



Welcome to the NCCoE

Federal Computer Security Program Manager's
Forum Meeting

April 11, 2013



Our 2013 Strategy is Driven by Business Cybersecurity Needs



Provide Practical Cybersecurity

Help people secure their data and digital infrastructure by equipping them with practical ways to implement cost-effective, repeatable and scalable cybersecurity solutions



Advance Cybersecurity

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



Increase Rate of Adoption

Enable companies to rapidly adopt commercially available cybersecurity technologies by reducing their total cost of ownership



Accelerate Adoption of Secure Technologies

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



Accelerate Effective Innovation

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

ITL/CSD

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.

Partnership

The NCCoE is motivated by results. Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE is dedicated to furthering innovation through the rapid identification, integration and adoption of practical cybersecurity solutions.

CSD Thought Leadership

- Cryptography
- Identity Management
- Key Management
- Risk Management
- Secure Virtualization
- Software Assurance
- Security Automation
- Security for Cloud and Mobility
- Trusted Roots of Hardware
- Vulnerability Management
- Secure Networking
- Usability and Security



Define + Articulate
Describe the Business Problem

Broadly define business problem and project description and refine them through specific use cases



Organize + Engage
Partner with Innovators

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



Implement + Test
Build a Usable Solution

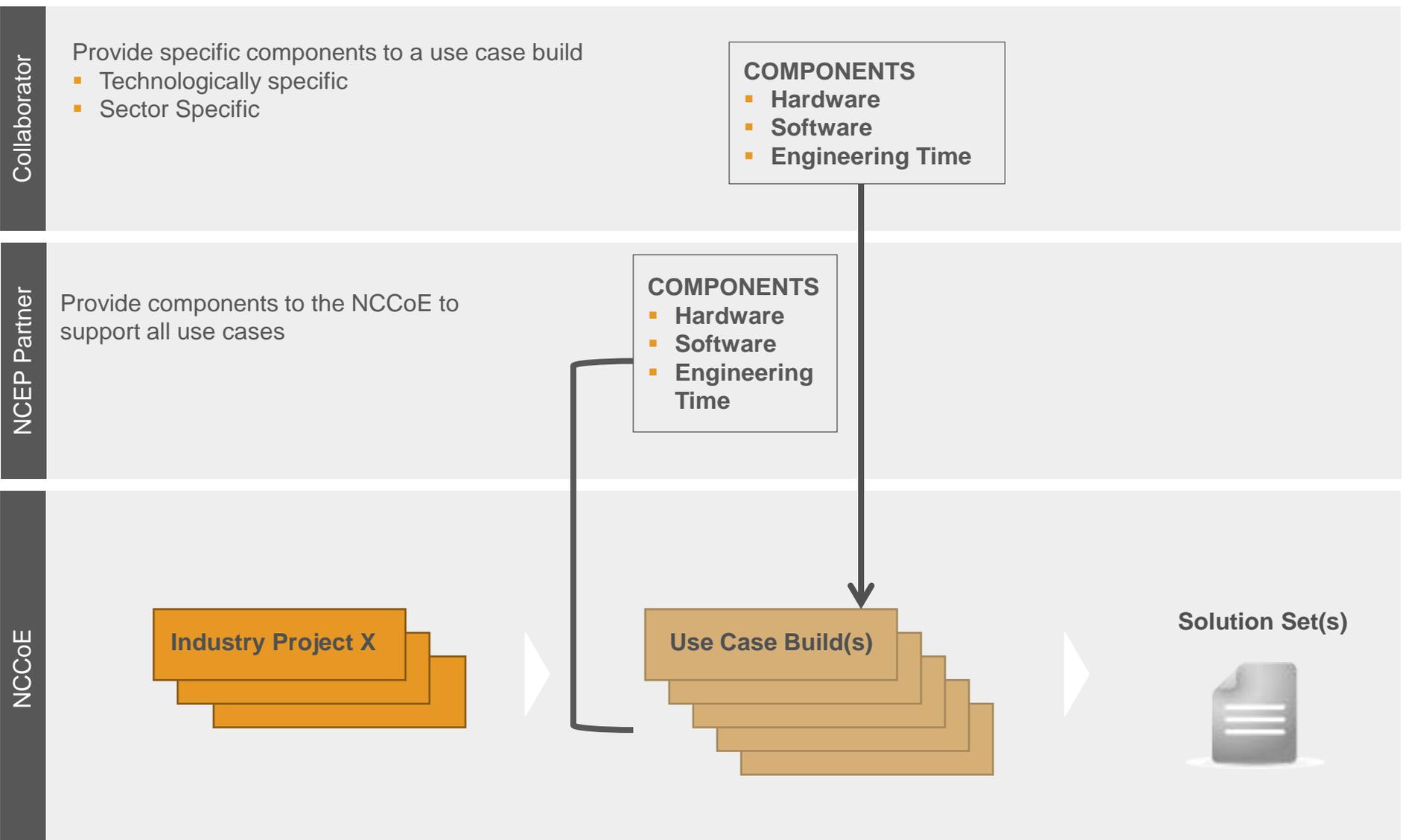
Practical, usable, repeatable and secure solution that addresses the business problem



