U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

NITRD Tailored Trustworthy Spaces Workshop

July 18-20, 2011

Hank Kenchington
Deputy Assistant Secretary R&D
Office of Electricity Delivery and Energy Reliability
Department of Energy

Edinburgh Castle – built around 1140 AD

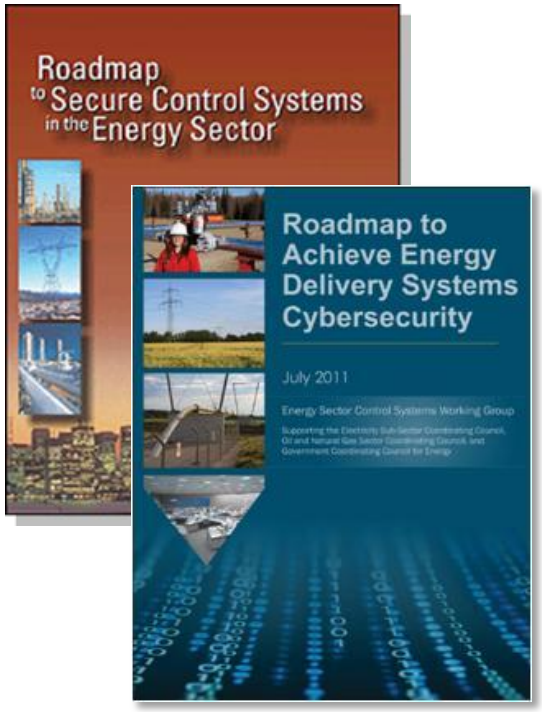
Grid Modernization – national priority

- Grid Modernization – A national priority
- Effective cyber security solutions are essential element to modernizing the nation's electric grid
- Requires effective public-private participation

A smarter, modernized, and expanded grid will be pivotal to the United States' world leadership in a clean energy future.

- A Policy Framework for the 21st Century Grid
June 2011

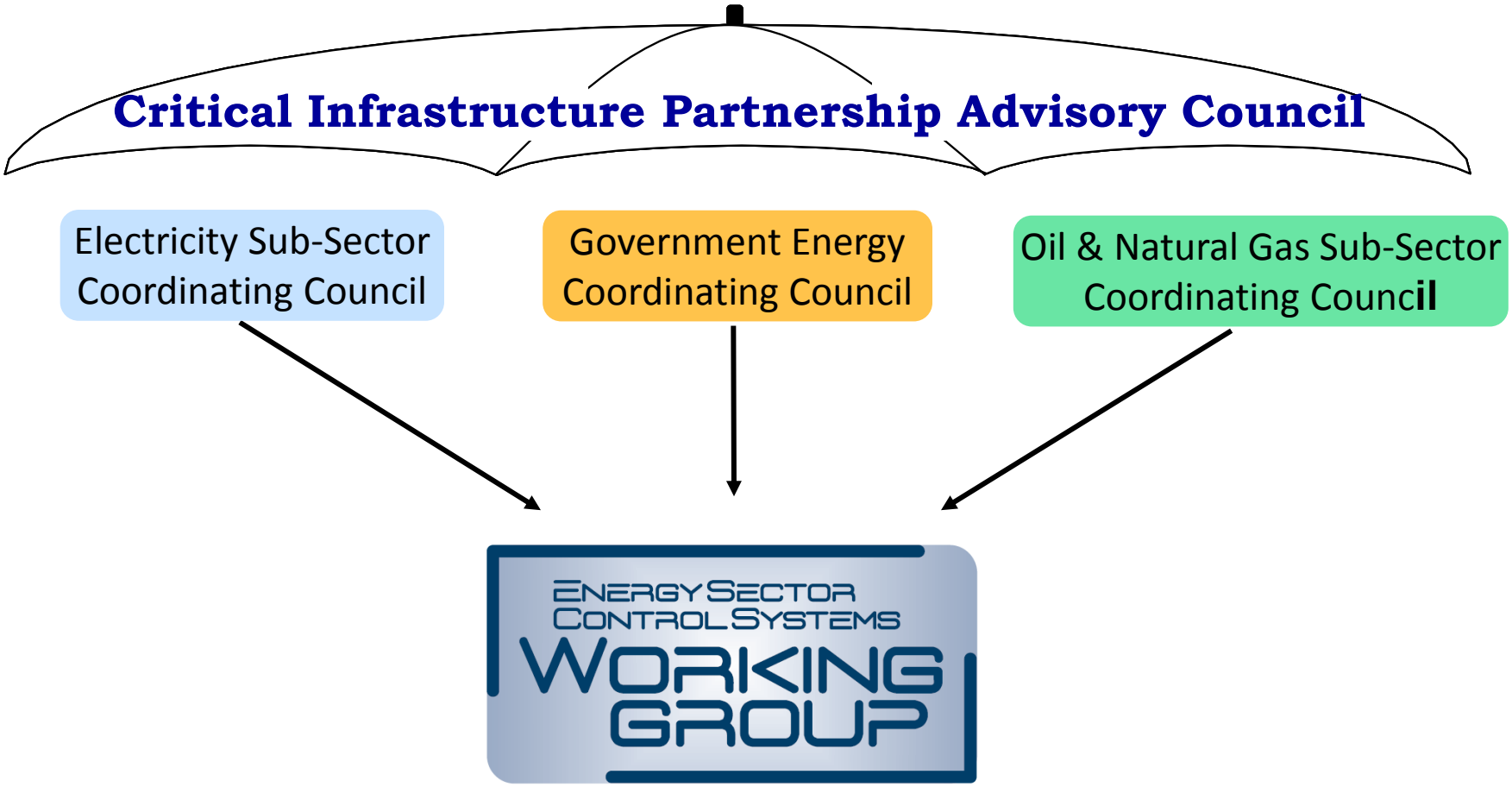
Roadmap – Energy Sector Framework for Public-Private Collaboration



