Roadmap Update Workshop Summaries

January 2011

Energy Sector Control Systems Working Group

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

Roadmap Development Process

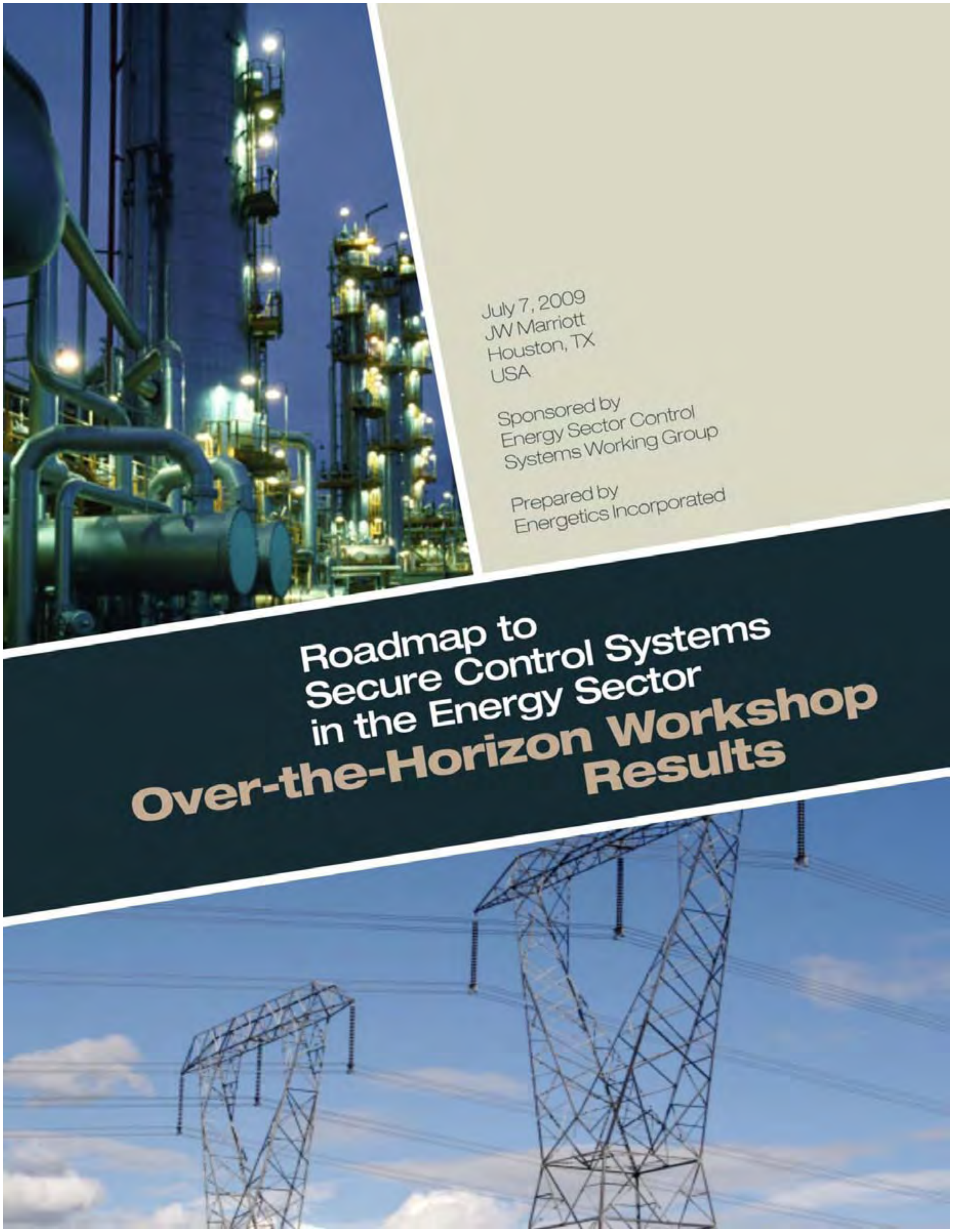
While much progress has been made, the public and private partners are keenly aware that there is more work to do with today's rapid pace of change and dynamic energy delivery systems landscape. The Energy Sector Control Systems Working Group (ESCSWG) collaborated with energy sector stakeholders to update the Roadmap in 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—the vision and goal areas—and provided recommendations to better align the framework with the wide range of complex energy delivery systems security needs the sector will need to address today and in the future.
- **Roadmap Update Workshop**: On September 2-3, 2009, more than 80 asset owners and operators, CIOs, researchers, technology developers, security specialists, and vendors renewed their commitment to the industry's vision and partnership efforts and tackled the most persistent challenges: vulnerability disclosure, technology gaps and advancements, innovative partnerships, and measuring progress. Participants defined the issues and identified a set of prioritized solutions the public-private partnership can act on immediately.
- **Roadmap Technical Review Workshop**: On November 18, 2009, 12 subject matter experts convened to clarify the technical challenges and recommend additional milestones to ensure the sector has a clear path to achieving Roadmap goals.
- **Roadmap Review**: The Working Group synthesized the results of the above efforts to update the 2006 Roadmap and create a draft Roadmap. The draft Roadmap was circulated among Roadmap Workshop participants, energy delivery systems experts, and on the ieRoadmap (www.controlsystemsroadmap.net) for comment and was revised for clarity and added insight.

The *Roadmap to Secure Energy Delivery Systems* was created to guide and align public and private efforts to achieve and sustain the energy sector's vision.

Table of Contents

1. Over-the Horizon Analysis



July 7, 2009
JW Marriott
Houston, TX
USA

Sponsored by
Energy Sector Control
Systems Working Group

Prepared by
Energetics Incorporated

Roadmap to
Secure Control Systems
in the Energy Sector

Over-the-Horizon Workshop
Results

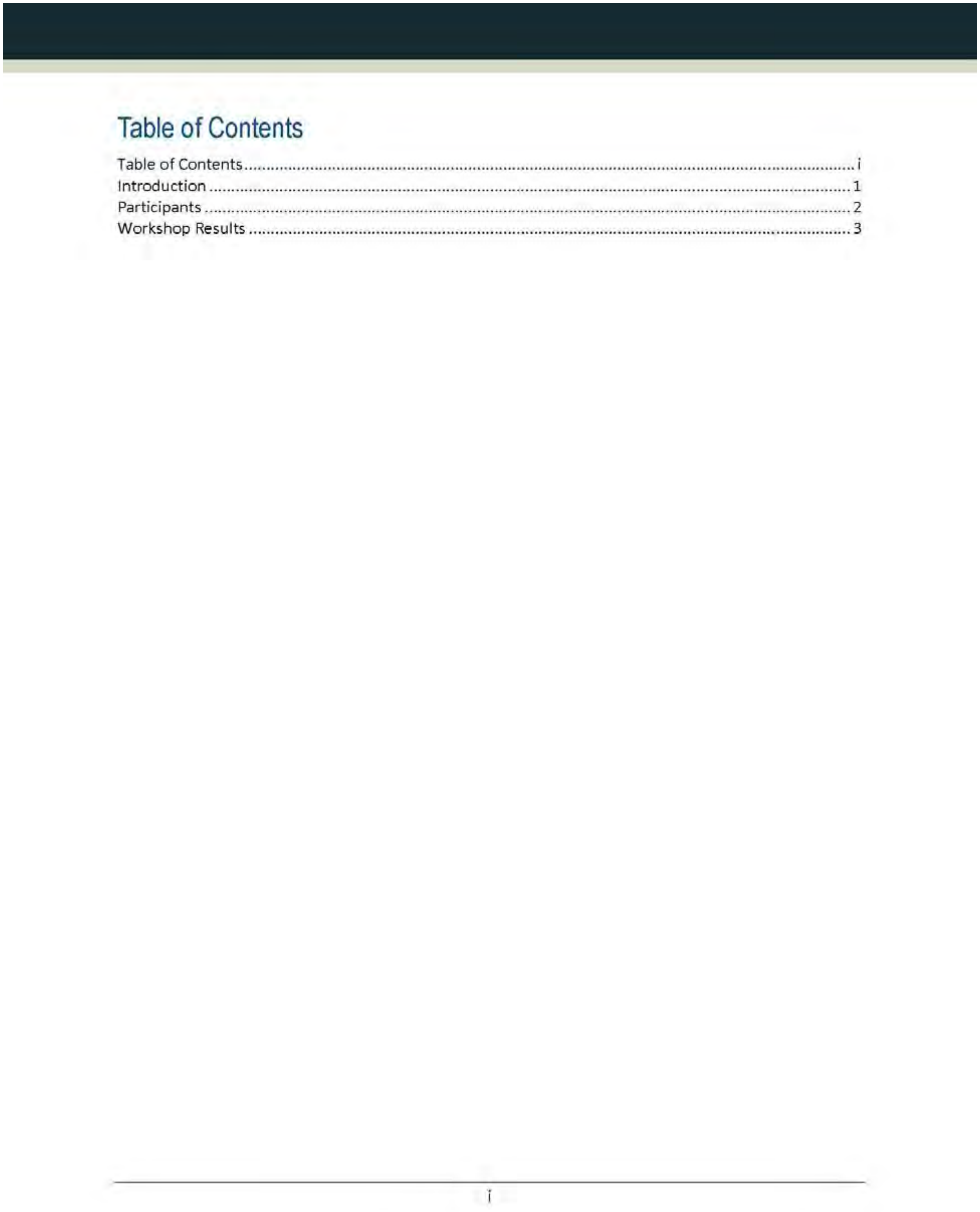
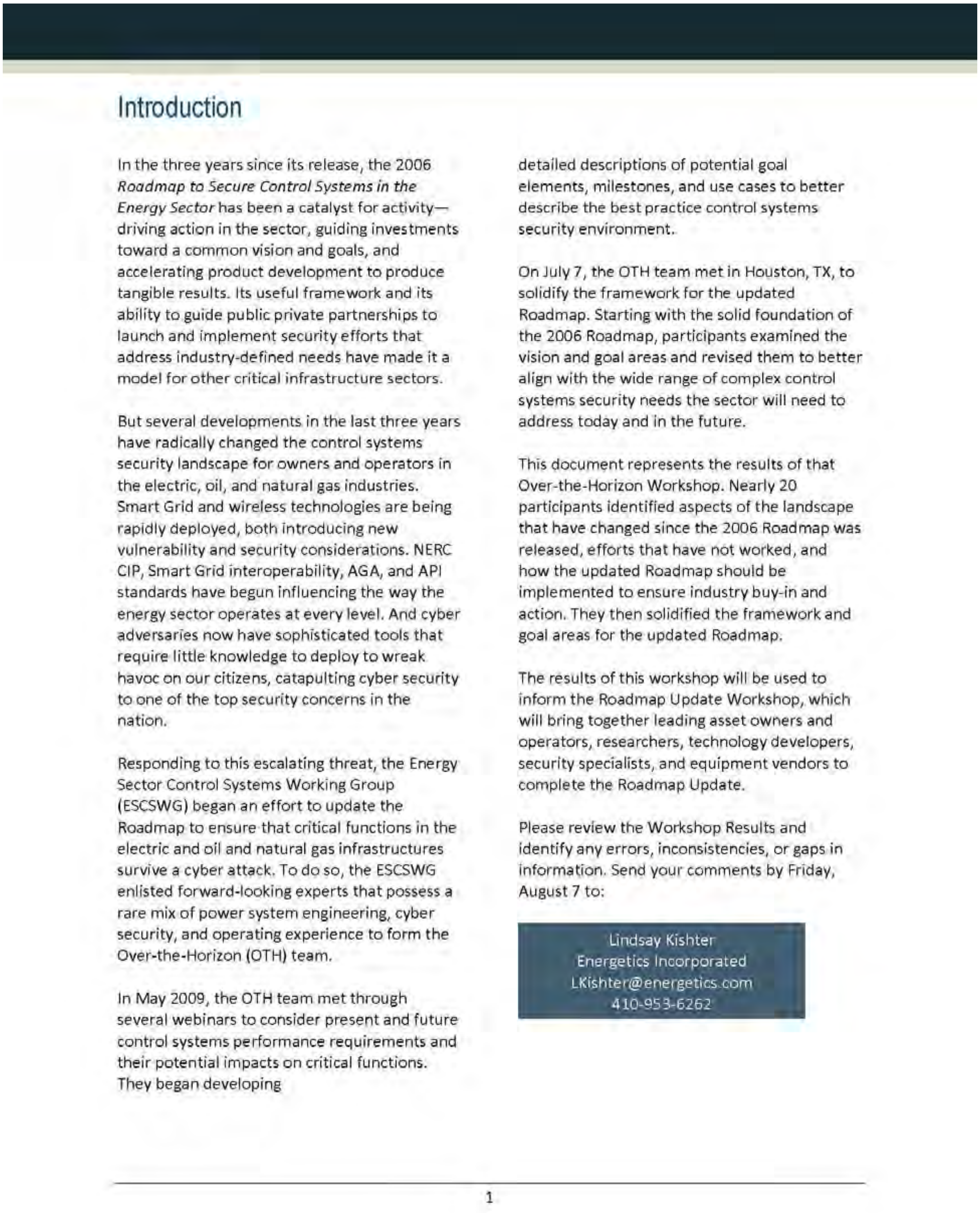


Table of Contents



Introduction

In the three years since its release, the 2006 *Roadmap to Secure Control Systems in the Energy Sector* has been a catalyst for activity—driving action in the sector, guiding investments toward a common vision and goals, and accelerating product development to produce tangible results. Its useful framework and its ability to guide public private partnerships to launch and implement security efforts that address industry-defined needs have made it a model for other critical infrastructure sectors.

But several developments in the last three years have radically changed the control systems security landscape for owners and operators in the electric, oil, and natural gas industries. Smart Grid and wireless technologies are being rapidly deployed, both introducing new vulnerability and security considerations. NERC CIP, Smart Grid interoperability, AGA, and API standards have begun influencing the way the energy sector operates at every level. And cyber adversaries now have sophisticated tools that require little knowledge to deploy to wreak havoc on our citizens, catapulting cyber security to one of the top security concerns in the nation.

Responding to this escalating threat, the Energy Sector Control Systems Working Group (ESCSWG) began an effort to update the Roadmap to ensure that critical functions in the electric and oil and natural gas infrastructures survive a cyber attack. To do so, the ESCSWG enlisted forward-looking experts that possess a rare mix of power system engineering, cyber security, and operating experience to form the Over-the-Horizon (OTH) team.

In May 2009, the OTH team met through several webinars to consider present and future control systems performance requirements and their potential impacts on critical functions. They began developing detailed descriptions of potential goal elements, milestones, and use cases to better describe the best practice control systems security environment.

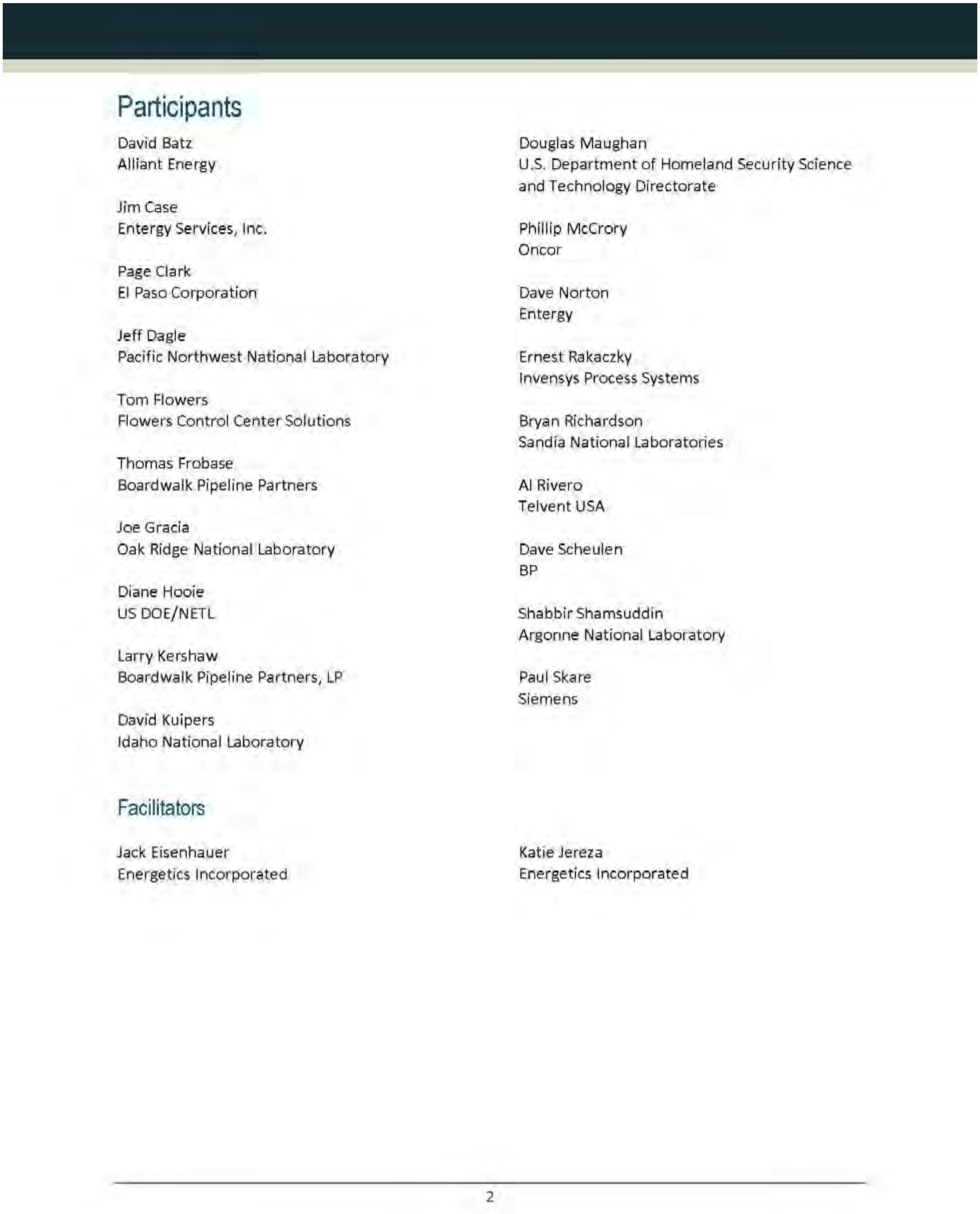
On July 7, the OTH team met in Houston, TX, to solidify the framework for the updated Roadmap. Starting with the solid foundation of the 2006 Roadmap, participants examined the vision and goal areas and revised them to better align with the wide range of complex control systems security needs the sector will need to address today and in the future.

This document represents the results of that Over-the-Horizon Workshop. Nearly 20 participants identified aspects of the landscape that have changed since the 2006 Roadmap was released, efforts that have not worked, and how the updated Roadmap should be implemented to ensure industry buy-in and action. They then solidified the framework and goal areas for the updated Roadmap.

The results of this workshop will be used to inform the Roadmap Update Workshop, which will bring together leading asset owners and operators, researchers, technology developers, security specialists, and equipment vendors to complete the Roadmap Update.

Please review the Workshop Results and identify any errors, inconsistencies, or gaps in information. Send your comments by Friday, August 7 to:

Lindsay Kishter
Energetics Incorporated
LKishter@energetics.com
410-953-6262



Participants

David Batz
Alliant Energy

Jim Case
Entergy Services, Inc.

Page Clark
El Paso Corporation

Jeff Dagle
Pacific Northwest National Laboratory

Tom Flowers
Flowers Control Center Solutions

Thomas Frobase
Boardwalk Pipeline Partners

Joe Gracia
Oak Ridge National Laboratory

Diane Hooie
US DOE/NETL

Larry Kershaw
Boardwalk Pipeline Partners, LP

David Kuipers
Idaho National Laboratory

Douglas Maughan
U.S. Department of Homeland Security Science and Technology Directorate

Phillip McCrory
Oncor

Dave Norton
Entergy

Ernest Rakaczky
Invensys Process Systems

Bryan Richardson
Sandia National Laboratories

Al Rivero
Telvent USA

Dave Scheulen
BP

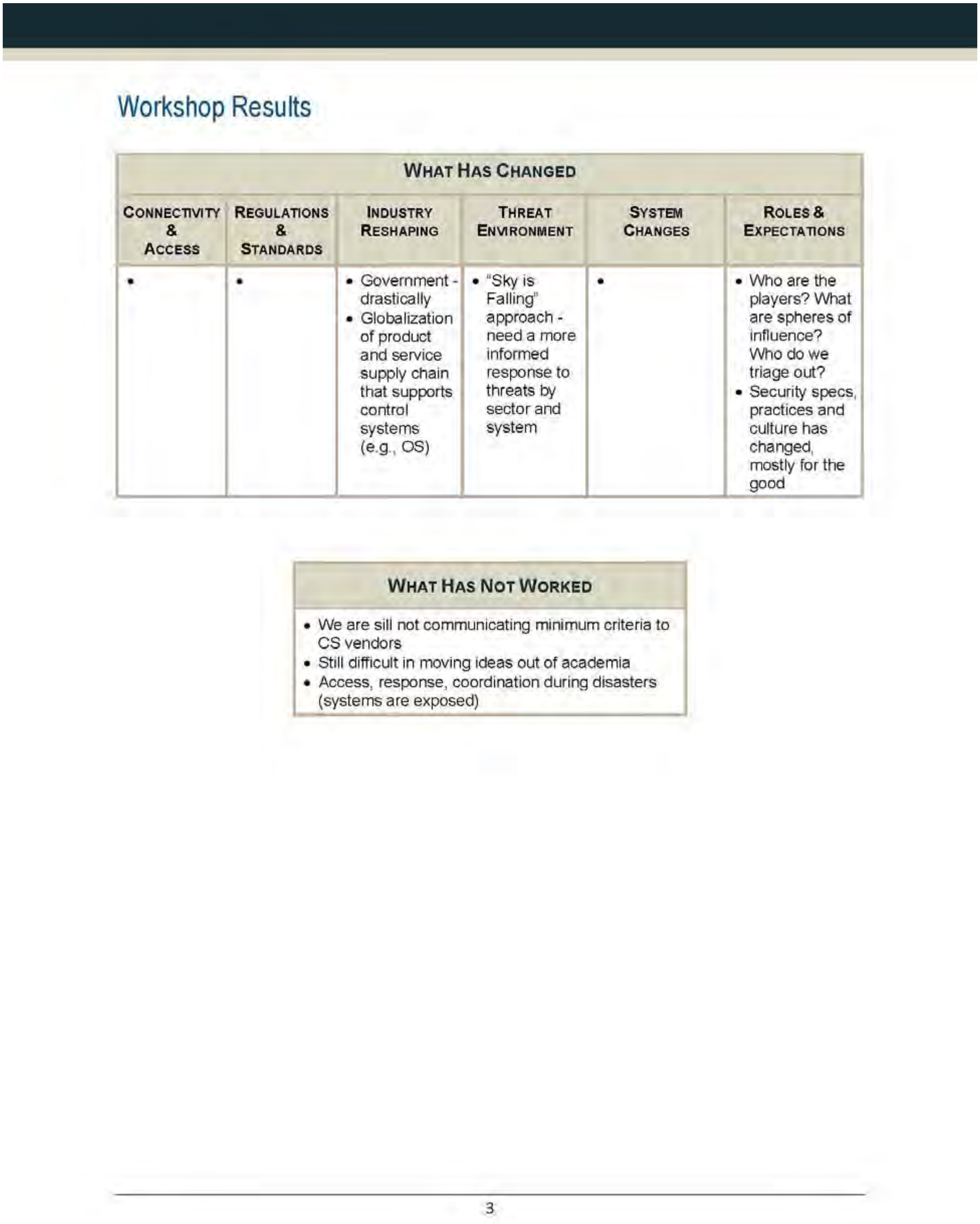
Shabbir Shamsuddin
Argonne National Laboratory

Paul Skare
Siemens

Facilitators

Jack Eisenhauer
Energetics Incorporated

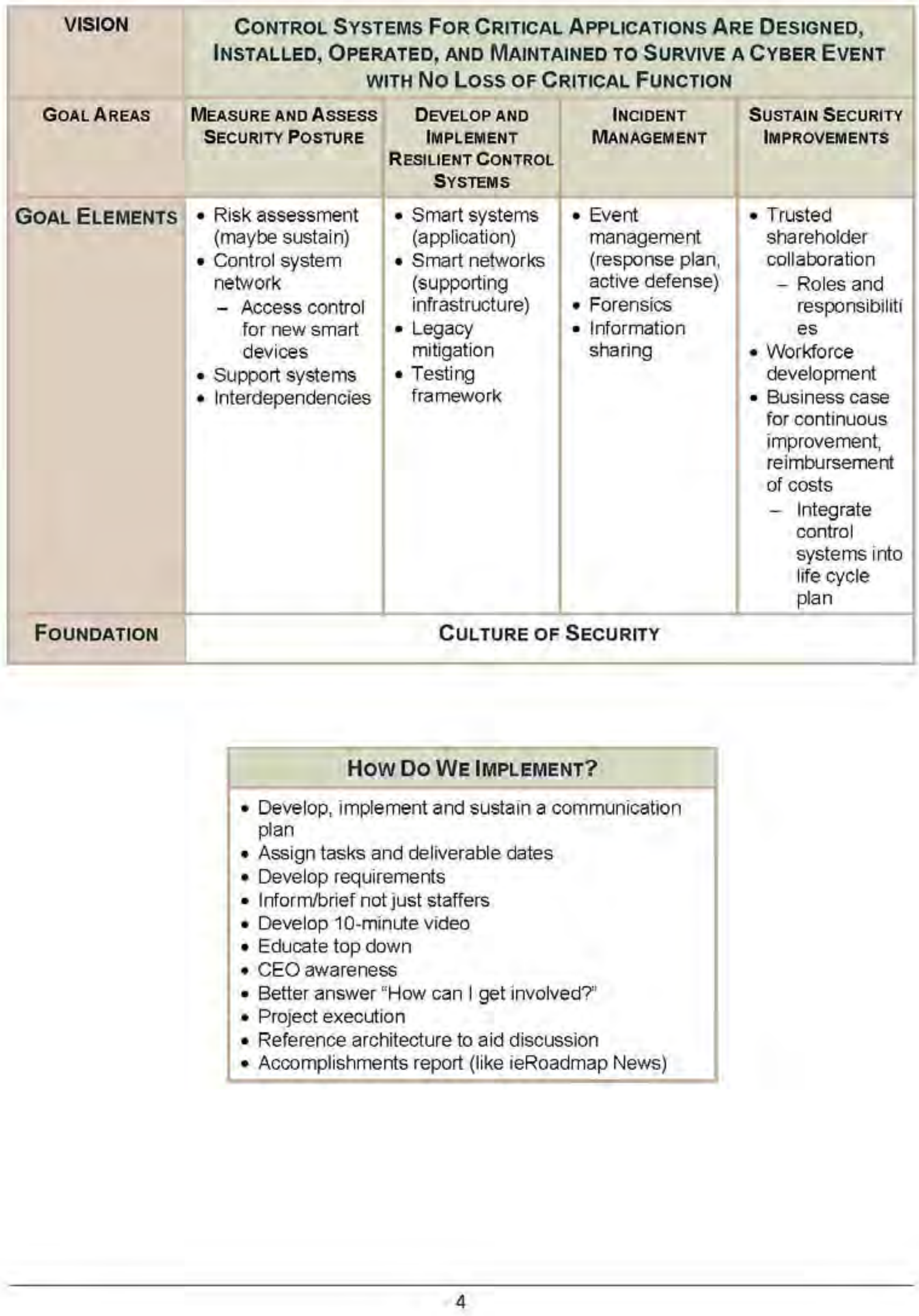
Katie Jereza
Energetics Incorporated



Workshop Results

What Has Changed					
Connectivity & Access	Regulations & Standards	Industry Reshaping	Threat Environment	System Changes	Roles & Expectations
•	•	• Government - drastically • Globalization of product and service supply chain that supports control systems (e.g., OS)	• "Sky is Falling" approach - need a more informed response to threats by sector and system	•	• Who are the players? What are spheres of influence? Who do we triage out? • Security specs, practices and culture has changed, mostly for the good

