U.S. Department of Energy

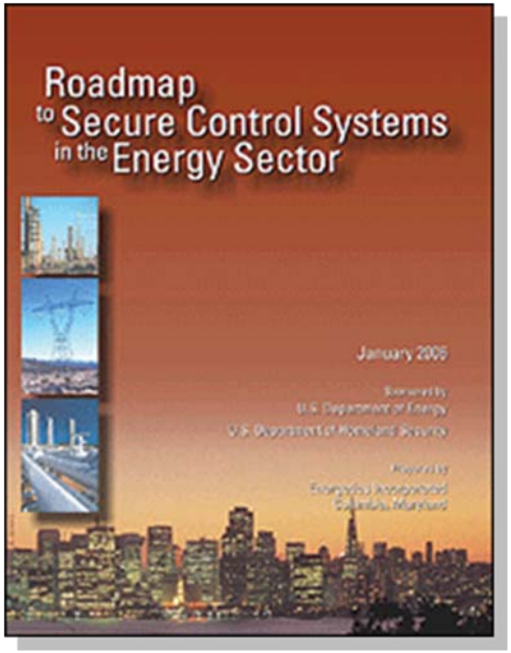
Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

July 20, 2010

Carol Hawk
Program Manager
U.S. Department of Energy

Roadmap – Framework for Public-Private Collaboration



Roadmap to Secure Control Systems in the Energy Sector

January 2006

Sponsored by
U.S. Department of Energy
U.S. Department of Homeland Security

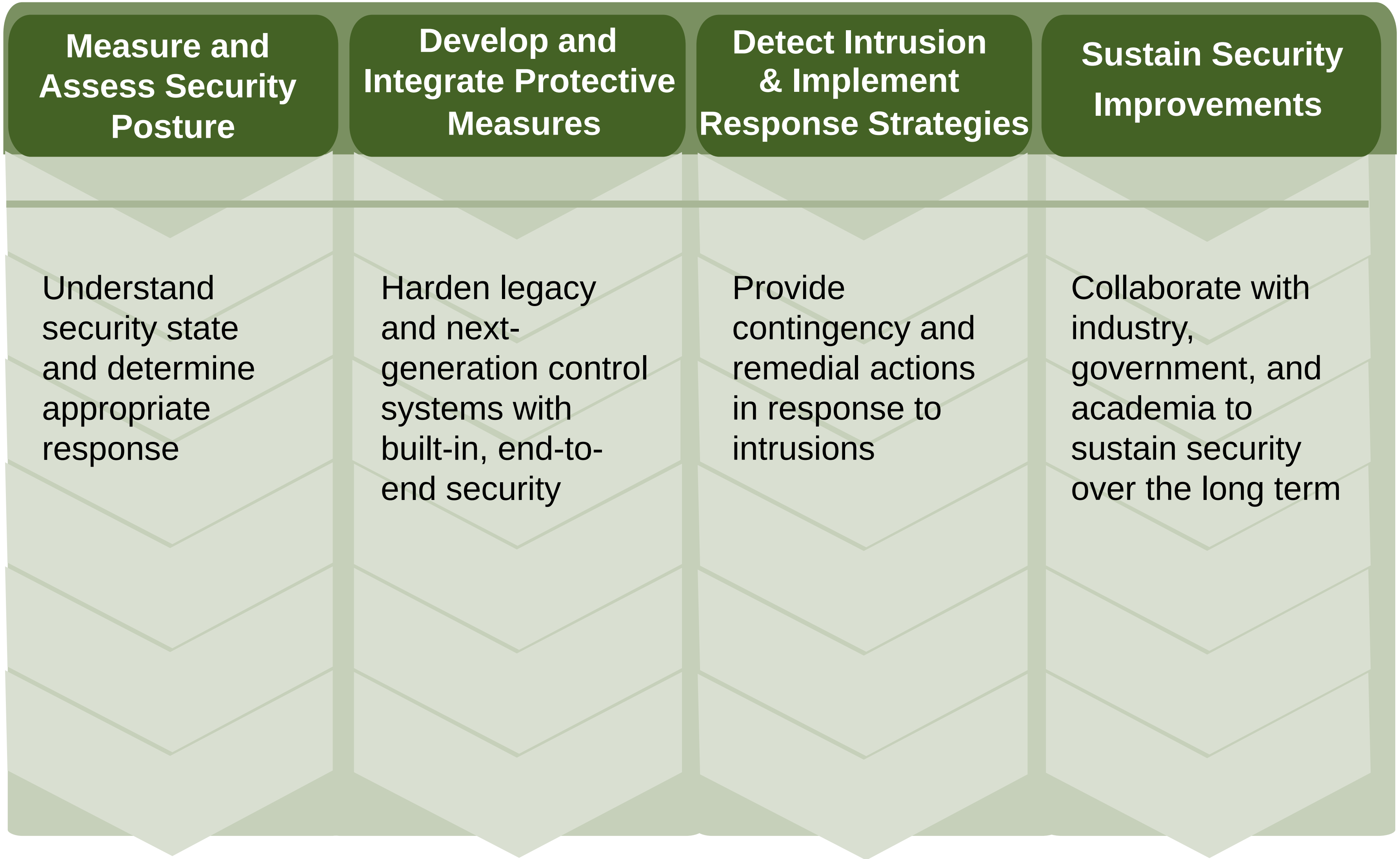
Prepared by
Energetics Incorporated
Columbia, Maryland

