

National Cybersecurity Center of Excellence (NCCoE) Energy Sector

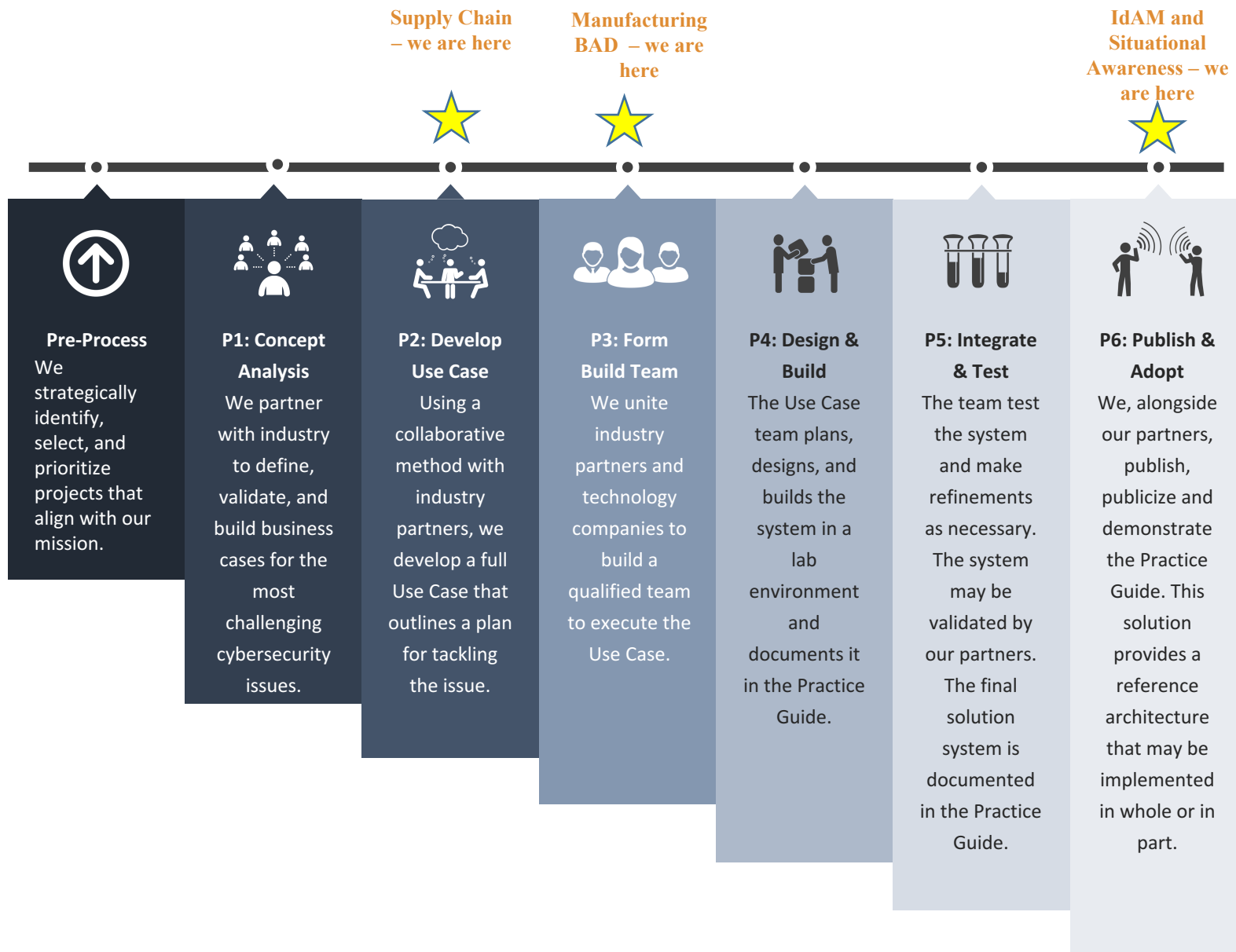
Energy Provider Community of Interest

28 March 2017

Agenda

- NCCoE Energy Sector Planned Activities
- Status of Energy Sector (and related) Projects
- Supply Chain Use Case Proposal
- EPC Open Discussion / Comments / Questions

- OSIssoft Annual User Conference, 03/20/17 - 03/23/17
San Francisco, CA
- 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



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

- **NCCoE Supply Chain (SC) Sub Working Group (SWG)**
 - Last call held on 02/24/2017
 - Drafted Use Case Proposal that incorporates several elements of ideas generated by SWG
 - SWG Action – provide comments by 04/07
 - Present to NCCoE Management in April for approval

- **Cybersecurity for Manufacturing**

- Behavioral Anomaly Detection (BAD)
- Final project description (PD) – 03/10/2017
- Federal Register Notice - 03/2017
- https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems

- **Identity and Access Management SP 1800-2 (a,b,c)**

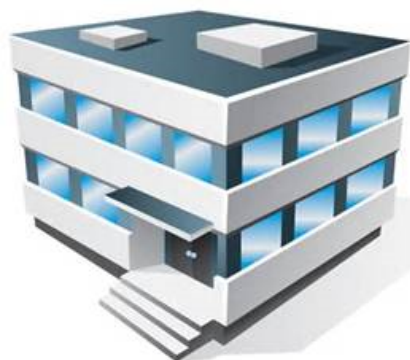
- Draft released - 08/2015
- Projected final document release – Spring 2017
- https://nccoe.nist.gov/projects/use_cases/idam

- Questions/comments





301-975-0200

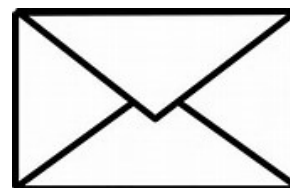


9700 Great Seneca Hwy,
Rockville, MD 20850

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



energy_nccoe@nist.gov



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

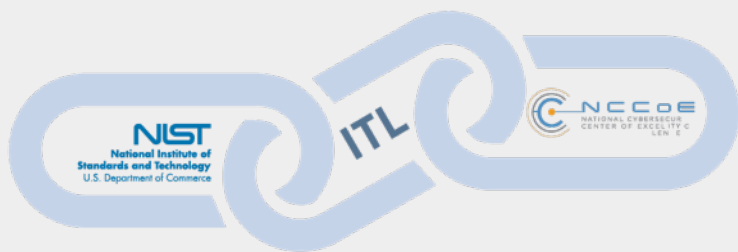
INCREASE RATE OF ADOPTION

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

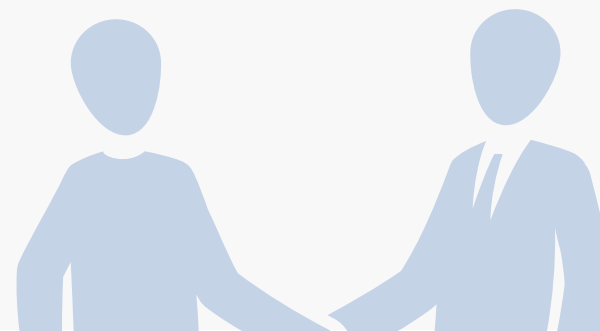


NIST ITL

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



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



Academia



Cybersecurity IT community



Individuals



Government



Systems integrators



DEFINE + ARTICULATE
Describe the business problem

Define business problems and project descriptions, refine into a specific use case



ORGANIZE + ENGAGE
Partner with innovators

Collaborate with partners from industry, government, academia and the IT community on reference design



IMPLEMENT + TEST
Build a usable reference design

Practical, usable, repeatable reference design that addresses the business problem



TRANSFER + LEARN
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)