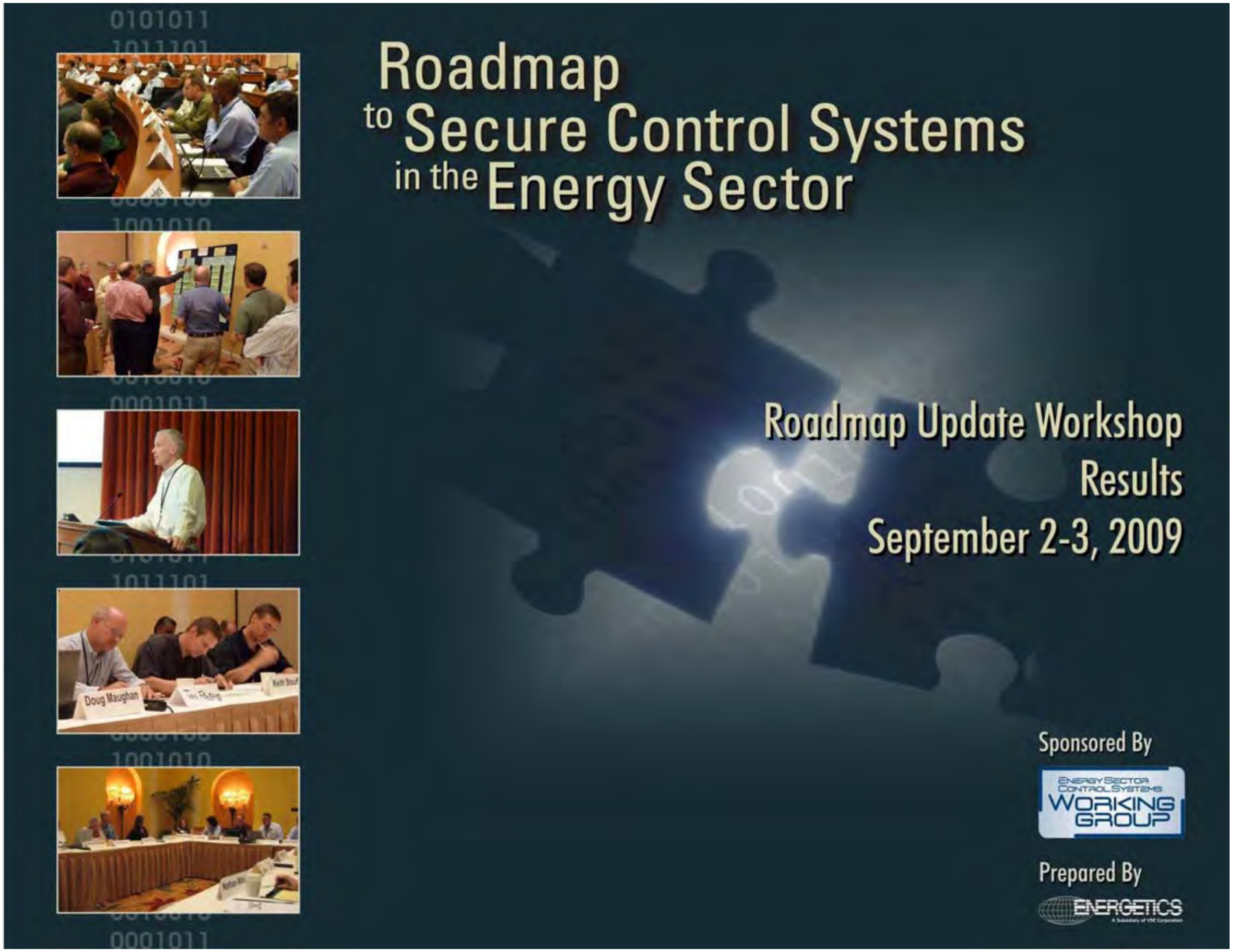
What Has Not Worked
• We are sill not communicating minimum criteria to CS vendors • Still difficult in moving ideas out of academia • Access, response, coordination during disasters (systems are exposed)



VISION	CONTROL SYSTEMS FOR CRITICAL APPLICATIONS ARE DESIGNED, INSTALLED, OPERATED, AND MAINTAINED TO SURVIVE A CYBER EVENT WITH NO LOSS OF CRITICAL FUNCTION			
GOAL AREAS	MEASURE AND ASSESS SECURITY POSTURE	DEVELOP AND IMPLEMENT RESILIENT CONTROL SYSTEMS	INCIDENT MANAGEMENT	SUSTAIN SECURITY IMPROVEMENTS
GOAL ELEMENTS	• Risk assessment (maybe sustain) • Control system network – Access control for new smart devices • Support systems • Interdependencies	• Smart systems (application) • Smart networks (supporting infrastructure) • Legacy mitigation • Testing framework	• Event management (response plan, active defense) • Forensics • Information sharing	• Trusted shareholder collaboration – Roles and responsibiliti es • Workforce development • Business case for continuous improvement, reimbursement of costs – Integrate control systems into life cycle plan
FOUNDATION	CULTURE OF SECURITY			

HOW DO WE IMPLEMENT?
• Develop, implement and sustain a communication plan • Assign tasks and deliverable dates • Develop requirements • Inform/brief not just staffers • Develop 10-minute video • Educate top down • CEO awareness • Better answer "How can I get involved?" • Project execution • Reference architecture to aid discussion • Accomplishments report (like ieRoadmap News)

2. Roadmap Update Workshop



Roadmap
to Secure Control Systems
in the Energy Sector

Roadmap Update Workshop
Results
September 2-3, 2009

Sponsored By

Energy Sector Control Systems Working Group

Prepared By

Energetics
A Subsidiary of VSE Corporation

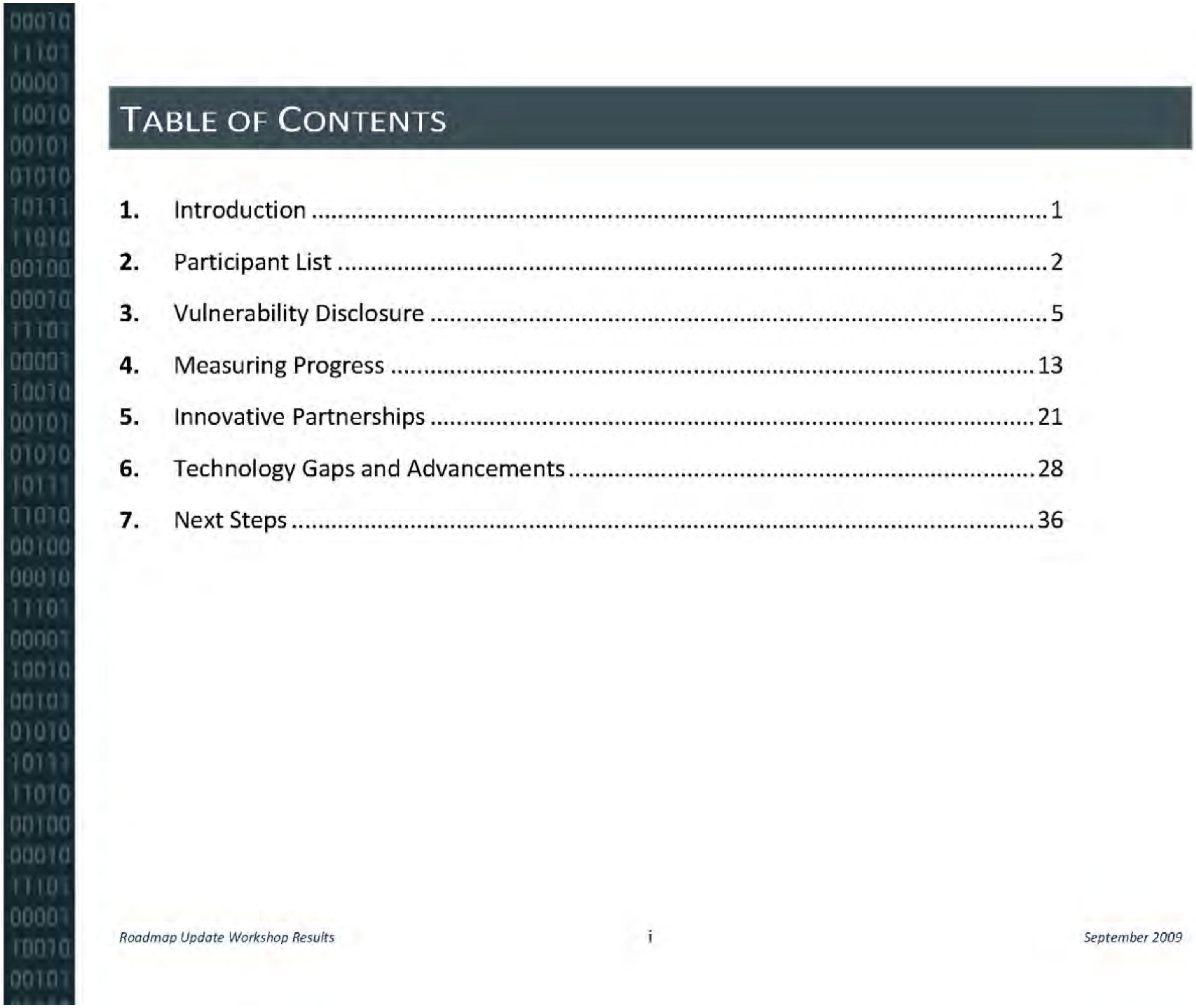
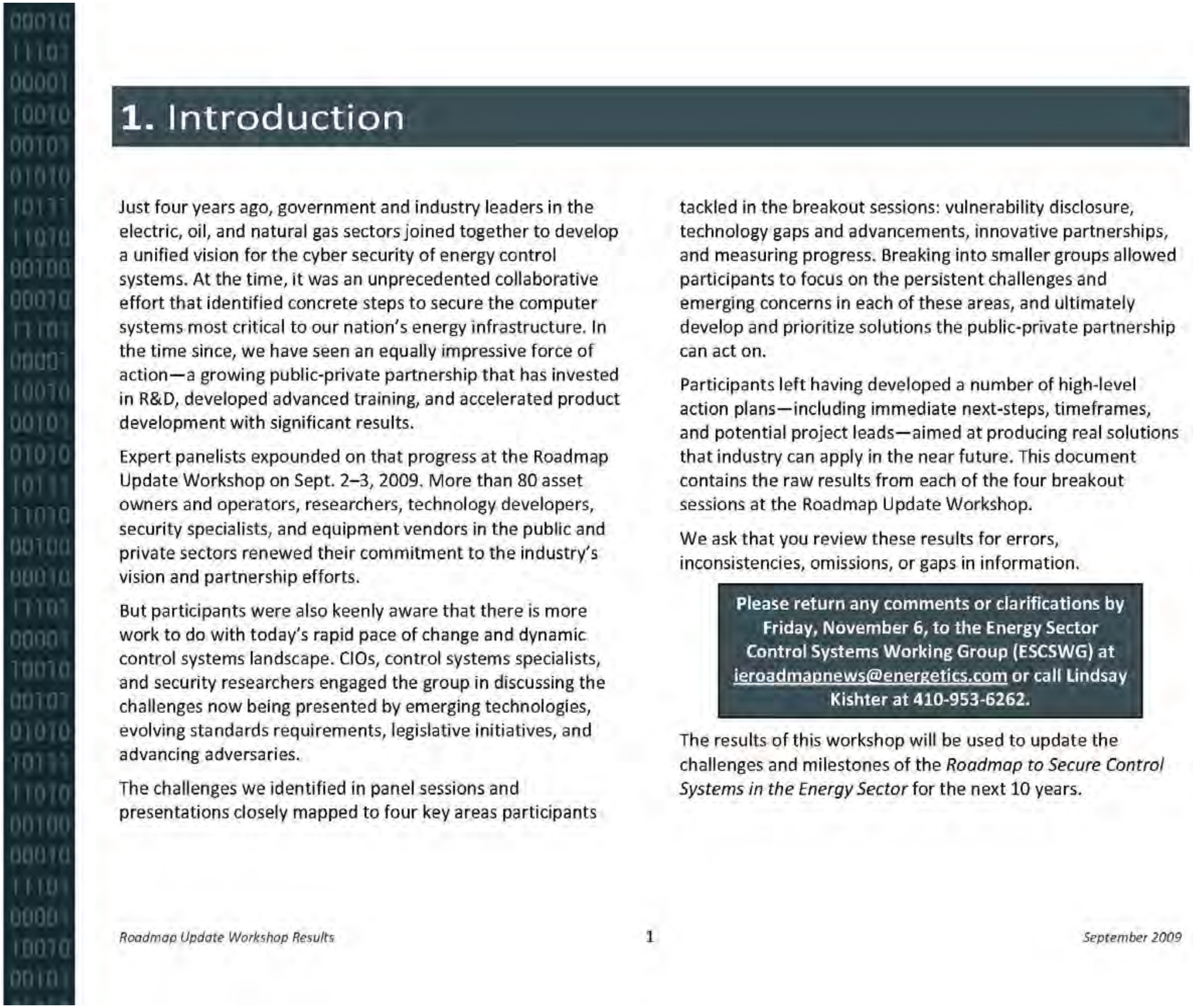


Table of Contents



1. Introduction

Just four years ago, government and industry leaders in the electric, oil, and natural gas sectors joined together to develop a unified vision for the cyber security of energy control systems. At the time, it was an unprecedented collaborative effort that identified concrete steps to secure the computer systems most critical to our nation's energy infrastructure. In the time since, we have seen an equally impressive force of action—a growing public-private partnership that has invested in R&D, developed advanced training, and accelerated product development with significant results.

Expert panelists expounded on that progress at the Roadmap Update Workshop on Sept. 2–3, 2009. More than 80 asset owners and operators, researchers, technology developers, security specialists, and equipment vendors in the public and private sectors renewed their commitment to the industry's vision and partnership efforts.

But participants were also keenly aware that there is more work to do with today's rapid pace of change and dynamic control systems landscape. CIOs, control systems specialists, and security researchers engaged the group in discussing the challenges now being presented by emerging technologies, evolving standards requirements, legislative initiatives, and advancing adversaries.

The challenges we identified in panel sessions and presentations closely mapped to four key areas participants tackled in the breakout sessions: vulnerability disclosure, technology gaps and advancements, innovative partnerships, and measuring progress. Breaking into smaller groups allowed participants to focus on the persistent challenges and emerging concerns in each of these areas, and ultimately develop and prioritize solutions the public-private partnership can act on.

Participants left having developed a number of high-level action plans—including immediate next-steps, timeframes, and potential project leads—aimed at producing real solutions that industry can apply in the near future. This document contains the raw results from each of the four breakout sessions at the Roadmap Update Workshop.

We ask that you review these results for errors, inconsistencies, omissions, or gaps in information.

Please return any comments or clarifications by Friday, November 6, to the Energy Sector Control Systems Working Group (ESCSWG) at ieroadmapnews@energetics.com or call Lindsay Kishter at 410-953-6262.

The results of this workshop will be used to update the challenges and milestones of the *Roadmap to Secure Control Systems in the Energy Sector* for the next 10 years.

2. Participant List

Nabil Adam
U.S. Department of Homeland Security

John Allen
International Electrcity Infrastructure Assurance Forum

Matt Antes
Energetics Incorporated

John Audia
Special Technologies Laboroatory

Phil Beekman
ABB, Inc.

Klaus Bender
Utilities Telecom Council

Steve Berberich
California ISO

Thomas Blair
DHS

Scott Bordenkircher
Arizona Public Service

James Briones
U.S. DOE/NETL

John Burnette
Pacific Northwest National Laboratory

Matthew Carpenter
InGuardians

Page Clark
El Paso Corporation

Samuel Clements
PNNL

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 ISER

David Dunn
IESO

Thomas Edgar
Pacific Northwest National Laboratory

Jack Eisenhauer
Energetics Incorporated

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. DOE/NETL

Jesse Hurley
North American Energy Standards Board

William Hutton
Pacific Northwest National Laboratory

Chris Jager
Energy Sector Security Consortium Inc.

Katie Jereza
Energetics Incorporated

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

Lindsay Kishter
Energetics Incorporated

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

Shawna McQueen
Energetics Incorporated

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

Melanie Seader
Energetics Incorporated

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
NAESB

Bill Winters
Arizona Public Service

3. Vulnerability Disclosure

Background

Credible, actionable, and timely information is essential to ensuring the energy sector can adequately mitigate control systems vulnerabilities before the adversary can exploit them. A key finding in the Energy Sector Control Systems Working Group's (ESCSWG) 2008 *Annual Report* was that vulnerability disclosure and information sharing between and among the U.S. government and industry remain persistent challenges for the energy sector. While addressing these issues was identified as a near-term milestone in the 2006 Roadmap, it's also key to compiling the evidence needed to build a compelling business case to increase private investment in control system security—another Roadmap near-term milestone. To encourage greater information exchange, Vulnerability Disclosure was selected as an area of focus for the Roadmap Update Workshop.

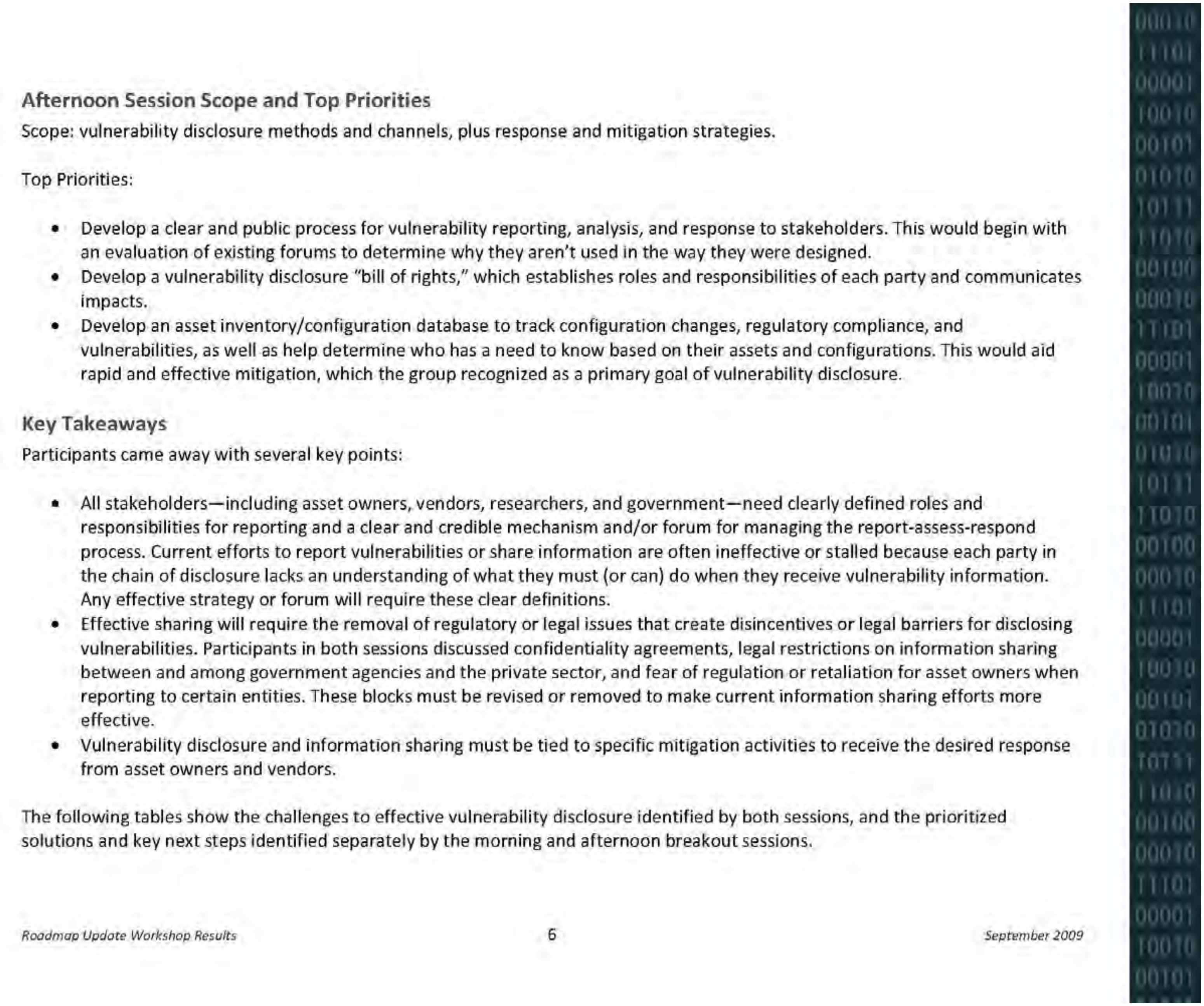
Vulnerability Disclosure was defined as: compatible terms, actionable methods, and useful forums for the public and private sectors to effectively share control systems vulnerability discoveries and mitigation strategies in a timely manner; as well as information sharing mechanisms for control systems security threats, risk management, and best practices.

Morning Session Scope and Top Priorities

Scope: vulnerability discovery, reporting, and mitigation strategies as well as threat and other information sharing mechanisms, recognizing a potential overlap in solutions for both needs.

Top Priorities:

- Develop a process and/or forum for bringing the right people to the table for sharing vulnerability and threat information. The forum would allow vulnerabilities to be vetted with subject matter experts and shared with the appropriate stakeholders, so that asset owners do not find out through the media or other open forums, where incorrect information may be shared. Participants recommended piggybacking on an online forum like EnergySec or developing something similar.
- Develop a matrix for action, including who found the vulnerability, the stakeholders affected, and the degree of risk in order for asset owners to better assess vulnerability information and prioritize response actions. Before these solutions can be realized, however, the group determined two overarching actions the industry must take: identifying expectations of both manufacturers and asset owners for vulnerability disclosure, and determining how government rules for information sharing might impede any of these needed actions.



Afternoon Session Scope and Top Priorities

Scope: vulnerability disclosure methods and channels, plus response and mitigation strategies.

Top Priorities:

- Develop a clear and public process for vulnerability reporting, analysis, and response to stakeholders. This would begin with an evaluation of existing forums to determine why they aren't used in the way they were designed.
- Develop a vulnerability disclosure "bill of rights," which establishes roles and responsibilities of each party and communicates impacts.
- Develop an asset inventory/configuration database to track configuration changes, regulatory compliance, and vulnerabilities, as well as help determine who has a need to know based on their assets and configurations. This would aid rapid and effective mitigation, which the group recognized as a primary goal of vulnerability disclosure.

Key Takeaways

Participants came away with several key points:

- All stakeholders—including asset owners, vendors, researchers, and government—need clearly defined roles and responsibilities for reporting and a clear and credible mechanism and/or forum for managing the report-assess-respond process. Current efforts to report vulnerabilities or share information are often ineffective or stalled because each party in the chain of disclosure lacks an understanding of what they must (or can) do when they receive vulnerability information. Any effective strategy or forum will require these clear definitions.
- Effective sharing will require the removal of regulatory or legal issues that create disincentives or legal barriers for disclosing vulnerabilities. Participants in both sessions discussed confidentiality agreements, legal restrictions on information sharing between and among government agencies and the private sector, and fear of regulation or retaliation for asset owners when reporting to certain entities. These blocks must be revised or removed to make current information sharing efforts more effective.
- Vulnerability disclosure and information sharing must be tied to specific mitigation activities to receive the desired response from asset owners and vendors.

The following tables show the challenges to effective vulnerability disclosure identified by both sessions, and the prioritized solutions and key next steps identified separately by the morning and afternoon breakout sessions.

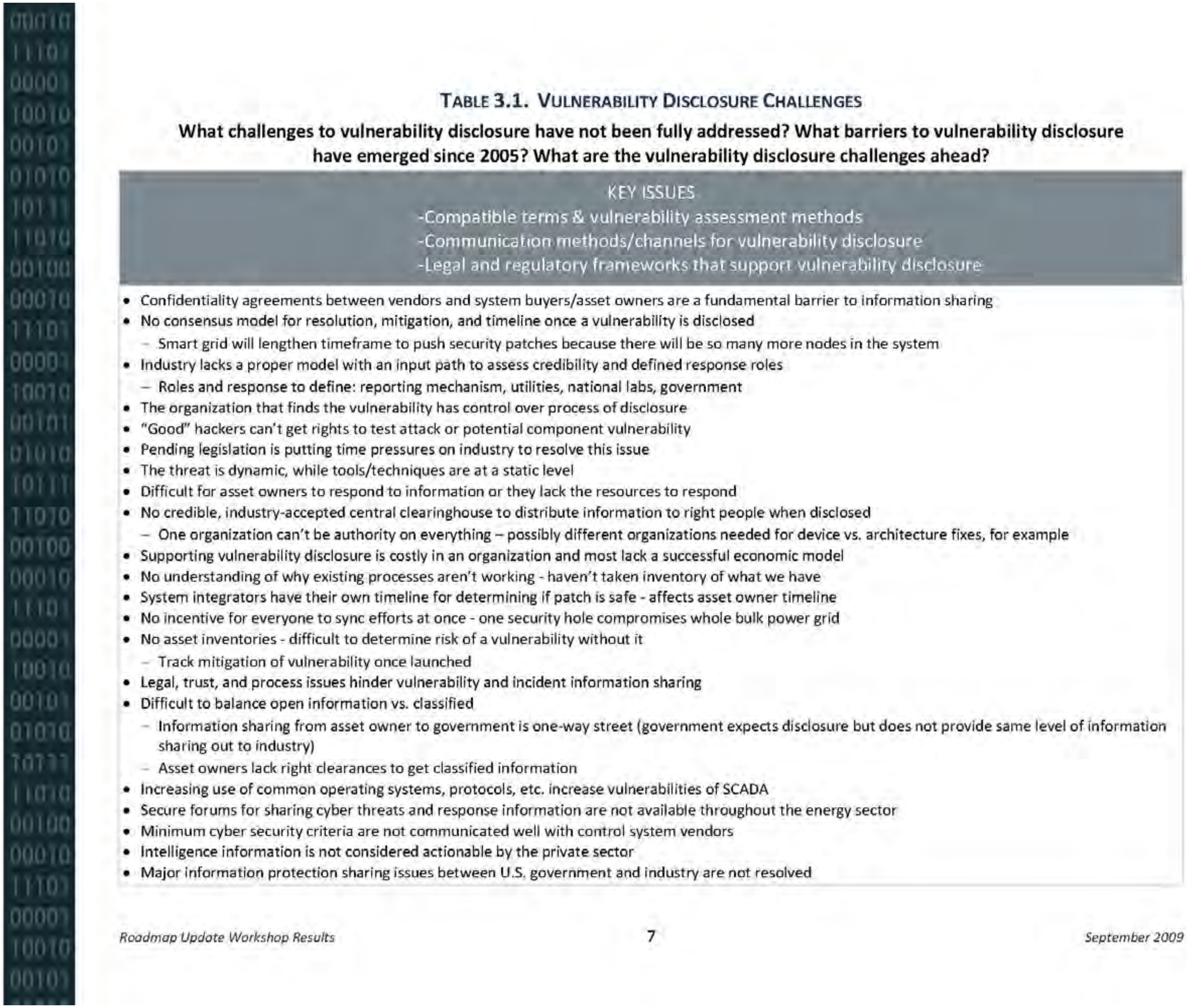


TABLE 3.1. VULNERABILITY DISCLOSURE CHALLENGES

What challenges to vulnerability disclosure have not been fully addressed? What barriers to vulnerability disclosure have emerged since 2005? What are the vulnerability disclosure challenges ahead?