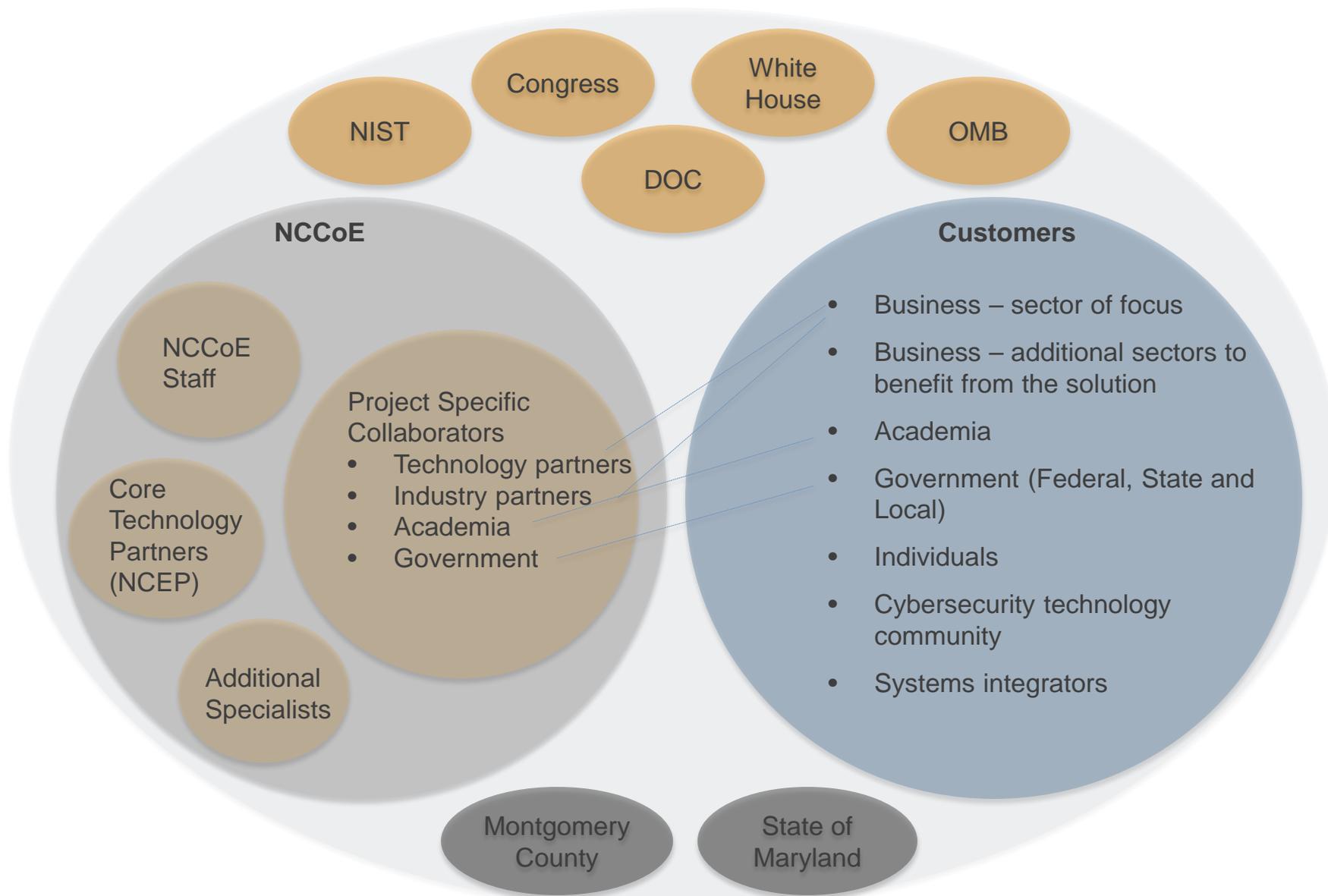
Transfer + Learn
Help People Adopt a Solution

