- *Understanding the Supply Chain Threat—A DOE-funded SNL project to develop an understanding of the nations involved in the control system life cycle, and develop a threat model that will allow the U.S. government to prioritize security solutions and guide new investment.*
- *Model-Based Technical and Experimental Security Assessment Tools—A DOE-funded Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project to apply the ASSESS automated security assessment technique to representative power grid information technology (IT) infrastructure to demonstrate optimal selection of security schemes to maximize security when faced with a budget constraint. Extends the Network Access Policy Tool (NetAPT) to perform a comprehensive security policy analysis.*

Mid-term

50% of asset owners and operators performing self-assessments of their control systems using consistent criteria

- The Energy Sector-Specific Plan states that "voluntarily conducted vulnerability assessments have not only improved sector security but have also demonstrated industry commitment to a secure and resilient Energy Sector. Many asset owners and operators conduct self-assessments or contract with third parties to perform energy vulnerability assessments and implement protective programs at their facilities."[39]
- Two utility consortia pooled resources to fund vulnerability assessments for the control systems they employ. Twelve utilities using ABB systems, including Austin Energy, Detroit Edison, Indianapolis Power & Light Company, ITC Transmission, Kansas City Power & Light Company, Lower Colorado River Authority (LCRA), New York Independent System Operator, Snowy Hydro Limited, and Tri-State Generation and Transmission Association, Inc. from the United States and Australia

formed a consortium to privately fund user-driven ABB system vulnerability assessments at INL. Utilities using AREVA systems have followed suit, forming their own consortium to leverage funding for follow-on testing of AREVA systems.

Common metrics available for benchmarking security posture

- *Primer Control Systems Cyber Security Framework and Technical Metrics*—A primer developed by DHS in 2009 to aid owners and operators in managing their control systems cybersecurity posture. The DHS National Cyber Security Division's framework consists of seven control systems cybersecurity dimensions related to risk and provides a set of 10 technical metrics that allow control systems owner-operators to track improvements or degradations in their individual control systems security posture.
- *Trustworthy Wireless for Critical Infrastructure Sites*—Working with other laboratories and industry groups, ORNL developed the Trustworthy Wireless Working Group within ISA 100 to promote the development of standards for wireless communications and define the metrics for trustworthiness in an industrial wireless sensor network.
- *21 Steps to Improve Cyber Security*—Institute for Information Infrastructure Protection (I3P) security metrics tool and guidance document that enables oil and gas industry asset owners to assess various cyber security options for control system networks. The tool uses five security performance levels to baseline the existing network and show the impact of security enhancements.

90% of energy sector asset owners conducting internal compliance audits

- By second quarter 2010, all system control centers and other facilities subject to NERC CIP-002 to CIP-009 must be auditably compliant with the standards, meaning the entity meets the full intent of the requirement and can demonstrate compliance to an auditor with documentation, logs, and records for the previous year. [40]

Long-term

Real-time security state monitoring for new and legacy systems commercially available

- The LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) program was formed to facilitate cooperative R&D, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems. LOGIIC is an ongoing collaboration of oil and natural gas companies and the DHS Science and Technology Directorate. The first LOGIIC project was a technology integration and demonstration effort that demonstrated an opportunity to reduce vulnerabilities of oil and gas process control environments by sensing, correlating, and analyzing abnormal events to identify and prevent cyber security threats. Current members of LOGIIC include BP, Chevron, Shell, Total, and other large oil and gas companies that operate significant global energy infrastructure. For more information about the LOGIIC program, visit *www.logiic.org*.
- *Security Core Component—Siemens Energy Automation is developing a near-real-time cyber and physical security situational awareness capability for the control system environment.*

- *Control System Situational Awareness Technology Interoperable Tool Suite—An INL project to develop a tool suite to enable operators to see all control system network communications, collect all wireless mesh network data message routes, view reports of unexpected data, monitor system health, distinguish between component failure and cybersecurity incidents, perform data fusion for situational awareness, and determine the global effects of local firewall rules.*

Develop and Integrate Protective Measures

Near-term

Consistent training materials on cyber and physical security for control systems widely available within the energy sector

- Control Systems Cybersecurity Training—INL has trained more than 2,300 operators and other stakeholders in introductory, intermediate, and advanced security courses, including two NERC-certified courses, conducted by DOE and DHS. These courses raise awareness of vulnerabilities, attack mechanisms, and operational issues. More than 224 energy company representatives from 126 different electric, oil, and natural gas entities and other third-party companies attended six Advanced Red/Blue Team industrial control system cybersecurity courses held in fiscal year (FY) 2009 and FY2010. Several days of classroom training culminated in a full-day, red/blue/white team exercise designed to leave participants with security techniques they could immediately take back and use in their facility.
- *Common Cyber Security Vulnerabilities Observed in Control System Assessments*—A report released by INL in November 2008 that provides suggested mitigations for each vulnerability category found during assessments of 16 control systems. It is an update to INL's 2006 *Lessons Learned from Cyber Security Assessments of SCADA and EMS*, and the 2005 *Mitigations for Security Vulnerabilities Found in Control Systems Networks*, which suggests mitigation strategies to common problems and vulnerabilities seen in onsite control system assessments.
- N*ERC Top Ten Vulnerabilities of Control Systems and their Associated Mitigations*—A report released in 2006 and updated in 2007 that lists the top 10 common vulnerabilities that put energy sector control systems at risk and the mitigations developed by INL.
- *Advanced Metering Infrastructure Security Considerations* —An outline of threats to advanced metering infrastructure (AMI), sources of the threats, damage mechanisms, attack consequences, and strategies and recommendations to reduce security risks to AMI. Developed by SNL in 2007.
- *Threat Analysis Framework* —A SNL report released in 2007 providing the key elements needed to perform a comprehensive threat analysis—identification of an adversary, development of generic threat profiles, identification of generic attack paths, discovery of adversary intent, and identification of mitigation strategies.
- *Cyber Security Procurement Language for Control Systems*—A summary released in 2008 by DHS that provides security principles that should be considered when designing and procuring control systems products and services, including software, systems, maintenance, and networks. The language was developed through collaboration with leading control systems security experts, purchasers, integrators, and technology providers and vendors across several industry sectors.
- *Secure ICCP Integration Considerations and Recommendations*—A report released by SNL in 2007 that describes the Inter-control Center Communications Protocol (ICCP), the security elements of Secure ICCP, and independent technologies that can be added when introducing Secure ICCP into utility control systems networks. The ICCP was developed to enable utility control centers, Independent System Operators (ISOs), Regional Transmission Operators (RTOs), and other electricity generators to exchange data over Wide Area Networks.

- *Education and Workforce Development—TCIPG project to extend and disseminate existing education resources including curricula that integrate cybersecurity and power systems topics, update an existing summer school course with smart grid security concepts, and offer the course to graduate students and industry practitioners.*

Mid-term

Field-proven best practices for control systems security available

- *Common Cyber Security Vulnerabilities Observed in Control System Assessments*—A report released by INL in November 2008 that provides suggested mitigations for each vulnerability category found during assessments of 16 control systems. It is an update to INL's 2006 *Lessons Learned from Cyber Security Assessments of SCADA and EMS*, and the 2005 *Mitigations for Security Vulnerabilities Found in Control Systems Networks*, which suggests mitigation strategies to common problems and vulnerabilities seen in onsite control system assessments.

- *NERC Top Ten Vulnerabilities of Control Systems and their Associated Mitigations*—A report released in 2006 and updated in 2007 that lists the top 10 common vulnerabilities that put energy sector control systems at risk and the mitigations developed by INL.

- The Advanced Security Acceleration Project - Smart Grid (ASAP-SG)—This partnership among the UCA International Users Group (UCAIug), Consumers Energy, Florida Power & Light, Southern California Edison, and DOE released two security profiles for smart grid applications, one for AMI and another for third-party data access. The AMI profile provides guidance and security controls to organizations developing and implementing AMI solutions. This profile was adopted and ratified in December 2009 by the AMI Security (AMI-SEC) Task Force within UCAIug and AMI-SEC released version 2.0 in June 2010. ASAP-SG's AMI profile accelerated the work of AMI-SEC, enabling the document to go from inception through ratification to version 2.0 status in less than a year. The AMI profile also served as a reference to the NIST Cyber Security Working Group's development of the NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*.

- *Control Systems Cyber Security: Defense in Depth Strategies*—Security guidance to help organizations defend their information architectures that involve business and control systems network components. This 2007 report prepared by INL for DHS discusses various attack vectors and how to isolate and protect assets. The defensive strategies discussed include the use of firewalls, demilitarized zones, intrusion detection systems, effective security policies, security training, and incident response.

- Object Linking and Embedding (OLE) for Process Control (OPC) Security White Papers—A series of three white papers providing observations and practices that will help end users secure their OPC systems. The final paper, *Hardening Guidelines for OPC Hosts*, was released in 2007 and focuses on securing host computers running OPC. The papers were commissioned by Kraft Foods Inc. and prepared by Digital Bond, British Columbia Institute of Technology, and Byres Research.