KEY ISSUES

-Compatible terms & vulnerability assessment methods

-Communication methods/channels for vulnerability disclosure

-Legal and regulatory frameworks that support vulnerability disclosure

- Confidentiality agreements between vendors and system buyers/asset owners are a fundamental barrier to information sharing
- No consensus model for resolution, mitigation, and timeline once a vulnerability is disclosed
  - Smart grid will lengthen timeframe to push security patches because there will be so many more nodes in the system
- Industry lacks a proper model with an input path to assess credibility and defined response roles
  - Roles and response to define: reporting mechanism, utilities, national labs, government
- The organization that finds the vulnerability has control over process of disclosure
- "Good" hackers can't get rights to test attack or potential component vulnerability
- Pending legislation is putting time pressures on industry to resolve this issue
- The threat is dynamic, while tools/techniques are at a static level
- Difficult for asset owners to respond to information or they lack the resources to respond
- No credible, industry-accepted central clearinghouse to distribute information to right people when disclosed
  - One organization can't be authority on everything – possibly different organizations needed for device vs. architecture fixes, for example
- Supporting vulnerability disclosure is costly in an organization and most lack a successful economic model
- No understanding of why existing processes aren't working - haven't taken inventory of what we have
- System integrators have their own timeline for determining if patch is safe - affects asset owner timeline
- No incentive for everyone to sync efforts at once - one security hole compromises whole bulk power grid
- No asset inventories - difficult to determine risk of a vulnerability without it
  - Track mitigation of vulnerability once launched
- Legal, trust, and process issues hinder vulnerability and incident information sharing
- Difficult to balance open information vs. classified
  - Information sharing from asset owner to government is one-way street (government expects disclosure but does not provide same level of information sharing out to industry)
  - Asset owners lack right clearances to get classified information
- Increasing use of common operating systems, protocols, etc. increase vulnerabilities of SCADA
- Secure forums for sharing cyber threats and response information are not available throughout the energy sector
- Minimum cyber security criteria are not communicated well with control system vendors
- Intelligence information is not considered actionable by the private sector
- Major information protection sharing issues between U.S. government and industry are not resolved

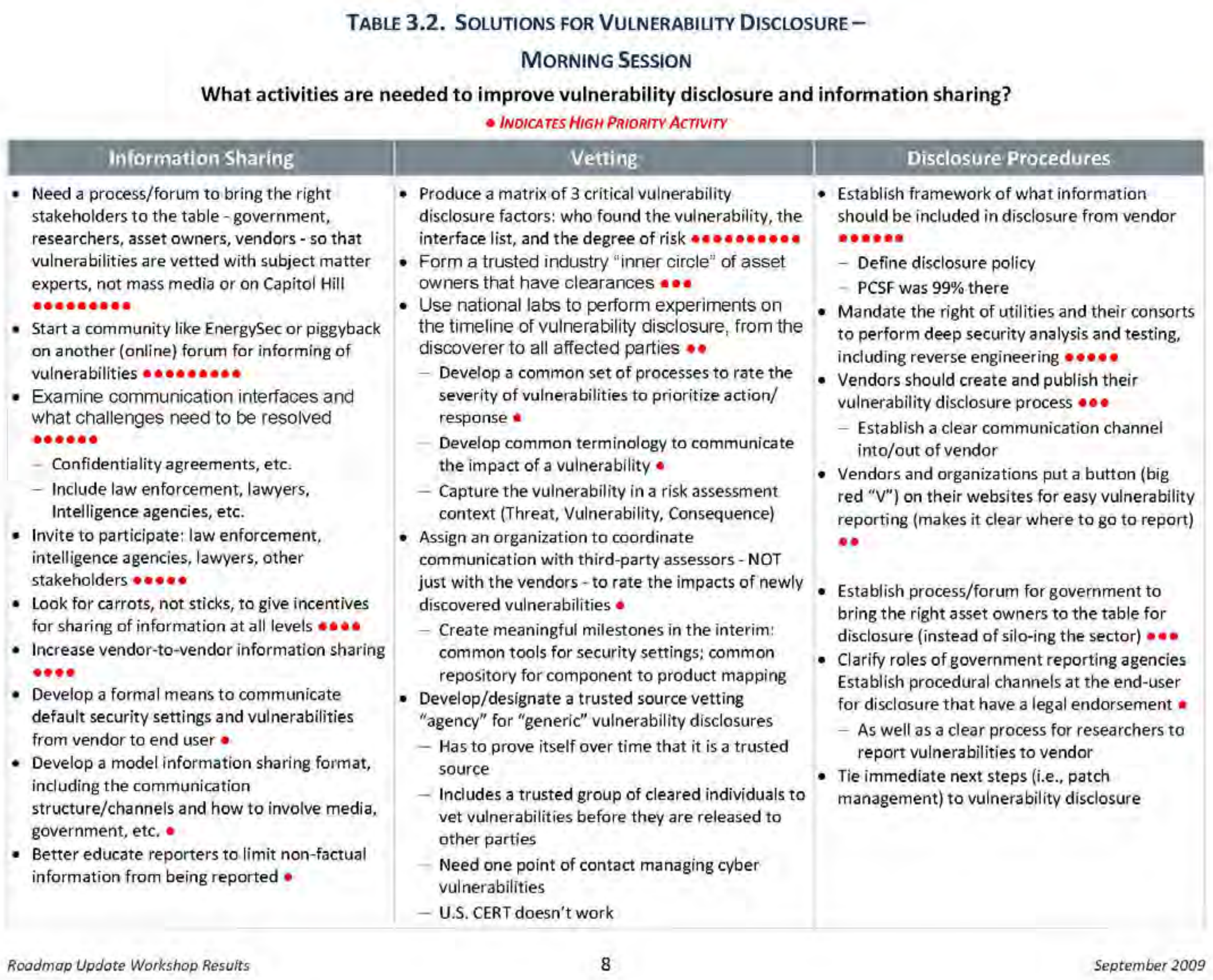


Table 3.2. Solutions for Vulnerability Disclosure – Morning Session

What activities are needed to improve vulnerability disclosure and information sharing?

● Indicates High Priority Activity

Information Sharing	Vetting	Disclosure Procedures
• Need a process/forum to bring the right stakeholders to the table - government, researchers, asset owners, vendors - so that vulnerabilities are vetted with subject matter experts, not mass media or on Capitol Hill ●●●●●●●●● • Start a community like EnergySec or piggyback on another (online) forum for informing of vulnerabilities ●●●●●●●●● • Examine communication interfaces and what challenges need to be resolved ●●●●●● – Confidentiality agreements, etc. – Include law enforcement, lawyers, Intelligence agencies, etc. • Invite to participate: law enforcement, intelligence agencies, lawyers, other stakeholders ●●●●● • Look for carrots, not sticks, to give incentives for sharing of information at all levels ●●●● • Increase vendor-to-vendor information sharing ●●●● • Develop a formal means to communicate default security settings and vulnerabilities from vendor to end user ● • Develop a model information sharing format, including the communication structure/channels and how to involve media, government, etc. ● • Better educate reporters to limit non-factual information from being reported ●	• Produce a matrix of 3 critical vulnerability disclosure factors: who found the vulnerability, the interface list, and the degree of risk ●●●●●●●●●● • Form a trusted industry "inner circle" of asset owners that have clearances ●●● • Use national labs to perform experiments on the timeline of vulnerability disclosure, from the discoverer to all affected parties ●● – Develop a common set of processes to rate the severity of vulnerabilities to prioritize action/ response ● – Develop common terminology to communicate the impact of a vulnerability ● – Capture the vulnerability in a risk assessment context (Threat, Vulnerability, Consequence) • Assign an organization to coordinate communication with third-party assessors - NOT just with the vendors - to rate the impacts of newly discovered vulnerabilities ● – Create meaningful milestones in the interim: common tools for security settings; common repository for component to product mapping • Develop/designate a trusted source vetting "agency" for "generic" vulnerability disclosures – Has to prove itself over time that it is a trusted source – Includes a trusted group of cleared individuals to vet vulnerabilities before they are released to other parties – Need one point of contact managing cyber vulnerabilities – U.S. CERT doesn't work	• Establish framework of what information should be included in disclosure from vendor ●●●●●● – Define disclosure policy – PCSF was 99% there • Mandate the right of utilities and their consorts to perform deep security analysis and testing, including reverse engineering ●●●●● • Vendors should create and publish their vulnerability disclosure process ●●● – Establish a clear communication channel into/out of vendor • Vendors and organizations put a button (big red "V") on their websites for easy vulnerability reporting (makes it clear where to go to report) ●● • Establish process/forum for government to bring the right asset owners to the table for disclosure (instead of silo-ing the sector) ●●● • Clarify roles of government reporting agencies Establish procedural channels at the end-user for disclosure that have a legal endorsement ● – As well as a clear process for researchers to report vulnerabilities to vendor • Tie immediate next steps (i.e., patch management) to vulnerability disclosure

Roadmap Update Workshop Results 8 *September 2009*

Table 3.3. Top Priorities and Next Steps for Vulnerability Disclosure – Morning Session

What are the immediate next steps?

● *Indicates High Priority Activity*

Top Priority	Immediate Next Steps			
Produce a matrix of 3 critical vulnerability disclosure factors: who found the vulnerability, the interface list, and the degree of risk				
Need a process/forum to bring the right stakeholders to the table - government, researchers, asset owners, vendors - so that vulnerabilities are vetted with subject matter experts, not in the mass media or on Capitol Hill	DOE would sponsor and define the motivation to participate	Bring all the "wheels" (sector coordinating councils and government coordinating councils) together to define roles	Identify core work of stakeholders to develop set of expectations and best practices	Identify industry expectations for vulnerability disclosure - manufacturers and asset providers
Start a community like EnergySec or piggyback on another (online) forum for informing of vulnerabilities	With a governing board of owner-operators and vendors			

Follow –Up:
Determine how to do any of these under the government rules for information sharing.

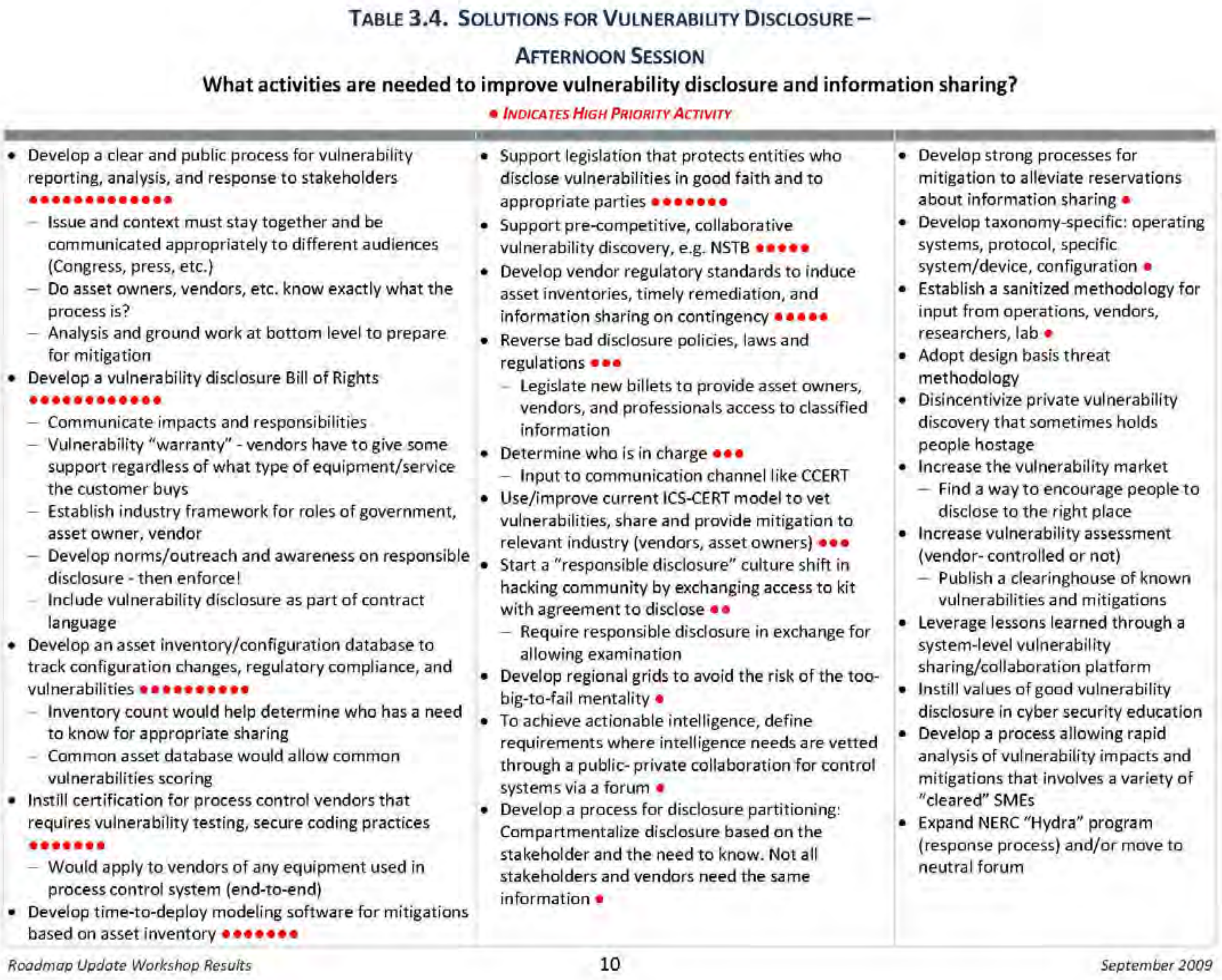


Table 3.4. Solutions for Vulnerability Disclosure – Afternoon Session

What activities are needed to improve vulnerability disclosure and information sharing?

● Indicates High Priority Activity

- Develop a clear and public process for vulnerability reporting, analysis, and response to stakeholders ●●●●●●●●●●●●●
  - Issue and context must stay together and be communicated appropriately to different audiences (Congress, press, etc.)
  - Do asset owners, vendors, etc. know exactly what the process is?
  - Analysis and ground work at bottom level to prepare for mitigation
- Develop a vulnerability disclosure Bill of Rights ●●●●●●●●●●●●
  - Communicate impacts and responsibilities
  - Vulnerability "warranty" - vendors have to give some support regardless of what type of equipment/service the customer buys
  - Establish industry framework for roles of government, asset owner, vendor
  - Develop norms/outreach and awareness on responsible disclosure - then enforce!
  - Include vulnerability disclosure as part of contract language
- Develop an asset inventory/configuration database to track configuration changes, regulatory compliance, and vulnerabilities ●●●●●●●●●●
  - Inventory count would help determine who has a need to know for appropriate sharing
  - Common asset database would allow common vulnerabilities scoring
- Instill certification for process control vendors that requires vulnerability testing, secure coding practices ●●●●●●●
  - Would apply to vendors of any equipment used in process control system (end-to-end)
- Develop time-to-deploy modeling software for mitigations based on asset inventory ●●●●●●●

- Support legislation that protects entities who disclose vulnerabilities in good faith and to appropriate parties ●●●●●●●
- Support pre-competitive, collaborative vulnerability discovery, e.g. NSTB ●●●●●
- Develop vendor regulatory standards to induce asset inventories, timely remediation, and information sharing on contingency ●●●●●
- Reverse bad disclosure policies, laws and regulations ●●●
  - Legislate new billets to provide asset owners, vendors, and professionals access to classified information
- Determine who is in charge ●●●
  - Input to communication channel like CCERT
- Use/improve current ICS-CERT model to vet vulnerabilities, share and provide mitigation to relevant industry (vendors, asset owners) ●●●
- Start a "responsible disclosure" culture shift in hacking community by exchanging access to kit with agreement to disclose ●●
  - Require responsible disclosure in exchange for allowing examination
- Develop regional grids to avoid the risk of the too-big-to-fail mentality ●
- To achieve actionable intelligence, define requirements where intelligence needs are vetted through a public- private collaboration for control systems via a forum ●
- Develop a process for disclosure partitioning: Compartmentalize disclosure based on the stakeholder and the need to know. Not all stakeholders and vendors need the same information ●

- Develop strong processes for mitigation to alleviate reservations about information sharing ●
- Develop taxonomy-specific: operating systems, protocol, specific system/device, configuration ●
- Establish a sanitized methodology for input from operations, vendors, researchers, lab ●
- Adopt design basis threat methodology
- Disincentivize private vulnerability discovery that sometimes holds people hostage
- Increase the vulnerability market
  - Find a way to encourage people to disclose to the right place
- Increase vulnerability assessment (vendor- controlled or not)
  - Publish a clearinghouse of known vulnerabilities and mitigations
- Leverage lessons learned through a system-level vulnerability sharing/collaboration platform
- Instill values of good vulnerability disclosure in cyber security education
- Develop a process allowing rapid analysis of vulnerability impacts and mitigations that involves a variety of "cleared" SMEs
- Expand NERC "Hydra" program (response process) and/or move to neutral forum

Roadmap Update Workshop Results 10 *September 2009*

Table 3.5. Top Priorities and Next Steps for Vulnerability Disclosure – Afternoon Session

What are the immediate next steps?

Top Priority	Immediate Next Steps			
Develop a clear and public process for vulnerability reporting, analysis, and response to stakeholders – Issue and context must stay together and be communicated appropriately to different audiences (Congress, press, etc.) – Do asset owners, vendors, etc. know exactly what the process is? – Conduct analysis and ground work at the bottom level to prepare for mitigation	Review vulnerability reporting process of U. S. CERT	Evaluate why the current process is not used	Establish clear lines of accountability for process ownership	Remove disincentives to report problems
Develop a vulnerability disclosure "Bill of Rights" – Communicate impacts and responsibilities – Vulnerability "warranty" - vendors have to give some support regardless of what type of equipment/service the customer buys – Establish industry framework for roles of government, asset owner, vendor – Develop norms/outreach and awareness on responsible disclosure - then enforce! – Include vulnerability disclosure as part of contract language	Start writing! - DOE lead	ICSJWG and ESCSWG work together	Determine if reporting is voluntary or a requirement	Protect reporters from liability
Develop an asset inventory/configuration database to track configuration changes, regulatory compliance, and vulnerabilities – Inventory count would help determine who has a need to know for appropriate sharing – Common asset database would allow common vulnerabilities scoring	De-emphasize critical vs. non-critical systems/components -- make it a list of all assets.	Build on existing national asset inventories, if possible.		

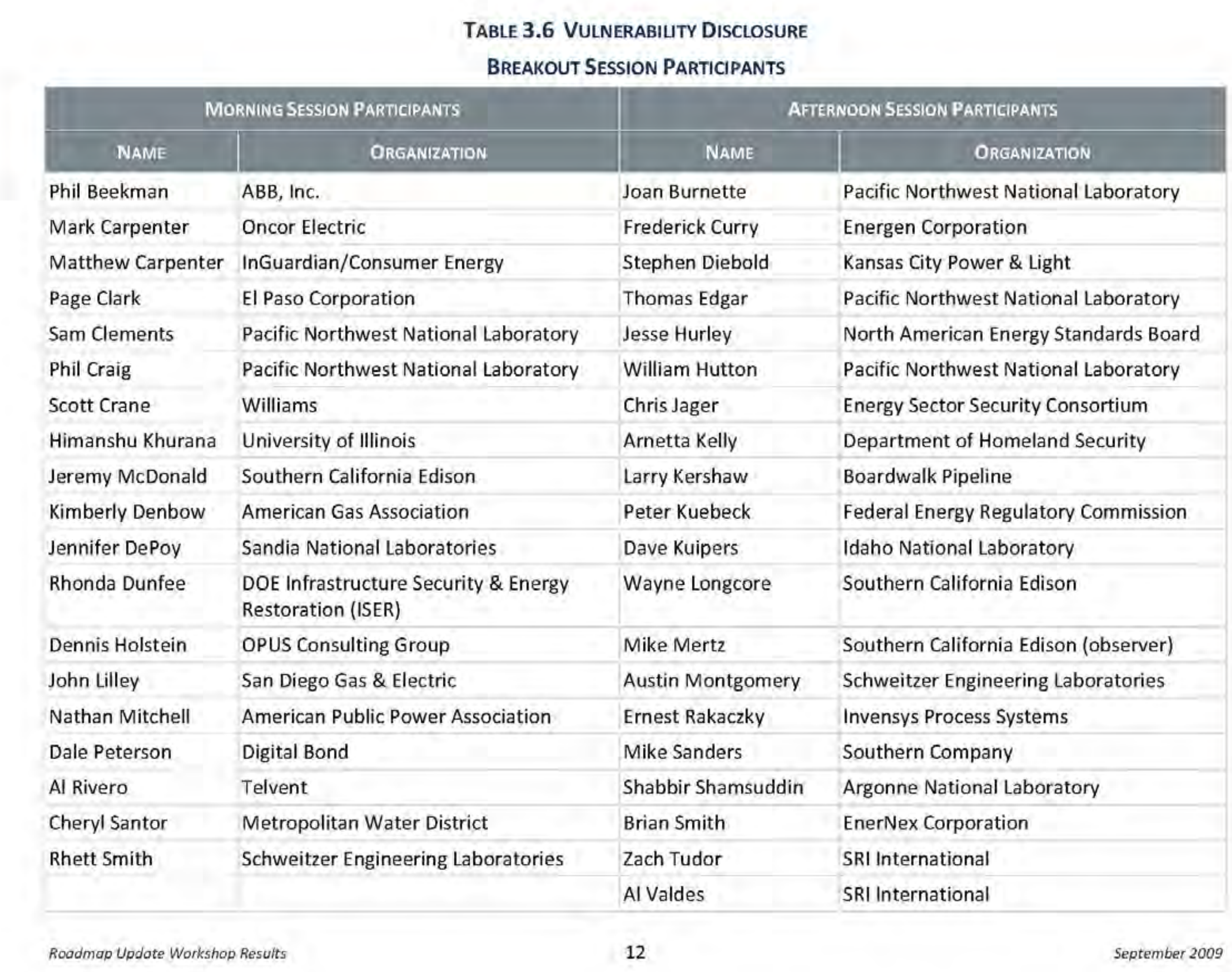
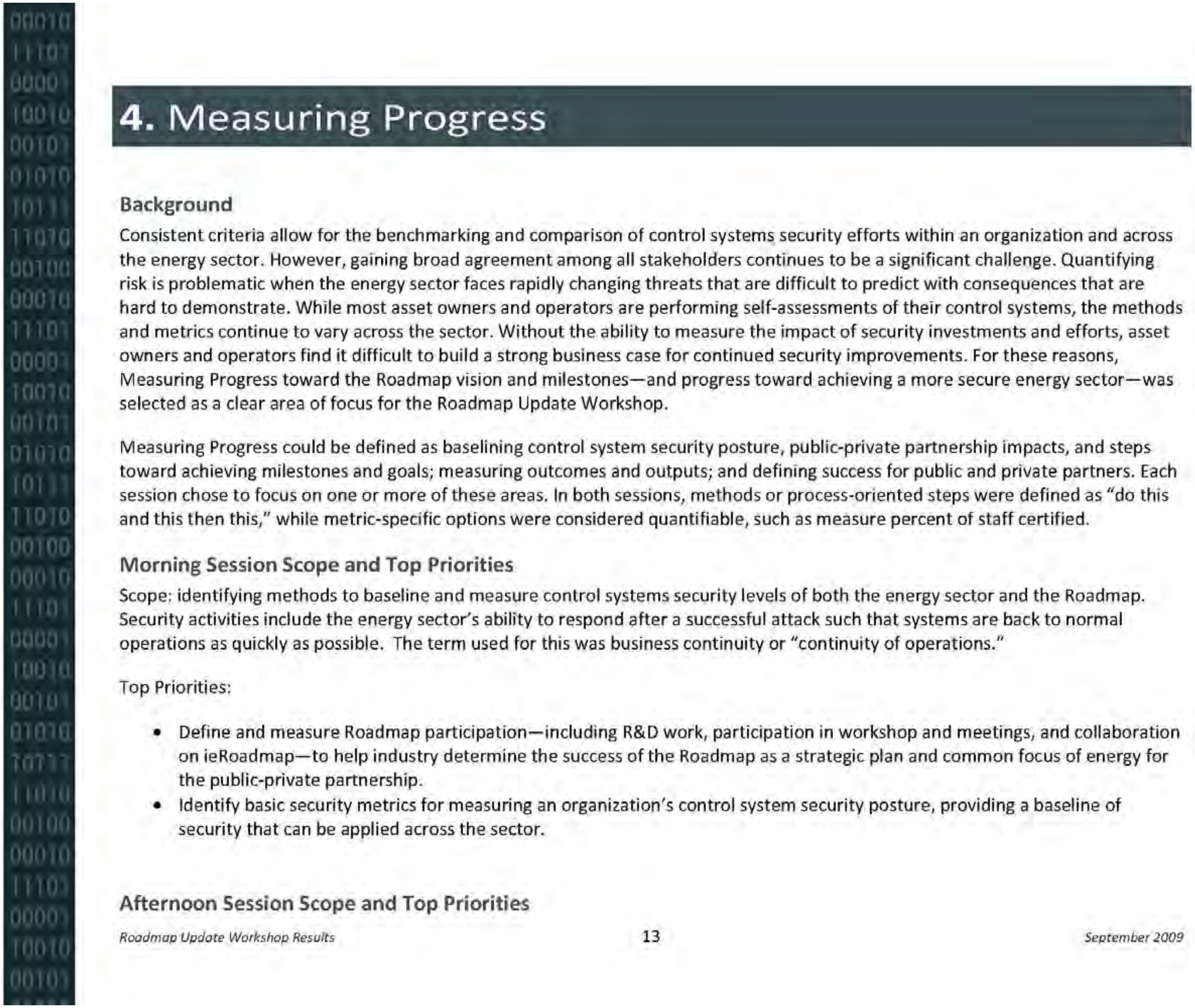


Table 3.6 Vulnerability Disclosure
Breakout Session Participants

Morning Session Participants		Afternoon Session Participants	
Name	**Organization**	**Name**	**Organization**
Phil Beekman	ABB, Inc.	Joan Burnette	Pacific Northwest National Laboratory
Mark Carpenter	Oncor Electric	Frederick Curry	Energen Corporation
Matthew Carpenter	InGuardian/Consumer Energy	Stephen Diebold	Kansas City Power & Light
Page Clark	El Paso Corporation	Thomas Edgar	Pacific Northwest National Laboratory
Sam Clements	Pacific Northwest National Laboratory	Jesse Hurley	North American Energy Standards Board
Phil Craig	Pacific Northwest National Laboratory	William Hutton	Pacific Northwest National Laboratory
Scott Crane	Williams	Chris Jager	Energy Sector Security Consortium
Himanshu Khurana	University of Illinois	Arnetta Kelly	Department of Homeland Security
Jeremy McDonald	Southern California Edison	Larry Kershaw	Boardwalk Pipeline
Kimberly Denbow	American Gas Association	Peter Kuebeck	Federal Energy Regulatory Commission
Jennifer DePoy	Sandia National Laboratories	Dave Kuipers	Idaho National Laboratory
Rhonda Dunfee	DOE Infrastructure Security & Energy Restoration (ISER)	Wayne Longcore	Southern California Edison
Dennis Holstein	OPUS Consulting Group	Mike Mertz	Southern California Edison (observer)
John Lilley	San Diego Gas & Electric	Austin Montgomery	Schweitzer Engineering Laboratories
Nathan Mitchell	American Public Power Association	Ernest Rakaczky	Invensys Process Systems
Dale Peterson	Digital Bond	Mike Sanders	Southern Company
Al Rivero	Telvent	Shabbir Shamsuddin	Argonne National Laboratory
Cheryl Santor	Metropolitan Water District	Brian Smith	EnerNex Corporation
Rhett Smith	Schweitzer Engineering Laboratories	Zach Tudor	SRI International
		Al Valdes	SRI International



4. Measuring Progress

Background

Consistent criteria allow for the benchmarking and comparison of control systems security efforts within an organization and across the energy sector. However, gaining broad agreement among all stakeholders continues to be a significant challenge. Quantifying risk is problematic when the energy sector faces rapidly changing threats that are difficult to predict with consequences that are hard to demonstrate. While most asset owners and operators are performing self-assessments of their control systems, the methods and metrics continue to vary across the sector. Without the ability to measure the impact of security investments and efforts, asset owners and operators find it difficult to build a strong business case for continued security improvements. For these reasons, Measuring Progress toward the Roadmap vision and milestones—and progress toward achieving a more secure energy sector—was selected as a clear area of focus for the Roadmap Update Workshop.