- Published in January 2006
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in control systems security

Roadmap Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to *survive* an intentional cyber assault with no loss of critical function.

Roadmap Strategies



Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion & Implement Response Strategies	Sustain Security Improvements
Understand security state and determine appropriate response	Harden legacy and next-generation control systems with built-in, end-to-end security	Provide contingency and remedial actions in response to intrusions	Collaborate with industry, government, and academia to sustain security over the long term

ieRoadmap – facilitates collaboration

ie Roadmap

interactive energy Roadmap
to secure control systems

- Online Roadmap mapping tool
- More than 65 projects mapped by 21 organizations

www.controlsystemsroadmap.net

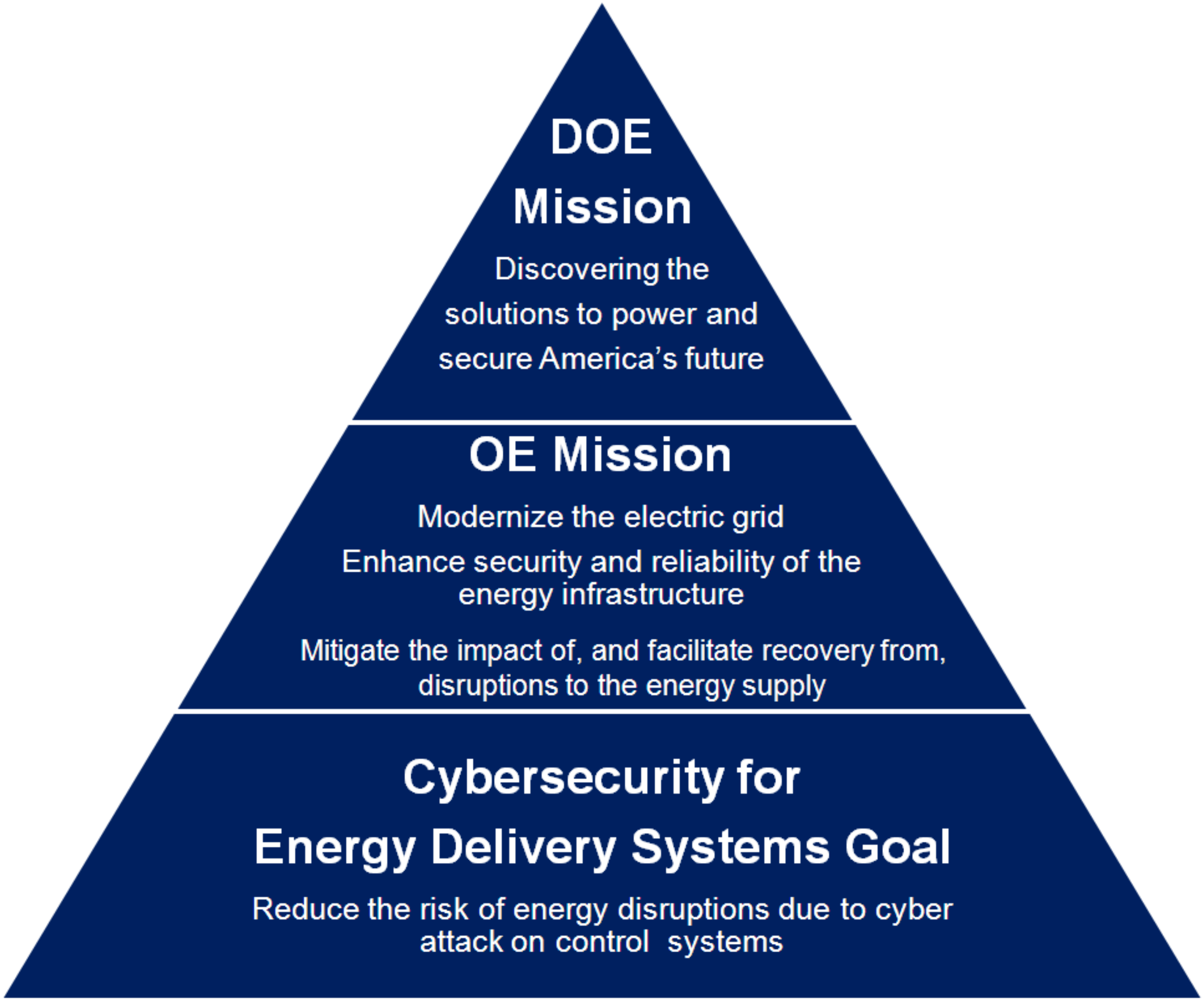
1. CIDG, Corp.
2. Cisco Systems
3. DHS HSARPA
4. DHS National Cyber Security Division CSSP
5. Digital Bond
6. DOD Technical Support Working Group
7. DOE Cybersecurity for Energy Delivery Systems Program (CEDS)
8. Electric Power Research Institute (EPRI)
9. Information Trust Institute (ITI)
10. Institute for Information Infrastructure Protection (I3P)
11. Mu Dynamics
12. MS-ISAC
13. NIST
14. PNNL NCSSR
15. Raytheon
16. Siemens Corporate Research
17. SRI International
18. Tenable Network Security
19. Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)
20. U. of Illinois at Urbana-Champagne
21. Wurldtech Security Technologies

Cybersecurity is a National Priority

