TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

# TCIPG OVERVIEW

NOVEMBER 12, 2014


## BILL SANDERS AND PETE SAUER

ON BEHALF OF THE ENTIRE TCIPG TEAM





FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

# OUTLINE

- Welcome and Introduction
- TCIPG Overview and Vision
- Project Structure
  - Clusters and threads
  - Crosscutting activities
  - Industry involvement
- TCIPG Legacy
- Summary

# WELCOME TO THE TCIPG 2014 INDUSTRY WORKSHOP

- Who is here?
  - TCIPG researchers and students
  - Representatives of industry: utilities, vendors, national labs, ...
  - Our sponsors and external advisory board
- Why have an annual industry workshop?
  - For TCIPG and sponsors:
    - to have impact
    - to communicate our results
    - to get feedback from industry
    - to help choose our research well
  - For industry:
    - to discover and explore TCIPG research
    - to influence future directions
    - to form productive collaborations that can profitably shape the evolving Smart Grid

# WELCOME TO THE TCIPG 2014 INDUSTRY WORKSHOP (CONT.)

- What happens during the Industry Workshop?
  - Sharing TCIPG research results and directions
  - Listening and learning about industry's perspective
  - Stimulating interaction between industry and academics in power and cyber
- Purpose of this talk?
  - Introduce TCIPG – provide context for navigating the next day and a half: who we are, what we do, and why we do it
  - Highlight progress on TCIPG activities
  - Document the TCIPG legacy
  - Invite your active participation in workshop and in the longer term as well

# TCIPG OVERVIEW

- **Objectives**
  - Identify and address critical security and resiliency needs at the cyber-physical junction in the evolving power grid
  - Engage industry (utility, control system vendors, technology providers)
  - Research excellence
  - Education
- **Technical Approach**
  - Identify and take on important & hard problems
  - Unique balance of long view of grid cyber security, with emphasis on practical solutions
  - Work to get solutions adopted

- **Schedule:** Sept 30, 2009 – Aug. 30, 2015
- **Level of Effort:** $15M DOE/DHS, $3M University Cost Share
- **Performers:** University of Illinois at Urbana-Champaign, Dartmouth College, University of California Davis, Washington State University
- **Partners:** 9-Member External Advisory Board (EAB) from utility and industry, as well as large Industry Interaction Board
- **Team**: 20+ Faculty, 15+ Technical Staff, 40+ Students and 3 Admin Staff contributed to the project in FY 2014

# THE CHALLENGE: PROVIDING TRUSTWORTHY SMART GRID OPERATION IN POSSIBLY HOSTILE ENVIRONMENTS

- Trustworthy
  - A system which does what is supposed to do, and nothing else
  - Availability, security, safety, …
- Hostile Environment
  - Accidental failures
  - Design flaws
  - Malicious attacks
- Cyber Physical
  - Must make the whole system trustworthy. This includes both physical components, cyber components, and their interaction.

# TCIPG VISION AND RESEARCH FOCUS

**Vision**: Create technologies which improve the design of a resilient and trustworthy cyber infrastructure for the current and future power grid, that is, a power grid that continues to operate through attacks