Measuring Progress could be defined as baselining control system security posture, public-private partnership impacts, and steps toward achieving milestones and goals; measuring outcomes and outputs; and defining success for public and private partners. Each session chose to focus on one or more of these areas. In both sessions, methods or process-oriented steps were defined as "do this and this then this," while metric-specific options were considered quantifiable, such as measure percent of staff certified.

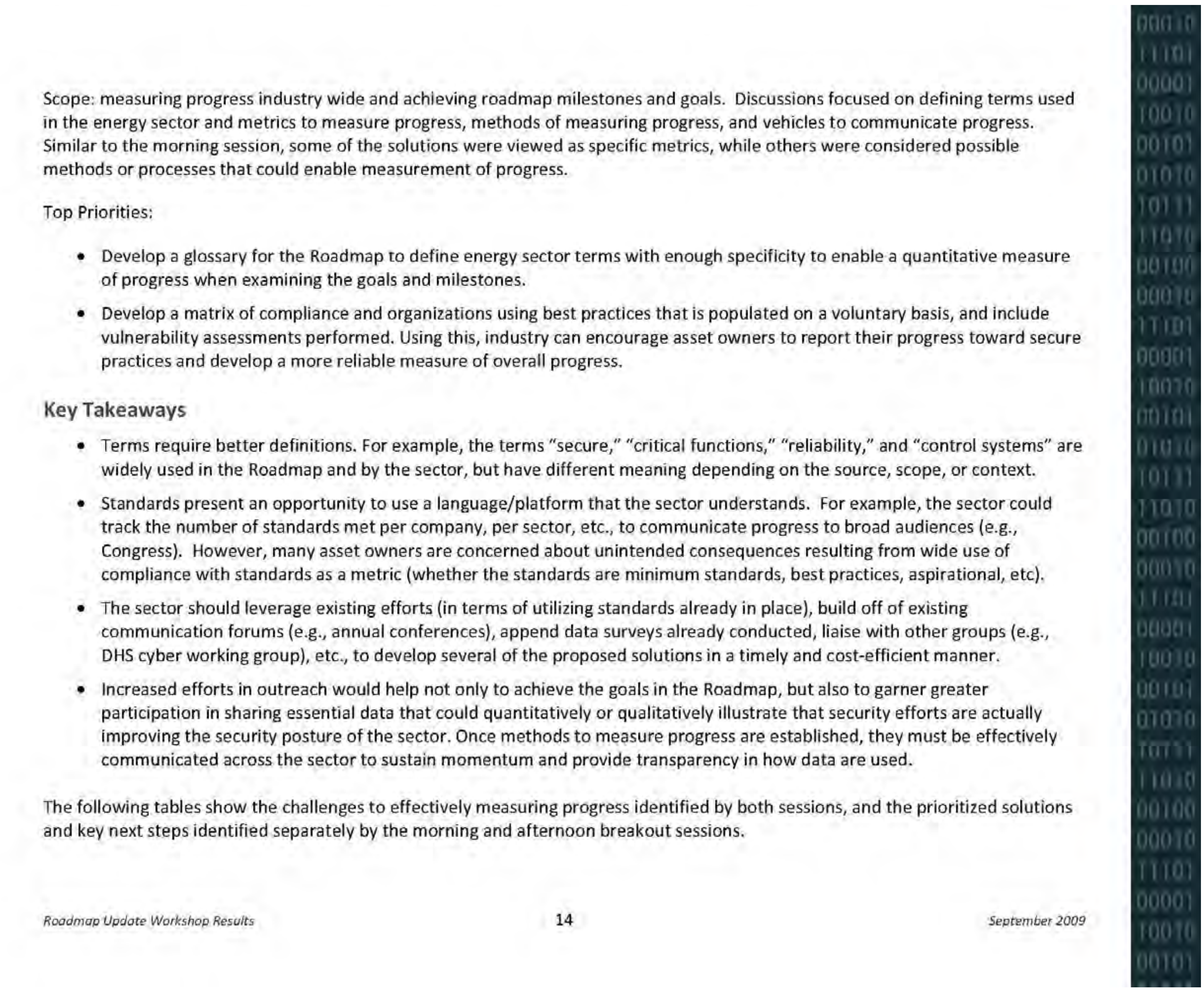
Morning Session Scope and Top Priorities

Scope: identifying methods to baseline and measure control systems security levels of both the energy sector and the Roadmap. Security activities include the energy sector's ability to respond after a successful attack such that systems are back to normal operations as quickly as possible. The term used for this was business continuity or "continuity of operations."

Top Priorities:

- Define and measure Roadmap participation—including R&D work, participation in workshop and meetings, and collaboration on ieRoadmap—to help industry determine the success of the Roadmap as a strategic plan and common focus of energy for the public-private partnership.
- Identify basic security metrics for measuring an organization's control system security posture, providing a baseline of security that can be applied across the sector.

Afternoon Session Scope and Top Priorities



Scope: measuring progress industry wide and achieving roadmap milestones and goals. Discussions focused on defining terms used in the energy sector and metrics to measure progress, methods of measuring progress, and vehicles to communicate progress. Similar to the morning session, some of the solutions were viewed as specific metrics, while others were considered possible methods or processes that could enable measurement of progress.

Top Priorities:

- Develop a glossary for the Roadmap to define energy sector terms with enough specificity to enable a quantitative measure of progress when examining the goals and milestones.
- Develop a matrix of compliance and organizations using best practices that is populated on a voluntary basis, and include vulnerability assessments performed. Using this, industry can encourage asset owners to report their progress toward secure practices and develop a more reliable measure of overall progress.

Key Takeaways

- Terms require better definitions. For example, the terms "secure," "critical functions," "reliability," and "control systems" are widely used in the Roadmap and by the sector, but have different meaning depending on the source, scope, or context.
- Standards present an opportunity to use a language/platform that the sector understands. For example, the sector could track the number of standards met per company, per sector, etc., to communicate progress to broad audiences (e.g., Congress). However, many asset owners are concerned about unintended consequences resulting from wide use of compliance with standards as a metric (whether the standards are minimum standards, best practices, aspirational, etc).
- The sector should leverage existing efforts (in terms of utilizing standards already in place), build off of existing communication forums (e.g., annual conferences), append data surveys already conducted, liaise with other groups (e.g., DHS cyber working group), etc., to develop several of the proposed solutions in a timely and cost-efficient manner.
- Increased efforts in outreach would help not only to achieve the goals in the Roadmap, but also to garner greater participation in sharing essential data that could quantitatively or qualitatively illustrate that security efforts are actually improving the security posture of the sector. Once methods to measure progress are established, they must be effectively communicated across the sector to sustain momentum and provide transparency in how data are used.

The following tables show the challenges to effectively measuring progress identified by both sessions, and the prioritized solutions and key next steps identified separately by the morning and afternoon breakout sessions.

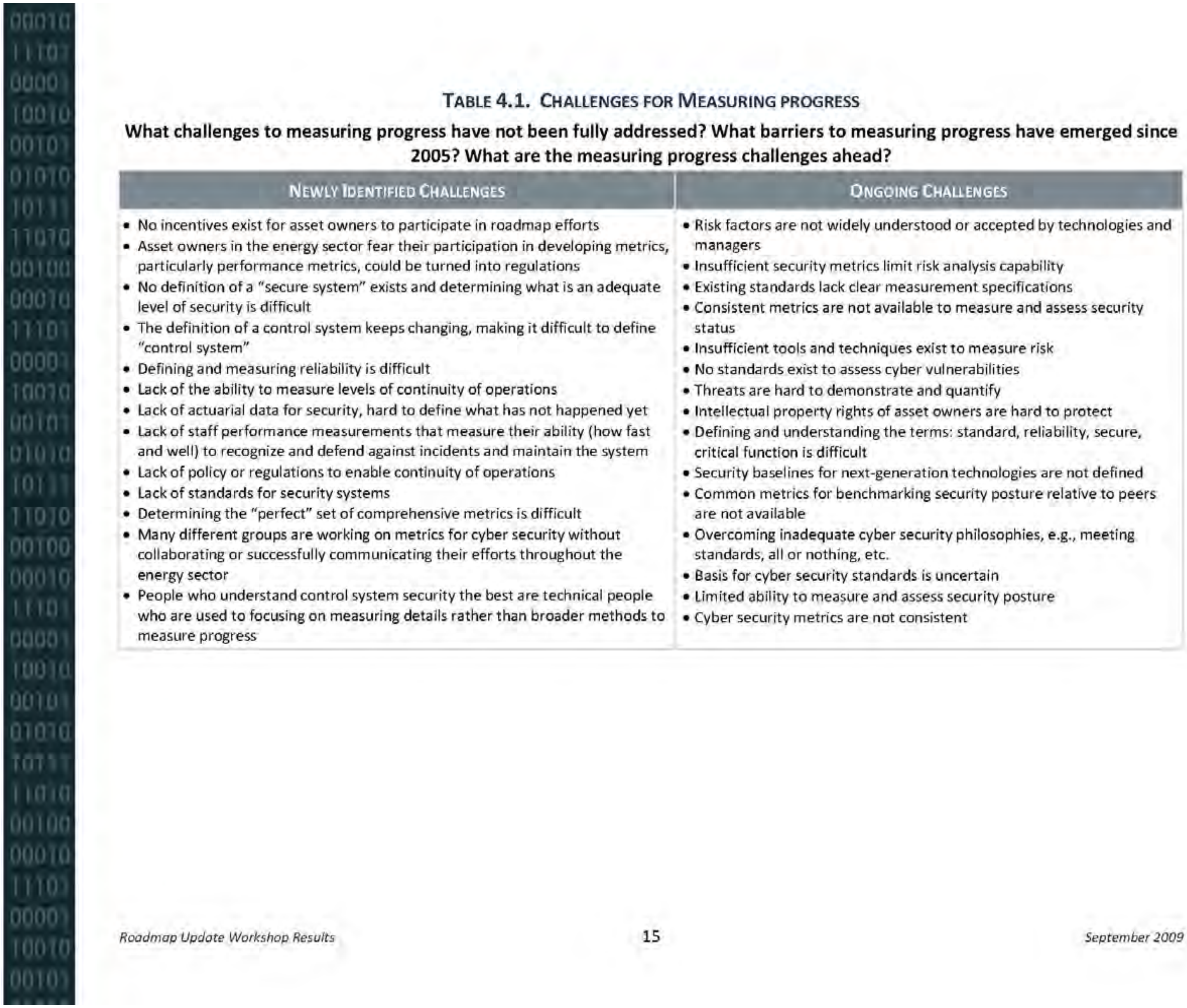


TABLE 4.1. CHALLENGES FOR MEASURING PROGRESS

What challenges to measuring progress have not been fully addressed? What barriers to measuring progress have emerged since 2005? What are the measuring progress challenges ahead?

NEWLY IDENTIFIED CHALLENGES	ONGOING CHALLENGES
• No incentives exist for asset owners to participate in roadmap efforts • Asset owners in the energy sector fear their participation in developing metrics, particularly performance metrics, could be turned into regulations • No definition of a "secure system" exists and determining what is an adequate level of security is difficult • The definition of a control system keeps changing, making it difficult to define "control system" • Defining and measuring reliability is difficult • Lack of the ability to measure levels of continuity of operations • Lack of actuarial data for security, hard to define what has not happened yet • Lack of staff performance measurements that measure their ability (how fast and well) to recognize and defend against incidents and maintain the system • Lack of policy or regulations to enable continuity of operations • Lack of standards for security systems • Determining the "perfect" set of comprehensive metrics is difficult • Many different groups are working on metrics for cyber security without collaborating or successfully communicating their efforts throughout the energy sector • People who understand control system security the best are technical people who are used to focusing on measuring details rather than broader methods to measure progress	• Risk factors are not widely understood or accepted by technologies and managers • Insufficient security metrics limit risk analysis capability • Existing standards lack clear measurement specifications • Consistent metrics are not available to measure and assess security status • Insufficient tools and techniques exist to measure risk • No standards exist to assess cyber vulnerabilities • Threats are hard to demonstrate and quantify • Intellectual property rights of asset owners are hard to protect • Defining and understanding the terms: standard, reliability, secure, critical function is difficult • Security baselines for next-generation technologies are not defined • Common metrics for benchmarking security posture relative to peers are not available • Overcoming inadequate cyber security philosophies, e.g., meeting standards, all or nothing, etc. • Basis for cyber security standards is uncertain • Limited ability to measure and assess security posture • Cyber security metrics are not consistent

Table 4.2. Solutions For Measuring Progress – Morning Session

What activities are needed to address the challenges/barriers?

● *Indicates High Priority Activity*

Methods to Measure Industry Progress		Methods to Measure Roadmap Progress
- [Method/Process] Identify a set of basic security metrics for measuring security posture. Use a common vulnerabilities document as the first step for measuring security. Adopt and enhance SCAP (NIST std) for vulnerability assessment and benchmarks. [Metric] Grade utilities for NERC CIP compliance (quality of policies and procedures). ●●●●●●●●●● - [Method/Process] Develop an operational security readiness certification program. [Metric] Determine what fraction of the ~3,100 utilities work security and operations together and measure % of these staff certified ●●●●●●●● - [Method/Process] Develop industry attack surface metrics. These should be annual and have industry agreed parameters ●●●●●● - [Method/Process] Develop legal agreements so that government and industry can share data ●●●●● - [Method/Process] Look in American Recovery & Reinvestment Act of 2009 (ARRA) proposals and determine what is proposed as needing fixing relevant to control system security. [Metric] Measure progress towards addressing these industry-identified needs ●●●●	- [Method/Process] Develop way to identifying whether an incident will be national-scale events. This will help us understand implications of small outages and scope government-level problems to be addressed ●● - [Method/Process] Develop case studies showing what is gained by security spending and a mechanism to share the studies with the energy sector ●● - [Metric] Measure progress of adopting certain standards and measure the performance of those standards ●● - [Method/Process] Define "security" and "results", and develop metrics on results including preventative, detective, and response (continuity of operations) ● - [Method/Process] Create a protocol for working with partners including suppliers, law enforcement, etc. ● - [Metric] Measure the degree of resiliency. Beyond CIA, cyber/physical in nature	- [Method/Process] Define roadmap participation metrics. Include roadmap participation that represents 50% of non-nuclear electricity generation, NSTB concept/technology exposure to 50% of non-nuclear electricity generation. [Metric] Define percentage of voluntary participation by R&D, vendors, industry to target and break that up generation, distribution, etc. Determine the number of entities using the roadmap, percentage of load/MW represented by these users, and the number of utilities participating in the roadmap workshops and meetings. [Method/Process] Use organizations like EnergySec to disseminate information to the industry asset owners ●●●●●●●●●●● - [Method/Process] Develop and publish a roadmap report card including self evaluation and industry survey. Provide online roadmap training and capability to track training to map against metrics. Include roadmap certification, documentation, and corresponding metrics ●●●●●●●●● - [Method/Process] List specific activities or progress on roadmap elements ●●●

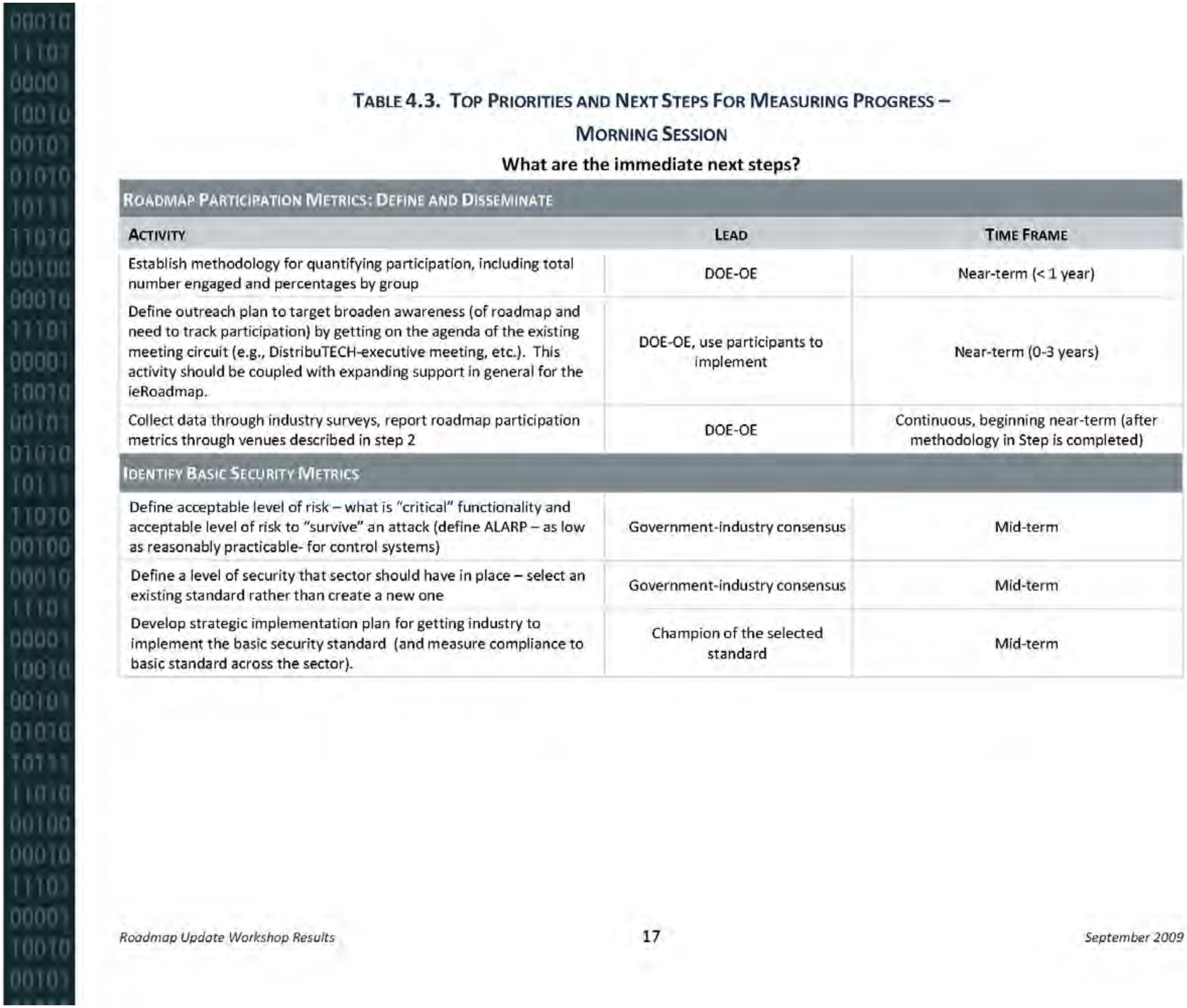


Table 4.3. Top Priorities and Next Steps For Measuring Progress – Morning Session

What are the immediate next steps?

Roadmap Participation Metrics: Define and Disseminate		
Activity	**Lead**	**Time Frame**
Establish methodology for quantifying participation, including total number engaged and percentages by group	DOE-OE	Near-term (< 1 year)
Define outreach plan to target broaden awareness (of roadmap and need to track participation) by getting on the agenda of the existing meeting circuit (e.g., DistribuTECH-executive meeting, etc.). This activity should be coupled with expanding support in general for the ieRoadmap.	DOE-OE, use participants to implement	Near-term (0-3 years)
Collect data through industry surveys, report roadmap participation metrics through venues described in step 2	DOE-OE	Continuous, beginning near-term (after methodology in Step is completed)
Identify Basic Security Metrics		
Define acceptable level of risk – what is "critical" functionality and acceptable level of risk to "survive" an attack (define ALARP – as low as reasonably practicable- for control systems)	Government-industry consensus	Mid-term
Define a level of security that sector should have in place – select an existing standard rather than create a new one	Government-industry consensus	Mid-term
Develop strategic implementation plan for getting industry to implement the basic security standard (and measure compliance to basic standard across the sector).	Champion of the selected standard	Mid-term

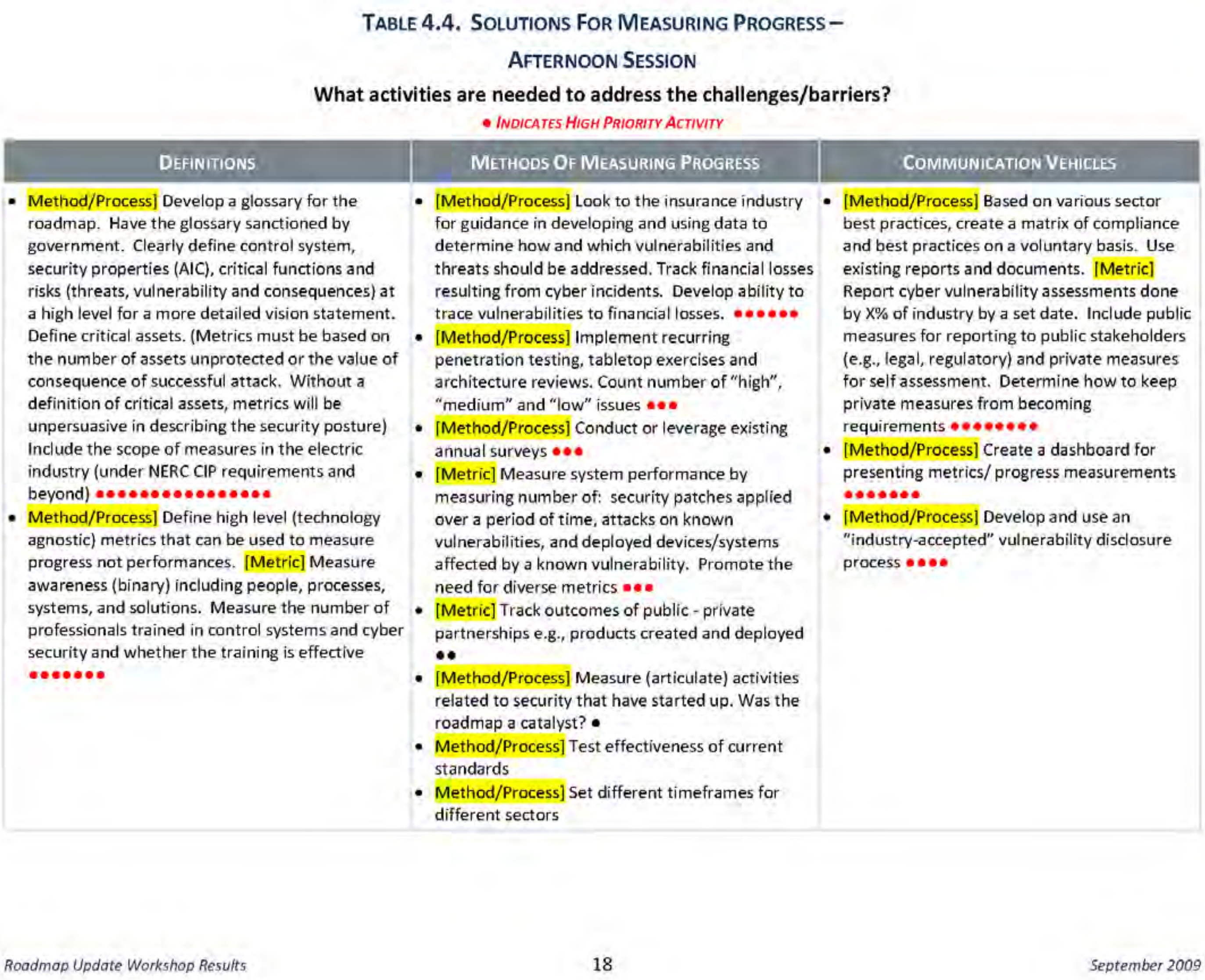


TABLE 4.4. SOLUTIONS FOR MEASURING PROGRESS – AFTERNOON SESSION

What activities are needed to address the challenges/barriers?

● *INDICATES HIGH PRIORITY ACTIVITY*

DEFINITIONS	METHODS OF MEASURING PROGRESS	COMMUNICATION VEHICLES
• Method/Process] Develop a glossary for the roadmap. Have the glossary sanctioned by government. Clearly define control system, security properties (AIC), critical functions and risks (threats, vulnerability and consequences) at a high level for a more detailed vision statement. Define critical assets. (Metrics must be based on the number of assets unprotected or the value of consequence of successful attack. Without a definition of critical assets, metrics will be unpersuasive in describing the security posture) Include the scope of measures in the electric industry (under NERC CIP requirements and beyond) ●●●●●●●●●●●●●●●● • Method/Process] Define high level (technology agnostic) metrics that can be used to measure progress not performances. [Metric] Measure awareness (binary) including people, processes, systems, and solutions. Measure the number of professionals trained in control systems and cyber security and whether the training is effective ●●●●●●●	• [Method/Process] Look to the insurance industry for guidance in developing and using data to determine how and which vulnerabilities and threats should be addressed. Track financial losses resulting from cyber incidents. Develop ability to trace vulnerabilities to financial losses. ●●●●●● • [Method/Process] Implement recurring penetration testing, tabletop exercises and architecture reviews. Count number of "high", "medium" and "low" issues ●●● • [Method/Process] Conduct or leverage existing annual surveys ●●● • [Metric] Measure system performance by measuring number of: security patches applied over a period of time, attacks on known vulnerabilities, and deployed devices/systems affected by a known vulnerability. Promote the need for diverse metrics ●●● • [Metric] Track outcomes of public - private partnerships e.g., products created and deployed ●● • [Method/Process] Measure (articulate) activities related to security that have started up. Was the roadmap a catalyst? ● • Method/Process] Test effectiveness of current standards • Method/Process] Set different timeframes for different sectors	• [Method/Process] Based on various sector best practices, create a matrix of compliance and best practices on a voluntary basis. Use existing reports and documents. [Metric] Report cyber vulnerability assessments done by X% of industry by a set date. Include public measures for reporting to public stakeholders (e.g., legal, regulatory) and private measures for self assessment. Determine how to keep private measures from becoming requirements ●●●●●●●● • [Method/Process] Create a dashboard for presenting metrics/ progress measurements ●●●●●●● • [Method/Process] Develop and use an "industry-accepted" vulnerability disclosure process ●●●●

Table 4.5. Top Priorities and Next Steps For Measuring Progress – Afternoon Session

What are the immediate next steps?