- *High-Level (4th Gen) Language Microcontroller Implementation—INL is working to harden microcontrollers against low-level cyber attacks and limit direct access to device memory by developing a standardized security library to implement secure authentication and data encryption down to the hardware level.*

- *Secure Communications Architecture for the Energy Sector—PNNL will identify requirements for secure and robust data transfer, develop a control system-specific solution, and create a best practices guide for asset owners to implement the technology. It will protect data flows across the control, business, and AMI systems.*

Secure connectivity between business systems and control systems within corporate network

- *Right-Sized SCADA Communication—Los Alamos National Laboratory (LANL) will develop a detailed cost-benefit modeling tool for legacy and next-generation SCADA communication architectures to help operators select appropriate communication technologies for each node or hierarchy level.*

Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy

- SSCP and Hallmark Cryptographic Serial Communication—Asset owners can secure communications between remote devices and control centers using the PNNL-developed Secure Serial Communications Protocol (SSCP). The SSCP marks original messages with a unique identifier and authenticator; the receiving device scans the identifier and validates the message, ensuring that the information comes from a trusted source and has not been altered in transit. Schweitzer Engineering Laboratories integrated the SSCP into a cryptographic card and link module, as part of the DOE-supported Hallmark project, to provide secure serial communications for existing and new energy control systems.

- Lemnos Interoperable Security—The Lemnos Interoperable Security project developed and demonstrated an interoperability configuration profile for creating a secure communications channel between two control system networks operated by different vendors. The project team identified the requirements for a secure channel that allows varying types of data to be exchanged between multiple locations. These requirements were then mapped to Internet protocol security (IPSec). The team set up an IPSec virtual private network between two networks with different vendors, which required more than one hundred parameters to be configured for some vendor systems. The Lemnos team recorded its work by developing an IPSec interoperability configuration profile (ICP) to reduce the complexity and streamline the configuration process for other vendors to replicate. Vendors including Schweitzer Engineering Laboratories, RuggedCom, Siemens, N-dimension, GarrettCom, Phoenix Contact, and Industrial Defender have tested and publicly demonstrated interoperability using the Lemnos ICP. The Lemnos profile was a DOE cost-shared project, which built on Sandia National Laboratories' Open PCS Architecture for Interoperable Design (OPSAID) project. The Lemnos profile has been accepted as the basis for an OpenSmartGrid (OpenSG) Security Working Group Task Force under UCAIug. Vendor products built to interoperable configuration profiles enable asset owners to better evaluate security functions and ensure that they are purchasing interoperable products.

- *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments*—A paper addressing the design principles and best practices for the secure implementation and operation of ZigBee wireless networks in industrial environments. ZigBee is a protocol standard developed by the ZigBee Alliance for the Low-Rate Wireless Personal Area Network wireless communication technology. This Lawrence Livermore National Laboratory paper was prepared for the Idaho National Laboratory Critical Infrastructure Protection Center and was released as a draft in 2007.

- *Securing Wireless Local Area Networks (WLANs) using 802.11i*—A draft paper addressing the design principles and best practices for the secure implementation and operation of IEEE 802.11 protocol wireless networks. The IEEE 802.11 protocol is a series of standards produced by the IEEE 802.11 Working Group for Wireless LAN communication networks. This Lawrence Livermore National Laboratory paper provides design principles and best practices for securely implementing and operating Wireless LAN (WLAN) communication networks based on the IEEE 802.11 protocol.

- *Secure Information Exchange Gateway (SIEGate)—Grid Protection Alliance is developing SIEGate, which provides secure communication of data between control centers.*

- *Centralized Cryptographic Key Management—Sypris Electronics is developing a cryptographic key management capability scaled to secure communications for the millions of smart meters within the smart grid advanced metering infrastructure.*
- *Watchdog—Schweitzer Engineering Laboratories is developing a managed switch for the control system local area network (LAN) that uses whitelist filtering and performs deep packet inspection.*
- *Field Device Management—PNNL is creating a vendor-independent software application that will enable asset owners to manage and enforce the configuration of all field devices from a central location.*
- *Cryptographic Trust Management—PNNL is creating a software application to manage cryptographic keys that is industry accepted, scalable, and meets the operational needs of asset owners.*
- *Protocol Analyzer—PNNL is incorporating the SSCP into both open-source and commercial protocol analyzer products to enhance the ability of asset owners to monitor secured communication.*
- *Next Generation Secure, Scalable Communication Network for the Smart Grid—ORNL is developing a secure, scalable communication network for the smart grid using an adaptive hybrid spread-spectrum modulation format to provide superior resistance to multipath, noise, interference, and jamming.*
- *Whitelist Anti-Virus for Control Systems—Schweitzer Engineering Laboratories is developing a whitelist antivirus solution for control systems integrated with substation-hardened computers and communication processor.*
- *Role-Based Access Control (RBAC)-Driven Least Privilege Architecture for Control Systems—Honeywell International is developing a least-privilege architecture for control systems driven by RBAC.*
- *Tools and Methods for Hardening Communication Security of Energy Delivery System—Telcordia Technologies is researching vulnerabilities in energy sector communication protocols and developing mitigations that harden these protocols against cyber attack while enforcing proper communications.*
- *Padlock—Schweitzer Engineering Laboratories is developing a low-power, small-size dongle (or plugin device) that provides strong authentication, logging, alarming, and secure communications for IEDs in the field operating at the distribution level.*
- *Encryption and Authentication Protocols—TCIPG is extending TCIPG-developed techniques in policy-based encryption, extending TCIPG-developed multicast authentication protocols, and developing new standards-compliant encryption and authentication protocols for advanced smart grid applications.*
- *Key Management and Trust Management Solutions—TCIPG is establishing a key management framework and extending its prototype implementation to efficiently establish multi-party trust between grid entities based on credentials and selective information disclosure policies.*
- *Trustworthy Computation Platforms—TCIPG is developing trustworthy platforms that serve as a foundation for resilient control and communication grid applications.*
- *Secure and Quality of Service (QoS) Assured Wide Area Communication Infrastructure—TCIPG is building on existing TCIPG designs and prototypes to develop a wide-area routed communication network for the resilient smart grid that provides end-to-end security and QoS guarantees.*
- *Integrated Designs for Select Power System Applications—TCIPG is enhancing previously developed distributed power system algorithms and techniques and integrating them with secure and timely data sharing protocols.*

Long-term

Nondestructive intrusions, isolation, and automated response exercises at 50% of critical control systems

- *Security Core Component—Siemens Energy Automation is developing a near-real-time cyber and physical security situational awareness capability for the control system environment.*

Security test harness available for evaluating next-generation architectures and individual components

- *SCADA Systems Cyber Security Testing Through Portable Acceptance Test Apparatus and Protocols—An ORNL project to provide an honest broker environment where the business cases for investments in control system security advances can be developed within the existing energy asset owner business cases.*

Detect Intrusion and Implement Response Strategies

Near-term

Incident reporting guidelines are published and available throughout the energy sector

- DOE Office of Electricity Delivery and Energy Reliability (OE) Infrastructure Security & Energy Restoration (ISER) Electric Emergency Incident and Disturbance Report—mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE uses the report to monitor major system incidents on electric power systems and to conduct after-action investigations on significant interruptions of electric power. As such, the report is designed to address timely initial filings. It is not designed to track incidents that happen within distribution electrical systems (or individual power plant outages). That responsibility is covered by the various regulatory entities composed of State public utility commissions and local governmental authorities. The information is used to meet DOE national security responsibilities and requirements, support reports to Congress, and provide input for coordinating Federal efforts regarding activities such as incidents/disturbances in critical infrastructure protection, continuity of electric industry operations, and the continuity of operations of the government.
- NERC Security Guideline for the Electricity Sector: Threat and Incident Reporting—Guideline to assist electric sector entities in identifying and classifying incidents from reporting to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The guideline includes the mandatory NERC and DOE and voluntary DHS and Public Safety Canada/Royal Canadian Mounted Police reporting.
- *Computer Security Incident Handling Guide*—NIST special publication 800-61, providing guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

Mid-term

Cyber incident response is part of emergency operating plans at 30% of critical control systems

- NERC CIP-008—Mandatory standard for the bulk electric system that requires responsible entities to develop and maintain a Cyber Security Incident Response Plan that contains a process for reporting Cyber Security Incidents to ES-ISAC. The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to ES-ISAC either directly or through an intermediary. [41]
- The Repository of Industrial Security Incidents (RISI)—A database of cybersecurity incidents pertaining to process control, industrial automation, or SCADA systems. RISI collects incident

data from reports submitted by members, public source searches, and data sharing agreements with strategic partner organizations. RISI reviews and verifies the incident data, removes information that may identify the source of the incident, assigns the incident a reliability rating, enters the incident into their database, and reports relevant statistics back to industry and members. RISI has recorded and shared over 175 incidents with member companies.

Commercial products in production that correlate all events across the enterprise network

- Portaledge—Asset owners can aggregate control system security events and correlate those events to help detect cyber attacks with the Portaledge release package from Digital Bond, developed in a DOE cost-shared project. Portaledge includes templates that aid an owner/operator in leveraging the installed base and capabilities of OSISoft's PI Server to collect, analyze, and report control system data that potentially signify an attack. User-customized event sequences will alert an operator to a potential attack, and operators can use the chain of individual events to respond to or analyze an incident. Version 1 is available to more than 200 Digital Bond subscribers.
- *Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector—PNNL will develop lightweight and mobile agents—called digital ants—whose activities correlate to produce emergent behavior and draw attention to anomalous conditions that could potentially indicate a cyber attack.*
- *Protecting Process Control Systems against Lifecycle Attacks Using Trust Anchors—SNL is developing trust anchors, which are independent monitoring and control devices that have access to the inner workings of system components and give operators unbiased measurements at the lowest levels of a system to independently verify system function, reveal deceptive malicious function, independently attest to system state, and verify the correctness of system tests.*

Long-term

Control systems network models for contingency and remedial action in response to intrusions and anomalies

- *Automated Attack Response Systems—TCIPG is making existing action recommendation algorithms scalable, integrating them into current Recovery and Response Engine (RRE) implementation, and adding capabilities to the RRE engine to support intrusion detection and response at the hardware, networking, and software levels.*

Self-configuring control systems network architectures in production

Sustain Security Improvements

Near-term

Major information protection and sharing issues resolved between the U.S. government and industry

- Critical Infrastructure Partnership Advisory Council (CIPAC)—A DHS partnership between government and critical infrastructure owners and operators that provides a forum in which they can engage in a broad spectrum of efforts to support and coordinate critical infrastructure protection. Security partners can have confidence in information shared in CIPAC activities and discussions, as they are protected from public disclosure and are exempt from the Federal Advisory Committee Act (FACA, P.L. 92-463).
- Protected Critical Infrastructure Information (PCII) Program—DHS program that institutes a means for the voluntary and protected sharing of private sector, state, and local critical infrastructure information with the federal government. PCII may be used to generate advisories, alerts, and warnings relevant to the private sector.