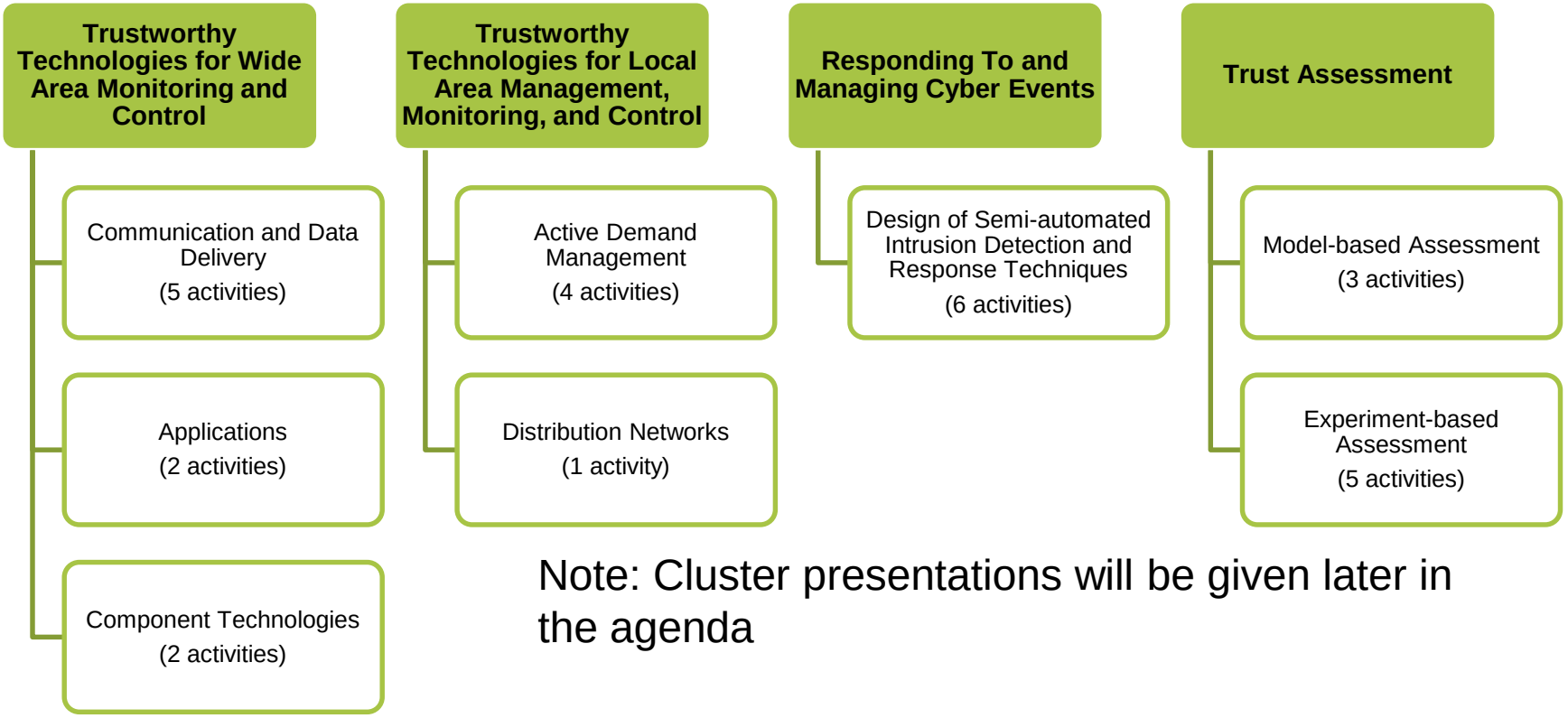
**Research focus:**

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications and architectures
- Quantifying security and resilience

# PROJECT STRUCTURE

- Site leads coordinate activities at partner schools
  - Dartmouth College (Sean Smith)
  - University of California Davis (Anna Scaglione)
  - Washington State University (Carl Hauser)
- TCIPG has stressed industry interaction from inception of research initiatives
  - Pete Sauer, Industry Interaction Lead, co-PI
  - External Advisory Board (small) and Industry Interaction Board (more than 500 members; all industry participants welcome)
- TCIPG is organized into clusters of research threads, supporting multiple activities
- Weekly grad-student-led reading group and all-hands meetings