- 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

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

Public-Private Working Group Oversees Roadmap Implementation



Tangible progress has been made to mitigate cyber risks in energy sector since 2006

Measure and Assess Security Posture

- 37 Vulnerability assessments of control systems and components by Idaho National Laboratory
- Bandolier Security Audit Files by Digital Bond enable asset owners to audit/ optimize the security configurations of control systems
- NERC Top Ten Vulnerabilities of Control Systems and Associated Mitigations

Develop and Integrate Protective Measures

- "Hardened" technologies now available and being deployed – secure SCADA communications protocol, SCADA/EMS (ABB, AREVA, Siemens, Telvent, et al)
- Lemnos Interoperable Security project -interoperable configuration profile for creating secure communications channels between various vendor products
- ASAP-SG security profiles for AMI and third-party data access

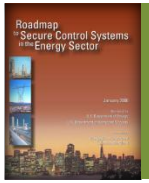
Detect Intrusion and Implement Response Strategies

- ICS-CERT established by DHS to address threats and vulnerabilities
- Over 2300 representatives from energy sector have participated in control systems security training events supported by DoE

Sustain Security Improvements

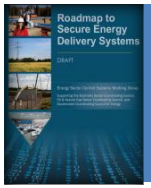
- FBI, DOE, DHS, and ES-ISAC collaborated to quickly provide *actionable guidance* on VPN vulnerability to the electricity industry
- The EnergySec online forum allows stakeholders to share threat and incident information, and communicate and coordinate confidentiality

2011 Roadmap – updated to reflect changing threat and technological landscape



2006 Roadmap

Measure and Assess Security Posture	Energy asset owners are able to perform fully automated security state monitoring of their control system networks with real-time remediation.
Develop and Integrate Protective Measures	Next-generation control system components and architectures that off built-in, end-to-end security will replace older legacy systems
Detect Intrusion and Implement Response Strategies	Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions
Sustain Security Improvements	Energy asset owners and operators are working collaboratively with government and sector stakeholders to accelerate security advances



2011 Roadmap

Build a Culture of Security	Cybersecurity practices are reflective and expected among all energy sector stakeholders
Assess and Monitor Risk	Continuous security state monitoring of all energy deliver system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators
Develop and Implement New Protective Measures to Reduce Risk	Next-generation energy delivery system architectures provide “defense in depth.” and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident
Manage Incidents	Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment
Sustain Security Improvements	Collaboration between industry, academia, and government maintains cybersecurity advances

DOE Strategic Approach to Energy Sector Cybersecurity

Work closely with Federal and State government, and the private sector to:

- Implement ***Roadmap to Achieve Energy Delivery Systems Cybersecurity***
- Identify and fund gaps in infrastructure R&D and testing to accelerate the development and deployment of resilient networks and systems
- Conduct vulnerability research to better understand weaknesses and develop mitigations
- Conduct analysis to assess risks, security posture, and increase ability to mitigate risks
- Encourage “culture of security”
- Provide secure sharing of threat information and facilitate incident response

