

2015 AAPA Port Security Seminar & Expo

Cyber Risk Management

Presenter: LT Josephine Long

Critical Infrastructure Protection Branch

Office of Port & Facility Compliance (CG-FAC)



Homeland
Security



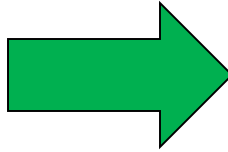
PRESENTATION OVERVIEW

- Goals
- Quick Review of How We Got Here
- Review of Coast Guard Strategy
- Discussion of Cyber Subcommittee on AMSCs
- Next Steps: NVIC, NIST Collaboration

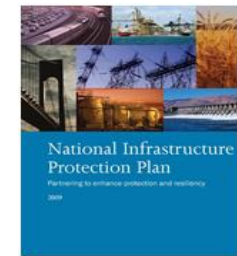
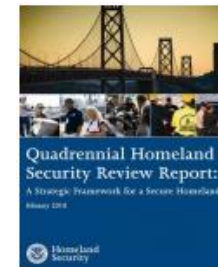
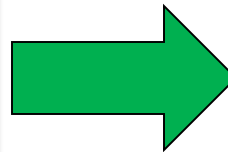


Policies, Directives and Mandates

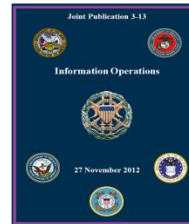
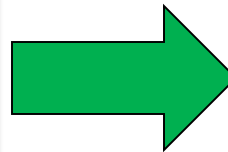
Presidential / National Policy



DHS Policies / Directives



DOD Policies / Directives



CG Policies / Directives



Homeland Security



Executive Order 13636

- **EO 13636: Improving Critical Infrastructure Cybersecurity Directs the Executive Branch to:**
 - Develop a technology-neutral voluntary cybersecurity framework (NIST)
 - Promote and incentivize the adoption of cybersecurity practices
 - Increase the volume, timeliness and quality of cyber threat information sharing
 - Explore the use of existing regulation to promote cyber security



Presidential Policy Directive-21

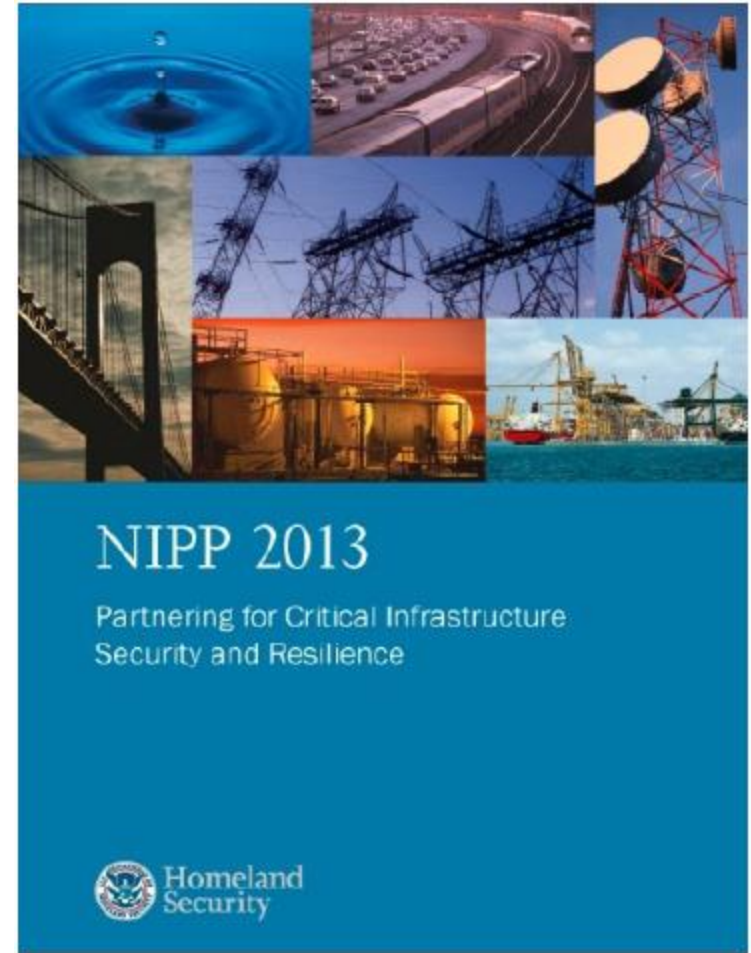
- **Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:**
 - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
 - Understand the cascading consequences of infrastructure failures
 - Evaluate and mature the public-private partnership
 - Update the National Infrastructure Protection Plan
 - Develop comprehensive research and development plan