- Electricity Sector Information Sharing and Analysis Center (ES-ISAC)—A center that disseminates threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants in taking protective actions. It facilitates communications between electricity sector participants, federal governments, and other critical infrastructures.
- Industrial Control Systems Cyber Emergency Response Team (ICS CERT)—Four expert teams provide onsite support for incident response and forensic analysis as part of the DHS ICS CERT, along with actionable intelligence and information sharing. The teams have been dispatched 13 times to investigate and help correct cyber incidents and attacks, including deliberate cyber intrusion and operator error. DHS plans to increase the number of teams in 2011.
- In January 2010, the Federal Bureau of Investigation (FBI) and DOE identified a virtual private network (VPN) vulnerability. Within 90 days of this discovery, an awareness bulletin was provided to industry including the details of the vulnerability and recommendations to mitigate risk. This actionable security product was a result of a joint collaboration between ES-ISAC, the sector lead agency (DOE), the FBI, and the Control System Security Program (CSSP) at DHS. The U.S. Government supplied technical and actionable information regarding observed cyber incidents. The ES-ISAC formed a team of network security experts from industry and worked with government partners to develop the bulletin.
- *In 2010, DOE announced an investment of $16.5 million by DOE, the Energy Sector Security Consortium, Inc. (EnergySec), and the Electric Power Research Institute (EPRI) to form two electric sector cybersecurity organizations, NESCO and NESCOR. NESCO, the National Electric Sector Cybersecurity Organization, led by EnergySec, works to improve electric system reliability by supplying data analysis and forensics capabilities for cyber-related threats. It also assists in creating a framework to identify and prepare for challenges to grid reliability; share information, best practices, resources, and solutions to and from domestic and international electric sector participants; and encourage key electric sector supplier and vendor support and interaction. NESCOR, the National Electric Sector Cybersecurity Organization Resource, led by EPRI, conducts assessment and analysis of cybersecurity requirements, results, and standards in addition to testing security technologies in laboratories and pilot projects in support of NESCO.*

Industry-driven awareness campaign launched

- Energy Sector Control Systems Working Group (ESCSWG)—A working group formed in December 2007 by public and private security experts from the energy sector. It is a joint working group that reports to the Electric Subsector Coordinating Council, the Oil and Natural Gas Coordinating Council, the Oil and Natural Gas Coordinating Council, and the Government Coordinating Council for Energy. The ESCSWG encourages collaboration, provides critiques of public and private research efforts, and offers near-term recommendations for sector improvement.
- Vendor user group meetings—Meetings that invite INL researchers to share vulnerability information found during INL's assessment of a system and share specific mitigation options available to users.

Mid-term

Secure forum for sharing cyber threat and response information

- EnergySec Online Forum—Energy sector asset owners, government representatives, and product vendors can share information, communicate, and coordinate with a network of peers through the EnergySec online forum (*www.energysec.org*), which seeks to provide actionable information directly from and to staff-level individuals.
- Homeland Security Information Network (HSIN)—Federal, state, local, tribal, private sector, and international partners can use HSIN, a secure, web-based platform able to facilitate Sensitive But Unclassified (SBU) information sharing and collaboration.

Compelling, evidence-based business case for investment in control system security

- Intrusion Detection Utility Requirements—ORNL documented the economic justification for deploying secure systems by examining their potential use cases and standards environments that affect asset owners' business cases.
- Risk-to-Mission Assessment Process (RiskMAP)—I3P oil industry tool for building a business case for investing in security. Provides decision support information and translates technical and business terms to allow manager to understand and make risk management decisions.
- EPRI Security Metrics for EMS (Energy Management Systems) project—Project that produced a prototype tool in 2008 that provides quantitative estimates of the value of security activities. The tool is currently under evaluation.
- *The Resilient Economy: Integrating Competitiveness and Security*—A 2007 report, developed by the Council on Competitiveness, promoting a strategy of resilience that supports both private sector competitiveness and the nation's homeland security. The report is based on five sector case studies (chemical, electric and gas utilities, financial services, petroleum, and pharmaceutical) to identify best practices, challenges, and priorities for managing risks and developing competitive, resilient enterprise solutions to homeland security.
- *Economics-Based Risk Assessment—TCIPG is developing new techniques that provide quantitative benefits of investment in cyber security technologies in terms of risk mitigation.*

Undergraduate curricula, grants, and internships in control system security

Effective Federal and state incentives to accelerate investment in secure control system technologies and practices

- National SCADA TestBed (NSTB)—A DOE program that increases the sector's awareness and understanding of control system security issues, R&D, and mitigation options through presentations and briefings at industry conferences and workshops. The program prepared a comprehensive portfolio of outreach products, such as informational CDs, project fact sheets, presentations, the ieRoadmap, case studies, and exhibit booths.
- Smart Grid Investment Grant Program—The American Recovery and Reinvestment Act of 2009 (Recovery Act) provided DOE with about $4.5 billion to modernize the electric power grid. Of this funding, $3.4 billion went into the Smart Grid Investment Grant Program (SGIG) to 99 competitively selected projects across the country. Total public-private investment in the SGIG projects totaled about $7.9 billion. SGIG project awardees are committed to developing and implementing a cybersecurity plan that includes an evaluation of cyber risks and planned mitigations, cybersecurity criteria for device and vendor selection, and relevant standards or best practices that the project will follow.[42]
- *Cybersecurity for Energy Delivery Systems (CEDS) Project Funding—DOE's budget for FY2010 through FY2012 includes over $80 million for industry-led, academia-led, and national laboratory-led research, development, and demonstration projects that will lead to improvements in the cybersecurity of communications and control systems of the U.S. energy infrastructure—including electricity generation, transmission, and distribution; and oil and natural gas production, refining, storage, and distribution.*

Long-term

Cyber security awareness, education, and outreach programs integrated into energy sector operations

- *Security Core Component—Siemens Energy Automation is developing a near-real-time cyber and physical security situational awareness capability for the control system environment.*

Appendix C: Contributors

The Energy Sector Control Systems Working Group

The working group currently includes 14 energy delivery systems experts from the public and private sectors. The ESCSWG members were first designated by the Electric Sub-sector Coordinating Council (SCC), the Oil and Natural Gas SCC, and the Energy Government Coordinating Council (GCC). As a Critical Infrastructure Partnership Advisory Council (CIPAC) working group (see Exhibit C.1), the efforts and discussions of the ESCSWG are protected from public disclosure and are exempt from the Federal Advisory Committee Act (FACA, P.L. 92-463). Although CIPAC-compliant meetings are exempt from FACA, the ESCSWG operates with the principle of government transparency in mind by following procedures designed to achieve a level of openness appropriate to support the homeland security mission while at the same time maintaining a level of confidentiality needed to share sensitive critical infrastructure information. The Working Group helps coordinate and measure the progress of the roadmap implementation.

Working Group:

Dave Batz
Edison Electric Institute

Jim Brenton
Electric Reliability
Council of Texas

David Dunn
Independent Electricity System
Operator Ontario

Gerard Williams
BP

Page Clark
El Paso Corporation

Steve Elwart
Ergon Refining Inc.

Ed Goff
Progress Energy

Brian Harrell
North American Electric
Reliability Corporation

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

Morgan Henrie
Alyeska Pipeline

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

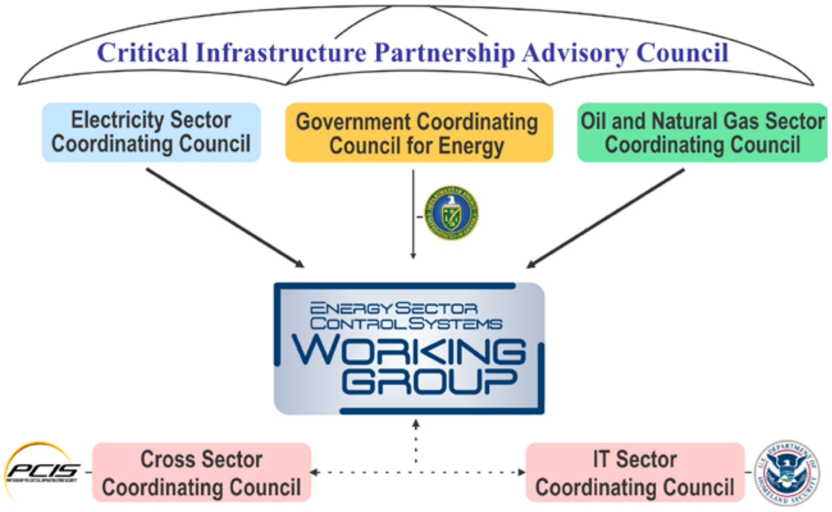
Doug Maughan
U.S. Department of Homeland
Security Science & Technology
Directorate

Lisa Kaiser
U.S. Department of Homeland
Security National Protection and
Programs Directorate

Dave Norton
Federal Energy Regulatory
Commission
Office of Electric Reliability

The U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) Cybersecurity for Energy Delivery Systems program sponsored the roadmap's development, which was led by the public and private sector members of the ESCSWG. Development of the roadmap was accomplished under the CIPAC framework, which offers government and private sector security partners a forum to engage in a broad spectrum of planning, coordination, and implementation efforts. The roadmap was prepared by Energetics Incorporated under the leadership and advisement of OE Deputy Assistant Secretary for Research and Development (R&D) Hank Kenchington and the ESCSWG.