Develop a Glossary for the Roadmap		
Activity	**Lead**	**Time Frame**
Assign a lead to develop a glossary of the terms that need to be defined	DOE-OE	Immediate
Form a technical committee that would propose definitions lead the attaining buy-in from public and private stakeholders	Assigned lead	Near-term (< 2 months)
Research/survey existing definitions of key terms and determine/propose/author working definitions, such that they have enough specificity to enable quantitative tracking of progress	Technical Committee	Near term (< 3 years)
Develop a Matrix of Compliance & Best Practices		
Assign a lead to develop the matrix	National Lab	Immediate
Investigate if this can be piggy-backed on an existing project. If this cannot be piggy-backed, then follow glossary process described above.	Assigned lead	Immediate

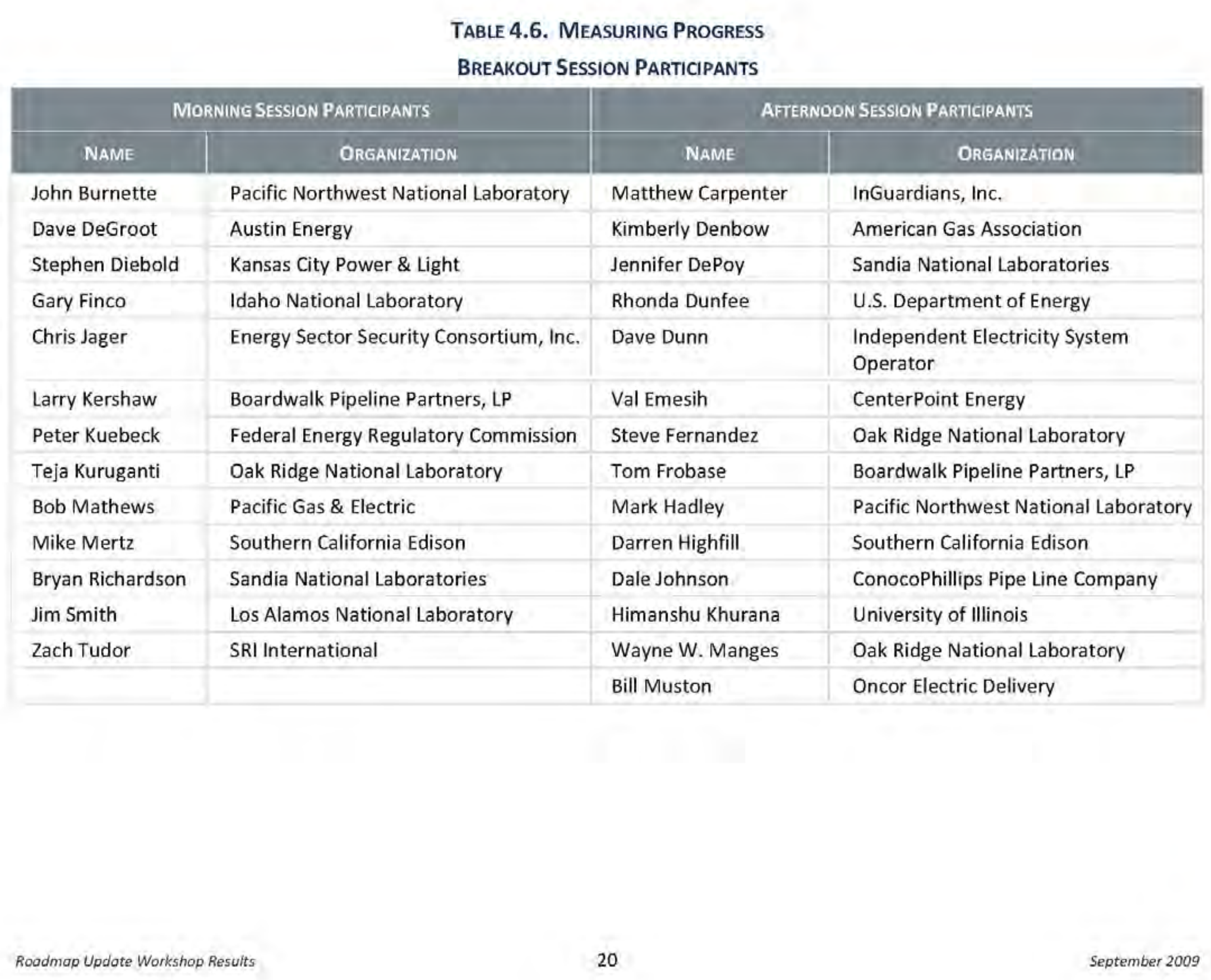
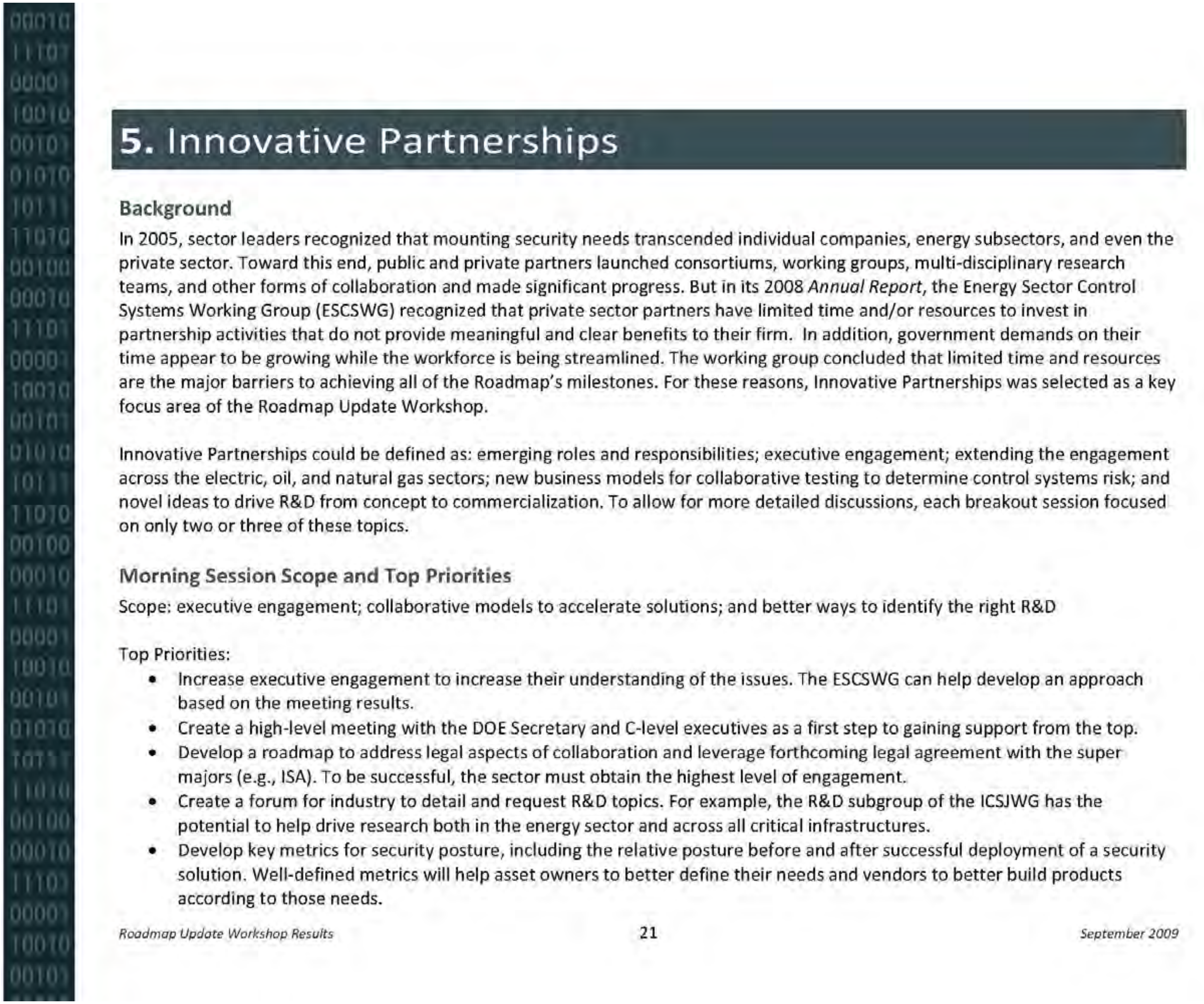


Table 4.6. Measuring Progress Breakout Session Participants

Morning Session Participants		Afternoon Session Participants	
Name	**Organization**	**Name**	**Organization**
John Burnette	Pacific Northwest National Laboratory	Matthew Carpenter	InGuardians, Inc.
Dave DeGroot	Austin Energy	Kimberly Denbow	American Gas Association
Stephen Diebold	Kansas City Power & Light	Jennifer DePoy	Sandia National Laboratories
Gary Finco	Idaho National Laboratory	Rhonda Dunfee	U.S. Department of Energy
Chris Jager	Energy Sector Security Consortium, Inc.	Dave Dunn	Independent Electricity System Operator
Larry Kershaw	Boardwalk Pipeline Partners, LP	Val Emesih	CenterPoint Energy
Peter Kuebeck	Federal Energy Regulatory Commission	Steve Fernandez	Oak Ridge National Laboratory
Teja Kuruganti	Oak Ridge National Laboratory	Tom Frobase	Boardwalk Pipeline Partners, LP
Bob Mathews	Pacific Gas & Electric	Mark Hadley	Pacific Northwest National Laboratory
Mike Mertz	Southern California Edison	Darren Highfill	Southern California Edison
Bryan Richardson	Sandia National Laboratories	Dale Johnson	ConocoPhillips Pipe Line Company
Jim Smith	Los Alamos National Laboratory	Himanshu Khurana	University of Illinois
Zach Tudor	SRI International	Wayne W. Manges	Oak Ridge National Laboratory
		Bill Muston	Oncor Electric Delivery



5. Innovative Partnerships

Background

In 2005, sector leaders recognized that mounting security needs transcended individual companies, energy subsectors, and even the private sector. Toward this end, public and private partners launched consortiums, working groups, multi-disciplinary research teams, and other forms of collaboration and made significant progress. But in its 2008 *Annual Report*, the Energy Sector Control Systems Working Group (ESCSWG) recognized that private sector partners have limited time and/or resources to invest in partnership activities that do not provide meaningful and clear benefits to their firm. In addition, government demands on their time appear to be growing while the workforce is being streamlined. The working group concluded that limited time and resources are the major barriers to achieving all of the Roadmap's milestones. For these reasons, Innovative Partnerships was selected as a key focus area of the Roadmap Update Workshop.

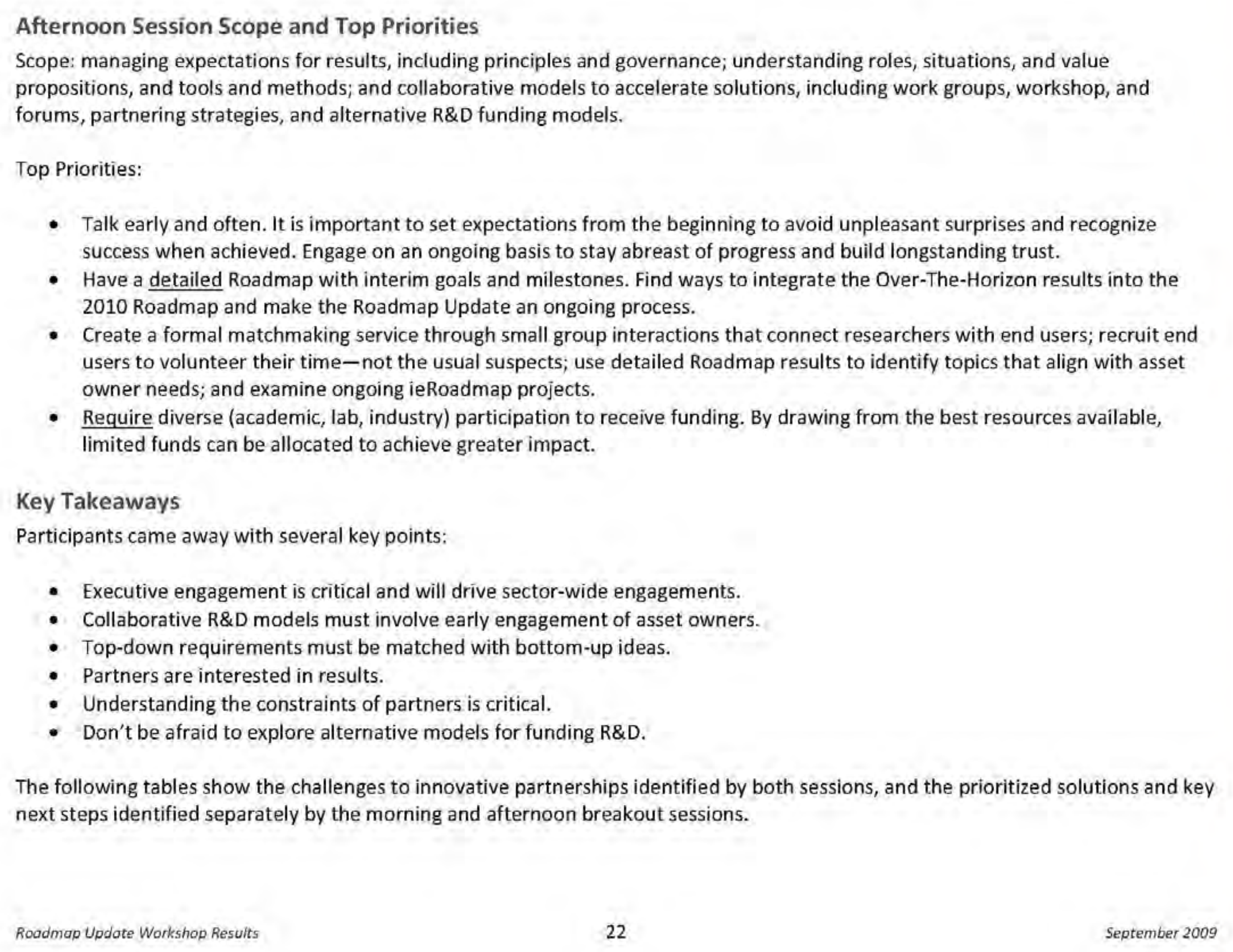
Innovative Partnerships could be defined as: emerging roles and responsibilities; executive engagement; extending the engagement across the electric, oil, and natural gas sectors; new business models for collaborative testing to determine control systems risk; and novel ideas to drive R&D from concept to commercialization. To allow for more detailed discussions, each breakout session focused on only two or three of these topics.

Morning Session Scope and Top Priorities

Scope: executive engagement; collaborative models to accelerate solutions; and better ways to identify the right R&D

Top Priorities:

- Increase executive engagement to increase their understanding of the issues. The ESCSWG can help develop an approach based on the meeting results.
- Create a high-level meeting with the DOE Secretary and C-level executives as a first step to gaining support from the top.
- Develop a roadmap to address legal aspects of collaboration and leverage forthcoming legal agreement with the super majors (e.g., ISA). To be successful, the sector must obtain the highest level of engagement.
- Create a forum for industry to detail and request R&D topics. For example, the R&D subgroup of the ICSJWG has the potential to help drive research both in the energy sector and across all critical infrastructures.
- Develop key metrics for security posture, including the relative posture before and after successful deployment of a security solution. Well-defined metrics will help asset owners to better define their needs and vendors to better build products according to those needs.



Afternoon Session Scope and Top Priorities

Scope: managing expectations for results, including principles and governance; understanding roles, situations, and value propositions, and tools and methods; and collaborative models to accelerate solutions, including work groups, workshop, and forums, partnering strategies, and alternative R&D funding models.

Top Priorities:

- Talk early and often. It is important to set expectations from the beginning to avoid unpleasant surprises and recognize success when achieved. Engage on an ongoing basis to stay abreast of progress and build longstanding trust.
- Have a detailed Roadmap with interim goals and milestones. Find ways to integrate the Over-The-Horizon results into the 2010 Roadmap and make the Roadmap Update an ongoing process.
- Create a formal matchmaking service through small group interactions that connect researchers with end users; recruit end users to volunteer their time—not the usual suspects; use detailed Roadmap results to identify topics that align with asset owner needs; and examine ongoing ieRoadmap projects.
- Require diverse (academic, lab, industry) participation to receive funding. By drawing from the best resources available, limited funds can be allocated to achieve greater impact.

Key Takeaways

Participants came away with several key points:

- Executive engagement is critical and will drive sector-wide engagements.
- Collaborative R&D models must involve early engagement of asset owners.
- Top-down requirements must be matched with bottom-up ideas.
- Partners are interested in results.
- Understanding the constraints of partners is critical.
- Don't be afraid to explore alternative models for funding R&D.

The following tables show the challenges to innovative partnerships identified by both sessions, and the prioritized solutions and key next steps identified separately by the morning and afternoon breakout sessions.

Table 5.1. Challenges for Innovative Partnerships

What are the challenges to creating innovative partnerships?

Current Situation	Key Challenges
• Compelling evidence-based business case to increase private investment in control system security is not available • Difficult to integrate issues that are fragmented across government and industry programs • Difficult to break "find-and-fix" mindset and shift to lifecycle operational risk • Culture clash among IT, controls, politics, media • Changing roles of stakeholders • Operations people are doing SCADA, and they don't think security [need training] • Highly technical and specialized subject • Major information sharing issues between government and industry not resolved • Urgent need to accelerate solutions development • Communicating in the C-level language → use facts and numbers • Legal challenges inhibit (NDA/anti-trust) collaboration	• How to engage executives • Novel ideas to accelerate R&D process • How to create collaborative models for vulnerability testing – Consequence based solution • Finding better ways to identify the right R&D • Improving information sharing for R&D and best practices • Managing expectations for results – Shared vision – Not clear understanding of technology development process

TABLE 5.2. SOLUTIONS FOR INNOVATIVE PARTNERSHIPS – MORNING SESSION

What are some of the approaches to overcoming these challenges?

● INDICATES HIGH PRIORITY ACTIVITY

INCREASE EXECUTIVE ENGAGEMENT (ESCSWG TO DEVELOP APPROACH)			COLLABORATIVE MODELS TO ACCELERATE SOLUTIONS (INCLUDES R&D AND BEST PRACTICES)		
TARGETED C-LEVEL INFORMATION ON ISSUES TO INCREASE UNDERSTANDING	SENIOR EXECUTIVE FORUM/COUNCIL FOCUSED ON CYBER ISSUES	HIGH LEVEL MEETINGS AND EVENTS WITH SENIOR GOVERNMENT LEADERS	OVERCOMING LEGAL ISSUES	ALTERNATIVE R&D MODELS	BETTER ASSET OWNER ENGAGEMENT
• Link to utility investment business case to include cost reduction and reliability enhancements ●●●● • Strong business case from product development to ownership ●●● • Create presentations to help executives understand issues - cheat sheets, talking pants • Better articulate our value proposition of research - in executive language	• DOE establish periodic forum to meet with "C-level" industry - increase awareness ●●●●● • Have cyber security asset owners issues over seen by Board of Directors (owners) and CEO/CIO bonuses tied directly to success of program ●● • Identify/create venue for C-level information exchange • DOE led (Secretary Level) NSTAC-Like Activities for C-suites, or get white house involved • Targeted focus group awareness and dialogue sessions by sector	• High level meeting/events with DOE secretary plus C-level executives ●●●●●●●●●● • Executive retreats with keynote speakers of interest - not just security focused business • Approach through risk management • DOE top/down FERC, DHS executive cyber awareness training	• Develop roadmap to legal aspects of collaboration ●●●●●●●●●● — Leverage legal agreement with the "super majors" — Highest level engagement • Streamline legal (CRADA/NDA) process for national labs to move technology to vendors and support multi-year funding at national labs ●●●	• Combine I3P, TCIP, SERC, and LOGIIC models to create an open, fair R&D, TE&T "system" ●●● • Consider dedicated funding to ensure productization of solutions - think "SBIR Phase 3" ● • Promote skunk works within large vendors, asset owners and research communities • Jointly fund R&D efforts to share risks/solutions among participating subscribers	• Hold joint vendor, asset owner, government vulnerability and threat analysis workshops ●●●●● • Promote end user involvement with vendors, government and academia ●● • Specific, early, and frequent industry involvement in R&D activities ● • Create project roles for asset owners as steering advisors in order to assure final results align with deployment objectives ● • Encourage two-way dialogue between R&D entities and asset owners to evaluate and vet ideas (user group meetings) • Engage more owners in solution testing, use trade groups to help enlist them.

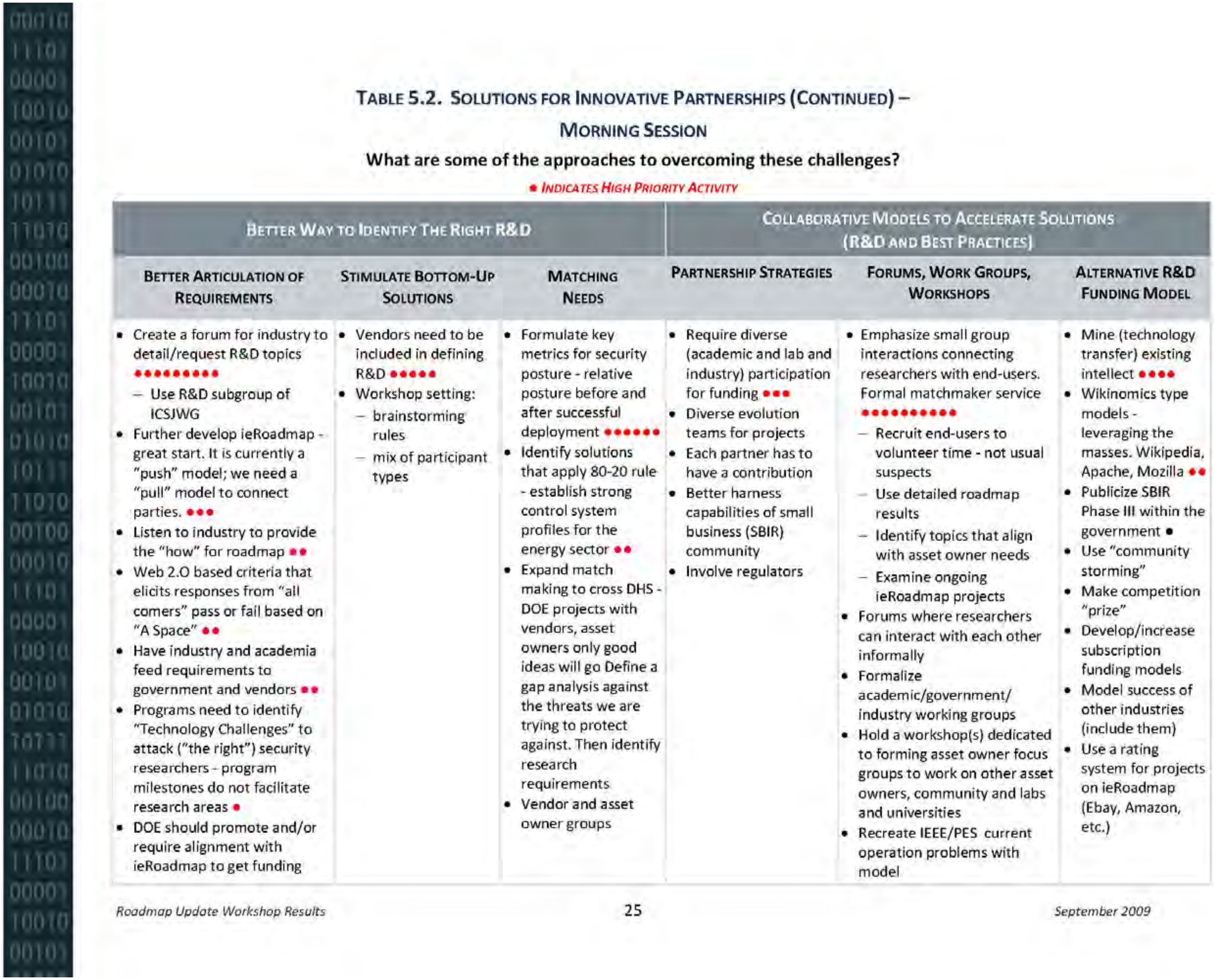


Table 5.2. Solutions for Innovative Partnerships (Continued) – Morning Session

What are some of the approaches to overcoming these challenges?

● *Indicates High Priority Activity*

Better Way to Identify The Right R&D			Collaborative Models to Accelerate Solutions (R&D and Best Practices)		
Better Articulation of Requirements	**Stimulate Bottom-Up Solutions**	**Matching Needs**	**Partnership Strategies**	**Forums, Work Groups, Workshops**	**Alternative R&D Funding Model**
• Create a forum for industry to detail/request R&D topics ●●●●●●●●● – Use R&D subgroup of ICSJWG • Further develop ieRoadmap - great start. It is currently a "push" model; we need a "pull" model to connect parties. ●●● • Listen to industry to provide the "how" for roadmap ●● • Web 2.O based criteria that elicits responses from "all comers" pass or fail based on "A Space" ●● • Have industry and academia feed requirements to government and vendors ●● • Programs need to identify "Technology Challenges" to attack ("the right") security researchers - program milestones do not facilitate research areas ● • DOE should promote and/or require alignment with ieRoadmap to get funding	• Vendors need to be included in defining R&D ●●●●● • Workshop setting: – brainstorming rules – mix of participant types	• Formulate key metrics for security posture - relative posture before and after successful deployment ●●●●●● • Identify solutions that apply 80-20 rule - establish strong control system profiles for the energy sector ●● • Expand match making to cross DHS - DOE projects with vendors, asset owners only good ideas will go Define a gap analysis against the threats we are trying to protect against. Then identify research requirements • Vendor and asset owner groups	• Require diverse (academic and lab and industry) participation for funding ●●● • Diverse evolution teams for projects • Each partner has to have a contribution • Better harness capabilities of small business (SBIR) community • Involve regulators	• Emphasize small group interactions connecting researchers with end-users. Formal matchmaker service ●●●●●●●●●● – Recruit end-users to volunteer time - not usual suspects – Use detailed roadmap results – Identify topics that align with asset owner needs – Examine ongoing ieRoadmap projects • Forums where researchers can interact with each other informally • Formalize academic/government/ industry working groups • Hold a workshop(s) dedicated to forming asset owner focus groups to work on other asset owners, community and labs and universities • Recreate IEEE/PES current operation problems with model	• Mine (technology transfer) existing intellect ●●●● • Wikinomics type models - leveraging the masses. Wikipedia, Apache, Mozilla ●● • Publicize SBIR Phase III within the government ● • Use "community storming" • Make competition "prize" • Develop/increase subscription funding models • Model success of other industries (include them) • Use a rating system for projects on ieRoadmap (Ebay, Amazon, etc.)

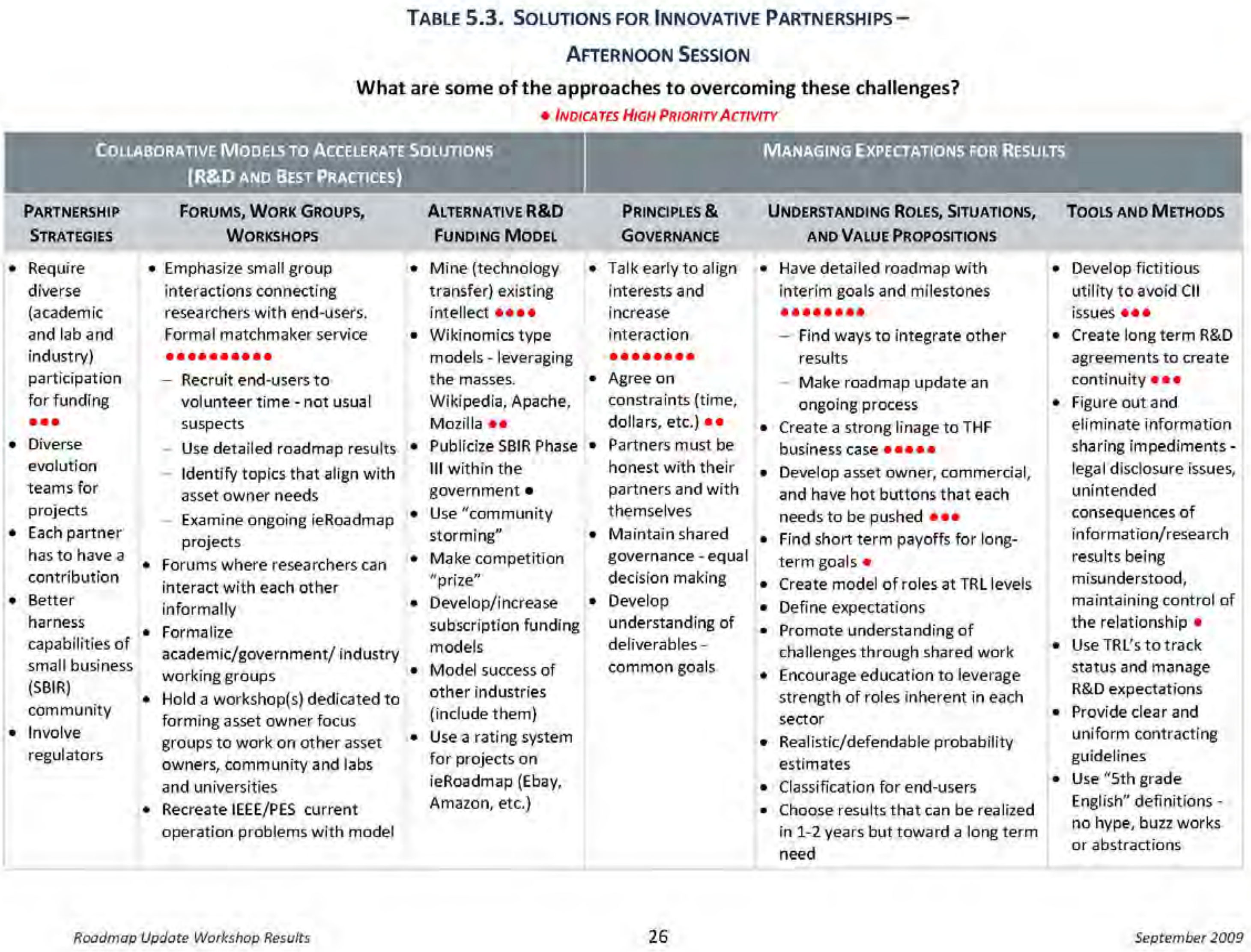


Table 5.3. Solutions for Innovative Partnerships – Afternoon Session

What are some of the approaches to overcoming these challenges?