Maritime Critical Infrastructure

The Coast Guard is the Sector Specific Agency (SSA) for the Maritime component of the Transportation Sector

- 1 of the 16 Critical Sectors
- Collaboration with our partners in TSA and DOT
- Protect maritime sector from all threats (physical, personnel, and cyber)

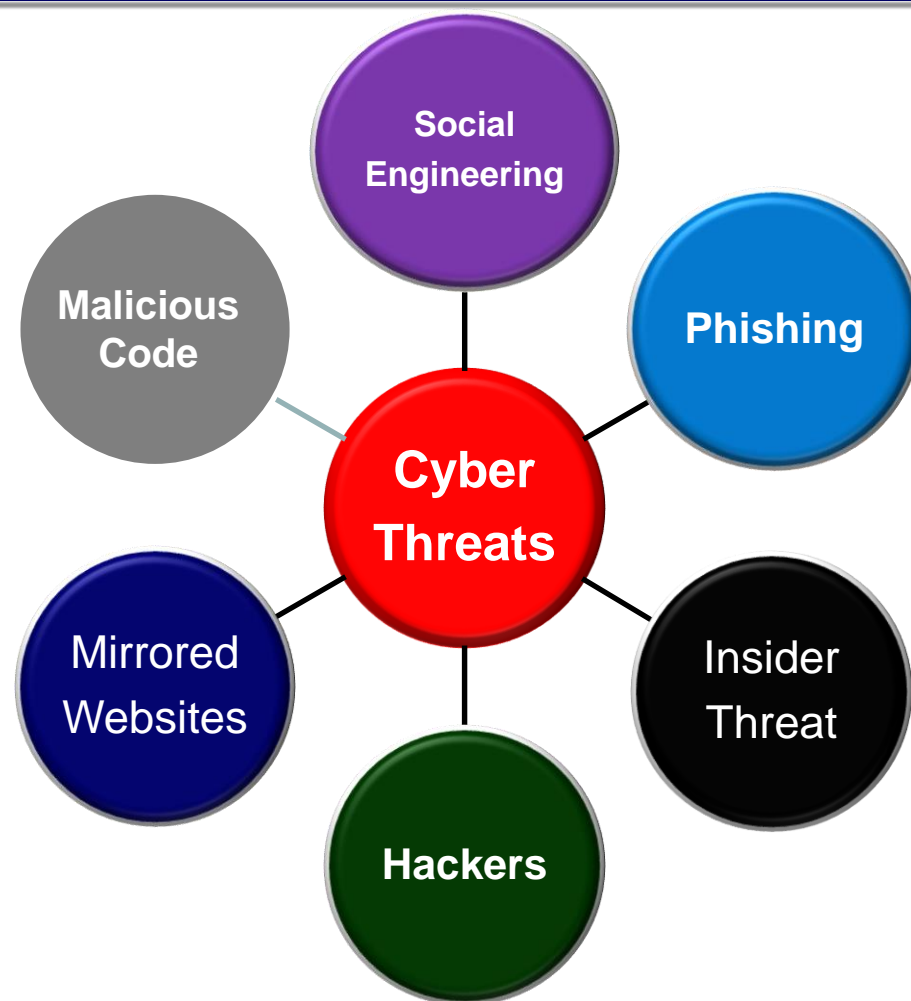


Homeland
Security



Types of Cyber Threats We are Facing

- Hackers/Intrusion Sets
- Phishing
- Social Engineering or Elicitation
- Malicious Code
- Mirrored Websites
- Insider Threat
- **How about accidents?**



GPS Spoofing

- In 2013, a University of Texas team conducted an experiment to take control of auto-pilot function by spoofing GPS
- The 213-foot White Rose is the US\$80M megayacht whose GPS navigational system was spoofed by about \$2,000-\$3,000 worth of equipment (Photo: U of Texas at Austin)



Homeland
Security



The background features a large, faint watermark of the United States Coast Guard emblem. The emblem is circular with a central shield containing a vertical striped pattern. Above the shield, the words "UNITED STATES COAST GUARD" are written in a circular path. Below the shield, the year "1790" is inscribed. The emblem is flanked by two crossed anchors. At the bottom of the emblem, there are four stars.