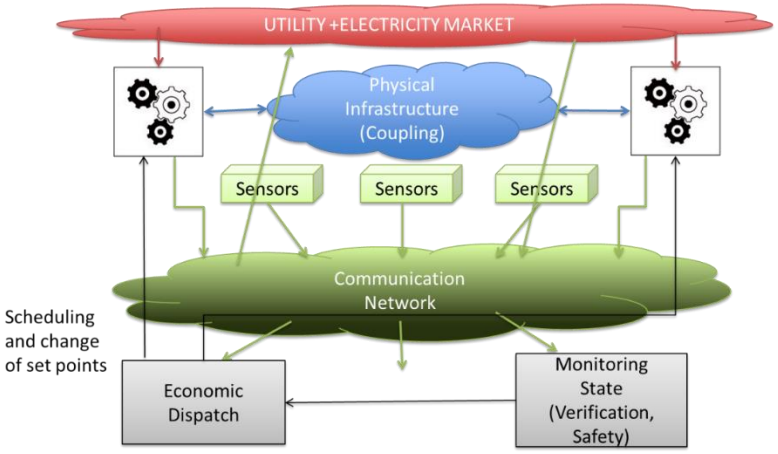
# TCIPG TECHNICAL CLUSTERS AND THREADS

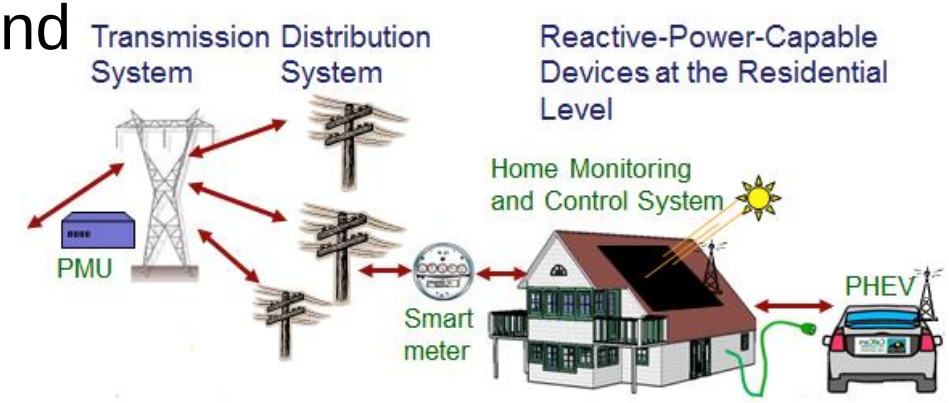



Note: Cluster presentations will be given later in the agenda

# CLUSTER THEMES (1 OF 2)
# (MORE DETAIL IN CLUSTER PRESENTATIONS)

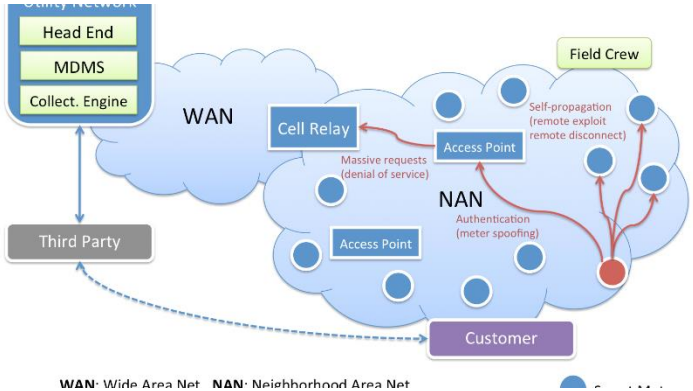
- Wide Area: Cyber infrastructure to support security and resiliency of wide area applications (primarily transmission system)
- Local Area: Meet the challenge of renewable integration, distribution automation, and customer involvement

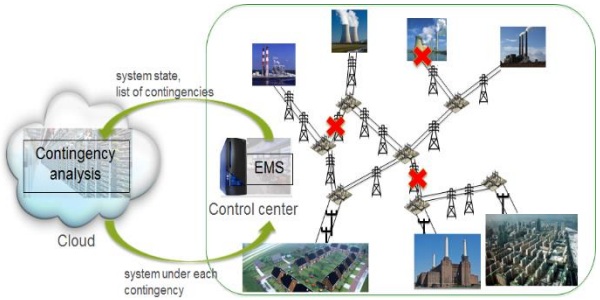


# CLUSTER THEMES (2 OF 2)
# (MORE DETAIL IN CLUSTER PRESENTATIONS)

- Cyber Events: Detect and respond to cyber events. Restore systems to a state more secure than before the event
- Trust Assessment: Methods and tools that use simulation, modeling, and experimentation to support quantitative trust assessment