Exhibit C.1 Energy Sector Control Systems Working Group Operational Framework


Critical Infrastructure Partnership Advisory Council
Electricity Sector Coordinating Council
Government Coordinating Council for Energy
Oil and Natural Gas Sector Coordinating Council
Energy Sector Control Systems Working Group
Cross Sector Coordinating Council
IT Sector Coordinating Council
PCIS

The Department of Energy and the working group would like to acknowledge everyone who contributed to the updated *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. It represents a strong, committed, and growing public-private partnership working to achieve a secure and resilient energy sector.

Roadmap Workshop Presenters

Phil Beekman
ABB, Inc.

Steve Berberich
California Independent System Operator Corporation

Matthew Carpenter
InGuardians, Inc.

Page Clark
El Paso Corporation, Energy Sector Control Systems Working Group

Stephen Diebold
Kansas City Power & Light

Tom Flowers
Control Center Solutions
(Presented at Roadmap Over-the-Horizon Workshop)

Darren Highfill
Southern California Edison

Chris Jager
Energy Sector Security Consortium

Dale Johnson
ConocoPhillips Pipe Line Company

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

Doug Maughan
U.S. Department of Homeland Security Science & Technology Directorate

Dale Peterson
Digital Bond

Ernest Rakaczky
Invensys Process Systems

Al Rivero
Telvent

Tim Roxey
North American Electric Reliability Corporation

Bill Sanders
Information Trust Institute

Paul Skare
Siemens

Rhett Smith
Schweitzer Engineering Laboratories

Dave Scheulen
Formerly of BP

Roadmap Workshop Participants

Nabil Adam
U.S. Department of Homeland Security

John Allen
International Electricity Infrastructure
Assurance Forum

John Audia
Special Technologies Laboratory

Phil Beekman
ABB, Inc.

Klaus Bender
Utilities Telecom Council

Steve Berberich
California Independent System Operator (ISO)

Thomas Blair
U.S. Department of Homeland Security

Scott Bordenkircher
Arizona Public Service

James Briones
U.S. Department of Energy/
National Energy Technology Laboratory (NETL)

John Burnette
Pacific Northwest National Laboratory

Curtis Canada
Los Alamos National Laboratory

Matthew Carpenter
InGuardians

Page Clark
El Paso Corporation

Samuel Clements
Pacific Northwest National Laboratory

Philip Craig
Pacific Northwest National Laboratory

Scott Crane
Williams

Frederick Curry
Energen Corporation

Jeffery Dagle
Pacific Northwest National Laboratory

David DeGroot
Austin Energy

Paul De Martini
Southern California Edison

Kimberly Denbow
American Gas Association

Jennifer Depoy
Sandia National Laboratories

Stephen Diebold
Kansas City Power & Light

Rhonda Dunfee
U.S. Department of Energy Infrastructure Security
& Energy Restoration (ISER)

David Dunn
Independent Electricity System Operator (IESO)
Ontario

Thomas Edgar
Pacific Northwest National Laboratory

Valentine Emesih
CenterPoint Energy

Steven Fernandez
Oak Ridge National Laboratory

Gary Finco
Idaho National Laboratory

Tom Flowers
Control Center Solutions

Thomas Frobase
Boardwalk Pipeline Partners, LP

Josh Gerber
San Diego Gas & Electric

Mark Hadley
Pacific Northwest National Laboratory

Darren Highfill
Southern California Edison

Mark Hinrichs
Los Alamos National Laboratory

Dennis Holstein
OPUS Consulting Group

Diane Hooie
U.S. Department of Energy/National Energy Technology Laboratory (NETL)

Jesse Hurley
North American Energy Standards Board

William Hutton
Pacific Northwest National Laboratory

Chris Jager
Energy Sector Security Consortium Inc.

Dale Johnson
ConocoPhillips Pipe Line Company

Arnetta Kelly
U.S. Department of Homeland Security

Henry Kenchington
U.S. Department of Energy

Larry Kershaw
Boardwalk Pipeline Partners, LP

Himanshu Khurana
Information Trust Institute

Stanley Klein
Open Secure Energy Control Systems, LLC

Peter Kuebeck
Federal Energy Regulatory Commission

David Kuipers
Idaho National Laboratory

Teja Kuruganti
Oak Ridge National Laboratory

John Lilley
San Diego Gas & Electric

Wayne Longcore
Consumers Energy

Greg Maciel
Uniloc

Wayne Manges
Oak Ridge National Laboratory

Robert Mathews
Pacific Gas & Electric

Jeremy McDonald
Southern California Edison

Mike Mertz
Southern California Edison

Nathan Mitchell
American Public Power Association

Austin Montgomery
Software Engineering Institute

Bill Muston
Oncor Electric Delivery

Waseem Naqvi
Raytheon

Dale Peterson
Digital Bond

Bob Pollock
Sandia National Laboratories

Ernest Rakaczky
Invensys Process Systems

Bryan Richardson
Sandia National Laboratories

Al Rivero
Telvent USA, Inc.

Tim Roxey
North American Electric Reliability Corporation

William Sanders
Information Trust Institute

Michael Sanders
Southern Company

Cheryl Santor
Metropolitan Water District

Dave Scheulen
BP

Shabbir Shamsuddin
Argonne National Laboratory

Paul Skare
Siemens Energy, Inc.

James P. Smith
Los Alamos National Laboratory

Rhett Smith
Schweitzer Engineering Laboratories

Brian Smith
EnerNex Corporation

Keith Stouffer
National Institute of Standards and Technology

Zachary Tudor
SRI International

Alfonso Valdes
SRI International

Seth Voltz
North American Energy Standards Board

Bill Winters
Arizona Public Service

Breakout Session Facilitators and Rapporteurs

Matt Antes
Energetics Incorporated
(Facilitator)

Jack Eisenhauer
Energetics Incorporated
(Facilitator)

Katie Jereza
Energetics Incorporated
(Facilitator)

Lindsay Kishter
Energetics Incorporated
(Rapporteur)

Shawna McQueen
Energetics Incorporated
(Facilitator)

Melanie Seader
Energetics Incorporated
(Rapporteur)

Appendix D: Overview of Energy Delivery Systems

Energy delivery systems are the backbone of the energy sector—a network of processes that produce, transfer, and distribute energy and the interconnected electronic and communication devices that monitor and control those processes. Energy delivery systems include control systems—the sensors and actuators that physically monitor and control the energy processes, the computer-based systems that analyze and store data, and the communication networks that interconnect the process and computer systems.

Sensors take process measurements and send this information to a computer-based system (e.g., a programmable logic controller). This computer system analyzes the process data using computer programs and operator inputs, and stores the data for future use. Control computer systems communicate instructions to process actuators that activate or deactivate process equipment, based on the results of that analysis. The electric power, oil, and natural gas industries are complex and capital intensive. Reliable, real-time process control enables efficient production, transmission, and distribution of energy.

Electric Power Industry

Electricity is produced by power plants, transmitted across the power transmission network or "electricity grid," and distributed to residential, institutional, and industrial consumers. The industry is demand driven—electricity is produced as it is used—with minimal storage capability. The industry relies on highly sophisticated, high-speed computer and communication systems to manage the generation and flow of electricity. Disturbances in this control can destroy critical process components and cause failures capable of stopping the generation and flow of electricity to end users across the nation. Exhibit D.1 is an overview of the electric power system and the basic communications between energy delivery systems throughout the major electricity processes.

Generation

In the United States, more than 17,000 power generators convert primary energy sources including coal, nuclear, natural gas, and renewable fuels (such as hydropower, biomass, wind, and solar) into electricity.[43] Generators are capital intensive with a wide range in generation capacity (which includes 640-megawatt [MW] solar generation systems and 449,389 MW natural gas generators).[44]

Control systems manage the operation of generators and other power plant equipment such as cooling, waste heat recovery, and emission control systems. Because electricity generation is demand driven, reliable and real-time control of the generation process is paramount in meeting consumer demand for electricity. During peak demand periods, the electric power industry operates near the limits of its physical capacity. Although modern energy delivery systems with enhanced communication and computing technologies enable the electricity system to meet peak demand, they leave little room for supply disruptions.