United States Coast Guard Cyber Strategy

Cyber Strategy

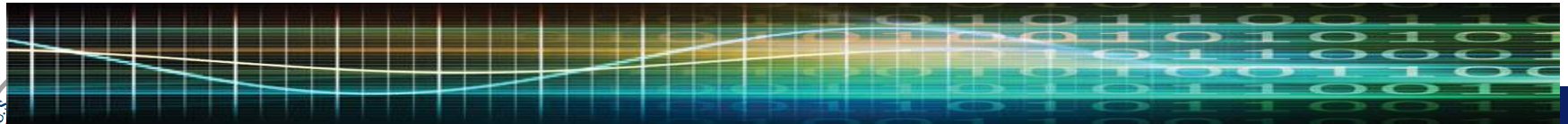
Three Strategic Priorities



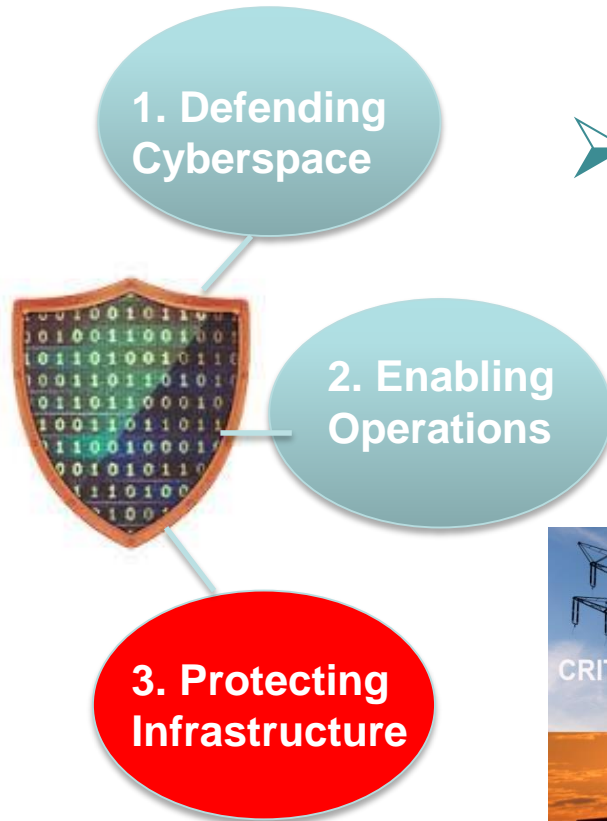
1. Defending Cyberspace

2. Enabling Operations

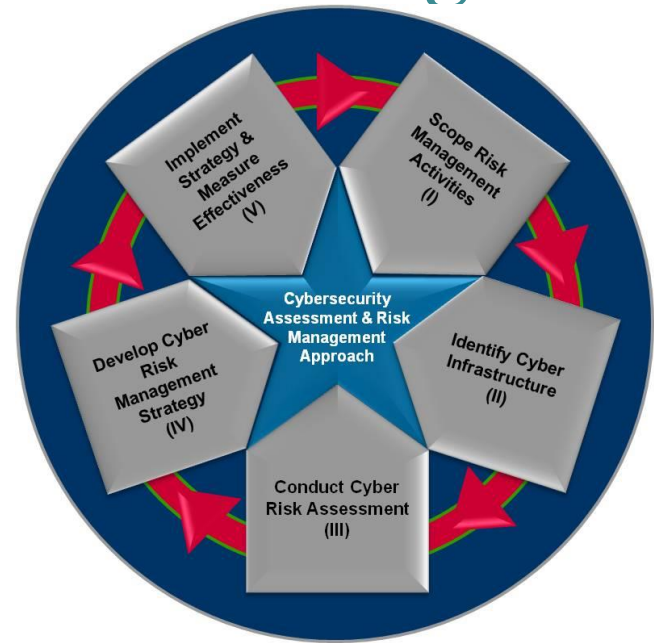
3. Protecting Infrastructure



3. Protecting Infrastructure



➤ **Goal 1. Risk Assessment – Promote Cyber Risk Awareness and Management**



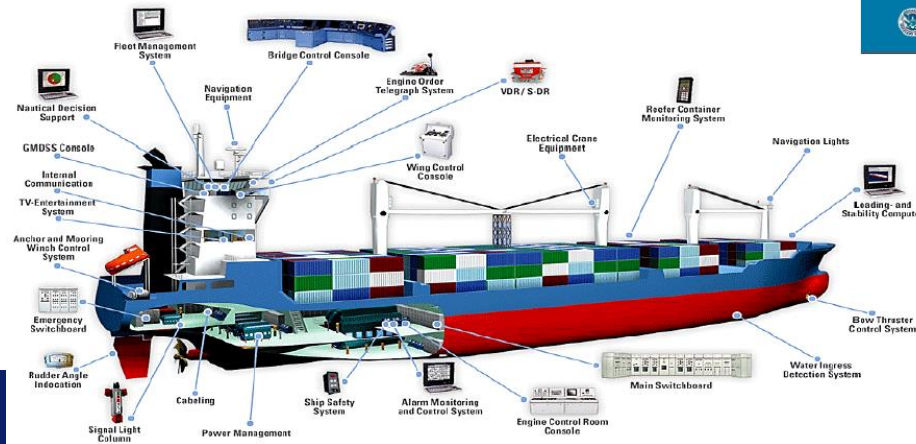
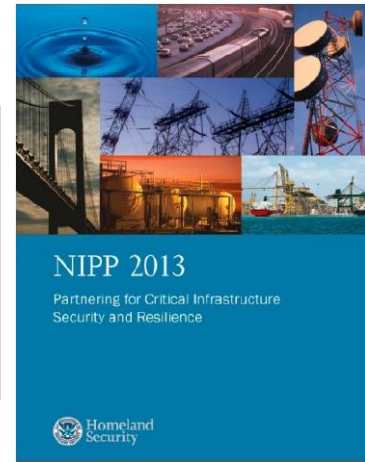
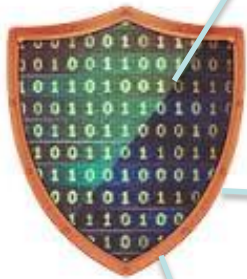
3. Protecting Infrastructure

1. Defending Cyberspace

2. Enabling Operations

3. Protecting Infrastructure

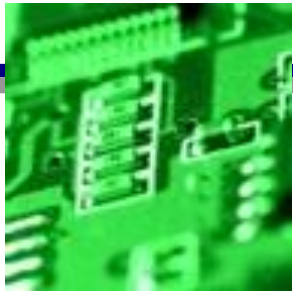
➤ Goal 2. Prevention – Reduce Cybersecurity Vulnerabilities in the MTS.



Homeland Security



Ensuring Long-Term Success Seven Cross-Cutting Factors



1. Recognize Cyberspace as an Operational Domain
2. Develop Operational Cyber Guidance/Define Mission Space
3. Leverage Partnerships
4. Communicate in Real-Time
5. Organize for Success
6. Build a Cyber Workforce
7. Invest in the Future



AMSC CYBER SUBCOMMITTEE

- **Recognized Best Practice for AMSCs**
 - Brings IT and Security Personnel together for Cyber Discussion!
- **13 AMSCs currently have some form of Cyber Subcommittee**
- **Blueprint & Draft Agenda found on Homeport**



Homeland
Security



Ongoing Initiatives

- Continue to evaluate and distribute voluntary risk assessment tools to industry
- Evaluate guidance for industry on risk reduction processes
- Review existing NVICs for cyber updates
- Standardize terms/definitions
- Clarify notification procedures
- Collaboration with the NIST CCOE



NVIC: VOLUNTARY GUIDANCE

- Scope: how can we define the “line in the sand”?
- Terms/Standards: What is acceptable cyber terminology and what is industry using (i.e. ISO 27000)?
- Risk Criteria: How does the NIST Framework support?
- Assessments: What is best cyber assessments to identify vulnerabilities and buy down risk?
- Drills and Exercises: How can cyber fit into existing requirements?
- 3rd Party Role
- Information Sharing
- Reporting
- Documentation Compliance