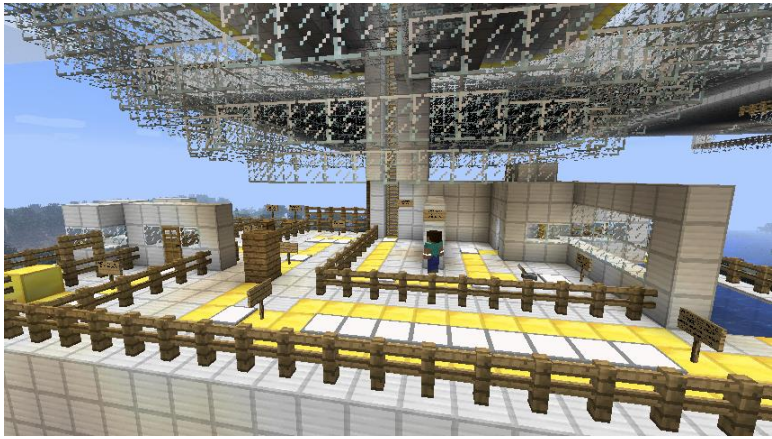



# CROSSCUTTING EFFORTS (MORE DETAIL IN LATER PRESENTATIONS)

- Education and Engagement
  - K-12
  - Outreach and Workforce Development
  - Consumer Education and Public Information
- Testbed
  - HW and SW Integration to support research
  - Testbed federation
  - Utility testbed interactions
- Industry Interaction and Technology Transition

# TCIPG EDUCATION, OUTREACH, AND TRAINING

- Education of professionals versed in cyber and power is the core mission
  - Degree programs
  - Internships
  - Continuing Education
  - TCIPG Reading Group
- K-12 education and outreach
  - Power and Energy applets continue to evolve, and are integrated into curriculum projects nationwide
  - TCIPG Minecraft World
  - Encouraging interest in STEM education and careers
  - Teachers, parents learn too!
- Assisting community colleges in smart grid curriculum development under IGEN Consortium



# TRAINING: TCIPG SUMMER SCHOOL

- Offered alternate years in Chicago area
- Last session was June 2013
  - Weeklong and intensive
  - 173 participants
  - Geared toward graduate students, utility practitioners, and consultants
  - 20 technical sessions, presented by leading subject matter experts
  - “Deep Dive” on selected topics
  - Hands-on SCADA security assessment training