"…that's why we're going to need all of you to keep coming together—government, industry, academia, think tanks, media and privacy and civil liberties groups—to work together, to develop the solutions we need to keep America safe and prosperous in cyberspace."

- President Barack Obama, July 14, 2010

Cybersecurity Aligned with DOE and OE Missions



DOE Mission

Discovering the solutions to power and secure America's future

OE Mission

Modernize the electric grid

Enhance security and reliability of the energy infrastructure

Mitigate the impact of, and facilitate recovery from, disruptions to the energy supply

Cybersecurity for Energy Delivery Systems Goal

Reduce the risk of energy disruptions due to cyber attack on control systems

Source: OE 2010 Strategic Plan, June 2010

CEDS FY10 Key Program Areas

	National SCADA Test Bed Projects	University Projects	Industry-led Projects
Next-Generation Control Systems	✓	✓	✓
System Vulnerability Assessments	✓		
Integrated Risk Analysis	✓	✓	
Partnership & Outreach	✓	✓	

National SCADA Test Bed (NSTB)

More Than 17 Facilities From 6 National Labs

ARGONNE National Laboratory
- Infrastructure Assurance Center

IDAHO National Laboratory
- Critical Infrastructure Test Range
- SCADA/Control System Test Bed
- Cyber Security Test Bed
- Wireless Test Bed
- Powergrid Test Bed
- Modeling and Simulation Test Bed
- Control Systems Analysis Center

LOS ALAMOS National Laboratory
- Cybersecurity Program

OAK RIDGE National Laboratory
- Cyber Security Program
- Large-Scale Cyber Security and Network Test Bed
- Extreme Measurement Communications Center

