



The National Cybersecurity Center of Excellence: Realizing a Vision

Donna F. Dodson
Acting Director, NCCoE
donna.dodson@nist.gov



Though no-one knows for sure, corporate America is believed to lose anything from \$100 billion to \$1 trillion a year from online theft of proprietary information—trade secrets, research findings, internal costs, marketing plans, personal information, credit-card numbers, bank-account details and much more –
Babbage (blog), The Economist, May 11, 2012

NCCoE Vision

Provide a world class, collaborative environment for integrating cybersecurity solutions that stimulate e-commerce and national economic growth.

NCCoE Mission

Foster the rapid adoption and broad deployment of integrated cybersecurity tools and techniques that enhance consumer confidence in U.S. information systems.



Key Center Goals:

Disseminate new principles and mechanics underlying security standards, metrics, and best practices for secure and privacy-preserving information technologies

Develop and test methods for composing, monitoring, and measuring the security posture of computer and enterprise systems

Achieve broad adoption of practical, affordable, and useful cybersecurity capabilities across the full range of commercial and government sectors



NCCoE Essentials:

Business Leaders...

Influence. Utilizing their breadth of knowledge into specific sector/market IT security needs.

Business Community...

Representation. Critical to understanding and identifying security needs the NCCoE may be well suited to address.

Cybersecurity Technologists...

Vision. Leading security integrators being linked through security technologies.

Public...

Interest. Benefitting from and capitalizing on the lessons learned through NCCoE efforts.

NCCoE: Operational and Business Model

Business sectors have real business needs:



A physician in a small clinic uses a preferred mobile device to assist with patient care during a visit. However, there is no secure, consistent means to transfer electronic health information from the physician's device to the clinic's main server.

Use cases help identify and scope a real business problem:



NCCoE will seek health IT solutions using open interface standards to encourage flexibility while ensuring privacy and security of health IT data.

Planning Phase

Business
Engagement &
Problem
Statement



Use Case



Implementation Phase

IT Industry
Components
Selection



Implement in
Operational
Environment

NCCoE Framework: Realizing the Vision

- Use Cases - *Center* of the Center
- Deep Dive Days - D³
- Implementation Workshops
- Academic and Innovation Engagement



Priming the Pump: First Use Cases Identified Internally

Use Case Initial Selections

- Health Care IT Use Case: Information Exchange – Q4FY12
- Cloud IT Use Case: Policy Enforcement – Q1FY13
- Federal Use Case: Continuous Monitoring – Q1FY13

Foster an Environment to Exchange Knowledge

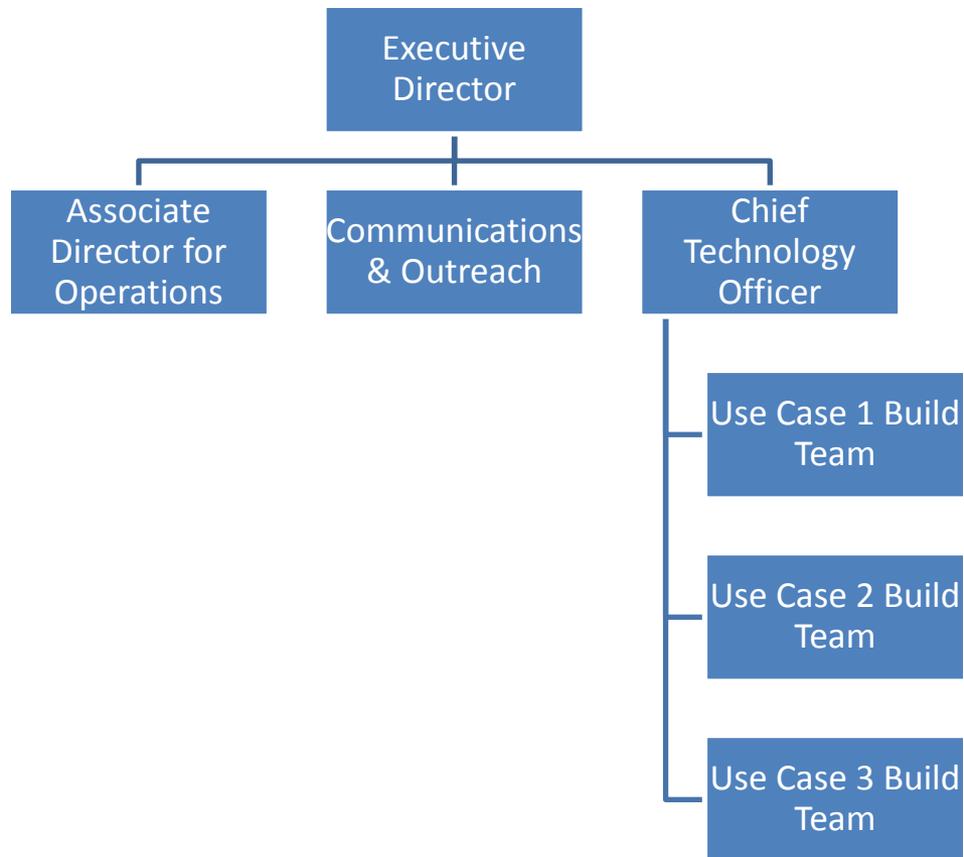
- Host a focused technology session centered around protected and signed BIOS – Q4FY12



NCCoE Operations: Realizing the Vision

- People and Partnerships
- Communications
- Facilities
- Resources

NCCoE Operational Model:



NCCoE Using Innovative Communications

- Workshops
 - Business discussions
 - Technology discussions
 - Innovation discussions

- Social Media



- Industry/Business Sector Events
- Federal Register Announcements

NCCoE Facilities:

Phase I Facility Identified

- Initial work space
- University of MD, Rockville
- 6,092 sq. ft., 4 labs, 8 offices, collaboration spaces
- IT infrastructure selected and purchased
- Furniture selected and purchased

Phase II Next Facility Under Design

- Contract awarded with architectural firm
- Working collaboratively with County and State

NCCoE Outputs: Realizing the Vision

Tools and Technologies

- Integrated security templates
- Practical technologies, tools, policies, and practices to create a trustworthy cybersecurity environment
- Broader awareness of cyber security technologies and standards
- Define innovation gaps and collaborate on ideas

Communications

- Meaningful discussions between businesses, technologists and academics
- Security discussions with peers in business sector events
- Business discussions with peers in security events
- Collaborative exchanges with public who share desire for applied solutions

NCCoE Outputs: Realizing the Vision

Metrics and Measures

- Baselines for success measures for business communities, IT industry, investors and consumers
- Data gathering techniques
- Measure – Report – Adjust
- Did we solve the business problem?

Value

- Reference materials output from builds
- Feedback on use of reference materials
- Partnerships in new sectors
- Integrator benefit through lessons learned
- Vendor-Consumer exchanges



NCCoE Value:

Expected NCCoE Benefits

- Accelerated adoption of practical, affordable, and usable cybersecurity solutions
- Increased opportunities for innovation
- Trusted environment for interaction among businesses and solution providers
- Innovation resulting in possible new cybersecurity products, services, and businesses
- Further the understanding of current cybersecurity technology capabilities and costs



Thank You!