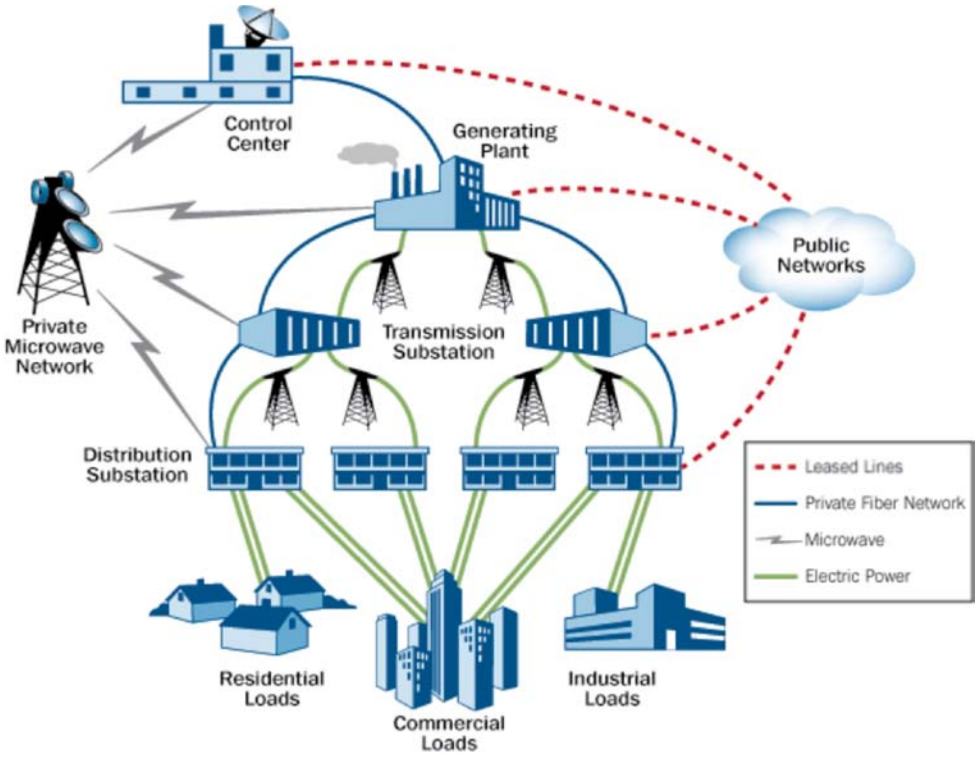


Exhibit D.1 Overview of the Electric Power System and Control Communications

Transmission

Power generation plants are often large and located in remote areas. The transmission system is a sophisticated network connecting power generation plants and power lines operating at different voltages to the end-user distribution system. Transmission lines move large amounts of power over substantial distances and directly serve large loads. Because the transport of electricity is most efficient at high voltage, transformers at transmission substations are used to increase or "step up" low-voltage power from power generation plants to high-voltage power for transmission to the regions where it will be consumed.

Control systems monitor and control transformer operation and electricity flow through some 211,000 miles of transmission lines.[45] Because the transmission system carries such large electricity loads, these systems are often redundant to increase the reliability of the system. Redundancy is built into the system by interconnecting multiple transmission lines so that electricity transmission can be rerouted to avoid the impacts of disturbances to the transmission system. If a transmission line fails without redundancy protection, then the disturbance cuts the flow of electricity to users, which lowers electricity demand and causes power plants to reduce generation. Problems in transmission lines must be resolved quickly before they cascade and cause blackouts. Flexible, reliable, and real-time control of the transmission system is essential to sustain the flow of electricity.

Distribution

Transmission lines feed into local distribution substations, which "step down" or lower the voltage for electricity users. Distribution systems deliver electricity to local areas using many branching lines that feed into homes, buildings, and industrial complexes. Little redundancy is built into the distribution system due to its size and the smaller impact of local outages.

Control systems monitor and control distribution operation and the flow of electricity through more than one million miles of distribution lines. Distribution operation includes distribution substation control as well as communication with the electricity meters at end-user sites that monitor the use of electricity.

Electricity meters allow utilities to charge consumers and enable the industry to balance electricity generation, transmission, and distribution against consumer demand.

Grid modernization efforts are integrating new technologies, services, and entities into electricity distribution. For example, smart meters are creating an advanced metering infrastructure with two-way capabilities for communicating information, controlling equipment, and distributing energy. New distribution technologies bring efficiency and reliability benefits and introduce new domains. Exhibit D.2 uses red circles to indicate the new domains (distribution, customer, and service provider) that need to address cybersecurity in the current electricity delivery systems landscape. Exhibit D.3 provides a detailed view of the customer domain for electricity, which gives an indication of just how complex an already very complex electricity system will become as smarter technologies are added to the electricity infrastructure.

The electricity distribution landscape will continue to evolve as new technologies, services, and entities integrate with existing infrastructure and organizations to meet future needs. Examples of this evolution may include the following:

- Customers: Electric appliances, such as air conditioners, that have the ability to be monitored, controlled, and/or displayed; energy generation resources, such as solar or wind, used to produce, store, and/or flow energy into the grid; electric vehicles plugged into the grid for recharging; and advanced metering infrastructure (AMI) used actively to manage energy consumption.
- Markets: A wide area energy market operation system providing high-level market signals for distribution companies; and wholesale market participants.
- Service Providers: Marketers, brokers, public agencies, cities, counties, or special districts that combine the loads of multiple end-use customers to facilitate the sale and purchase of energy; and a third party providing a business function outside of the utility.

Exhibit D.2 Domains for the Current Electricity Delivery Systems Landscape[46]

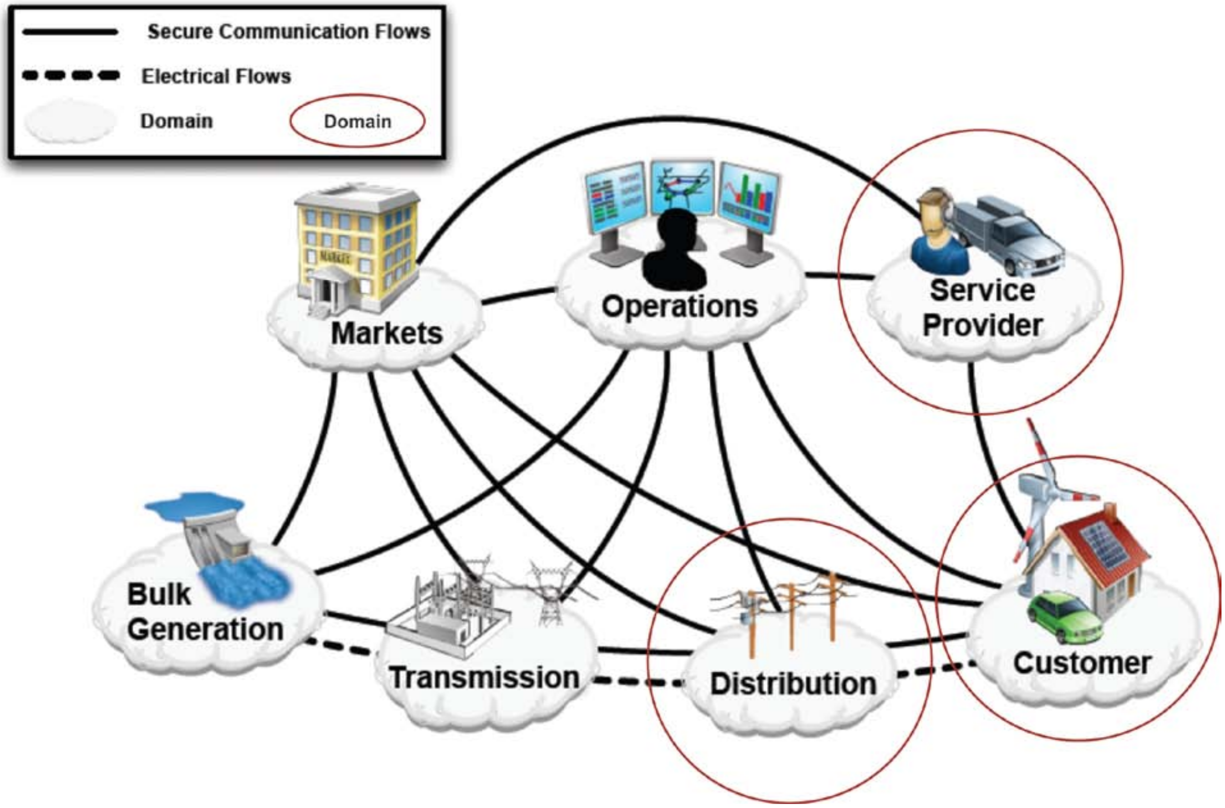
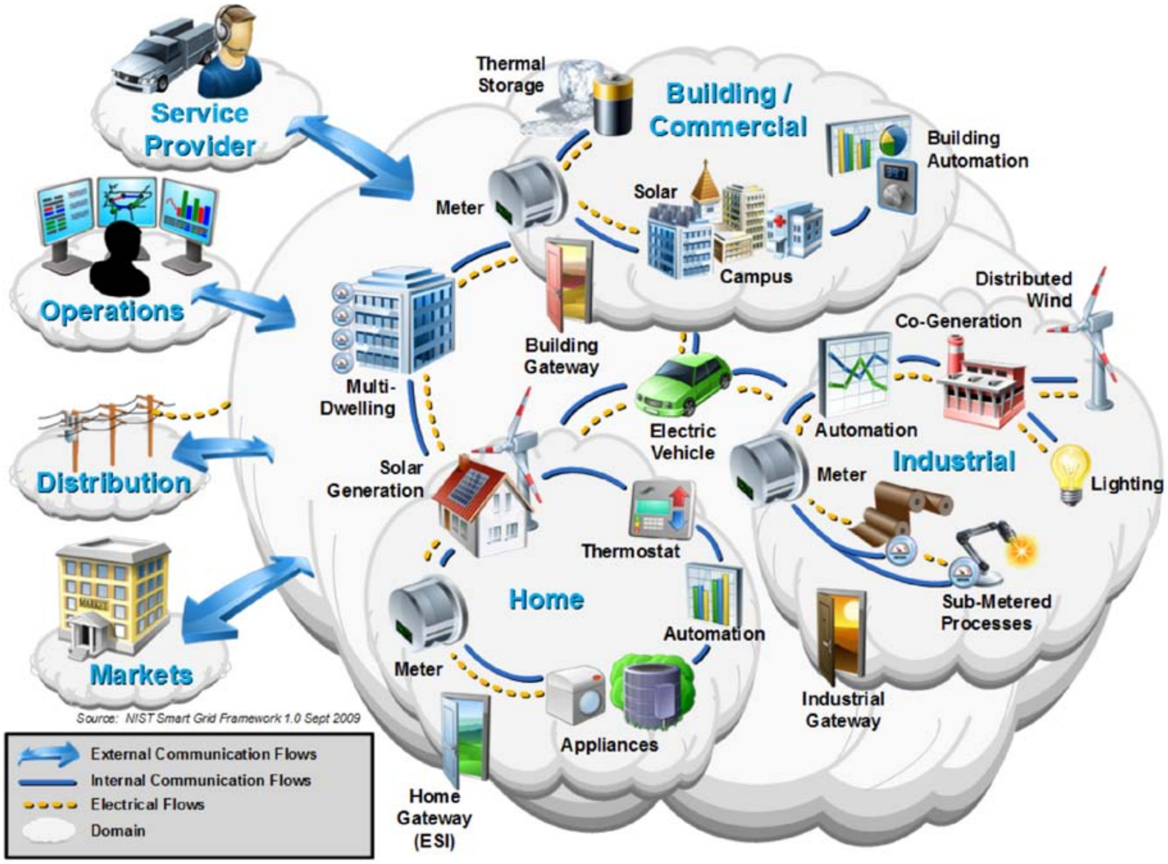