DOE R&D and Outreach – a portfolio approach to developing and deploying solutions

Research, Development, and Demonstration Activities

Higher Risk, Longer Term Projects
- → Core NSTB Program
- → Academia Projects
- → No Cost Share

Medium Risk, Mid Term Projects
- → National Laboratory Led Projects
- → Lower Cost Share

Lower Risk, Short Term Projects
- → Industry Led Projects
- → Higher Cost Share

Partnering

Path to Commercialization

Training, Education, Standards Development, and Other Outreach Activities

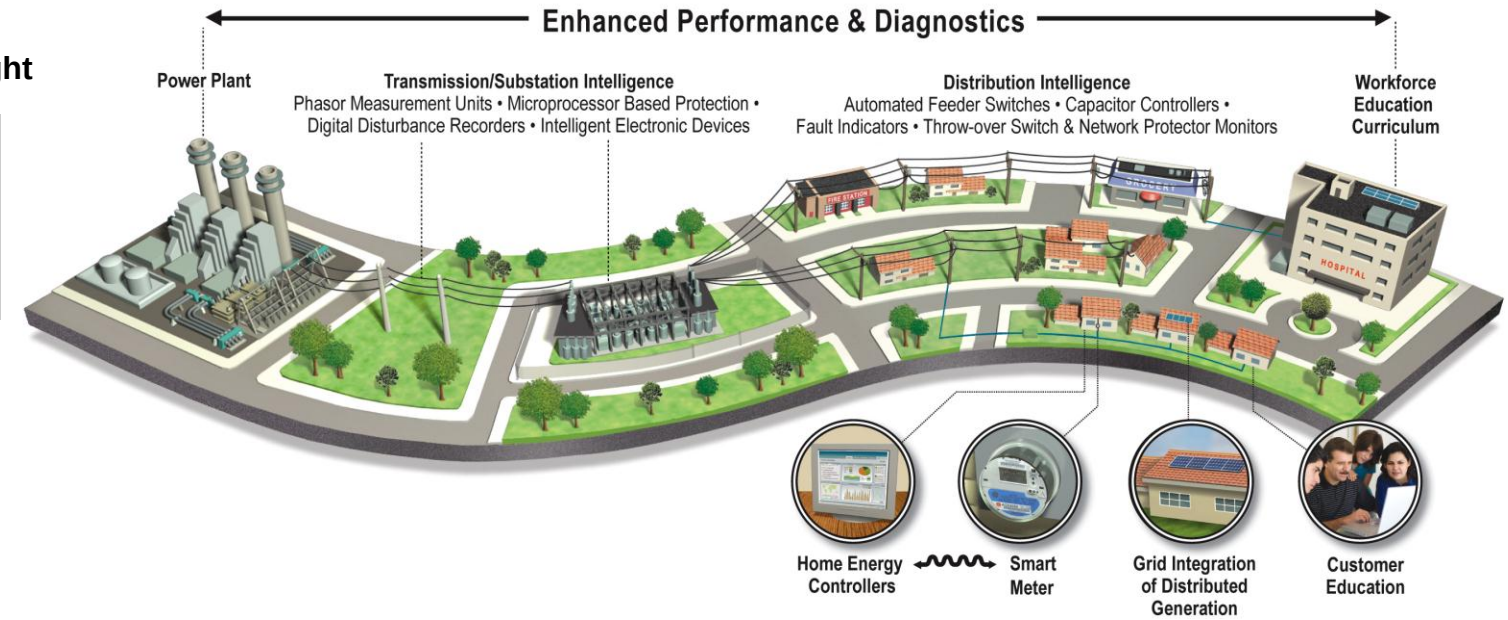
Core NSTB Program
- Argonne National Laboratory
- Idaho National Laboratory
- Oak Ridge National Laboratory
- Los Alamos National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories

Academia Projects (TCIPG)
- Cornell University
- Dartmouth College
- University of California, Davis
- University of Illinois
- Washington State University

