

National Cybersecurity Center of Excellence (NCCoE) Energy Sector

Energy Provider Community of Interest

18 July 2017

Agenda

- NCCoE Energy Sector Planned Activities
- Status of Energy Sector Projects
- Manufacturing Update (New COI)
- Guest Speaker: PDV Wireless
- EPC Open Discussion / Comments / Questions

- **GridSecCon 2017**, October 17-20, St. Paul, MN
Abstract Submitted: *Convergence of Cybersecurity Situational Awareness Capabilities for the Energy Sector*
Proposed Panelists: NCCoE Energy Sector Team, UMd, PNNL, Dots and Bridges, LLC
- **RSA Charge 2017**, October 17-19, Dallas, TX
SP-1800-7: Energy Sector Situational Awareness Practice Guide

■ **Energy Sector Asset Management (ESAM)**

- Focus on asset management capability for Energy Sector
- Will give strong consideration to remote and geographically dispersed assets
- Business Case Phase I: approved
- Into Business Case Phase II approval process

■ **Situational Awareness SP 1800-7 (a,b,c)**

- Released public draft - 02/16/2017
 - Comment period closed- 04/17/2017
 - Final draft expected Fall / 2017
- https://nccoe.nist.gov/projects/use_cases/situational_awareness



Manufacturing Behavioral Anomaly Detection Use Case :

- <https://nccoe.nist.gov/sites/default/files/library/project-descriptions/mf-ics-1-project-description-final.pdf>
- Build Team Kickoff: 07/06/2015
- Projected Draft Practice Guide Release Date: 02/2018
- Request sent to Energy COI to join Mfg. COI.

➤ **NCCoE Manufacturing BAD Build Team (Final)**

- ❑ Cyber-X
- ❑ GuardX
- ❑ OSIsoft
- ❑ SecureNok
- ❑ Security Matters
- ❑ Ultra-3eTi