Exhibit D.3 Customer Domain for Electricity [47]



Source: NIST Smart Grid Framework 1.0 Sept 2009

Oil and Natural Gas Industries

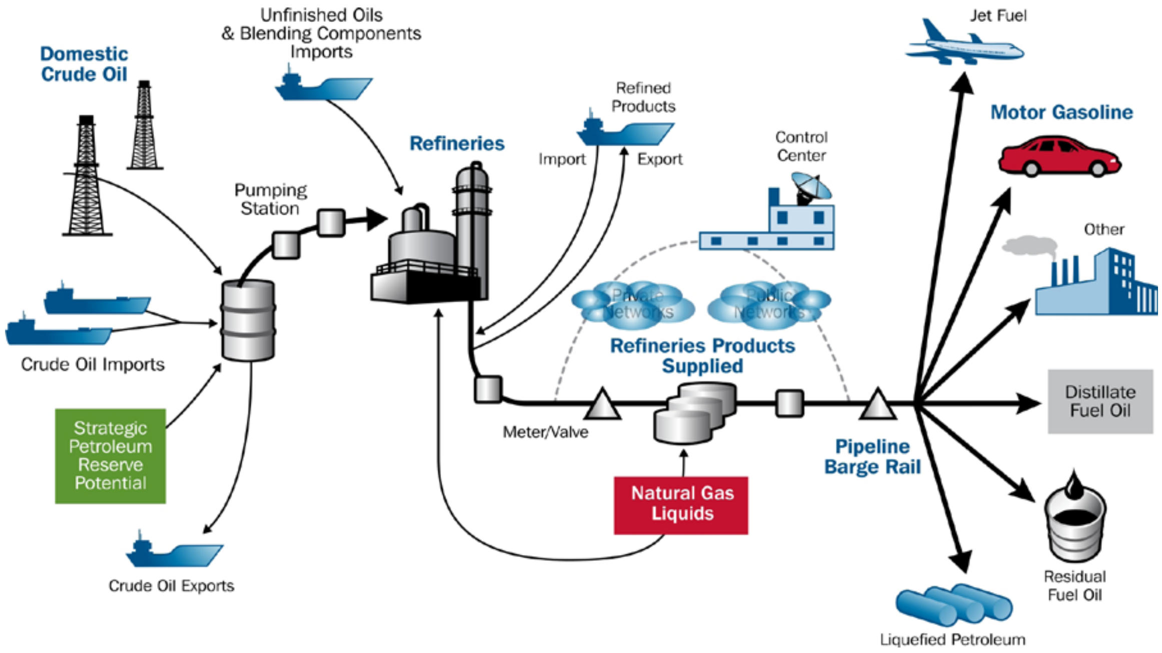
Oil and natural gas is drilled, transported, and refined before it is distributed to consumers. Control systems monitor and adjust operating parameters to enable efficient and safe drilling, transmission, distribution, and refining operations. Disturbances in the control of these systems can be costly and result in hazardous conditions due to the combustibility of oil and natural gas. Exhibits D.4 and D.5 provide overviews of the oil and natural gas systems and the basic communications by control systems between the major processes within each industry.

Drilling

Crude oil and natural gas is either imported or drilled. The drilling and extraction of oil and natural gas from wells occurs both on and off shore. There are more than 500,000 crude oil-producing wells in the United States, providing approximately 25% of U.S. consumption, and more than 445,000 U.S. wells producing about 90% of U.S. natural gas consumption.[48] Natural gas comes from oil wells, gas wells, and condensate wells.

Control systems take measurements and control operations at oil and natural gas wells, reducing the need for manual surveillance to prevent and minimize the impacts of leaks and other hazardous conditions. They are also used in gas and oil separation plants, dehydration units, emulsion breaker units, sweetening units, compressor stations, water treatment units, and other facilities upstream of the processing and refining operations.

Exhibit D.4 Overview of Petroleum System and Control Communications

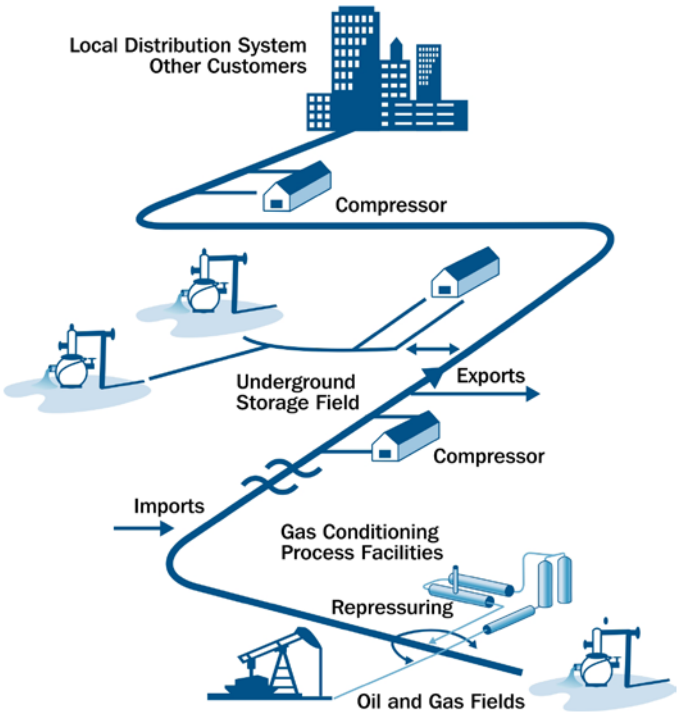


Processing and Refining

Oil is transported to refineries for the production of end-user energy (e.g., gasoline) and other chemical products. There are about 150 refineries in the United States, which produce approximately 23% of the world's refinery products. Natural gas is purified by 500 processing plants in the United States.

Control systems control gas processing and oil refining processes by automating the unit operations within each process. They take measurements such as temperature and pressure, analyze measurements against set points, and activate actuators that open and close valves and turn process equipment on and off.

Exhibit D.5 Overview of Natural Gas System and Control Communications


Local Distribution System Other Customers
Compressor
Underground Storage Field
Exports
Compressor
Imports
Gas Conditioning Process Facilities
Repressuring
Oil and Gas Fields

Transmission and Distribution

The oil and gas industries rely on pipelines as well as other methods (e.g., barge, rail, and tank truck) to transport oil and natural gas to refineries and end users. More than 2 million miles of pipelines gather, transport, and deliver oil and natural gas to consumers across the United States. Approximately 95,000 miles of pipelines receive and deliver crude oil to refineries, and 95,000 miles of lines deliver refined petroleum products. More than 300,000 miles of pipelines receive and transmit natural gas from drilling, processing, and storage facilities, and 1.8 million miles deliver natural gas to consumers.[49]

This extensive pipeline network depends on control systems to monitor operating and safety parameters and control routing, flow, volume, pressure, temperature, and operating status of pipeline facilities. Control of these pipelines demands extremely reliable, real-time communication across the interconnecting interstate and intrastate pipeline systems.

Computer and Network Components of Energy Delivery Systems

Energy delivery systems use various computer and networking components, including supervisory control and data acquisition (SCADA) systems, energy management systems (EMS), distributed control systems (DCS), programmable logic controllers (PLC), intelligent electronic devices (IED), and remote terminal units (RTU) (see Exhibits D.6 and D.7).[50] SCADA systems, which acquire and transmit data to provide centralized monitoring and control, are often used for oil and natural gas pipelines and electric utility transmission and distribution systems.