Set of all material necessary to implement and easily adopt the secure solution

Project Lifecycle



Partnership with NCCoE Stakeholders



- Advance your organization's adoption of practical cybersecurity solutions that are usable, repeatable and secure
- Access integrated cybersecurity solutions that match your industry's specific business needs
- Rely on cybersecurity solutions that are built on commercially available technologies
- Increase your organization's ability to innovate by bridging technology gaps
- Work with cyber innovators in a trusted, state-of-the-art and collaborative environment
- Deepen your organization's understanding of cybersecurity capabilities, relevant costs and integration and adoption methods
- Broaden your organization's awareness of cybersecurity technologies and standards

Background

- Released on February 12, 2013
- Titled “Improving Critical Infrastructure Cybersecurity”
- Directs NIST to lead the development of framework of cybersecurity voluntary standards and best practices

Framework

- Rely on existing security frameworks and consensus-based standards to fullest extent possible
- Make it compatible with current regulatory authorities and regulations
- Develop in collaboration with industry to ensure it meets business and operational needs

RFI Status

- Published a Request for Information in Federal Register
- Set goal of collecting input from critical infrastructure owners and operators, federal agencies, state, local, territorial and tribal governments, standards-setting organizations, other members of industry, consumers, solutions providers and stakeholders

RFI Goals

- Share information on current risk management practices, use of frameworks, standards, guidelines, best practices and other industry practices
- Use information to hold workshops over next several months to collect additional input

Appendix

Engagement and Business Model

Describe + Articulate Business Problem		Organize + Engage Partners and Collaborators		Implement + Test Solution Build		Transfer + Learn Solution Adoption	
Action	Outputs	Action	Outputs	Action	Outputs	Action	Outputs
Describe/ID Business Problem	<ul style="list-style-type: none"> Draft Problem Statement Draft Project Description Draft Use Cases 	Publish Project/Use Cases and Solicit Responses	<ul style="list-style-type: none"> Process for Participation Letter of Interest Business Processes Priority Responses 	Build Solution	<ul style="list-style-type: none"> Use Case Validation Technical Architecture Building Block Interfaces Integration Source Code 	Collect Solution Documents	<ul style="list-style-type: none"> Problem + Use Case Architecture Reqs + Specs Source Code Test Environment Lab notebooks and decision memos
Create Market Research	<ul style="list-style-type: none"> Stakeholder List Threat Landscape Industry Standards and Guidelines Regulatory Requirements Preliminary Metrics 	Select Partners and Collaborators	<ul style="list-style-type: none"> Stakeholder Analysis Feasibility and Interoperability Analysis Initial List of Collaborators 	Test Solution	<ul style="list-style-type: none"> Test Harness Security Interoperability Security Standards Conformance Final Metrics 	Tech Transfer	<ul style="list-style-type: none"> Demonstrations Interactive Media User Guides Templates Blueprints Toolkits How Tos
Vet Project & Use Case Descriptions	<ul style="list-style-type: none"> Final Problem Statement and Project Description Use Case requirements Product Category(s) and security requirements 	Sign CRADA	<ul style="list-style-type: none"> Signed CRADAs Execution Plan with Roles and Responsibilities 	Identify Solution Gaps	<ul style="list-style-type: none"> Requirement Gaps Technology Gaps Standards and Guidelines Gaps Mitigation Plan ROI Business Case 	Document Lessons Learned and Archive	<ul style="list-style-type: none"> Project Archive Internal and External Lessons Learned Recommended Practices Lessons + Practices
Outcome	Outcome		Outcome		Outcome		
Broadly define business problem and project description and refine them through specific use cases	Collaborate with partners from industry, government, academia and the IT community to design one (or more) solutions		Practical, usable, repeatable and secure solution that addresses the business problem		Set of all material necessary to implement and easily adopt the secure solution		