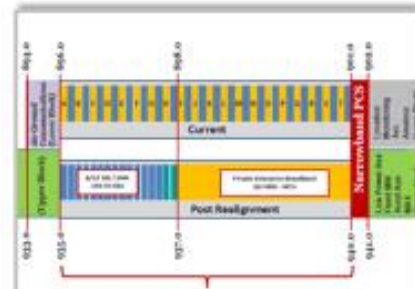
pdvWIRELESS

**Presented by Alice Moy-Gonzalez
Director of Strategic Development**

pdvWIRELESS Overview



Founded in 2004- Push-to-Talk over mobile application



2014- pdvWIRELESS acquires the largest nationwide 900 MHz spectrum



2014-15 Raised \$300 MM in equity funding and listed on NASDAQ



2017 +- Wideband and migration to Broadband for CI

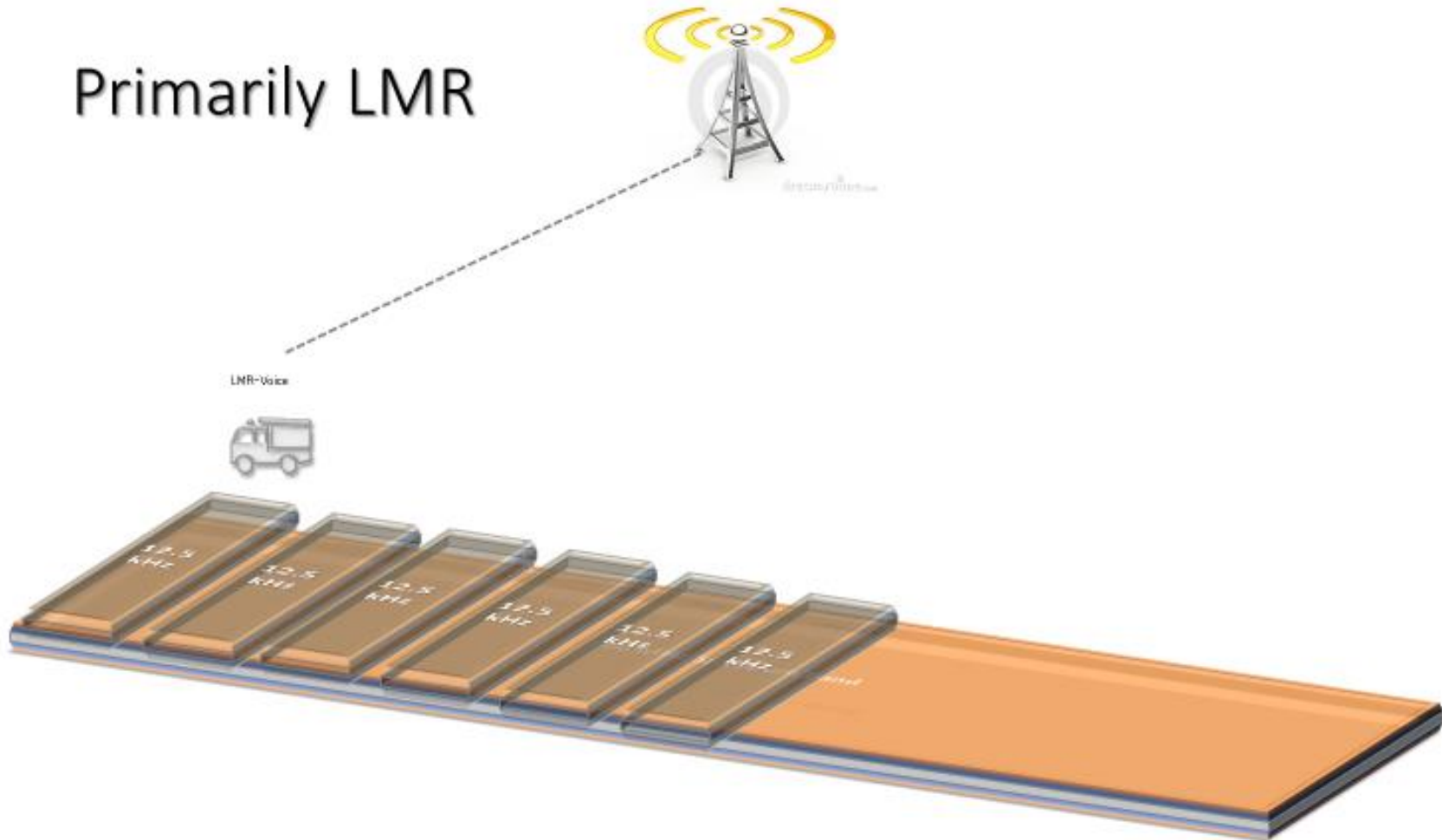
Joint Proposal

- Modernize the 900MHz band
 - to enable innovative use cases -and-
 - the coexistence of incumbents
- Provide flexible use of low band spectrum
 - to enable private enterprise networks,
 - including the potential for priority access to broadband for Critical Infrastructure
 - For LTE, IoT, LPWA, and other technologies