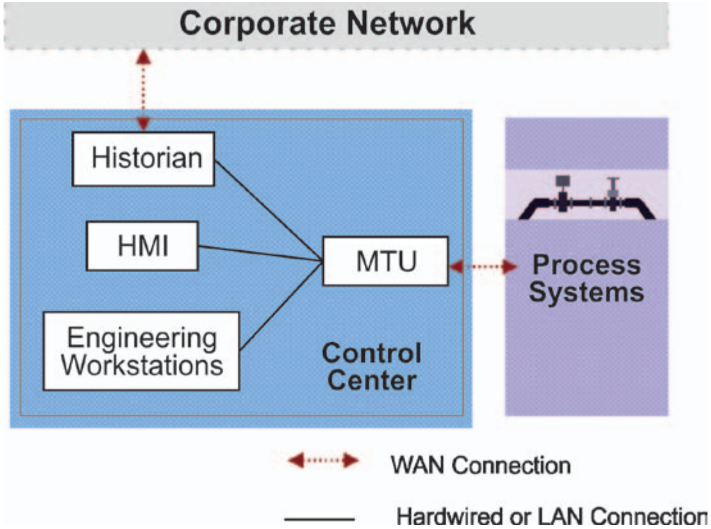
Typical SCADA control center hardware includes a master terminal unit (MTU), historian, human machine interface (HMI), and engineering workstations. Exhibit D.7 depicts the general architecture of a SCADA system. The MTU is the control server, which stores and processes information to and from the historian, HMI, and engineering workstations within the control center. The MTU also stores and processes information between the process systems and the control center.

Exhibit D.6 SCADA Architecture

TYPE	USE
SCADA	Centralized monitoring and control for vast and widely dispersed operations
EMS	Used with SCADA systems to optimize energy delivery system performance
DCS	Small geographical areas and single facilities
PLC	Local control for complex processes
IED	Local processing and control
RTU	Control for a specific application at a remote location

The historian is a database that stores process information. In the past few years, a new generation of data historians—called enterprise historians—have become a part of the control system architecture. Enterprise historians have the capability of interfacing with business (enterprise) computer systems, linking plant operations to the business side of an energy company. Enterprise historians collect, display, and analyze (correlate) process data for a company's operations and for corporate-level business decision making.

Exhibit D.7 SCADA Architecture



The HMI provides an interface for operators to display, monitor, and configure process systems at one or multiple local or remote sites. These field sites may contain one or more process controllers such as a PLC, IED, and/or RTU, which are used to directly monitor and control the process actuators and sensors. The hardware components in a control center are typically interconnected by a local area network (LAN), and the control center MTU communicates with the corporate network and the process system through a wide area network (WAN), such as a private network or the Internet. Local and wide area networks can be supported by switched telephone, leased lines, or power line-based, radio, microwave, cellular, or satellite communication vehicles.

Evolution of Energy Delivery Systems

Many energy delivery systems were designed for operation and reliability when cybersecurity was a low priority. These systems operated in isolated environments and typically relied on physical security and proprietary software, hardware, and communication technology for monitoring and control. Infiltrating these systems often required specific knowledge of individual system architectures and physical access to the system components.

Over the past decade, new technologies have redefined the energy infrastructure, increasing reliability, speed, sophistication, and communication at both the operational and business levels of energy companies. The integration of shared telecommunication technologies into normal business operations spawned increased levels of interconnectivity among corporate networks, energy delivery systems, other asset owners, and the outside world. Expansion, deregulation, and increased market competition changed the energy delivery system architecture for the energy sector. Asset owners and operators extended the connectivity of their energy delivery systems to improve communication and increase system efficiency. They increasingly adopted commercial off-the-shelf (COTS) technologies that provided higher levels of interoperability required among their system components. Standard operating systems, such as Windows or UNIX, became widely adopted in control centers and were typically connected to remote controllers via private networks. The continued expansion of the energy sector and the addition of new and often remote facilities dictated greater reliance on public telecommunications networks, such as the Internet, to monitor and communicate with those assets.

However, each auxiliary connection to a public network provides a fresh point of entry for prospective cyber attacks and increases the burden on asset owners to manage the progressively complex paths of incoming and outgoing information. This elevated system accessibility exposes network assets to potential cyber infiltration and subsequent manipulation of sensitive operations in the energy sector.

Appendix E: Acronyms

AMI	advanced metering infrastructure
AMI-SEC	AMI Security
ANTFARM	Advanced Network Toolkit for Assessments and Remote Mapping
API	American Petroleum Institute
ARRA	American Recovery and Reinvestment Act of 2009
ASAP-SG	Advanced Security Acceleration Project – Smart Grid
CEDS	Cybersecurity for Energy Delivery Systems program
CIP	Critical Infrastructure Protection
CIO	chief information officer
CIPAC	DHS Critical Infrastructure Partnership Advisory Council
CISO	chief information security officer
COTS	commercial off the shelf
CS2SAT	Control System Cyber Security Self-Assessment Tool
CSSP	DHS Control System Security Program
DCS	distributed control system
DHS	U.S. Department of Homeland Security
DNP3	Distributed Network Protocol
DOE	U.S. Department of Energy
EMS	energy management system
EnergySec	Energy Sector Security Consortium, Inc.
EPACT	Energy Policy Act of 2005
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas
ERO	Electricity Reliability Organization
ESCC	Electricity Sub-sector Coordinating Council
ESCSWG	Energy Sector Control Systems Working Group
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
ESP	electronic security perimeter
FACA	Federal Advisory Committee Act
FBI	Department of Justice, Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard
FY	fiscal year
GCC	Government Coordinating Council

HAN	home area network
HMI	human machine interface
HSIN	Homeland Security Information Network
I3P	Institute for Information Infrastructure Protection
ICCP	Inter-control Center Communications Protocol
ICP	IPSec interoperability configuration profile
ICS	industrial control system
ICS CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers
ieRoadmap	interactive energy Roadmap website, *www.controlsystemsroadmap.net*
IESO	independent electricity system operator
IETF	Internet Engineering Task Force
INL	Idaho National Laboratory
IP	Internet Protocol
IPSec	Internet protocol security
ISA	International Society of Automation
ISER	Infrastructure Security & Energy Restoration
ISO	independent system operator
IT	information technology
LAN	local area network
LANL	Los Alamos National Laboratory
LCRA	Lower Colorado River Authority
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
MTU	master terminal unit
MW	megawatt
NAESB	North American Energy Standards Board
NERC	North American Electric Reliability Corporation
NESCO	National Electric Sector Cybersecurity Organization
NESCOR	National Electric Sector Cybersecurity Organization Resource
NetAPT	Network Access Policy Tool
NETL	National Energy Technology Laboratory
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology

NISTIR	NIST Interagency Report
NSTB	National SCADA Test Bed
OE	Office of Electricity Delivery and Energy Reliability
OLE	object linking and embedding
OPC	OLE for process control
OpenSG	OpenSmartGrid
OPSAID	Open PCS Architecture for Interoperable Design
ORNL	Oak Ridge National Laboratory
OS	operating system
PCII	DHS Protected Critical Infrastructure Information
PCS	process control system
PLC	programmable logic controller
PNNL	Pacific Northwest National Laboratory
QoS	quality of service
R&D	research and development
RBAC	role-based access control
RISI	Repository of Industrial Security Incidents
RiskMAP	Risk-to-Mission Assessment Process
RRE	Recovery and Response Engine
RTO	regional transmission operator
RTU	remote terminal unit
SBU	Sensitive But Unclassified
SCADA	supervisory control and data acquisition
SCC	Sector Coordinating Council
SDL	security development life cycle
SEL	Schweitzer Engineering Laboratory
SGIP-CSWG	Smart Grid Interoperability Panel - Cyber Security Working Group
SIEGate	Secure Information Exchange Gateway
SSCP	Secure SCADA Communications Protocol
SSP	Sector-Specific Plan
TCIPG	Trustworthy Cyber Infrastructure for the Power Grid
UCAIug	UCA International Users Group
U.S.	United States
VPN	virtual private network
WAN	wide area network
WLAN	wireless local area network

Appendix F: References

1. Reproduced by permission from Donald Satterlee, *ISO Control Room*, digital photograph (California ISO), accessed November 10, 2010, *http://www.caiso.com/14c9/14c9b13039800.html*.

2. Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.*Stuxnet Dossier:* February 2011 (Cupertino, CA: Symantec, 2011), *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*.

3. United States Government Accountability Office, *Electricity Grid Modernization Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed* (Report to Congressional Requesters), GAO-11-117 (Washington, DC: U.S. Government Accountability Office, January 2011),*http://www.gao.gov/products/GAO-11-117*.

4. Howard Schmidt, "Progress Report on Cybersecurity," *The White House Blog*, July 14, 2010, *http://www.whitehouse.gov/blog/2010/07/14/progress-report-cybersecurity*.

5. Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*: February 2011 (Cupertino, CA: Symantec, 2011), *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*.

6. Electricity Sub-sector Coordinating Council (ESCC), *Critical Infrastructure Strategic Roadmap* (Washington, DC: North American Electric Reliability Cooperation, November 2010), *http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf*.

7. North American Electric Reliability Corporation (NERC) and U.S. Department of Energy (DOE), *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (Princeton, NJ: NERC and DOE, June 2010), *http://www.nerc.com/files/HILF.pdf*.

8. "*Recovery Act Selections for Smart Grid Investment Grant Awards – By Category*," U.S. Department of Energy, accessed January 7, 2011, *http://www.energy.gov/recovery/smartgrid_maps/SGIGSelections_Category.pdf*.

9. Water Sector Coordinating Council Cyber Security Working Group, *Roadmap to Secure Control Systems in the Water Sector* (Washington, DC: American Water Works Association and U.S. Department of Homeland Security, March 2008), *http://www.nawc.org/policy-issues/utility-security-resources/Final%20Water%20Security%20Roadmap%2003-19-08.pdf*.