PACIFIC NORTHWEST National Laboratory
- Electricity Infrastructure Operations Center
- SCADA Laboratory
- National Visualization and Analytics Center
- Critical Infrastructure Protection Analysis Laboratory

SANDIA National Laboratories
- Center for SCADA Security
- Distributed Energy Technology Laboratory
- Network Laboratory
- Cryptographic Research Facility
- Red Team Facility
- Advanced Information Systems Laboratory

FY10 Industry-Led Projects and Academic Partnerships

Industry-Led Projects

- **Cyber Security Audit and Attack Detection Toolkit—**Digital Bond
- **Hallmark Cryptographic Serial Communication—**Schweitzer Engineering Laboratories
- **Lemnos Interoperable Security—**EnerNex
- **Integrated Security System (ISS)—**Siemens Corporate Research

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

- University of Illinois at Urbana-Champaign
- Dartmouth College
- Cornell University
- University of California at Davis
- Washington State University

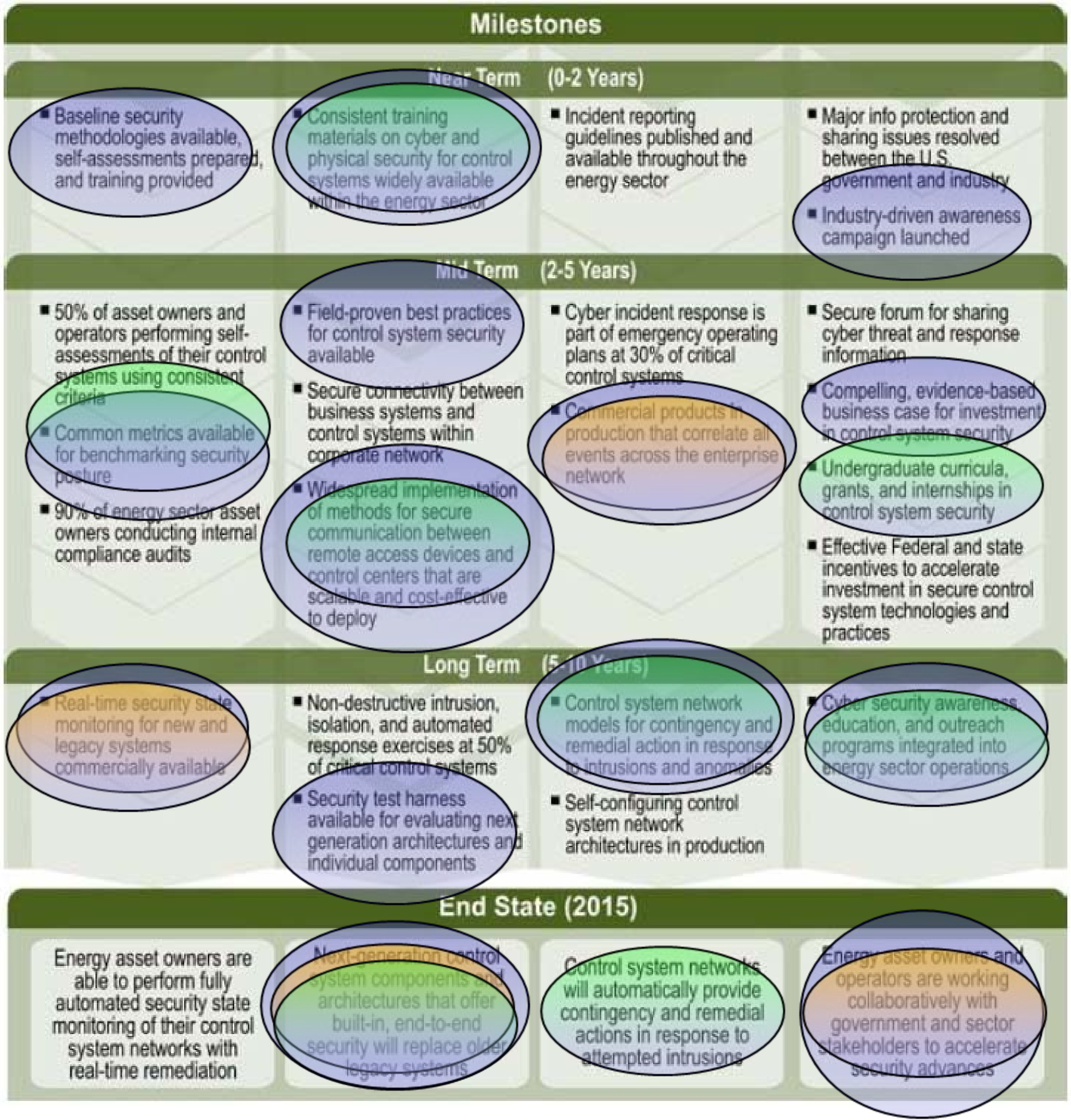
Software Engineering Institute

- Carnegie Mellon University

CEDS Activities Directly Support the *Roadmap*

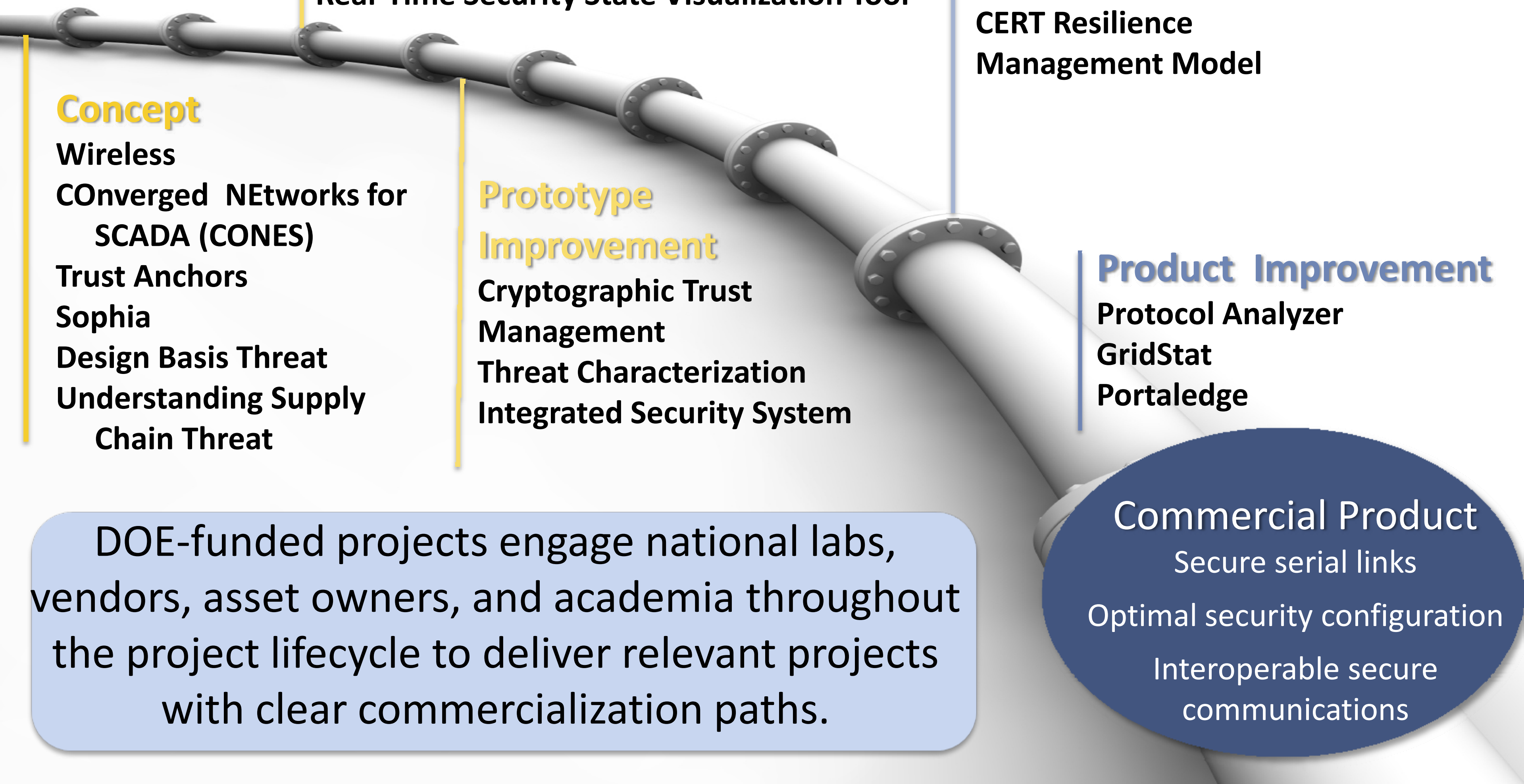
<u>Key Roadmap Strategies</u>

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



Milestones			
Near Term (0-2 Years)			
■ Baseline security methodologies available, self-assessments prepared, and training provided	■ Consistent training materials on cyber and physical security for control systems widely available within the energy sector	■ Incident reporting guidelines published and available throughout the energy sector	■ Major info protection and sharing issues resolved between the U.S. government and industry ■ Industry-driven awareness campaign launched