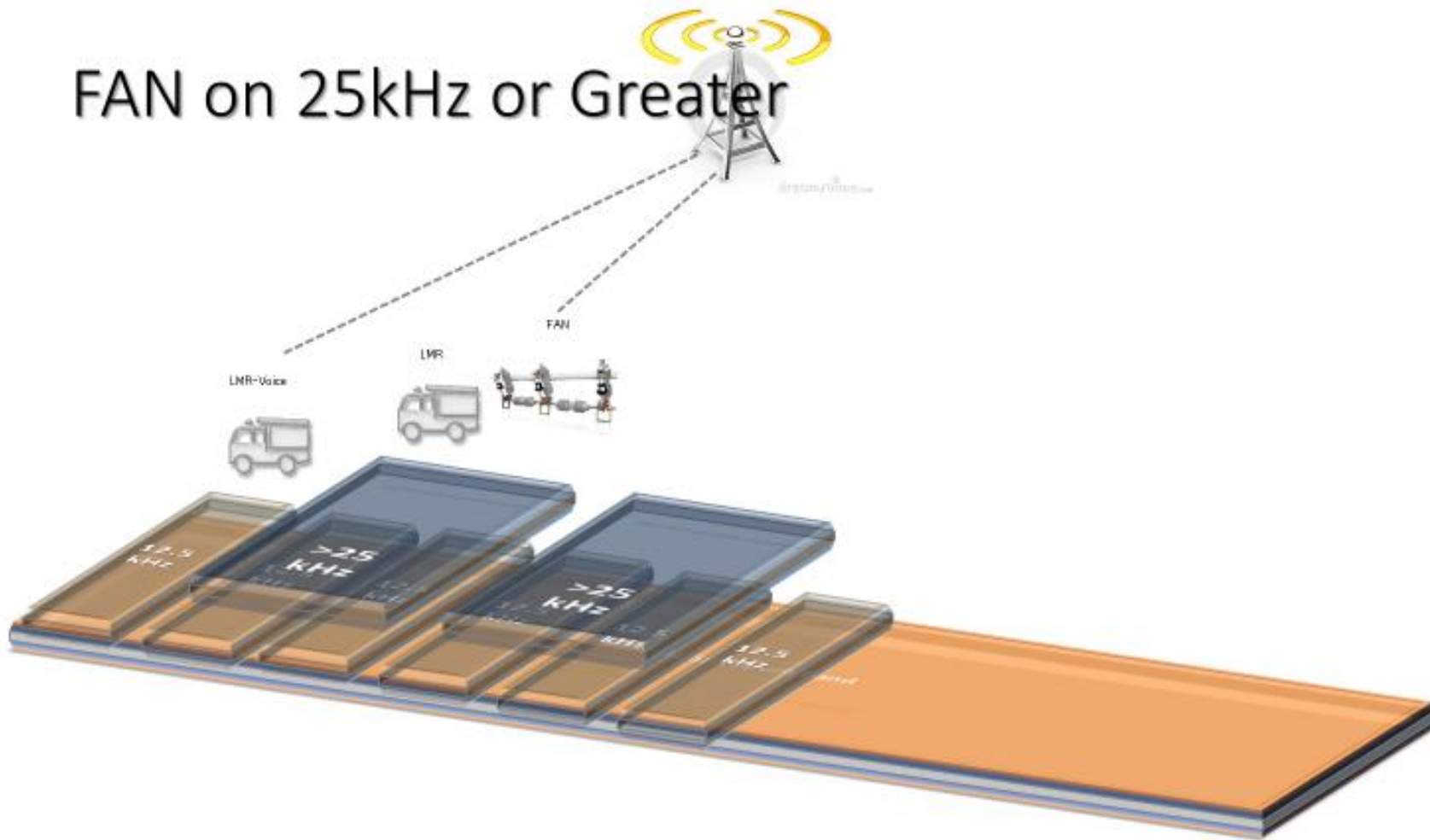
Nationwide Landscape



Primarily LMR

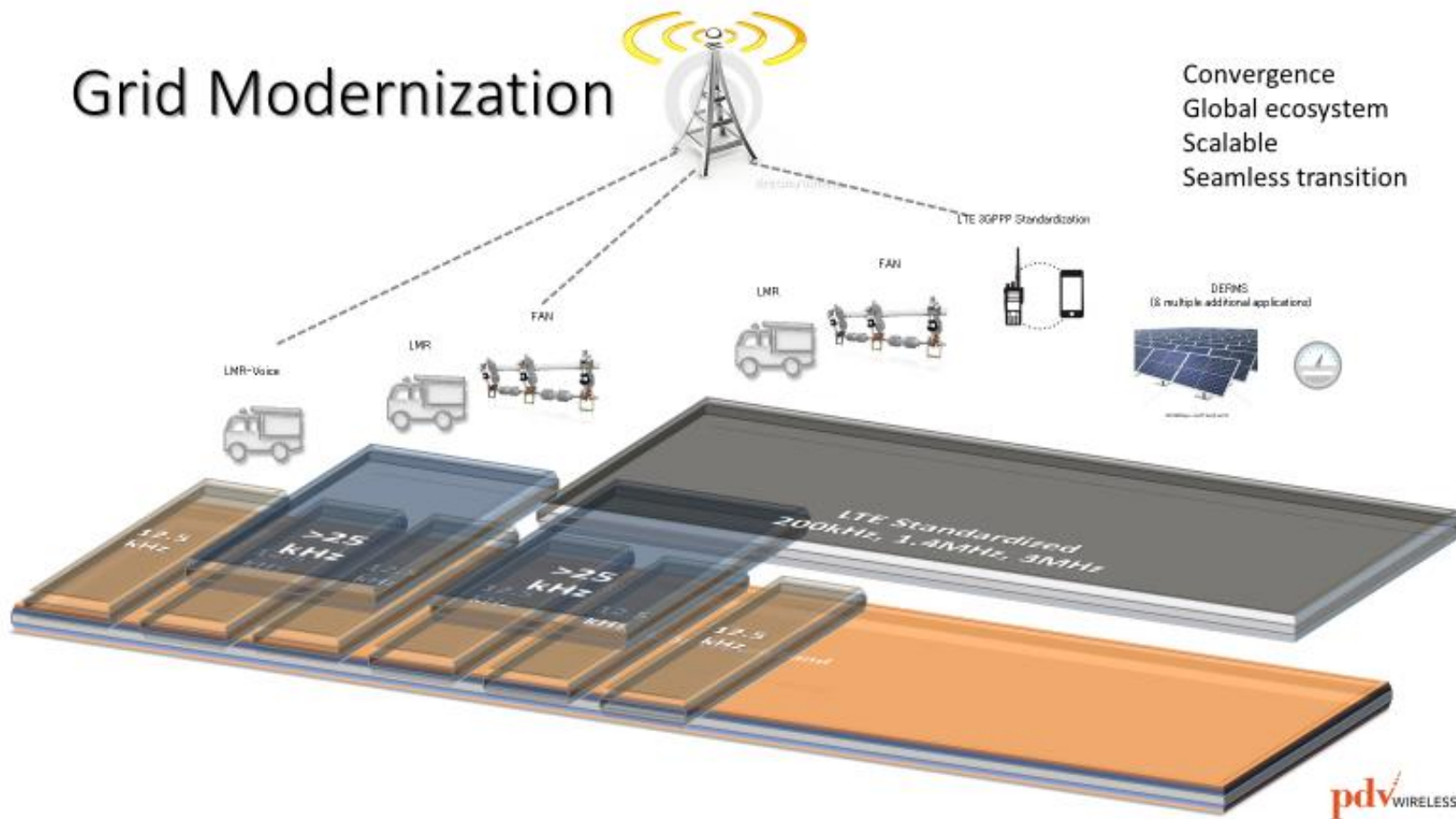


FAN on 25kHz or Greater



Grid Modernization

Convergence
Global ecosystem
Scalable
Seamless transition



Unified Utility Strategy



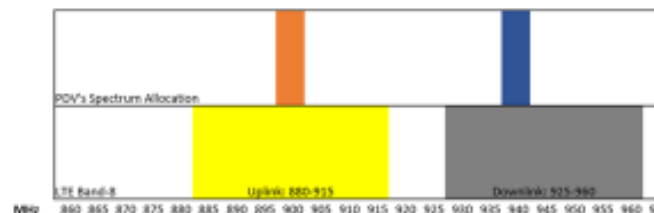
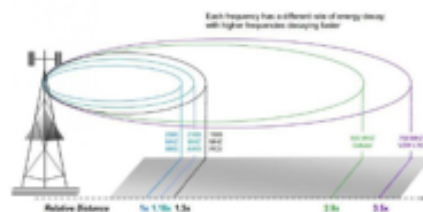
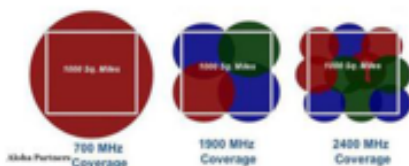
Utility Requirements

- Reliability
- Security
- Efficiency

900 MHz Value to Grid Modernization

Low band spectrum- Lower TCO

Licensed band enables higher reliability



- PDV Spectrum is compatible with the "LTE Band-8" allocation
- Equipment has been developed for use internationally- global ecosystem
 - Decrease obsolescence risk
 - Leverage economies of scale

Network Cost per Subscriber/User and Payback Period (Months)	700MHz Propagation	1900MHz Propagation	2400MHz Propagation
Total Network Cost @\$130,000/cell	\$130,000	\$520,000	\$1,300,000
Network Cost per Sub (@800/cell)	\$163	\$650	\$1,625
Network Cost per Sub (@200/cell)	\$650	\$2,600	\$6,500
# of Months Payback (\$20/mo.)	33 months	130 months	325 months