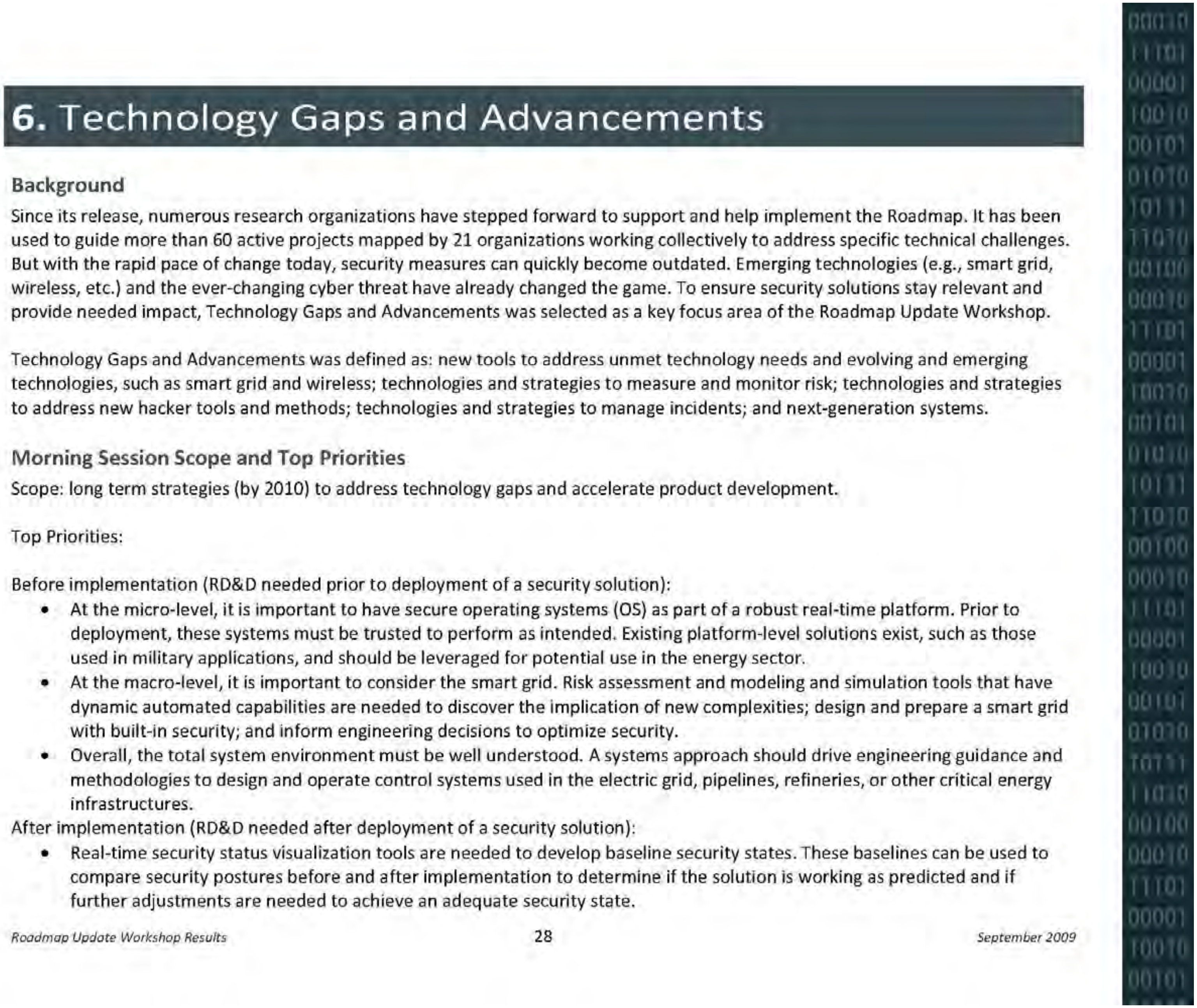
● *Indicates High Priority Activity*

Collaborative Models to Accelerate Solutions (R&D and Best Practices)			Managing Expectations for Results		
Partnership Strategies	**Forums, Work Groups, Workshops**	**Alternative R&D Funding Model**	**Principles & Governance**	**Understanding Roles, Situations, and Value Propositions**	**Tools and Methods**
• Require diverse (academic and lab and industry) participation for funding ●●● • Diverse evolution teams for projects • Each partner has to have a contribution • Better harness capabilities of small business (SBIR) community • Involve regulators	• Emphasize small group interactions connecting researchers with end-users. Formal matchmaker service ●●●●●●●●●● – Recruit end-users to volunteer time - not usual suspects – Use detailed roadmap results – Identify topics that align with asset owner needs – Examine ongoing ieRoadmap projects • Forums where researchers can interact with each other informally • Formalize academic/government/ industry working groups • Hold a workshop(s) dedicated to forming asset owner focus groups to work on other asset owners, community and labs and universities • Recreate IEEE/PES current operation problems with model	• Mine (technology transfer) existing intellect ●●●● • Wikinomics type models - leveraging the masses. Wikipedia, Apache, Mozilla ●● • Publicize SBIR Phase III within the government ● • Use "community storming" • Make competition "prize" • Develop/increase subscription funding models • Model success of other industries (include them) • Use a rating system for projects on ieRoadmap (Ebay, Amazon, etc.)	• Talk early to align interests and increase interaction ●●●●●●●● • Agree on constraints (time, dollars, etc.) ●● • Partners must be honest with their partners and with themselves • Maintain shared governance - equal decision making • Develop understanding of deliverables – common goals	• Have detailed roadmap with interim goals and milestones ●●●●●●●● – Find ways to integrate other results – Make roadmap update an ongoing process • Create a strong linage to THF business case ●●●●● • Develop asset owner, commercial, and have hot buttons that each needs to be pushed ●●● • Find short term payoffs for long-term goals ● • Create model of roles at TRL levels • Define expectations • Promote understanding of challenges through shared work • Encourage education to leverage strength of roles inherent in each sector • Realistic/defendable probability estimates • Classification for end-users • Choose results that can be realized in 1-2 years but toward a long term need	• Develop fictitious utility to avoid CII issues ●●● • Create long term R&D agreements to create continuity ●●● • Figure out and eliminate information sharing impediments - legal disclosure issues, unintended consequences of information/research results being misunderstood, maintaining control of the relationship ● • Use TRL's to track status and manage R&D expectations • Provide clear and uniform contracting guidelines • Use "5th grade English" definitions - no hype, buzz works or abstractions

Roadmap Update Workshop Results 26 *September 2009*

Table 5.4. Innovative Partnerships Breakout Session Participants

Morning Session Participants		Afternoon Session Participants	
Name	**Organization**	**Name**	**Organization**
Ernest Rakaczky	Invensys Process Systems	Jeff Dagle	Pacific Northwest National Laboratory
Bob Pollock	Sandia National Laboratories	Bill Sanders	Information Trust Institute
Douglas Maughan	DHS Science and Technology Directorate	Mark Hinrichs	Los Alamos National Laboratory
Tom Frobase	Boardwalk Pipeline Partners	David Scheulen	BP
Keith Stouffer	National Institute of Standards and Technology	Sam Clements	Pacific Northwest National Laboratory
Mark Hadley	Pacific Northwest National Laboratory	John Allen	International Electricity Infrastructure Assurance Forum
David Kuipers	Idaho National Laboratory	Bill Winters	Arizona Public Service
Austin Montgomery	Software Engineering Institute	Scott Bordenkircher	Arizona Public Service
David Dunn	IESO	Josh Gerber	San Diego Gas & Electric
Greg Maciel	Uniloc	Stan Klein	Open Secure Energy Control Systems
Klaus Bender	Utilities Telecom Council	Phil Beekman	ABB
Bill Muston	Oncor Electric Delivery	Tom Flowers	Flowers Control Center Solutions
		Diane Hooie	U.S. Department of Energy / NETL



6. Technology Gaps and Advancements

Background

Since its release, numerous research organizations have stepped forward to support and help implement the Roadmap. It has been used to guide more than 60 active projects mapped by 21 organizations working collectively to address specific technical challenges. But with the rapid pace of change today, security measures can quickly become outdated. Emerging technologies (e.g., smart grid, wireless, etc.) and the ever-changing cyber threat have already changed the game. To ensure security solutions stay relevant and provide needed impact, Technology Gaps and Advancements was selected as a key focus area of the Roadmap Update Workshop.

Technology Gaps and Advancements was defined as: new tools to address unmet technology needs and evolving and emerging technologies, such as smart grid and wireless; technologies and strategies to measure and monitor risk; technologies and strategies to address new hacker tools and methods; technologies and strategies to manage incidents; and next-generation systems.

Morning Session Scope and Top Priorities

Scope: long term strategies (by 2010) to address technology gaps and accelerate product development.

Top Priorities:

Before implementation (RD&D needed prior to deployment of a security solution):

- At the micro-level, 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 exist, such as those used in military applications, and should be leveraged for potential use in the energy sector.
- At the macro-level, it is important to consider the smart grid. Risk assessment and modeling and simulation tools that have dynamic automated capabilities are needed to discover the implication of new complexities; design and prepare a smart grid with built-in security; and inform engineering decisions to optimize security.
- Overall, the total system environment must be well understood. A systems approach should drive engineering guidance and methodologies to design and operate control systems used in the electric grid, pipelines, refineries, or other critical energy infrastructures.

After implementation (RD&D needed after deployment of a security solution):

- Real-time security status visualization tools are needed to develop baseline security states. These baselines can be used to compare security postures before and after implementation to determine if the solution is working as predicted and if further adjustments are needed to achieve an adequate security state.

- Real-time computer-assisted response capabilities are needed to achieve resiliency objectives. When the system operates outside design and performance specifications, operators can use these tools to react intelligently and quickly in order to sustain critical functions.

Afternoon Session Scope and Top Priorities

Scope: near- (< 3 years) and mid-term (4-7 years) strategies to address technology gaps and accelerate product development and deployment.

Top Priorities:

- Develop scientifically defensible metrics for cyber security robustness, with known utility. Although metrics were being addressed in another session, participants felt this was a technical challenge requiring collaborative R&D, not only to validate the metrics, but to also test and validate the robustness of next generation systems consistent with the metrics.
- Define security architecture. While some definitions currently exist, each sector must develop and adopt their own within the context of their environment.
- Develop non-bootable patching (hot patching) capability for the overall system. While some hot patching capabilities currently exist, they cannot be applied system wide. To realize the full potential of this capability it needs to be deployed throughout the system.
- Adopt agreed upon and available intrinsic data and source integrity in SCADA/DCS protocols to develop control systems that will inherently respond to and defend themselves against internal and external threats.
- Provide explicit, managed trust. Trusting communications as valid is essential to effective response to a cyber event. It is more difficult to determine an appropriate response if the integrity of a communication is uncertain.

Key Takeaways

Participants came away with three key points:

- Approach cyber security using a total systems approach.
- Leverage existing technologies to accelerate the development of energy sector-specific solutions.
- As an immediate next step, identify key activities to achieve priority objectives and methods to accelerate progress.

The following tables show the challenges to advancing control systems security technologies identified by both sessions, and the prioritized solutions and key next steps identified separately by the morning and afternoon breakout sessions.

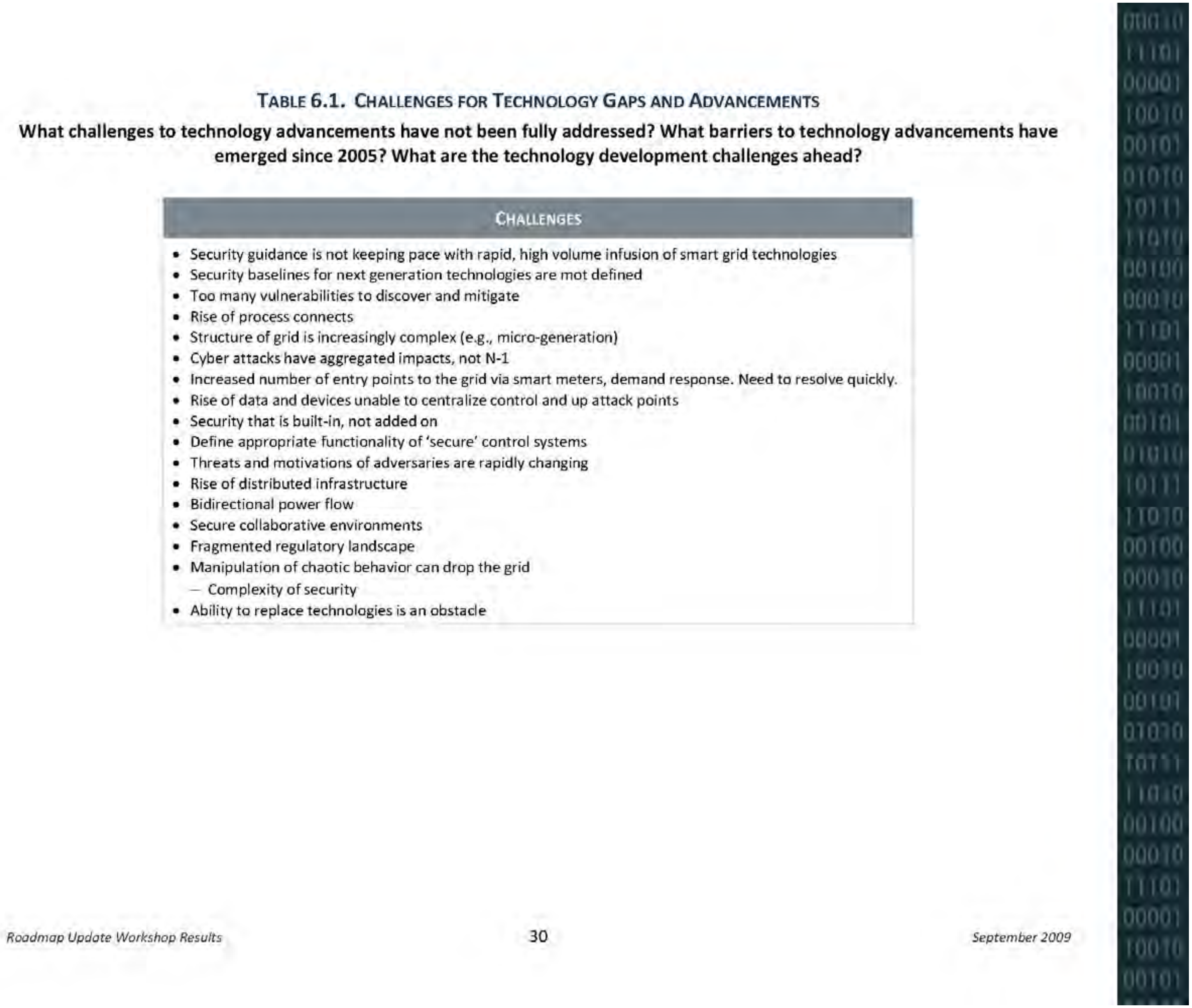


TABLE 6.1. CHALLENGES FOR TECHNOLOGY GAPS AND ADVANCEMENTS

What challenges to technology advancements have not been fully addressed? What barriers to technology advancements have emerged since 2005? What are the technology development challenges ahead?

CHALLENGES
• Security guidance is not keeping pace with rapid, high volume infusion of smart grid technologies
• Security baselines for next generation technologies are mot defined
• Too many vulnerabilities to discover and mitigate
• Rise of process connects
• Structure of grid is increasingly complex (e.g., micro-generation)
• Cyber attacks have aggregated impacts, not N-1
• Increased number of entry points to the grid via smart meters, demand response. Need to resolve quickly.
• Rise of data and devices unable to centralize control and up attack points
• Security that is built-in, not added on
• Define appropriate functionality of 'secure' control systems
• Threats and motivations of adversaries are rapidly changing
• Rise of distributed infrastructure
• Bidirectional power flow
• Secure collaborative environments
• Fragmented regulatory landscape
• Manipulation of chaotic behavior can drop the grid
— Complexity of security
• Ability to replace technologies is an obstacle

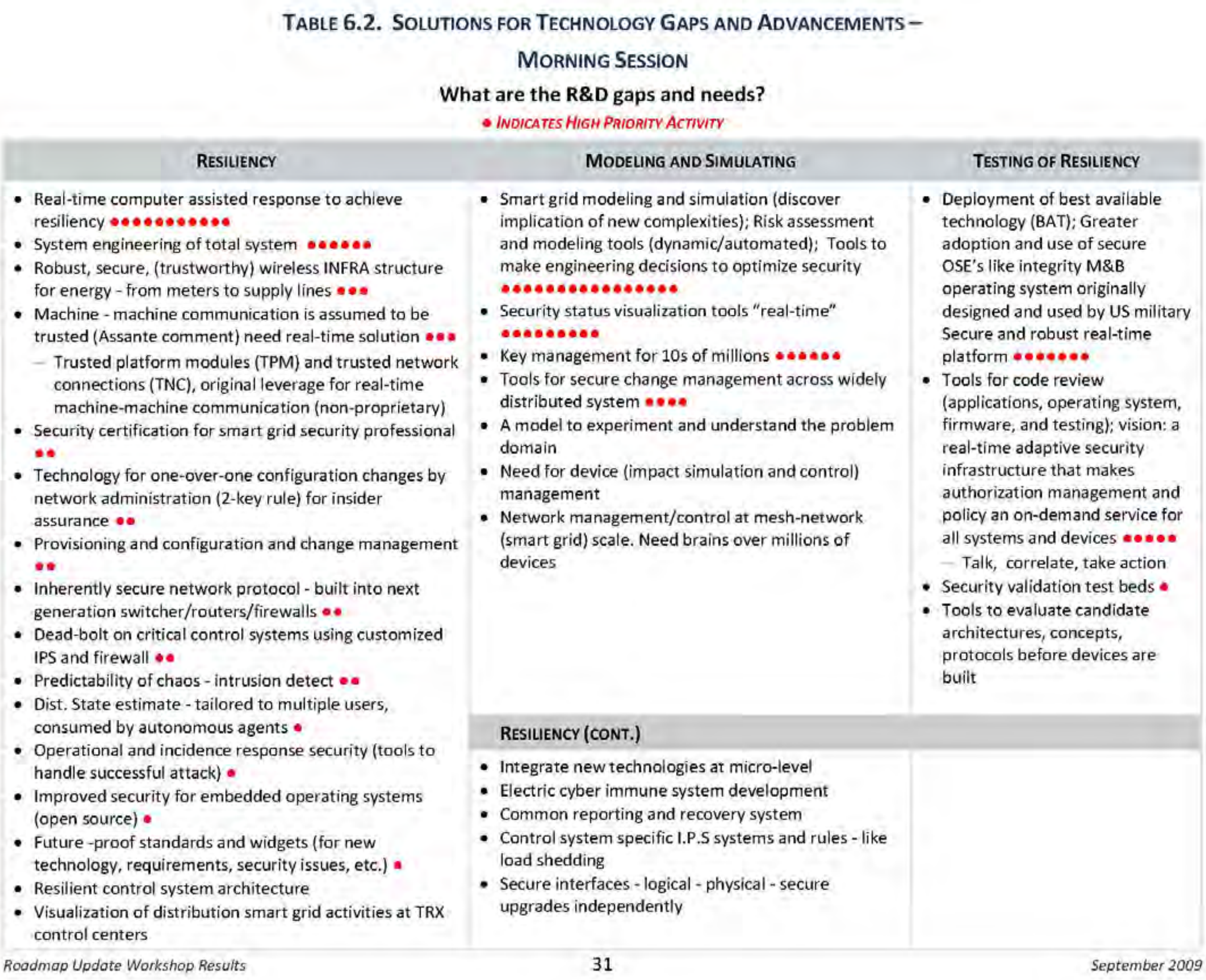


Table 6.2. Solutions for Technology Gaps and Advancements – Morning Session

What are the R&D gaps and needs?

● Indicates High Priority Activity

Resiliency	Modeling and Simulating	Testing of Resiliency
• Real-time computer assisted response to achieve resiliency ●●●●●●●●●●● • System engineering of total system ●●●●●● • Robust, secure, (trustworthy) wireless INFRA structure for energy - from meters to supply lines ●●● • Machine - machine communication is assumed to be trusted (Assante comment) need real-time solution ●●● – Trusted platform modules (TPM) and trusted network connections (TNC), original leverage for real-time machine-machine communication (non-proprietary) • Security certification for smart grid security professional ●● • Technology for one-over-one configuration changes by network administration (2-key rule) for insider assurance ●● • Provisioning and configuration and change management ●● • Inherently secure network protocol - built into next generation switcher/routers/firewalls ●● • Dead-bolt on critical control systems using customized IPS and firewall ●● • Predictability of chaos - intrusion detect ●● • Dist. State estimate - tailored to multiple users, consumed by autonomous agents ● • Operational and incidence response security (tools to handle successful attack) ● • Improved security for embedded operating systems (open source) ● • Future -proof standards and widgets (for new technology, requirements, security issues, etc.) ● • Resilient control system architecture • Visualization of distribution smart grid activities at TRX control centers	• Smart grid modeling and simulation (discover implication of new complexities); Risk assessment and modeling tools (dynamic/automated); Tools to make engineering decisions to optimize security ●●●●●●●●●●●●●●●● • Security status visualization tools "real-time" ●●●●●●●●● • Key management for 10s of millions ●●●●●● • Tools for secure change management across widely distributed system ●●●● • A model to experiment and understand the problem domain • Need for device (impact simulation and control) management • Network management/control at mesh-network (smart grid) scale. Need brains over millions of devices	• Deployment of best available technology (BAT); Greater adoption and use of secure OSE's like integrity M&B operating system originally designed and used by US military Secure and robust real-time platform ●●●●●●● • Tools for code review (applications, operating system, firmware, and testing); vision: a real-time adaptive security infrastructure that makes authorization management and policy an on-demand service for all systems and devices ●●●●● – Talk, correlate, take action • Security validation test beds ● • Tools to evaluate candidate architectures, concepts, protocols before devices are built
	Resiliency (cont.)	
	• Integrate new technologies at micro-level • Electric cyber immune system development • Common reporting and recovery system • Control system specific I.P.S systems and rules - like load shedding • Secure interfaces - logical - physical - secure upgrades independently	

Roadmap Update Workshop Results 31 *September 2009*

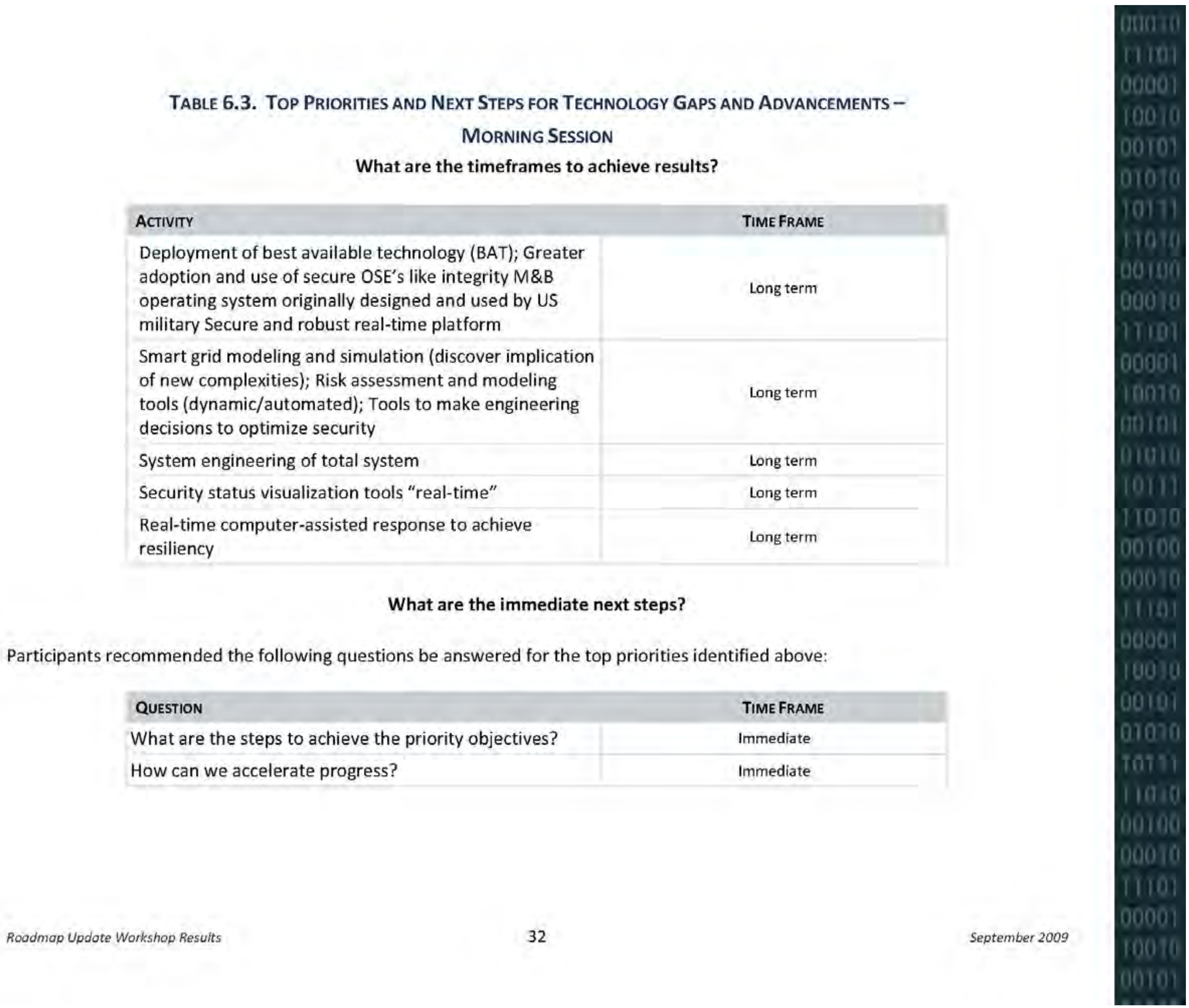


Table 6.3. Top Priorities and Next Steps for Technology Gaps and Advancements – Morning Session

What are the timeframes to achieve results?