Mid Term (2-5 Years)			
■ 50% of asset owners and operators performing self-assessments of their control systems using consistent criteria ■ Common metrics available for benchmarking security posture ■ 90% of energy sector asset owners conducting internal compliance audits	■ Field-proven best practices for control system security available ■ Secure connectivity between business systems and control systems within corporate network ■ Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy	■ Cyber incident response is part of emergency operating plans at 30% of critical control systems ■ Commercial products in production that correlate all events across the enterprise network	■ Secure forum for sharing cyber threat and response information ■ Compelling, evidence-based business case for investment in control system security ■ Undergraduate curricula, grants, and internships in control system security ■ Effective Federal and state incentives to accelerate investment in secure control system technologies and practices
Long Term (5-10 Years)			
■ Real-time security state monitoring for new and legacy systems commercially available	■ Non-destructive intrusion, isolation, and automated response exercises at 50% of critical control systems ■ Security test harness available for evaluating next generation architectures and individual components	■ Control system network models for contingency and remedial action in response to intrusions and anomalies ■ Self-configuring control system network architectures in production	■ Cyber security awareness, education, and outreach programs integrated into energy sector operations
End State (2015)			
Energy asset owners are able to perform fully automated security state monitoring of their control system networks with real-time remediation	Next-generation control system components and architectures that offer built-in, end-to-end security will replace older legacy systems	Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions	Energy asset owners and operators are working collaboratively with government and sector stakeholders to accelerate security advances

From Concept to Commercialization: Building a Project Pipeline



Concept

Wireless COnverged NEtworks for SCADA (CONES)

Trust Anchors

Sophia

Design Basis Threat

Understanding Supply Chain Threat

Prototype

Secure Data Transfer

Real-Time Security State Visualization Tool

Prototype Improvement

Cryptographic Trust Management

Threat Characterization

Integrated Security System

Product

CERT Resilience Management Model

Product Improvement

Protocol Analyzer

GridStat

Portaledge

Commercial Product

Secure serial links

Optimal security configuration

Interoperable secure communications

DOE-funded projects engage national labs, vendors, asset owners, and academia throughout the project lifecycle to deliver relevant projects with clear commercialization paths.

CEDS Peer Reviewers

- **David Dunn**
  IESO Ontario
- **Tom Flowers**
  Control Center Solutions
- **Morgan Henrie**
  Alyeska Pipeline/MH Consulting
- **Chris Klemm**
  Cybersecurity Energy Systems
- **Pete Knutsen**
  Dominion Resources Services
- **Scott Mix**
  NERC
- **Dave Norton**
  Entergy
- **Thomas Pearce**
  Public Utilities Commission of Ohio
- **Tracy Rolstad**
  Avista Corporation

Blue indicates Energy Sector Control Systems Working Group member

For more info contact:

Carol Hawk

U.S. Department of Energy

carol.hawk@hq.doe.gov

202-586-3247

www.oe.energy.gov/controlsecurity