Source: Aloha partners

Global Ecosystem

More options and lower risk

Global Vendor Ecosystem

Narrow and Wideband Applications



Leverage a global ecosystem of equipment providers



LTE Band 8 Capable Equipment/Device



Flexible Deployment and Acquisition



Broad Set of Use Cases Across Industries

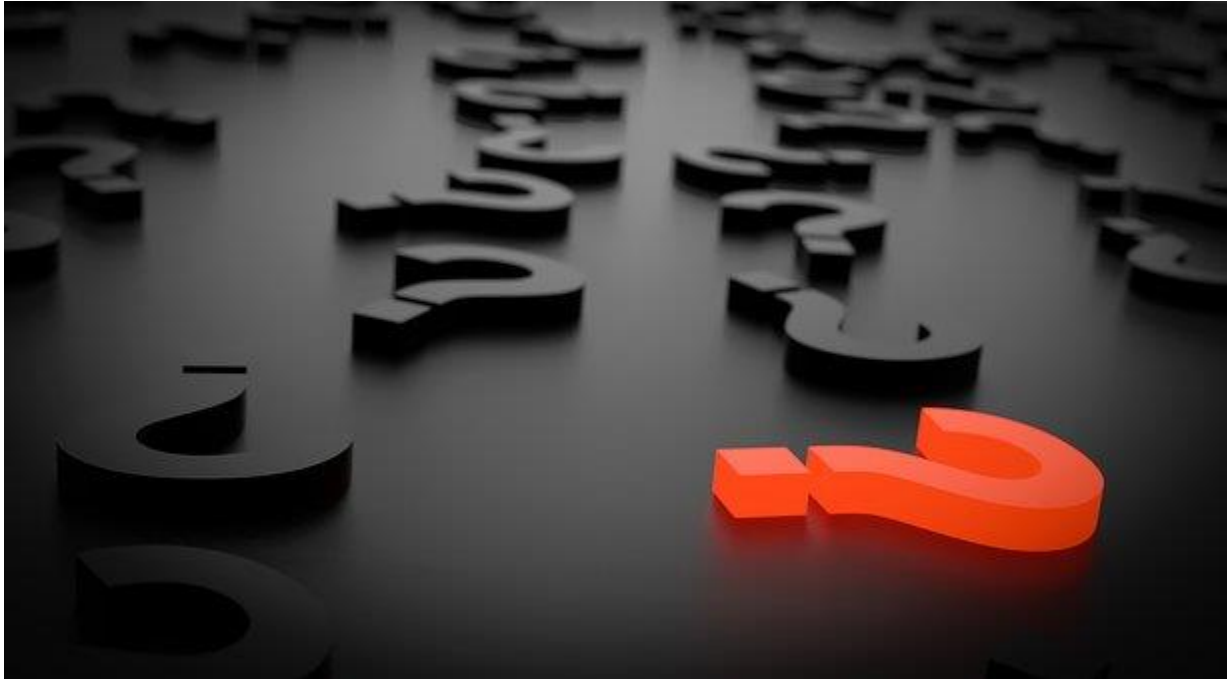


Critical Infrastructure and Enterprise Use-Cases:

- Use Cases supporting reliable:
 - Mission Critical Voice
 - Data applications
 - IoT
 - Fixed and mobile
 - Narrowband, wideband and broadband
- Private network slicing with prioritization
- Enhanced by low-band licensed spectrum in 900MHz band



- Questions/comments





301-975-0200

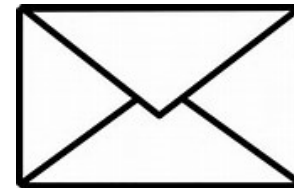


9700 Great Seneca Hwy,
Rockville, MD 20850

<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

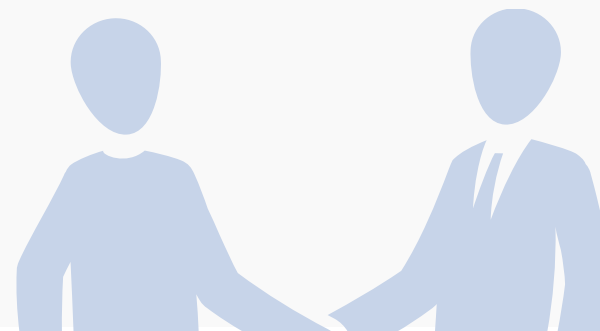


NIST ITL













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



Tech firms



Academia



Project managers



National Cybersecurity Excellence Partners (NCEP)



National Cybersecurity FFRDC*



Industry



Government



Project-specific collaborators



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)