Activity	Time Frame
Deployment of best available technology (BAT); Greater adoption and use of secure OSE's like integrity M&B operating system originally designed and used by US military Secure and robust real-time platform	Long term
Smart grid modeling and simulation (discover implication of new complexities); Risk assessment and modeling tools (dynamic/automated); Tools to make engineering decisions to optimize security	Long term
System engineering of total system	Long term
Security status visualization tools "real-time"	Long term
Real-time computer-assisted response to achieve resiliency	Long term

What are the immediate next steps?

Participants recommended the following questions be answered for the top priorities identified above:

Question	Time Frame
What are the steps to achieve the priority objectives?	Immediate
How can we accelerate progress?	Immediate

TABLE 6.4. SOLUTIONS FOR TECHNOLOGY GAPS AND ADVANCEMENTS – AFTERNOON SESSION

What are the R&D gaps and needs?

● INDICATES HIGH PRIORITY ACTIVITY

- Develop scientifically defensible metrics for security robustness, with known utility; conduct collaborative R&D on cyber robustness of next generation systems ●●●●●●●●●
- Defining security architecture ●●●●●●●●
- Agreed upon and available in transit data and source integrity in SCADA/DCS protocols ●●●●●●●
- Non-bootable patching (hot patching) ●●●●●●
- Explicit, managed trust ●●●●●
- Technology to preserve autonomy ●●●●●
- Automated security source testing tool ●●●●
- Secure automated tools to manage the growing number of devices (smart grid) ●●●●
- Operating system white list - nothing runs unless authorized ●●●●
- End point security for the insider threat (DARPA Res.) ●●●
- Better understanding of the threats ●●●
- Large-scale, high-resolution, multi-infrastructure - Mod and Sim ●●●
- Better understanding of interoperability requirements and needs ●●●
- Trust management ●●
- How to manage security in a highly federated environment ●
- Immutable (no more changes) secure operation environment for in-field devices with notification ●
- No IDs - true event collaboration and prevention ●
- Resilience R&D - security is not absolute operations in context of security and vice versa ●
- Understand control theory for smarter grid (security must be done in operation context) ●
- Robust protocol stacks that can withstand sustained fuzzing and negative protocol testing ●
- Flexible technology - threat space changes at internet speed, not human speed ●
- Flexible, self configuring reporting and healing devices ●
- Non-consolidated invasive assessment tools (to address complexity)
- Design systems security into devices to make them a close to plug and play as possible
- Cross system security maintenance/ administration
- Streamline security administration practices
- Preserve legacy functions or feel of HMI by separating HW/SW components and address issues independently
- Migrate infrastructure from inherently unsecure to inherently secure
- Validation of recovery initialization capability
- Cyber security aware AI for security management
- Anomaly based IDs
- Adaptive learning algorithms for 0-day events (IDS/IPS)
- O.S. independent CPU guarantee by process
- Interdependency of the 1,000's of new configuration options

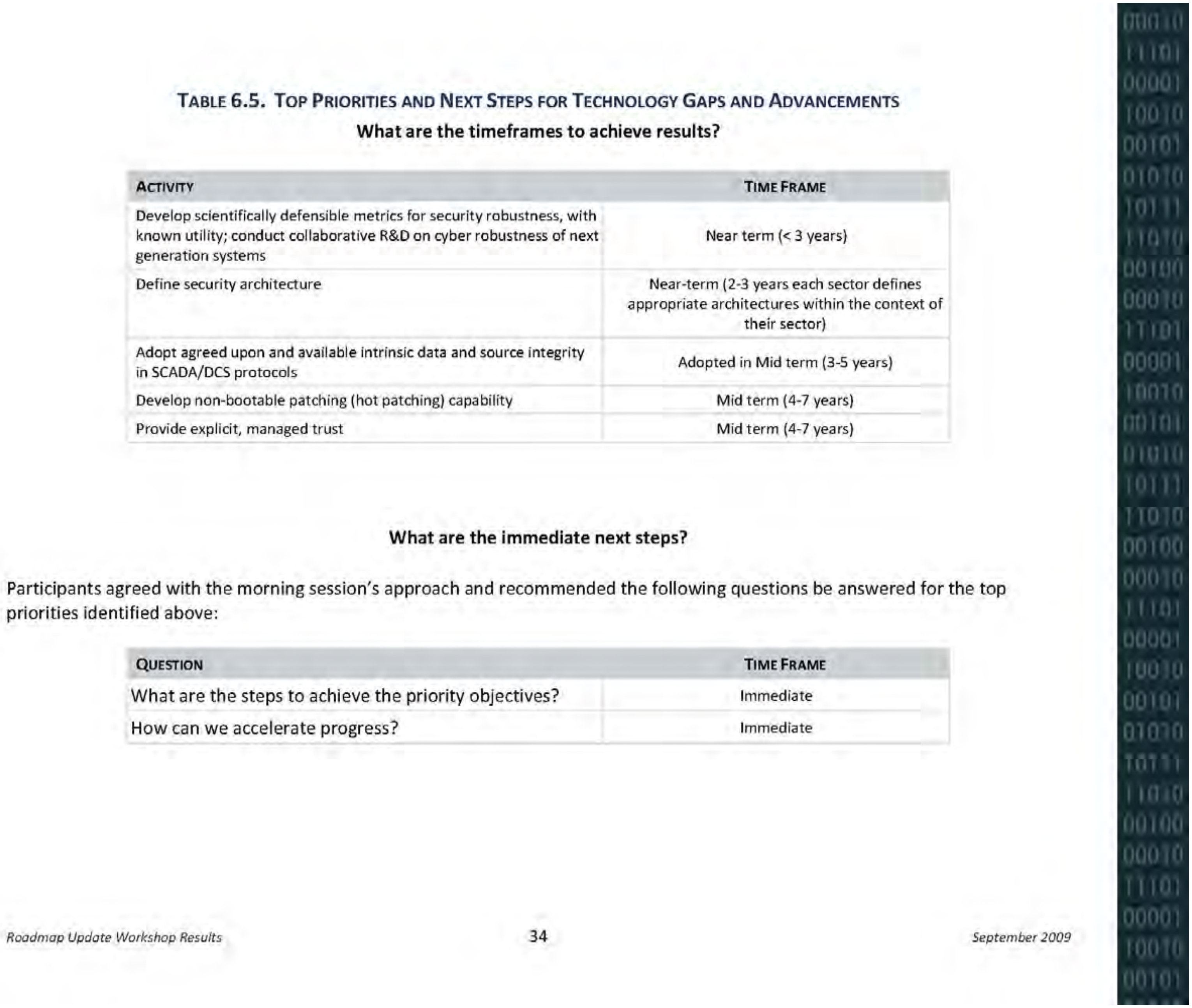


Table 6.5. Top Priorities and Next Steps for Technology Gaps and Advancements

What are the timeframes to achieve results?

Activity	Time Frame
Develop scientifically defensible metrics for security robustness, with known utility; conduct collaborative R&D on cyber robustness of next generation systems	Near term (< 3 years)
Define security architecture	Near-term (2-3 years each sector defines appropriate architectures within the context of their sector)
Adopt agreed upon and available intrinsic data and source integrity in SCADA/DCS protocols	Adopted in Mid term (3-5 years)
Develop non-bootable patching (hot patching) capability	Mid term (4-7 years)
Provide explicit, managed trust	Mid term (4-7 years)

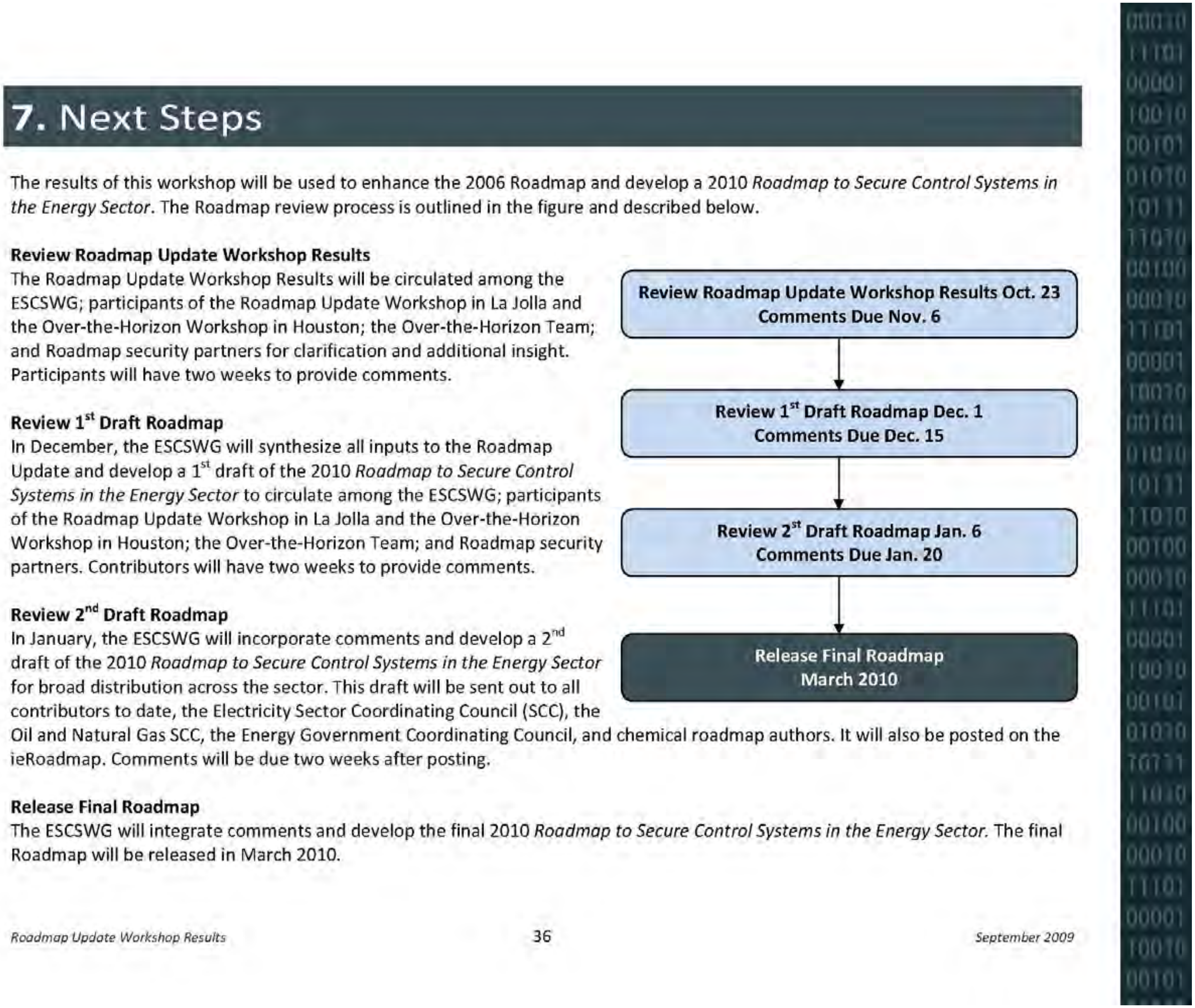
What are the immediate next steps?

Participants agreed with the morning session's approach and recommended the following questions be answered for the top priorities identified above:

Question	Time Frame
What are the steps to achieve the priority objectives?	Immediate
How can we accelerate progress?	Immediate

Table 6.3. Technology Gaps and Advancements Breakout Session Participants

Morning Session Participants		Afternoon Session Participants	
Name	Organization	Name	Organization
Scott Bordenkircher	Arizona Public Service	Klaus Bender	Utilities Telecom Council
Frederick Curry	Energen Corporation	James Briones	Department of Energy
Jeff Dagle	Pacific Northwest National Laboratory	Page Clark	El Paso Electric
Thomas Edgar	Pacific Northwest National Laboratory	Philip Craig	Pacific Northwest National Laboratory
Val Emesih	CenterPoint Energy	Dave DeGroot	Austin Energy
Josh Gerber	San Diego Gas & Electric	Gary Finco	Idaho National Laboratory
Mark Hinrichs	Los Alamos National Laboratory	Dennis Holstein	OPUS Consulting Group
William Hutton	Pacific Northwest National Laboratory	Bob Matthews	Pacific Gas & Electric
Dale Johnson	Conoco Phillips Pipe Line Company	Greg McGill	Uniloc
Stan Klein	Open Secure Energy Control Systems (OSECS)	Nathan Mitchell	American Public Power Association
Wayne Longcore	Southern California Edison	Dale Peterson	Digital Bond
Wayne Manges	Oak Ridge National Laboratory	Bob Pollock	Sandia National Laboratories
Bill Sanders	University of Illinois	Bryan Richardson	Sandia National Laboratories
Mike Sanders	Southern Company	Al Rivero	Telvent
Dave Scheulen	BP	Jim Smith	Los Alamos National Laboratory
Brian Smith	EnerNex Corporation	Rhett Smith	Schweitzer Engineering Laboratories
Al Valdes	SRI International	Keith Stouffer	National Institute of Standards and Technology
Bill Winters	Arizona Public Service		



7. Next Steps

The results of this workshop will be used to enhance the 2006 Roadmap and develop a 2010 *Roadmap to Secure Control Systems in the Energy Sector*. The Roadmap review process is outlined in the figure and described below.

Review Roadmap Update Workshop Results Oct. 23
Comments Due Nov. 6

Review 1st Draft Roadmap Dec. 1
Comments Due Dec. 15

Review 2st Draft Roadmap Jan. 6
Comments Due Jan. 20

Release Final Roadmap
March 2010

Review Roadmap Update Workshop Results

The Roadmap Update Workshop Results will be circulated among the ESCSWG; participants of the Roadmap Update Workshop in La Jolla and the Over-the-Horizon Workshop in Houston; the Over-the-Horizon Team; and Roadmap security partners for clarification and additional insight. Participants will have two weeks to provide comments.

Review 1st Draft Roadmap

In December, the ESCSWG will synthesize all inputs to the Roadmap Update and develop a 1st draft of the 2010 *Roadmap to Secure Control Systems in the Energy Sector* to circulate among the ESCSWG; participants of the Roadmap Update Workshop in La Jolla and the Over-the-Horizon Workshop in Houston; the Over-the-Horizon Team; and Roadmap security partners. Contributors will have two weeks to provide comments.

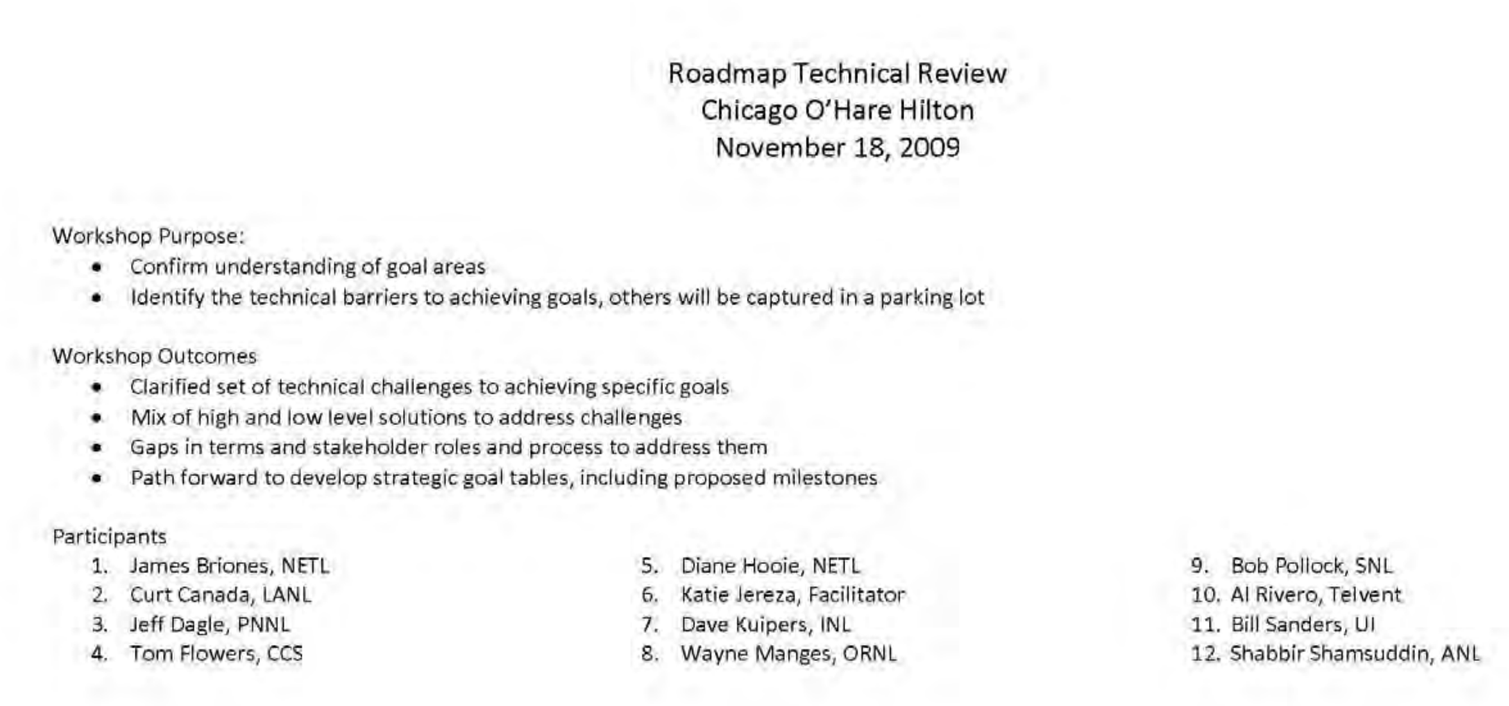
Review 2nd Draft Roadmap

In January, the ESCSWG will incorporate comments and develop a 2nd draft of the 2010 *Roadmap to Secure Control Systems in the Energy Sector* for broad distribution across the sector. This draft will be sent out to all contributors to date, the Electricity Sector Coordinating Council (SCC), the Oil and Natural Gas SCC, the Energy Government Coordinating Council, and chemical roadmap authors. It will also be posted on the ieRoadmap. Comments will be due two weeks after posting.

Release Final Roadmap

The ESCSWG will integrate comments and develop the final 2010 *Roadmap to Secure Control Systems in the Energy Sector.* The final Roadmap will be released in March 2010.

3. Roadmap Technical Review Workshop



Roadmap Technical Review
Chicago O'Hare Hilton
November 18, 2009

Workshop Purpose:

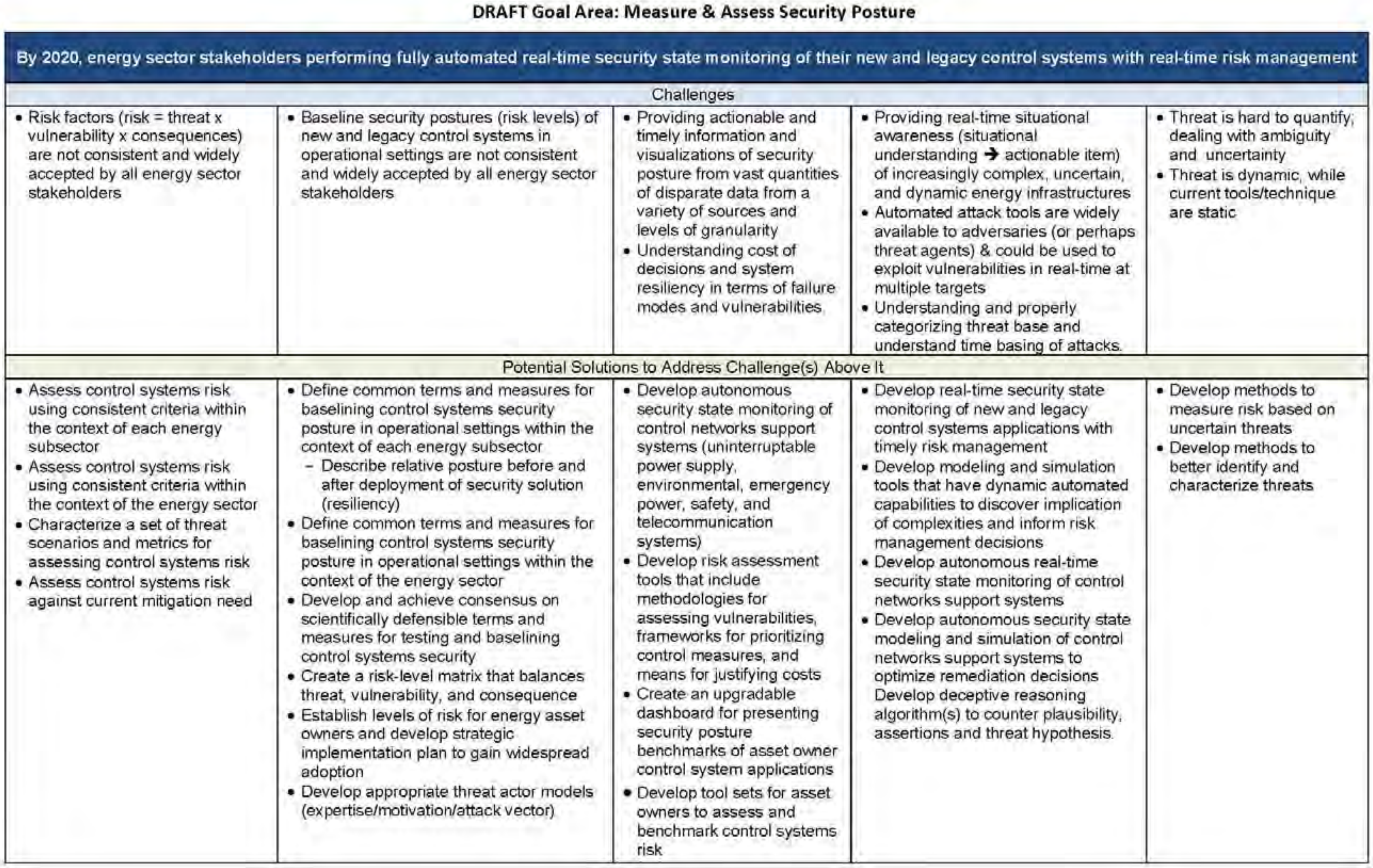
- Confirm understanding of goal areas
- Identify the technical barriers to achieving goals, others will be captured in a parking lot

Workshop Outcomes

- Clarified set of technical challenges to achieving specific goals
- Mix of high and low level solutions to address challenges
- Gaps in terms and stakeholder roles and process to address them
- Path forward to develop strategic goal tables, including proposed milestones

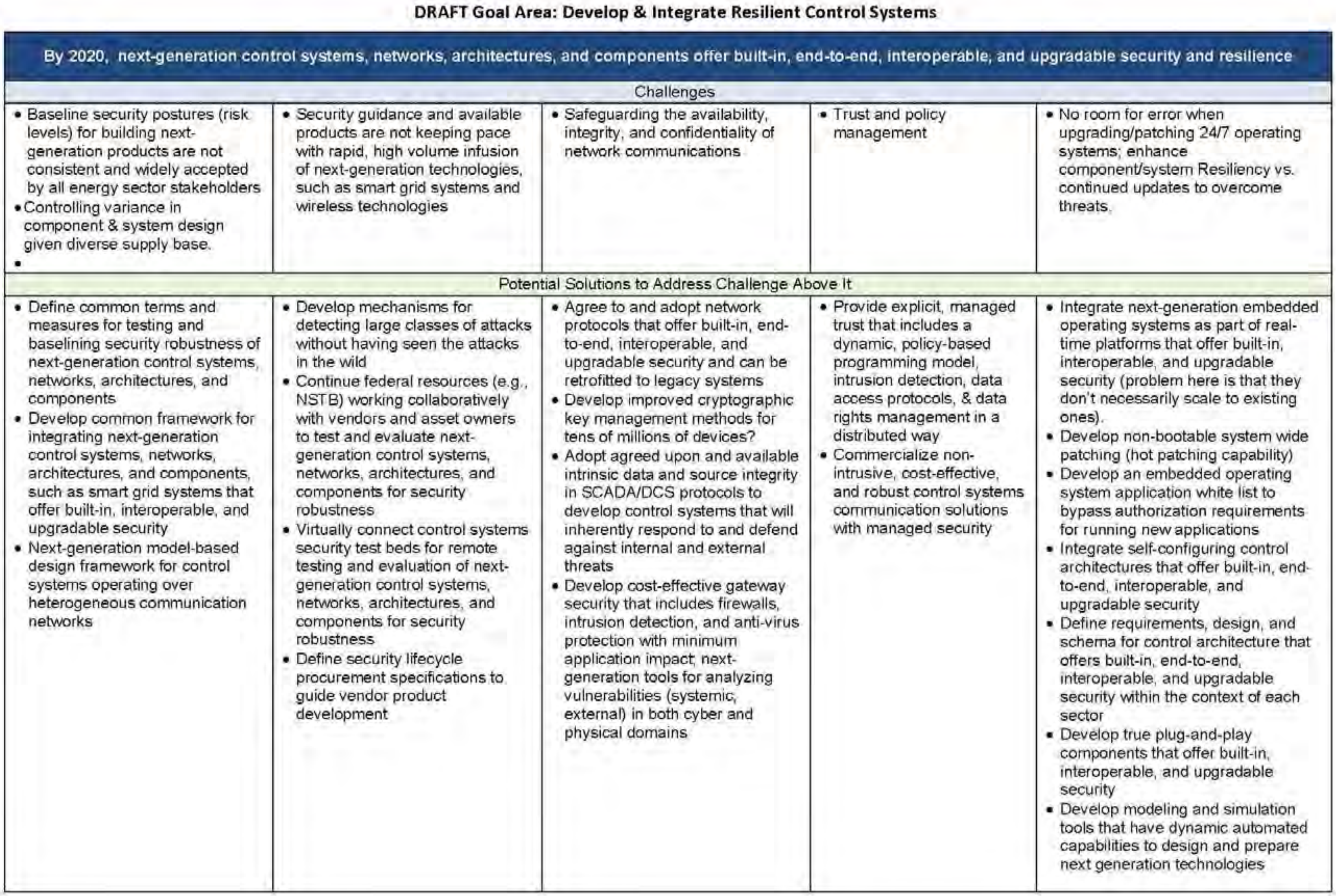
Participants

1. James Briones, NETL
2. Curt Canada, LANL
3. Jeff Dagle, PNNL
4. Tom Flowers, CCS
5. Diane Hooie, NETL
6. Katie Jereza, Facilitator
7. Dave Kuipers, INL
8. Wayne Manges, ORNL
9. Bob Pollock, SNL
10. Al Rivero, Telvent
11. Bill Sanders, UI
12. Shabbir Shamsuddin, ANL



