NCCOE: Current Status and Future Plans

Donna Dodson
Acting Associate Director
Acting Chief Cybersecurity Advisor
Information Technology Laboratory

Visiting Committee on Advanced Technology
June 2013

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

NCCoE Foundations

NIST

Part of

- NIST Information Technology Laboratory

As a part of the NIST family, the Center has access to a foundation of prodigious expertise, resources, relationships and experience.

Partnerships

- NIST
- State of Maryland
- Montgomery County
- Industry communities of interest
- Secure technology vendors
- Other Government Agencies

Building on ITL's 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

Strategic Plan

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 cybersecurity capabilities that address business needs

Customers

- Business – sector of focus
- Business – additional sectors to benefit from the solution
- Academia
- Government (federal, state, local)
- Individuals
- Cybersecurity technology community
- Systems integrators

Engagement and Business Model

Define + Articulate
Describe the business problem

Define business problem and project description broadly 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 tailored to each audience

Current Activities

- **Industry engagement –** working with communities of interest across various industry sectors to capture cybersecurity concerns / potential use cases (Health Care, Energy, Financial Services, Manufacturing, Government)
- **Core partnerships (NCEP) –** recruiting large IT and cybersecurity companies to participate as National Cybersecurity Excellence Partners
- **Project-based use cases –** in collaboration with IT and cybersecurity vendors (NCEPs and others), build technical solutions to address industry's cybersecurity concerns
- **Building blocks –** working with small groups of vendors to address security challenges that cut across multiple industry sectors
- **Business process / strategic planning –** capturing and continually revising the NCCoE business process
- **FFRDC –** proceeding through the legal and acquisition processes to establish the first Federally Funded Research and Development Center (FFRDC) dedicated to cybersecurity (also the first DOC FFRDC)

NCEP Companies

Current core partners

- **Intel**
- **HyTrust**
- **McAfee**
- **Splunk**
- **Cisco**
- **RSA**
- **Symantec**
- **Microsoft**
- **Vanguard**
- **Hewlett-Packard**
- **Venafi**
- **Tripwire**
- **CA, Inc.**

Contributions from our Partners

NCEP companies will have a persistent presence at the center that includes:

- **Technology –** the building blocks (software, hardware, tools, services) necessary to create example integrated "builds" to address industry's cybersecurity challenges
- **Personnel –** engineers who will work in the NCCoE side-by-side with engineers from other companies, NIST, and other federal agencies to integrate their technologies into the composed solution

NCCoE Projects and Use Cases

Project	**Health Care**	
Use Cases	*Current*	*Under Discussion*
	Mobile access and data exchange security	Medical device security
		Secure patient access and control
Project	**Energy**	
Use Cases	*Current*	*Under Discussion*
	Data aggregation and monitoring	Virtualized SCADA services
	Identity and access management	Securing the home area network
Project	**Financial Services**	
Use Cases	*Under Discussion*	
	Cross-institution practical unified symmetric key management	
	Scalable key management for multiple financial services organizations	
	Secure and scalable linked I&A and confidentiality applications to support wireless banking	
Project	**Manufacturing**	
Use Cases	*Under Discussion*	
	Controlled distribution of proprietary information	
	Manufacturing control system security	
	Linked multifactor I&A and role-based access control for process control applications	

NCCoE Building Blocks

“Building Blocks” are the specific technology components that National Cybersecurity Excellence Partners donate to the center’s efforts to address cybersecurity issues.

Building Block	Status
Trusted Geolocation in the Cloud	Developing v2 that captures many more security features of a "trusted" cloud infrastructure
Authenticated Email	Initiated
Continuous Monitoring: Automated Software Inventory	Initiated
Security Automation	Initiated
Mobile Device Integrity	Initiated

Active Use Cases

Health Care: Mobile Access and Data Exchange Security

Business Need	The secure exchange of electronic information among health care providers and to patients on mobile devices
Status	Met with vendors on April 17, 2013 to discuss technological components they can contribute; CRADAs under review

Energy: Data Aggregation and Monitoring

Business Need	Among increasing amounts of data, analysts need more powerful surveillance tools for the detection of tampering with SCADA systems and other security incidents
Status	Refining use case architecture

Energy: Identity and Access Management

Business Need	Improved control over who has access--and what levels of access--to which IT and operational technology systems, and ability to know who did what (when something goes wrong)
Status	Refining use case architecture

FFRDC

Rationale

- Advantages to being supported as an FFRDC
  - Scaling – Can rapidly expand and contract in a variety of areas to meet changing needs
  - Bench strength – Will be supported by a company with readily available experts
  - No profit motive – Supporting company unbiased, will not promote one product or solution over another

Progress

- Preparing second of three Federal Register Notices to announce intent and solicit comments
- Responding to questions generated by first FRN from
  - OMB
  - Professional Services Council (trade organization)
  - others

FFRDC Costs and Impacts

Funding Information and Assumptions

- $10M/year (min)
- Average FFRDC annual cost to operate a lab $1.1M
- Projected FFRDC annual overhead of $1.4M
- Projected (fully-loaded) annual facilities cost of $2-$3M
- Phase 2 facility expected to have at least 8 labs + space for workshops and project demos
- State/county contribute a building
- Full $10M can be used to fund FFRDC operations and FFRDC overhead

FFRDC Costs and Impacts

Project Projections and Implications

- Average Sector Specific Project 18 – 24 months
- 3-6 use cases per project
- 3-10 vendors per use case
- Projected average vendors per project per year = 17
- Operate eight labs in steady state
- Estimate hosting 65 unique vendors per year
- Project hosting 6-12 demonstrations per workshops per year
- Tackle industry priorities and maintain momentum
- Cycle through the NCCoE pipeline, providing fresh projects and use cases for vendor partners to address