10. Chemical Sector Roadmap Working Group, *Roadmap to Secure Control Systems in the Chemical Sector* (Washington, DC: U.S. Department of Homeland Security and Chemical Sector Coordinating Council, September 2009), *http://www.us-cert.gov/control_systems/pdf/ChemSec_Roadmap.pdf*.

11. U.S. Department of Homeland Security and U.S. Department of Energy (DOE), *Energy: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted)* (Washington, DC: DOE, May 2007), *http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_Public.pdf*.

12. North American Electric Reliability Corporation (NERC), *2009 Long-Term Reliability Assessment: 2009-2018* (Princeton, NJ: NERC, October 2009), *http://www.nerc.com/files/2009_LTRA.pdf*.

13. National Infrastructure Advisory Council (NIAC), *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Counc*il (Washington, DC: NIAC, October 19, 2010), *http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf*.

14. U.S. Department of Homeland Security (DHS) Science and Technology Directorate, A *Roadmap for Cybersecurity Research* (Washington, DC: DHS, November 2009), *http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf*.

15. U.S. Department of Homeland Security (DHS) National Cyber Security Division, *Strategy for Securing Control Systems: Coordinating and Guiding Federal, State, and Private Sector Initiatives* (Washington, DC: DHS, October 2009), *http://www.us-cert.gov/control_systems/pdf/Strategy%20for%20Securing%20Control%20Systems.pdf*.

16. The White House, *Cyberspace Policy Review* (Washington, DC: White House, May 2009), *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*.

17. "A number of efforts exist to define visions for some technology or infrastructure sectors. For example, the U.S. Department of Energy, in collaboration with industry, in 2005 published a 10-year roadmap for securing control systems used in the power grid." The White House, *Cyberspace Policy Review* (Washington, DC: White House, May 2009), 32*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*; "The NIAC recommends…the Department of Homeland Security (DHS) and Sector-Specific Agencies (SSAs) collaborate with their respective owner/operator sector partners to develop sector-specific roadmaps using the Energy Sector Roadmap as a model." National Infrastructure Advisory Council, Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group, *Final Report and Recommendations by the Council* (Washington, DC: NIAC, January 16, 2007), 3, *http://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf*; "The Critical Infrastructure Protection Committee recommends that the North American Electric Reliability Council (NERC) endorse the Roadmap to Secure Control Systems in the Energy Sector and provide an active role in guiding the implementation of the Roadmap." North American Electric Reliability Council (now North American Electric Reliability Corporation), "Critical Infrastructure Protection Committee Meeting Highlights" (Critical Infrastructure Protection Committee Meeting, Arlington, Virginia, June 20-21, 2006), 2, *http://www.nerc.com/docs/cip/highlights_cipc_20jun2006-1.pdf*.

18. The White House, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy* (Washington, DC: White House, April 15, 2011), *http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*.

19. National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel to the Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, Draft NISTIR 7628 (Gaithersburg, MD: NIST, August 2010), *http://csrc.nist.gov/publications/PubsNISTIRs.html*.

20. National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel to the Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol 1, Supportive Analyses and References*, NISTIR 7628 (Gaithersburg, MD: NIST, August 2010), *http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf*.

21. National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel to the Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol 3, Supportive Analyses and References*, NISTIR 7628 (Gaithersburg, MD: NIST, August 2010), *http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf*.

22. Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*: February 2011 (Cupertino, CA: Symantec, 2011), *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*.

23. North American Electric Reliability Corporation (NERC), *2009 Long-Term Reliability Assessment: 2009-2018* (Princeton, NJ: NERC, October 2009), *http://www.nerc.com/files/2009_LTRA.pdf*.

24. U.S. Government Accountability Office (GAO), *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats*, statement of Gregory Wilshusen and David Powner, GAO-10-230T (Washigton, DC: GAO, November 17, 2009), *http://www.gao.gov/new.items/d10230t.pdf*.

25. National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel to the Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, Draft NISTIR 7628 (Gaithersburg, MD: NIST, August 2010), *http://csrc.nist.gov/publications/PubsNISTIRs.html*.

26. U.S. Government Accountability Office (GAO), *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats*, statement of Gregory Wilshusen and David Powner, GAO-10-230T (Washington, DC: GAO, November 17, 2009), *http://www.gao.gov/new.items/d10230t.pdf*.

27. Lewis Branscomb, Philip Auerswald, Todd La Porte, et al., *Seeds of Disaster, Roots of Response How Private Action Can Reduce Public Vulnerability* (Cambridge, MA: Cambridge University Press, 2006).

28. Vince Mancuso, "Moving from Theory to Practice: Integrating Human Factors into an Organization" (1996), Neil Krey's CRM Developers Forum, accessed April 18, 2010, *http://www.crm-devel.org/ftp/mancuso.pdf*.

29. IEEE Power & Energy Society, U.S. Power and Energy Engineering Workforce Collaborative, Management Steering Committee, P*reparing the U.S. Foundation for Future Electric Energy Systems: A Strong Power and Energy Engineering Workforce* (New York: IEEE, April 2009), *http://www.ieee-pes.org/images/pdf/US_Power_&_Energy_Collaborative_Action_Plan_April_2009_Adobe72.pdf*.

30. National Institute of Standards and Technology (NIST), *The Economic Impacts of Inadequate Infrastructure for Software Testing*, Planning Report 02-3, produced by RTI International, Research Triangle Park, NC (Gaithersburg, MD: NIST, May 2002), *http://www.nist.gov/director/planning/upload/report02-3.pdf*.

31. U.S. Department of Energy (DOE), S*mart Grid System Report* (Washington, DC: DOE, July 2009), *http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf*.

32. National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel to the Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, Draft NISTIR 7628 (Gaithersburg, MD: NIST, August 2010), *http://csrc.nist.gov/publications/PubsNISTIRs.html*.

33. Richard Caralli, James Stevens, Charles Wallen, et al., *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management*, CMU/SEI-2006-TN-009, prepared by Carnegie Mellon University Software Engineering Institute< Pittsburgh, Pennsylvania (Pittsburgh, PA: Carnegie Mellon University, April 2006), *www.cert.org/archive/pdf/sustainoperresil0604.pdf*.

34. National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel to the Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, Draft NISTIR 7628 (Gaithersburg, MD: NIST, August 2010), *http://csrc.nist.gov/publications/PubsNISTIRs.html*.

35. U.S. Department of Homeland Security (DHS) Control Systems Security Program, National Cyber Security Division, *Recommended Practice; Developing an Industrial Control Systems Cybersecurity Incident Response Capability* (Washington, DC: DHS, October 2009), *http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf*.

36. "Utilities are focusing on regulatory compliance instead of comprehensive security. The existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity. Specifically, experts told us that utilities focusing on achieving minimum regulatory requirements rather than designing a comprehensive approach to systems security. In addition, one expert stated that security requirements are inherently incomplete, and having a culture that views the security problem as being solved once those requirements are met will leave an organization vulnerable to cyber attack. Consequently, without a comprehensive approach to security, utilities leave themselves open to unnecessary risk." United States Government Accountability Office, *Electricity Grid Modernization Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed* (Report to Congressional Requesters), GAO-11-117 (Washington, DC: U.S. Government Accountability Office, January 2011), 23, *http://www.gao.gov/products/GAO-11-117*.

37. Dennis C. Blair, *Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence* (Washington, DC: Office of the Director of National Intelligence, February 2, 2010), *http://www.dni.gov/testimonies/20100202_testimony.pdf*.

38. "Current Research Projects," Digital Bond, accessed January 7, 2011, *http://www.digitalbond.com/index.php/research/*.

39. U.S. Department of Energy, *Energy Sector-Specific Plan* (Washington, DC: U.S. Department of Energy, May 2007), 41, *http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf*.

40. North American Electric Reliability Corporation (NERC), *(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1* (Princeton, NJ: NERC), *http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf*.

41. North American Electric Reliability Corporation (NERC), "Cyber Security – Incident Reporting and Response Planning," Standard CIP-008-3 of Critical Infrastructure Protection Reliability Standards (Princeton, NJ: NERC, December 16, 2009), accessed January 7, 2011, *http://www.nerc.com/page.php?cid=2|20*.

42. "Recovery Act Selections for Smart Grid Investment Grant Awards – By Category," U.S Department of Energy, accessed January 7, 2011, *http://www.energy.gov/recovery/smartgrid_maps/SGIGSelections_Category.pdf*.

43. U.S. Energy Information Administration, "Existing Capacity by Energy Source, 2009,"table 1.2 in *Electric Power Annual with data for 2009* (Washington, DC: U.S. Department of Energy, revised January 4, 2011), *http://www.eia.doe.gov/cneaf/electricity/epa/epat1p2.html*.

44. Ibid.

45. "About NERC: Understanding the Grid," North American Electric Reliability Corporation (NERC), accessed January 7, 2011, *http://www.nerc.com/page.php?cid=1|15*.

46. National Institute of Standards and Technology (NIST), *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, SP 1108 (Gaithersburg, MD: NIST, January 2010), 33, *http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf*.

47. Ibid., 131.

48. "Natural Gas Supply," NaturalGas.org, accessed January 7, 2011, *http://www.naturalgas.org/business/supply.asp.*

49. "Welcome to Pipeline 101," Pipeline 101, accessed January 7, 2011, *http://www.pipeline101.com*.

50. Keith Stouffer, et al., Guide to Industrial Control Systems (ICS) Security: Recommendations of the National Institute of Standards and Technology, Final Public Draft, NIST SP 800-82 (Gaithersburg, MD: National Institute of Standards and Technology, 2008), *http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf*.