# National Cybersecurity Center of Excellence (NCCoE)
# Energy Sector

*Energy Provider Community of Interest*

25 April 2017

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Agenda

- NCCoE Energy Sector Planned Activities
- Status of Energy Sector (and related) Projects
- Guest Speaker:  Peter Tseronis, CEO, Dots and Bridges LLC
- EPC Open Discussion / Comments / Questions

# NCCOE ENERGY SECTOR PLANNED ACTIVITIES

- Second Annual Intelligence and Nationals Security Forum 04/20/2017, Tyson's Corner, VA

- American Council for Technology (ACT) and Industry Advisory Council (IAC), Cybersecurity Community of Interest Monthly Meeting, 04/28/2017, Washington, DC

# PROJECT PHASES

Supply Chain – we are here

Manufacturing BAD – we are here

IdAM and Situational Awareness – we are here

**Pre-Process**
We strategically identify, select, and prioritize projects that align with our mission.

**P1: Concept Analysis**
We partner with industry to define, validate, and build business cases for the most challenging cybersecurity issues.

**P2: Develop Use Case**
Using a collaborative method with industry partners, we develop a full Use Case that outlines a plan for tackling the issue.

**P3: Form Build Team**
We unite industry partners and technology companies to build a qualified team to execute the Use Case.

**P4: Design & Build**
The Use Case team plans, designs, and builds the system in a lab environment and documents it in the Practice Guide.

**P5: Integrate & Test**
The team test the system and make refinements as necessary. The system may be validated by our partners. The final solution system is documented in the Practice Guide.

**P6: Publish & Adopt**
We, alongside our partners, publish, publicize and demonstrate the Practice Guide. This solution provides a reference architecture that may be implemented in whole or in part.

- **Situational Awareness SP 1800-7 (a,b,c)**
  - Released public draft - 02/16/2017
  - Comment period closed- 04/17/2017
  - https://nccoe.nist.gov/projects/use_cases/situational_awareness

- **NCCoE Supply Chain (SC) Sub Working Group (SWG)**
  - Drafted Use Case Proposal that incorporates several elements of ideas generated by SWG
  - Presented to NCCoE Management for approval and/or modifications – 04/18/2017

# ENERGY SECTOR PROJECT STATUS

- **Cybersecurity for Manufacturing**
  - Behavioral Anomaly Detection (BAD)
  - Federal Register Notice - 03/23/2017
  - Collaborator selection process underway
  - https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems

- **Identity and Access Management SP 1800-2 (a,b,c)**
  - Draft released - 08/2015
  - Projected final document release – Spring 2017
  - https://nccoe.nist.gov/projects/use_cases/idam

# GUEST SPEAKER

- Peter Tseronis, Founder and CEO, Dots And Bridges LLC
  Former CTO of the US Department of Energy

  "*Convergence of IOT, Cyber and Advanced Analytics in the Energy Sector* "

- Questions/comments

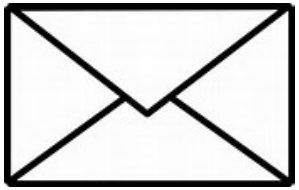
# CONTACT US

301-975-0200

http://nccoe.nist.gov/forums/energy

energy_nccoe@nist.gov

9700 Great Seneca Hwy,
Rockville, MD 20850



100 Bureau Drive, Mail Stop 2002,
Gaithersburg, MD 20899

***Thank You***

## VISION

### ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

## MISSION

### ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

## GOAL 1

### PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

## GOAL 2

### INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

## GOAL 3

### ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

## NIST ITL

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships
and experience.

## PARTNERSHIPS

Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.



## NIST CYBERSECURITY THOUGHT LEADERSHIP

- Cryptography
- Identity management
- Key management
- Risk management
- Secure virtualization
- Software assurance
- Security automation
- Security for cloud and mobility
- Hardware roots of trust
- Vulnerability management
- Secure networking
- Usability and security

# STAKEHOLDERS

## SPONSORS

Advise and facilitate the center's strategy

- White House
- National Institute of Standards and Technology
- U.S. Department of Commerce
- U.S. Congress
- Montgomery County
- State of Maryland

## TEAM MEMBERS

Collaborate to build real-world cybersecurity capabilities for end users

**Sponsored by NIST, the National Cybersecurity Federally Funded Research & Development Center (FFRDC) is operated by the MITRE Corporation*

- NCCoE
- National Cybersecurity FFRDC*
- Tech firms
- Industry
- Academia
- Government
- Project managers
- Project-specific collaborators
- National Cybersecurity Excellence Partners (NCEP)

## END USERS

Work with center on use cases to address cybersecurity challenges

- Business sectors
- Individuals
- Academia
- Government
- Cybersecurity IT community
- Systems integrators

# ENGAGEMENT & BUSINESS MODEL

| | |
|---|---|
|  DEFINE + ARTICULATE<br>Describe the business problem | Define business problems and project descriptions, refine into a specific use case |
|  ORGANIZE + ENGAGE<br>Partner with innovators | Collaborate with partners from industry, government, academia and the IT community on reference design |
|  IMPLEMENT + TEST<br>Build a usable reference design | Practical, usable, repeatable reference design that addresses the business problem |
|  TRANSFER + LEARN<br>Guide users to stronger cybersecurity | Set of all material necessary to implement and easily adopt the reference design |

## Cybersecurity solutions that are:


based on standards and best practices


usable, repeatable and can be adopted rapidly


modular, end-to-end and commercially available


developed using open and transparent processes


matched to specific business needs and bridge technology gaps

## The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

## Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)