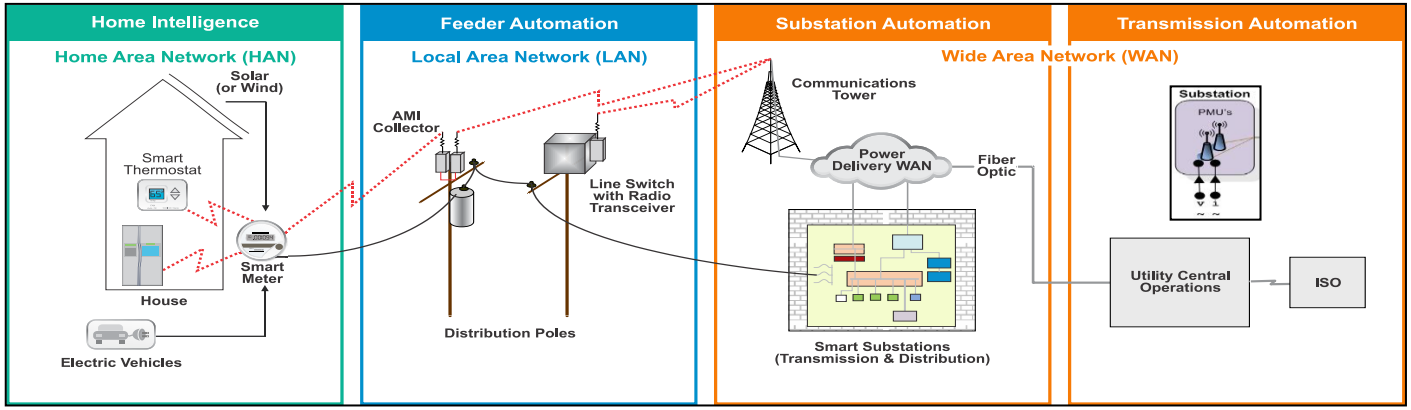
+$9 billion in public/private investments in Smart Grid technologies now being deployed

Grid modernization requires seamless, secure communications across multiple interconnected domains and platforms