**2015 Summer School**
**June 15-19, 2015**
**Reception: June 14**

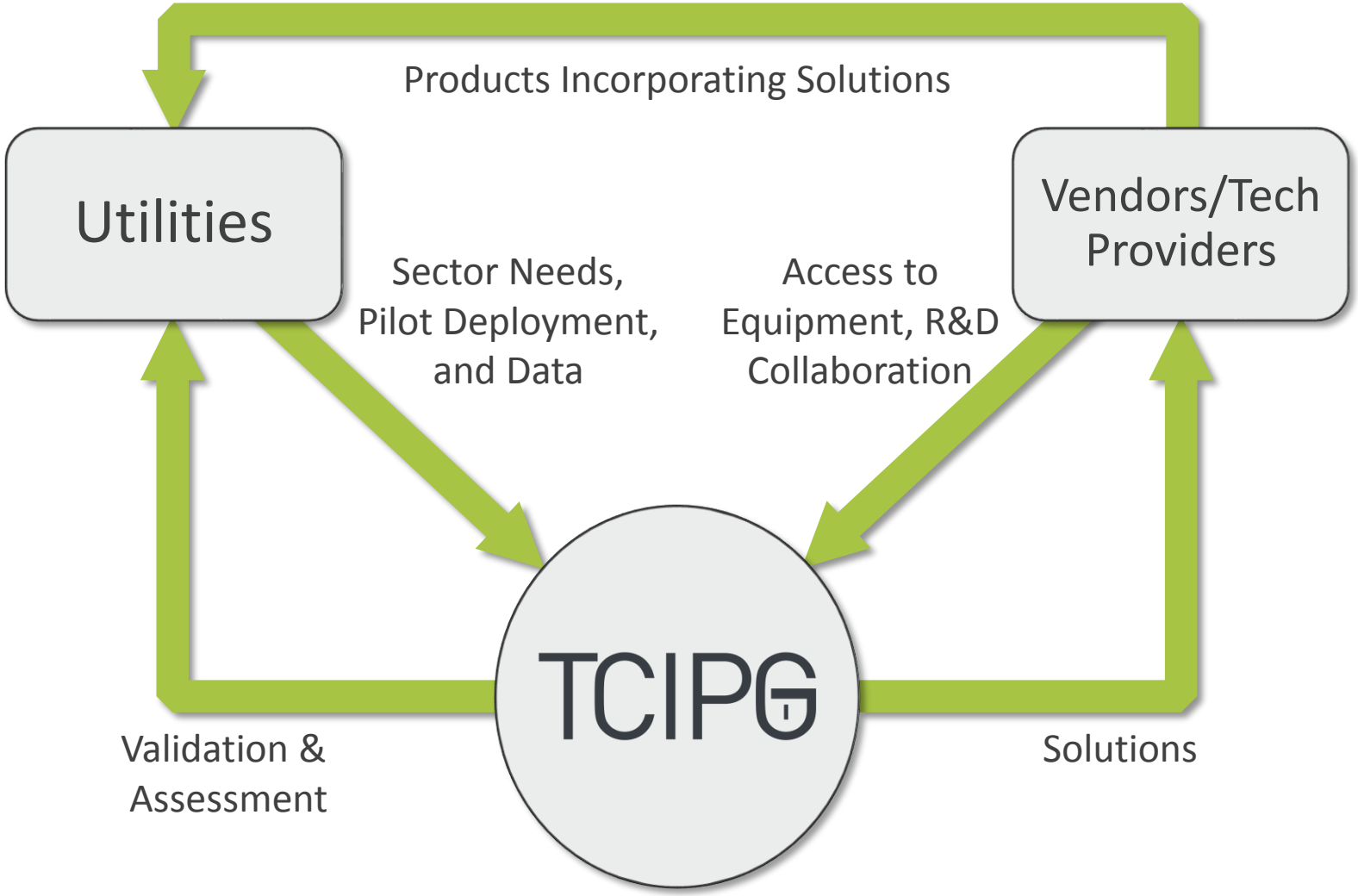
# TESTBEDS

- Enabling advanced research for smart grid efforts throughout the world
- Helping to define national direction for cyber physical testbeds and the research that is conducted in them
- Illinois
  - Primary TCIPG Testbed
  - Illinois Center for a Smarter Electric Grid
- Washington State University
  - Energy Systems Innovation Center
  - Smart Grid Demonstration and Investigation Lab
- Dartmouth
  - ZigBee and other misc. equipment
- UC-Davis
  - Cyber physical SCADA testbed

# TCIPG INDUSTRY INTERACTION

- Engage with industry early and deeply
- Work on problems where fundamentals can make difference *and* whose solution will be high impact to industry
- Supplement grad student/faculty researchers with professional programmers and power and security engineers to insure “industrial quality” of developed product
- Strategically decide the best method for transfer. Options include: open source, incorporation in existing product, new product, or start-up company
- Employ in-house utility expert to help focus research ideas and find appropriate tech transfer targets
- During testing, engage deeply with a small number of users first, and then expand the circle as concept/product develops
- Provide technology transfer support to researchers

# TCIPG AS CATALYST FOR ACCELERATING INDUSTRY INNOVATION



# TCIPG IMPACT

# TCIPG SCHOLARLY IMPACT*

- Degrees**
  - 22 Doctoral
  - 25 Master
  - 20 Bachelor
- Publications
  - 240+ publications in refereed journals/conference proceedings, books/book chapters, articles, technical reports, dissertations, and theses.
- Presentations
  - 600+ presentations at conferences, workshops, symposia or for various industry, academic, research, or regulatory groups.