... ABOUT THE NCCOE





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





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



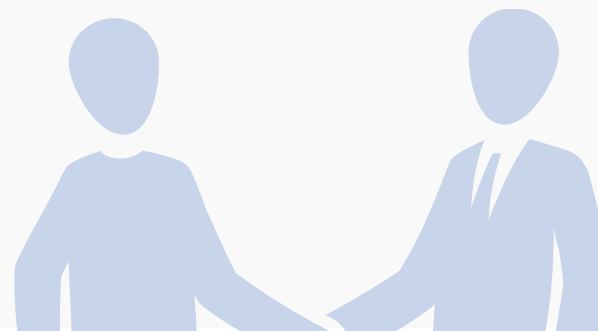


NIST ITL













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



Homeland Security
the NCCoE





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

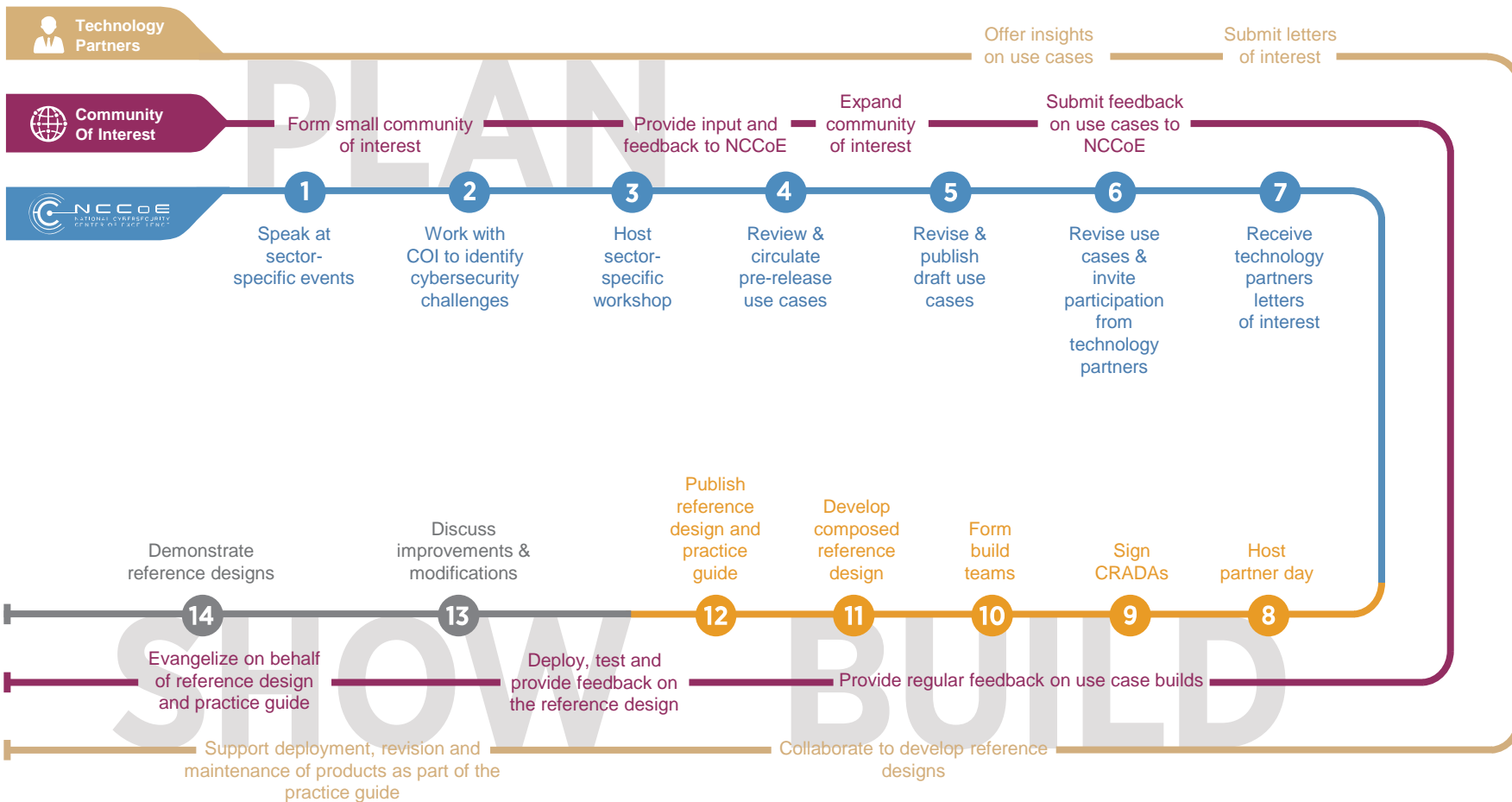


TRANSFER + LEARN

Guide users to stronger cybersecurity

Set of all material necessary to implement and easily adopt the reference design





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)