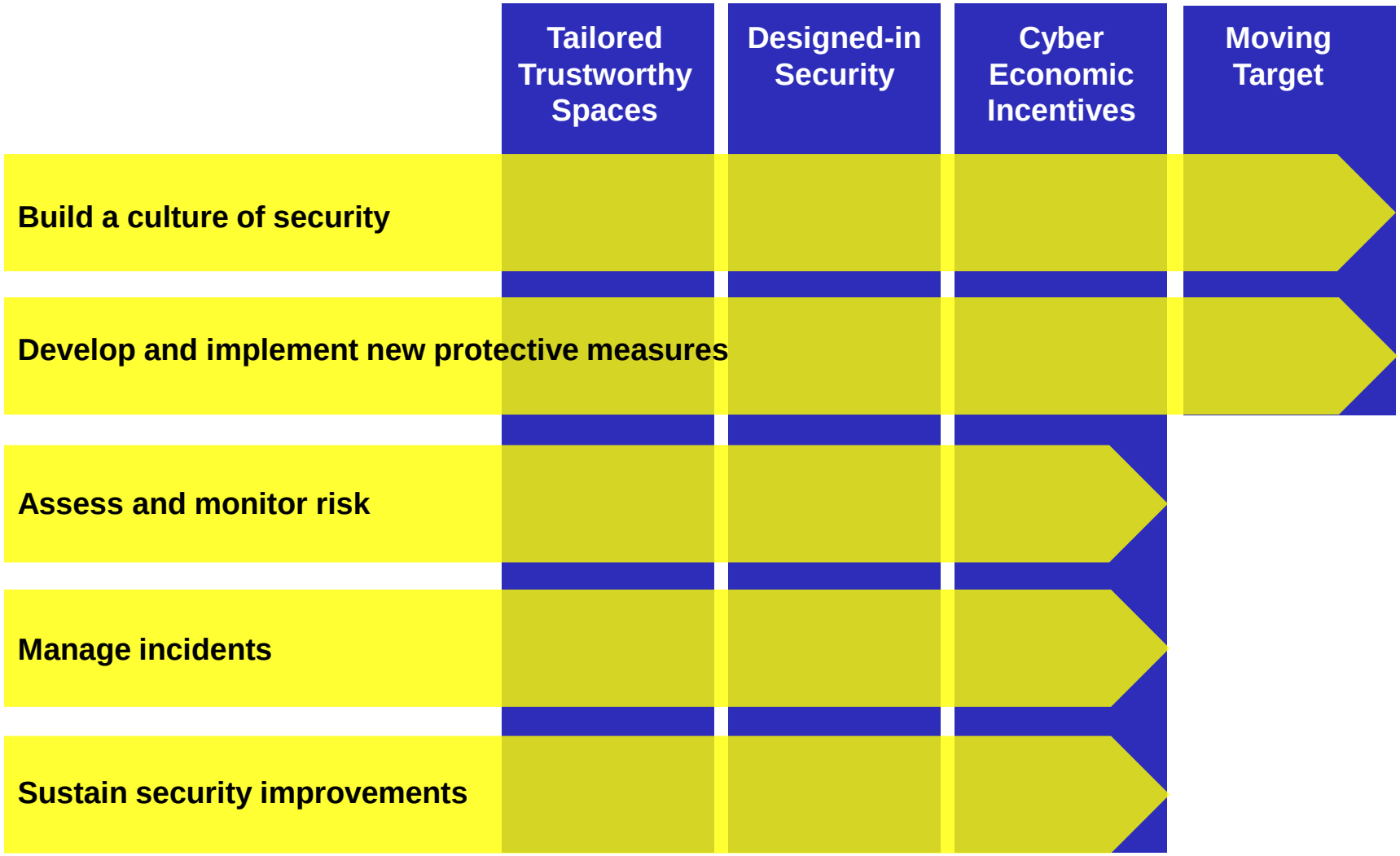
Florida Power and Light



Generic Smart Grid Communications Architectures



NITRD cybersecurity strategies support Energy Roadmap goals



Many Energy Roadmap needs support NITRD “game changing” strategies

Tailored Trustworthy Spaces supports context specific trust decisions

- Develop techniques to provide explicit, managed communications trust
- Develop trusted platform modules and trusted network connections for real-time communications that are nonproprietary

Moving Target provides resilience through agility

- Develop security validation test beds
- Develop tools for secure change management across widely distributed systems

Cyber Economic Incentives provide incentives to good security

- Increase executive understanding of energy delivery cybersecurity issues and risks
- Integrate cybersecurity awareness, education, and outreach programs into energy sector and vendor operations

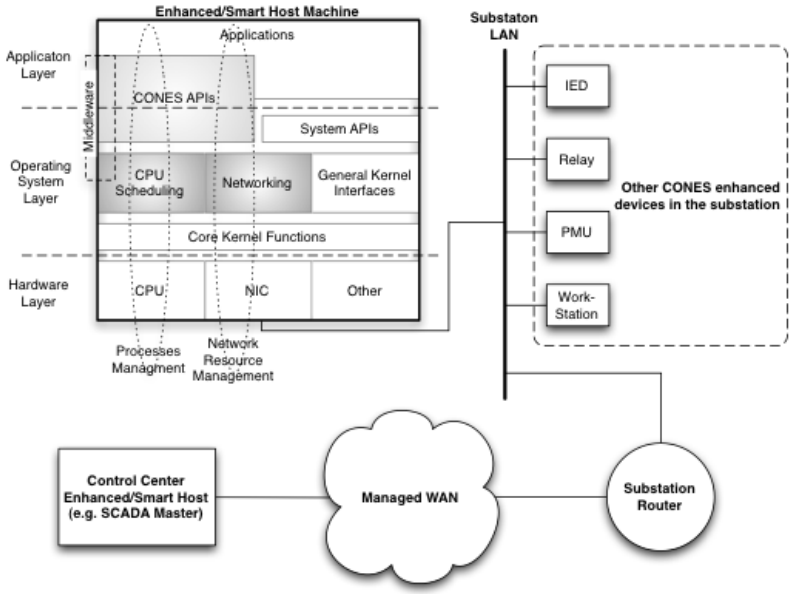
Designed-in Security develop and evolve secure software systems

- Develop scalable built-in security for embedded operating systems
- Adopt agreed upon, available intrinsic data and source integrity in SCADA/EMS protocols to develop control systems that will inherently respond to and defend themselves against internal and external threats

Several DOE efforts utilize Tailored Trustworthy Spaces concepts

- **SIEGate** – a secure information exchange gateway that provides secure communication of data between control centers (Grid Protection Alliance, University of Illinois, PNNL, PJM, AREVA T&D)

- **Secure and real-time communication substrate** - trustworthy cyber infrastructure and technologies for wide-area monitoring and control, and active demand management (TCIPG)
  - Converged Networks for SCADA (CONES) an architecture and platform for maintaining real-time and secure communications for control in a converged network



- **Trust Anchors** – Monitoring and control devices to independently verify systems function, reveal deceptive malicious function, attest to system state, and verify correctness of system tests (SNL)

Conclusions

- Effective cybersecurity solutions are critical to grid modernization
- Cyber threat capabilities are outpacing defenses
- When you can’t win the game – change the game!
- Application of tailored trustworthy spaces concepts in smart grid technologies/applications can help “change the game”
- Game changers are needed TODAY!

Thank you!