***For the period January 1, 2010 thru September 30, 2014. **Awarded to students participating in the TCIPG project.**

# TCIPG INDUSTRY IMPACT*

- Collaboration, internship arrangements, data sharing, or pilot deployments with Ameren, American Transmission Co., Commonwealth Edison, First Energy, Southern Cal Edison
- Collaboration, research, or internship arrangements, or other agreements with SEL, ABB, Honeywell, Fujitsu, Qualcomm
- Collaboration with LANL (quantum crypto) and LBL (SCADA security, TCIPG-UC Davis), EPRI
- NERC evaluation of NP View
- Over 130 organizations have attended TCIPG Events

***For the period January 1, 2010 thru June 30, 2014.**

# COLLABORATION EXAMPLES

- Utilities
  - AMI Security pilot with First Energy
  - Ameren collaboration on DNP3 IDS
  - ATC collaboration on PMU data quality and analysis
  - Engagement with EPRI on various fronts
  - NetAPT (a.k.a NP-View) as NERC CIPS pre-audit and audit tool
  - SECURE, open communication gateway with Grid Protection Alliance (GPA)
- Industry
  - Schweitzer incorporating TCIPG embedded system security approach in their products
    - Schweitzer is a major donor of TCIPG testbed equipment
  - Honeywell collaboration on Role Based Access Control (RBAC) project in automation systems
- National Labs
  - Demonstrated Los Alamos NL quantum cryptography in the TCIPG testbed, securing PMU communications using a hardware-in-the-loop experiment
  - NetAPT integrated with Idaho NL Sophia security visualization tool
  - SCADA security collaboration, LBNL and TCIPG-UC Davis
- International
  - “In-Depth Defense of SCADA and Control Systems”, UI and University of Twente (NL), facilitated by DHS S&T and Netherlands Organization for Scientific Research (NWO). Kicked off June 2014.

# TRANSITION EXAMPLES

- Startups: Network Perception and River Loop Security
- XUTools structured text analyzer, useful for, e.g., change detection in device configurations
- Open source transition of hardware IDS platform and tools for security assessment of wireless networks and SECURE open communication gateway
- Open source SCADA protocol parsers now part of the BRO framework

# PATENTS (FILED AND GRANTED)

- NetAPT technologies
- GridStat technology involving distributed key storage
- Secure Inter-chip Communication System
- Hardware Intrusion Detection System Using Resistive-Capacitive Circuit
- Smart Meter Research Platform
- Robust and Secure Timing Device Based on Multiple Cooperative GNSS Receivers

# SMART GRID CYBER SECURITY CURRICULUM

- A modular, phased learning platform
  - Diverse topic areas spiraling deeper into topic areas of interest (tracks)
  - Lecture material, exercise environment, and hands-on exercises
- Fully open and available
  - Material is widely usable and different experts can easily contribute new content and revise existing content as the landscape changes
  - Made to be accessible to anyone, including CEOs, engineers, and office staff while taking a project-based, hands-on active-learning approach to reinforce the subject matter
- Target BETA: Nov 2014. Official release: Sept 2015.

# SUMMARY

- TCIPG is addressing a complex, multifaceted mission
- TCIPG is a world-leading research center, but uniquely positioned with relationships to industry
  - Identifying and taking on important hard problems
  - Uniquely balancing of long view of grid cyber security, with emphasis on practical solutions
  - Working to get solutions adopted through industry partnerships, startups, and open source
- TCIPG exemplifies excellence in research, education, and impact
- For more information: www.tcipg.org