-  **Standards-based**
Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards
-  **Modular**
Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications
-  **Repeatable**
Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions
-  **Commercially available**
Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry
-  **Usable**
Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations
-  **Open and transparent**
Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

HEALTH IT SECTOR:

- 1) Securing Electronic Health Care Records on Mobile Devices
- 2) Wireless Medical Infusion Pmps

ENERGY SECTOR:

- 1) Identity and Access Management
- 2) Situational Awareness

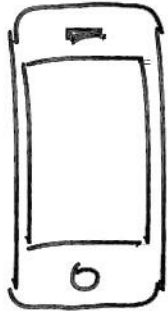
FINANCIAL SERVICES SECTOR:

- 1) IT Asset Management
- 2) Access Rights Management

BUILDING BLOCK:

- 1) Attribute Based Access Control



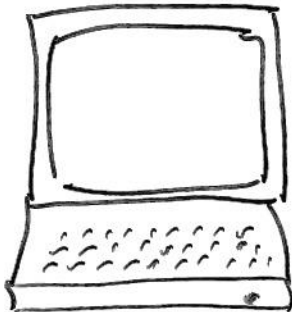


240-314-6800

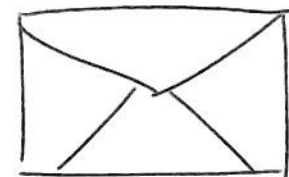


nccoe@nist.gov

Participate



<http://nccoe.nist.gov>

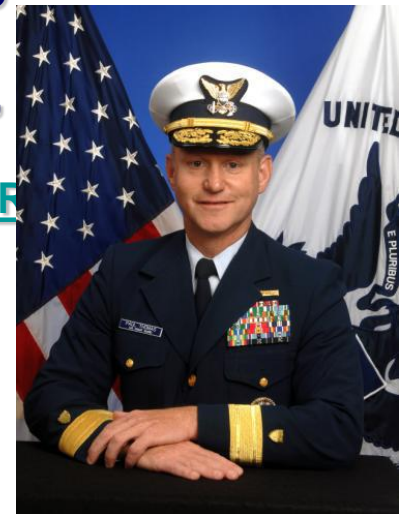


9600 Gudelsky Drive
Rockville, MD 20850

Quote from Rear Admiral Paul Thomas, Assistant Commandant for Prevention Policy

“THERE WERE QUESTIONS FROM THE AUDIENCE ABOUT TIMELINES AND INCENTIVES THAT I’D LIKE TO ADDRESS. THE COAST GUARD JUST RECENTLY CONDUCTED A STUDY ABOUT THE COST BURDEN TO INDUSTRY OF ALL THE REGULATIONS THAT WE HAVE PUBLISHED SINCE 1973. WE FOUND THAT 88% OF THE ENTIRE COST BURDENS OF ALL REGULATIONS, OVER ALL THOSE YEARS, WERE DUE TO TWO REGULATIONS, OPA 90 AND MTSA. BOTH OF THESE REGULATIONS FOLLOWED PREDICTABLE DISASTERS. THE LESSON LEARNED SHOULD BE THAT WE SHOULD NOT WAIT FOR AN INCIDENT TO OCCUR THAT WILL MAKE US MOVE FORWARD ON REACTIVE, MORE EXPENSIVE, REGULATIONS; WE NEED TO BE PROACTIVE IN APPROACHING THIS. WE ARE HERE TO HAVE A DISCUSSION WITH INDUSTRY SO WE CAN DEVELOP A STANDARD TOGETHER, ONE THAT WORKS AND IS REASONABLE IN TERMS OF THE COST BENEFIT. IF WE WAIT UNTIL AN INCIDENT OCCURS, THAT OPPORTUNITY GOES AWAY.”

[HTTPS://WWW.YOUTUBE.COM/WATCH?V=RZOVc1ZOUVY&FEATURE=EMBEDDED#T=9568](https://www.youtube.com/watch?v=RZOVc1ZOUVY&feature=embedded#t=9568)



Homeland
Security



Thank You for your time!

QUESTIONS?



Homeland
Security