DRAFT Goal Area: Measure & Assess Security Posture

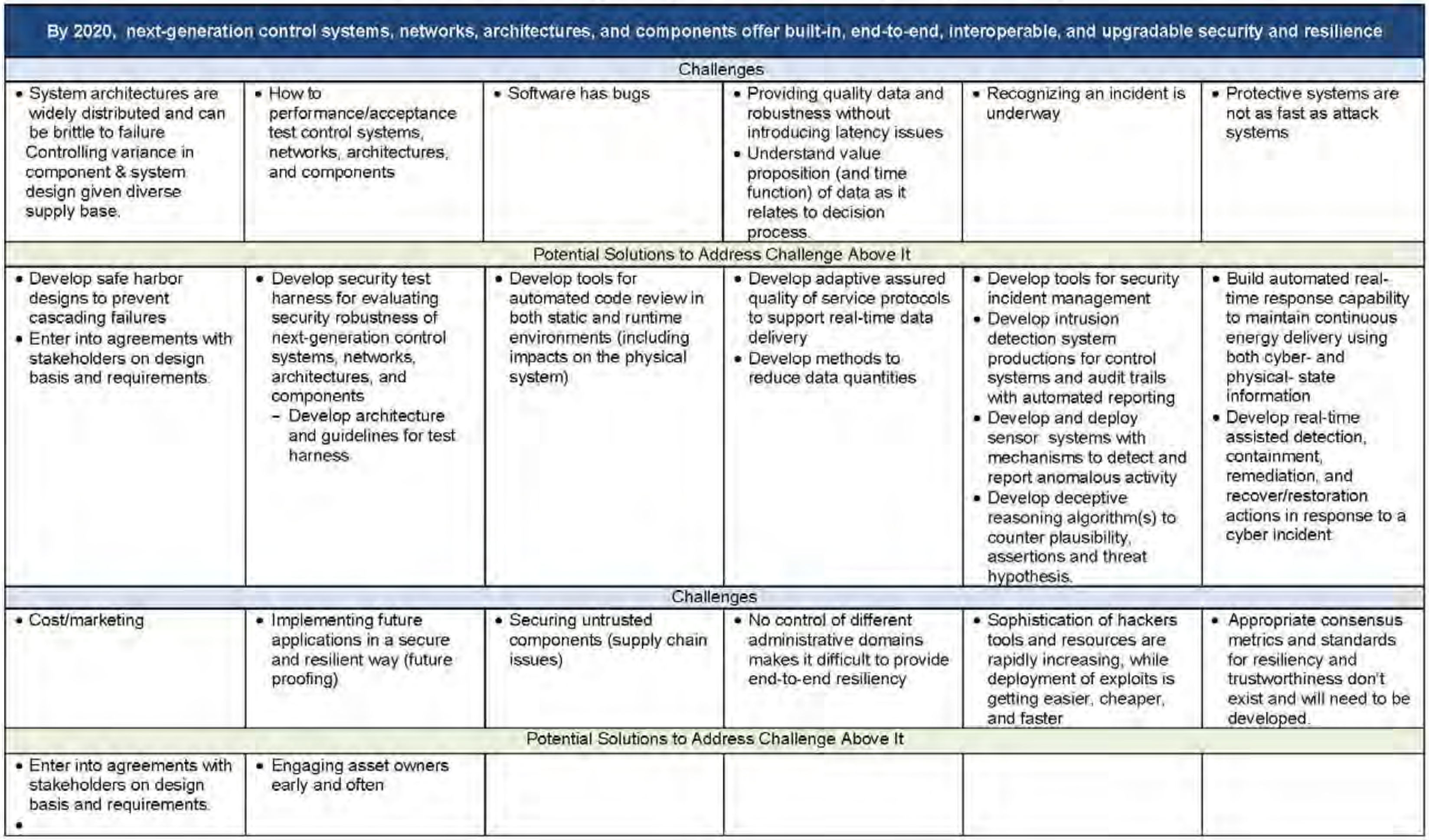
By 2020, energy sector stakeholders performing fully automated real-time security state monitoring of their new and legacy control systems with real-time risk management				
Challenges				
• Risk factors (risk = threat x vulnerability x consequences) are not consistent and widely accepted by all energy sector stakeholders	• Baseline security postures (risk levels) of new and legacy control systems in operational settings are not consistent and widely accepted by all energy sector stakeholders	• Providing actionable and timely information and visualizations of security posture from vast quantities of disparate data from a variety of sources and levels of granularity • Understanding cost of decisions and system resiliency in terms of failure modes and vulnerabilities	• Providing real-time situational awareness (situational understanding → actionable item) of increasingly complex, uncertain, and dynamic energy infrastructures • Automated attack tools are widely available to adversaries (or perhaps threat agents) & could be used to exploit vulnerabilities in real-time at multiple targets • Understanding and properly categorizing threat base and understand time basing of attacks.	• Threat is hard to quantify, dealing with ambiguity and uncertainty • Threat is dynamic, while current tools/technique are static
Potential Solutions to Address Challenge(s) Above It				
• Assess control systems risk using consistent criteria within the context of each energy subsector • Assess control systems risk using consistent criteria within the context of the energy sector • Characterize a set of threat scenarios and metrics for assessing control systems risk • Assess control systems risk against current mitigation need	• Define common terms and measures for baselining control systems security posture in operational settings within the context of each energy subsector – Describe relative posture before and after deployment of security solution (resiliency) • Define common terms and measures for baselining control systems security posture in operational settings within the context of the energy sector • Develop and achieve consensus on scientifically defensible terms and measures for testing and baselining control systems security • Create a risk-level matrix that balances threat, vulnerability, and consequence • Establish levels of risk for energy asset owners and develop strategic implementation plan to gain widespread adoption • Develop appropriate threat actor models (expertise/motivation/attack vector)	• Develop autonomous security state monitoring of control networks support systems (uninterruptable power supply, environmental, emergency power, safety, and telecommunication systems) • Develop risk assessment tools that include methodologies for assessing vulnerabilities, frameworks for prioritizing control measures, and means for justifying costs • Create an upgradable dashboard for presenting security posture benchmarks of asset owner control system applications • Develop tool sets for asset owners to assess and benchmark control systems risk	• Develop real-time security state monitoring of new and legacy control systems applications with timely risk management • Develop modeling and simulation tools that have dynamic automated capabilities to discover implication of complexities and inform risk management decisions • Develop autonomous real-time security state monitoring of control networks support systems • Develop autonomous security state modeling and simulation of control networks support systems to optimize remediation decisions Develop deceptive reasoning algorithm(s) to counter plausibility, assertions and threat hypothesis.	• Develop methods to measure risk based on uncertain threats • Develop methods to better identify and characterize threats



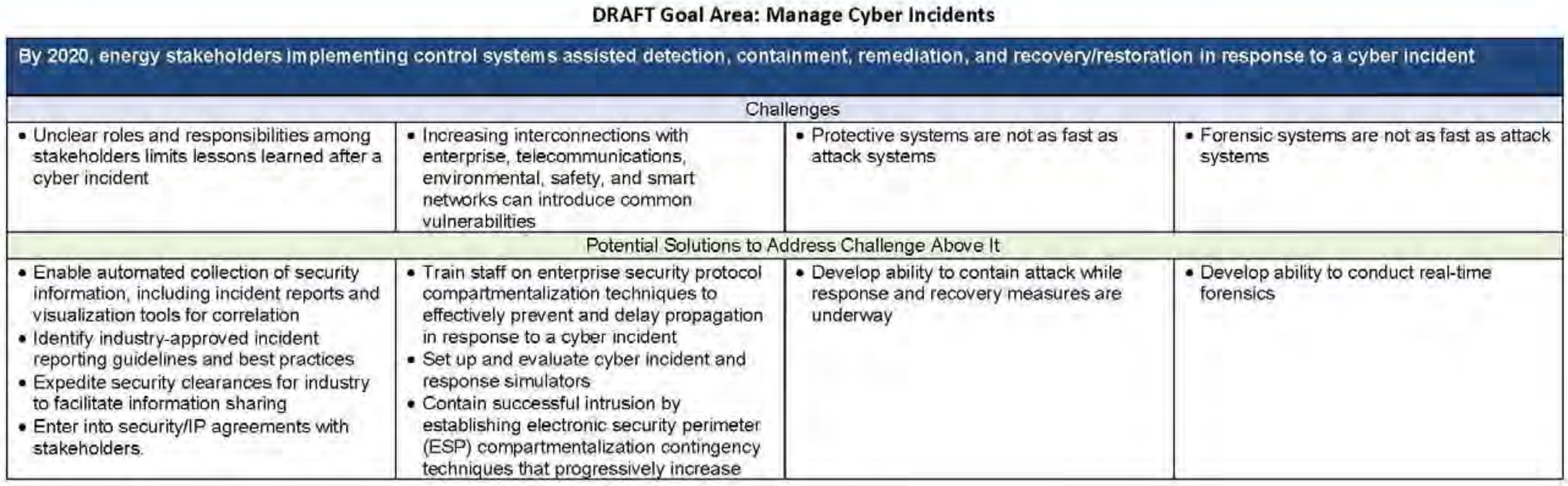
DRAFT Goal Area: Develop & Integrate Resilient Control Systems

By 2020, next-generation control systems, networks, architectures, and components offer built-in, end-to-end, interoperable, and upgradable security and resilience				
Challenges				
• Baseline security postures (risk levels) for building next-generation products are not consistent and widely accepted by all energy sector stakeholders • Controlling variance in component & system design given diverse supply base. •	• Security guidance and available products are not keeping pace with rapid, high volume infusion of next-generation technologies, such as smart grid systems and wireless technologies	• Safeguarding the availability, integrity, and confidentiality of network communications	• Trust and policy management	• No room for error when upgrading/patching 24/7 operating systems; enhance component/system Resiliency vs. continued updates to overcome threats.
Potential Solutions to Address Challenge Above It				
• Define common terms and measures for testing and baselining security robustness of next-generation control systems, networks, architectures, and components • Develop common framework for integrating next-generation control systems, networks, architectures, and components, such as smart grid systems that offer built-in, interoperable, and upgradable security • Next-generation model-based design framework for control systems operating over heterogeneous communication networks	• Develop mechanisms for detecting large classes of attacks without having seen the attacks in the wild • Continue federal resources (e.g., NSTB) working collaboratively with vendors and asset owners to test and evaluate next-generation control systems, networks, architectures, and components for security robustness • Virtually connect control systems security test beds for remote testing and evaluation of next-generation control systems, networks, architectures, and components for security robustness • Define security lifecycle procurement specifications to guide vendor product development	• Agree to and adopt network protocols that offer built-in, end-to-end, interoperable, and upgradable security and can be retrofitted to legacy systems • Develop improved cryptographic key management methods for tens of millions of devices? • Adopt agreed upon and available intrinsic data and source integrity in SCADA/DCS protocols to develop control systems that will inherently respond to and defend against internal and external threats • Develop cost-effective gateway security that includes firewalls, intrusion detection, and anti-virus protection with minimum application impact; next-generation tools for analyzing vulnerabilities (systemic, external) in both cyber and physical domains	• Provide explicit, managed trust that includes a dynamic, policy-based programming model, intrusion detection, data access protocols, & data rights management in a distributed way • Commercialize non-intrusive, cost-effective, and robust control systems communication solutions with managed security	• Integrate next-generation embedded operating systems as part of real-time platforms that offer built-in, interoperable, and upgradable security (problem here is that they don't necessarily scale to existing ones). • Develop non-bootable system wide patching (hot patching capability) • Develop an embedded operating system application white list to bypass authorization requirements for running new applications • Integrate self-configuring control architectures that offer built-in, end-to-end, interoperable, and upgradable security • Define requirements, design, and schema for control architecture that offers built-in, end-to-end, interoperable, and upgradable security within the context of each sector • Develop true plug-and-play components that offer built-in, interoperable, and upgradable security • Develop modeling and simulation tools that have dynamic automated capabilities to design and prepare next generation technologies

DRAFT Goal Area: Develop & Integrate Resilient Control Systems (CONTINUED)

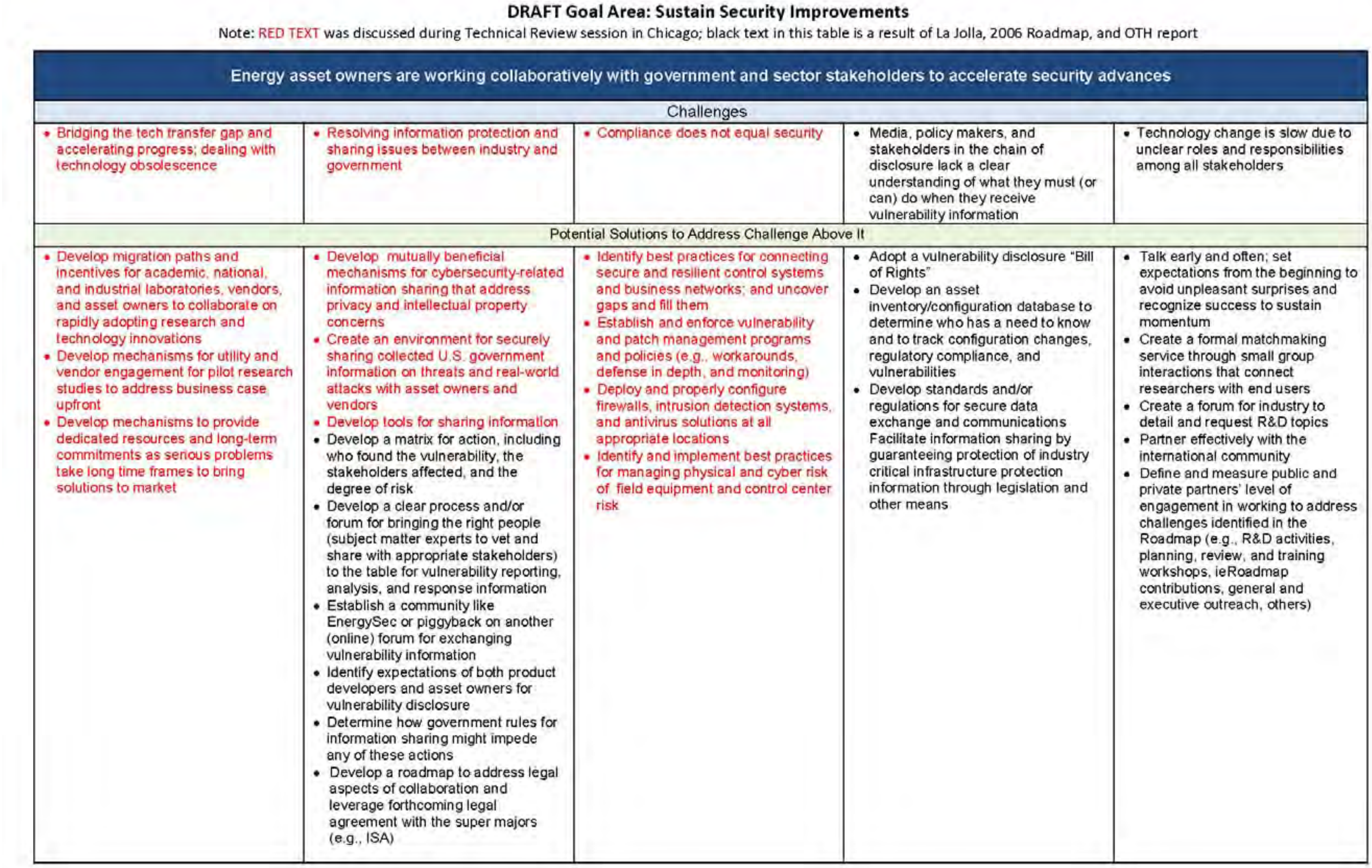


By 2020, next-generation control systems, networks, architectures, and components offer built-in, end-to-end, interoperable, and upgradable security and resilience					
Challenges					
• System architectures are widely distributed and can be brittle to failure Controlling variance in component & system design given diverse supply base.	• How to performance/acceptance test control systems, networks, architectures, and components	• Software has bugs	• Providing quality data and robustness without introducing latency issues • Understand value proposition (and time function) of data as it relates to decision process.	• Recognizing an incident is underway	• Protective systems are not as fast as attack systems
Potential Solutions to Address Challenge Above It					
• Develop safe harbor designs to prevent cascading failures • Enter into agreements with stakeholders on design basis and requirements.	• Develop security test harness for evaluating security robustness of next-generation control systems, networks, architectures, and components – Develop architecture and guidelines for test harness	• Develop tools for automated code review in both static and runtime environments (including impacts on the physical system)	• Develop adaptive assured quality of service protocols to support real-time data delivery • Develop methods to reduce data quantities	• Develop tools for security incident management • Develop intrusion detection system productions for control systems and audit trails with automated reporting • Develop and deploy sensor systems with mechanisms to detect and report anomalous activity • Develop deceptive reasoning algorithm(s) to counter plausibility, assertions and threat hypothesis.	• Build automated real-time response capability to maintain continuous energy delivery using both cyber- and physical- state information • Develop real-time assisted detection, containment, remediation, and recover/restoration actions in response to a cyber incident
Challenges					
• Cost/marketing	• Implementing future applications in a secure and resilient way (future proofing)	• Securing untrusted components (supply chain issues)	• No control of different administrative domains makes it difficult to provide end-to-end resiliency	• Sophistication of hackers tools and resources are rapidly increasing, while deployment of exploits is getting easier, cheaper, and faster	• Appropriate consensus metrics and standards for resiliency and trustworthiness don't exist and will need to be developed.
Potential Solutions to Address Challenge Above It					
• Enter into agreements with stakeholders on design basis and requirements. •	• Engaging asset owners early and often				



DRAFT Goal Area: Manage Cyber Incidents

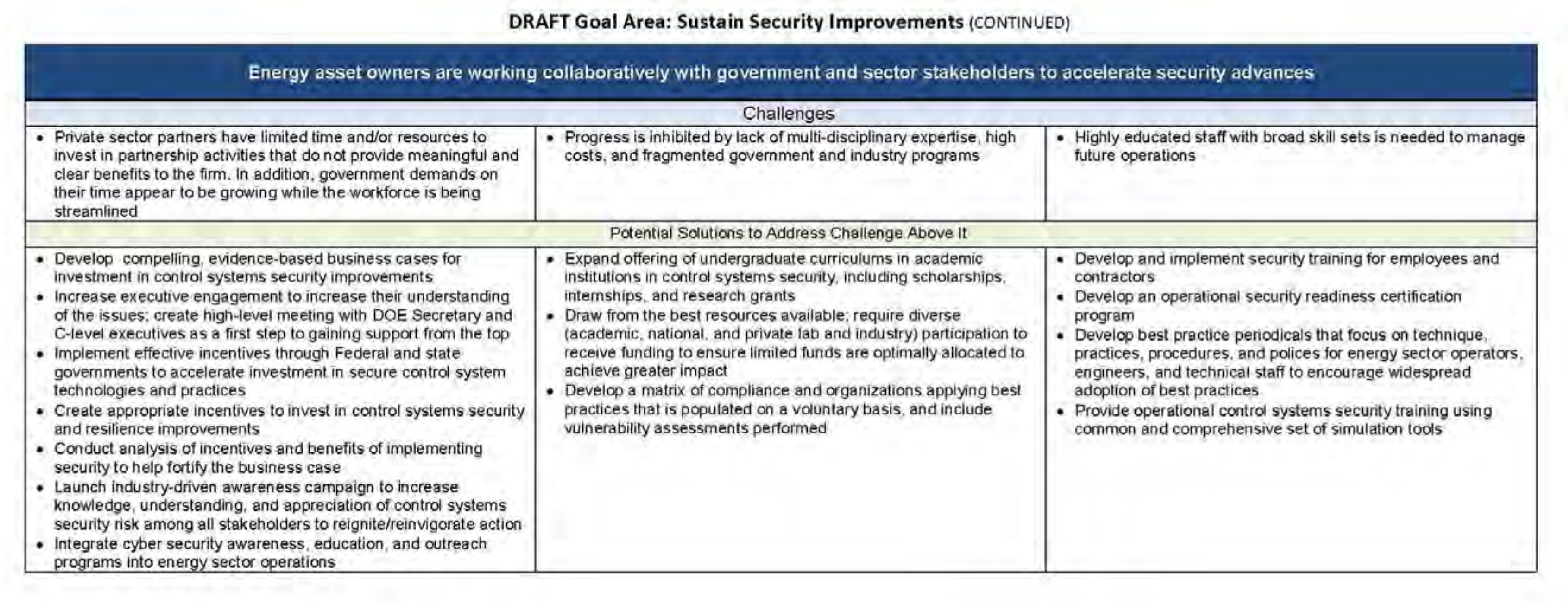
By 2020, energy stakeholders implementing control systems assisted detection, containment, remediation, and recovery/restoration in response to a cyber incident			
Challenges			
• Unclear roles and responsibilities among stakeholders limits lessons learned after a cyber incident	• Increasing interconnections with enterprise, telecommunications, environmental, safety, and smart networks can introduce common vulnerabilities	• Protective systems are not as fast as attack systems	• Forensic systems are not as fast as attack systems
Potential Solutions to Address Challenge Above It			
• Enable automated collection of security information, including incident reports and visualization tools for correlation • Identify industry-approved incident reporting guidelines and best practices • Expedite security clearances for industry to facilitate information sharing • Enter into security/IP agreements with stakeholders.	• 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 • Contain successful intrusion by establishing electronic security perimeter (ESP) compartmentalization contingency techniques that progressively increase	• Develop ability to contain attack while response and recovery measures are underway	• Develop ability to conduct real-time forensics



DRAFT Goal Area: Sustain Security Improvements

Note: RED TEXT was discussed during Technical Review session in Chicago; black text in this table is a result of La Jolla, 2006 Roadmap, and OTH report

Energy asset owners are working collaboratively with government and sector stakeholders to accelerate security advances				
Challenges				
• Bridging the tech transfer gap and accelerating progress; dealing with technology obsolescence	• Resolving information protection and sharing issues between industry and government	• Compliance does not equal security	• Media, policy makers, and stakeholders in the chain of disclosure lack a clear understanding of what they must (or can) do when they receive vulnerability information	• Technology change is slow due to unclear roles and responsibilities among all stakeholders
Potential Solutions to Address Challenge Above It				
• Develop migration paths and incentives for academic, national, and industrial laboratories, vendors, and asset owners to collaborate on rapidly adopting research and technology innovations • Develop mechanisms for utility and vendor engagement for pilot research studies to address business case upfront • Develop mechanisms to provide dedicated resources and long-term commitments as serious problems take long time frames to bring solutions to market	• Develop mutually beneficial mechanisms for cybersecurity-related information sharing that address privacy and intellectual property concerns • Create an environment for securely sharing collected U.S. government information on threats and real-world attacks with asset owners and vendors • Develop tools for sharing information • Develop a matrix for action, including who found the vulnerability, the stakeholders affected, and the degree of risk • Develop a clear process and/or forum for bringing the right people (subject matter experts to vet and share with appropriate stakeholders) to the table for vulnerability reporting, analysis, and response information • Establish a community like EnergySec or piggyback on another (online) forum for exchanging vulnerability information • Identify expectations of both product developers and asset owners for vulnerability disclosure • Determine how government rules for information sharing might impede any of these actions • Develop a roadmap to address legal aspects of collaboration and leverage forthcoming legal agreement with the super majors (e.g., ISA)	• Identify best practices for connecting secure and resilient control systems and business networks; and uncover gaps and fill them • Establish and enforce vulnerability and patch management programs and policies (e.g., workarounds, defense in depth, and monitoring) • Deploy and properly configure firewalls, intrusion detection systems, and antivirus solutions at all appropriate locations • Identify and implement best practices for managing physical and cyber risk of field equipment and control center risk	• Adopt a vulnerability disclosure "Bill of Rights" • 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 and/or regulations for secure data exchange and communications Facilitate information sharing by guaranteeing protection of industry critical infrastructure protection information through legislation and other means	• Talk early and often; set expectations from the beginning to avoid unpleasant surprises and recognize success to sustain momentum • Create a formal matchmaking service through small group interactions that connect researchers with end users • Create a forum for industry to detail and request R&D topics • Partner effectively with the international community • Define and measure public and private partners' level of engagement in working to address challenges identified in the Roadmap (e.g., R&D activities, planning, review, and training workshops, ieRoadmap contributions, general and executive outreach, others)



DRAFT Goal Area: Sustain Security Improvements (CONTINUED)

Energy asset owners are working collaboratively with government and sector stakeholders to accelerate security advances		
Challenges		
• Private sector partners have limited time and/or resources to invest in partnership activities that do not provide meaningful and clear benefits to the firm. In addition, government demands on their time appear to be growing while the workforce is being streamlined	• Progress is inhibited by lack of multi-disciplinary expertise, high costs, and fragmented government and industry programs	• Highly educated staff with broad skill sets is needed to manage future operations
Potential Solutions to Address Challenge Above It		
• Develop compelling, evidence-based business cases for investment in control systems security improvements • Increase executive engagement to increase their understanding of the issues; create high-level meeting with DOE Secretary and C-level executives as a first step to gaining support from the top • Implement effective incentives through Federal and state governments to accelerate investment in secure control system technologies and practices • Create appropriate incentives to invest in control systems security and resilience improvements • Conduct analysis of incentives and benefits of implementing security to help fortify the business case • Launch industry-driven awareness campaign to increase knowledge, understanding, and appreciation of control systems security risk among all stakeholders to reignite/reinvigorate action • Integrate cyber security awareness, education, and outreach programs into energy sector operations	• Expand offering of undergraduate curriculums in academic institutions in control systems security, including scholarships, internships, and research grants • Draw from the best resources available; require diverse (academic, national, and private lab and industry) participation to receive funding to ensure limited funds are optimally allocated to achieve greater impact • Develop a matrix of compliance and organizations applying best practices that is populated on a voluntary basis, and include vulnerability assessments performed	• Develop and implement security training for employees and contractors • Develop an operational security readiness certification program • Develop best practice periodicals that focus on technique, practices, procedures, and polices for energy sector operators, engineers, and technical staff to encourage widespread adoption of best practices • Provide operational control systems security training using common and comprehensive set of simulation tools

Draft Terms Defined

- Resiliency – time-measured ability of system to recover to system's function, operations, and utility capability prior to attack.
- Critical Control Systems Applications – critical applications for control systems encompass several types of control systems, networks, architectures, and components.
  - Control systems – a general term, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), remote terminal units (RTU), and programmable logic controllers (PLC). Note: we dropped industrial from NIST's definition.[1]
  - Control networks - comprise devices used to access the critical control system application, the services provided by the system, supporting elements of the networks, and all means of moving, storing, processing, and protecting information[2]
  - Control architectures - the design principles, physical configuration, functional organization, operational procedures, and data formats used as the bases for the design, construction, modification, and operation of a control network.[3]
  - Control components – encompass people who operate the control systems and the devices used to build and maintain control systems, networks, and architectures.[2]
- Survive – the critical control systems application must be resilient against physical damage, unauthorized manipulation, and electronic assault[2]
- Cyber Incident – any unauthorized access to computer networks and equipment with actions resulting in some form of negative consequence to the asset owners. Damage might include stolen data, exposure of private or business sensitive information, interruption of key services, a shutdown of production operations, and damage to physical equipment and the environment.[4] From an all hazards perspective, a cyber incident occurs when a terrorist attack, other intentional act, natural disaster, or other hazard destroys, incapacitates, or exploits all or part of a control system and its networks[5]
- Loss of Critical Function – any operation, task, or service that, were it to fail or be compromised, would produce major safety, health, operational, or economic consequences[6]
- Security Robustness – The measure or extent of the ability a security system to continue to function despite the existence of faults in its component subsystems or parts. *Note:* System performance may be diminished or otherwise altered until the faults are corrected.[3]
- Security Objectives - include availability, integrity, and confidentiality:
  - Availability – "providing the data when needed or "ensuring timely and reliable access to and use of information…."c A loss of availability is the disruption of access to or use of information from an information system."[7]
  - Integrity – "ensuring that the data presented are the true valid master source of the data or "guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity…."d A loss of integrity is the unauthorized modification, insertion, or destruction of information.[7]

[1] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, Final Public Draft, September 29, 2008

[2] Cyberspace Policy Review, http://www.controlsystemsroadmap.net/pdfs/Cyberspace_Policy_Review.pdf, May 2009

[3] ATIS Glossary, http://www.atis.org/glossary/using.aspx, 2007

[4] DHS CSSP, Developing an Industrial Control Systems Cybersecurity Incident Response Capability, Oct 2009

[5] NIPP, http://www.controlsystemsroadmap.net/pdfs/NIPP_Plan.pdf, 2006

[6] Energy Roadmap, www.controlsystemsroadmap.net, 2006

[7] DHS CSSP, Cyber Security Procurement Language for Control Systems, Oct 2009

- Confidentiality – “keeping the data unseen by others, or “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information....”. A loss of confidentiality is the unauthorized disclosure of information.” [7]