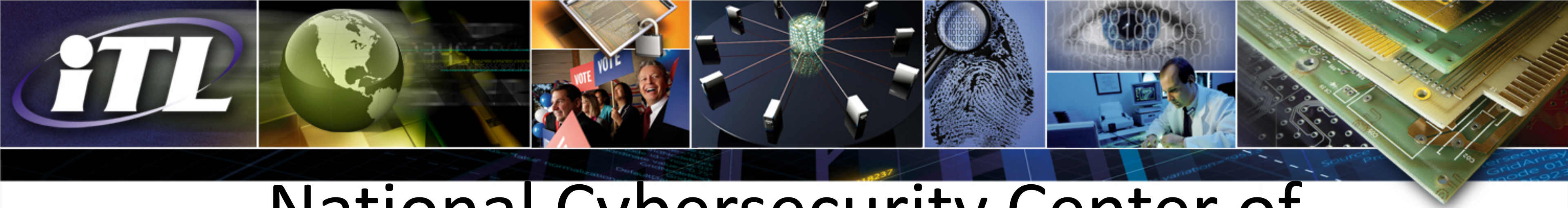
National Cybersecurity Center of Excellence

Update, Operational and Business Model

Charles H. Romine, Director
Information Technology Laboratory
June 20, 2012



National Cybersecurity Center of Excellence (NCCoE) Update

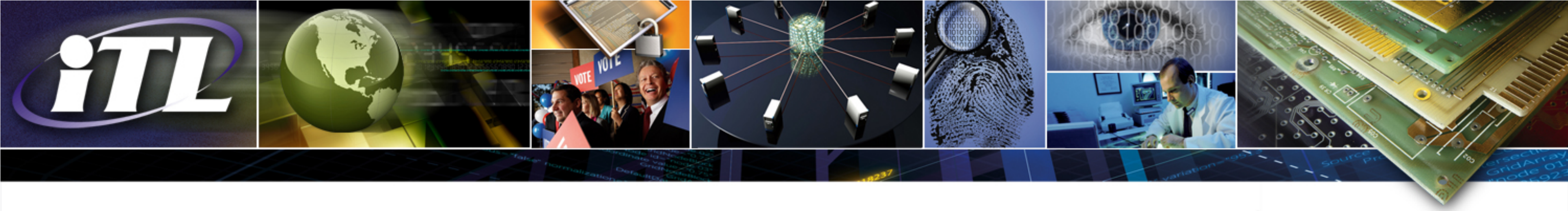
"…cyber crime hurts individuals, businesses and government agencies. We want to bring together the best minds and provide them with the best tools to create and test solutions…" *Pat Gallagher, February 2012*

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



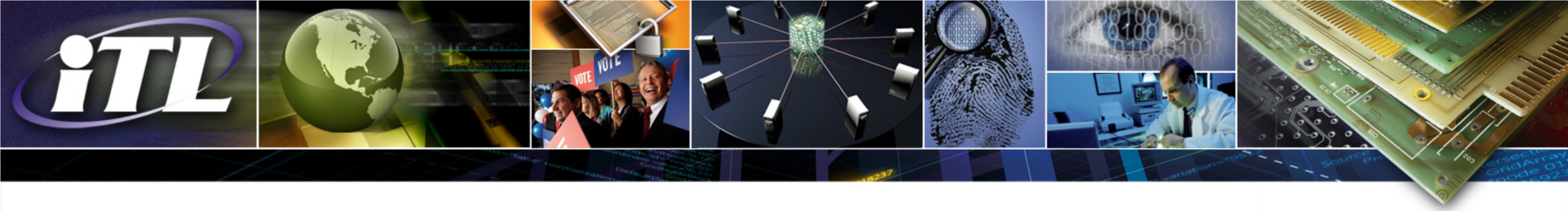
NCCoE Update: First Use Cases Identified Internally

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 Update: Staff and Support

NIST Staff

- 8.25 FTEs
- 3 FTEs in hiring process

Contract Support

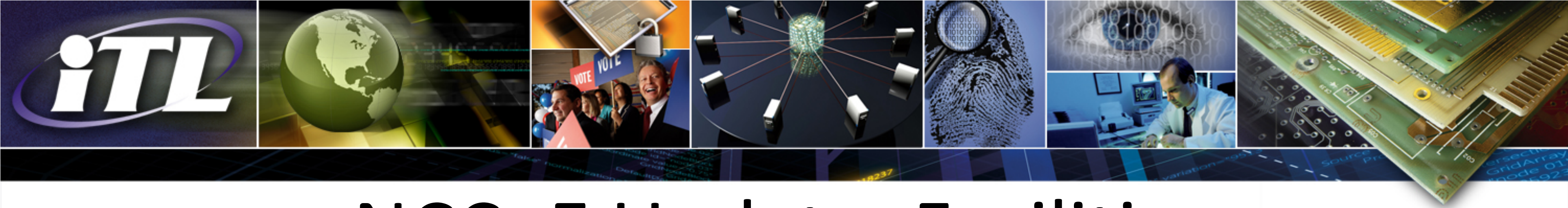
Current Acquisitions

- Support Services and Build Out
- Communications
- Metrics Development

Federal Staff Detailed to NIST

In process

- DHS
- NSA



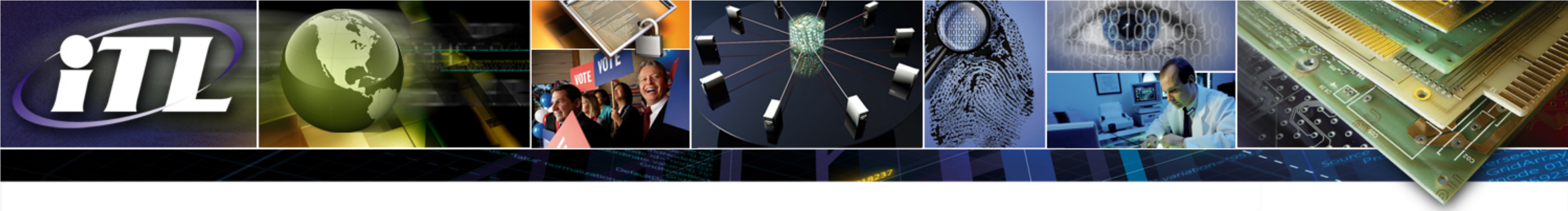
NCCoE Update: Facilities

Phase 1 Facilities 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 2 Next Facilities Under Design

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



NCCoE Update: Immediate Next Steps

1st Workshop

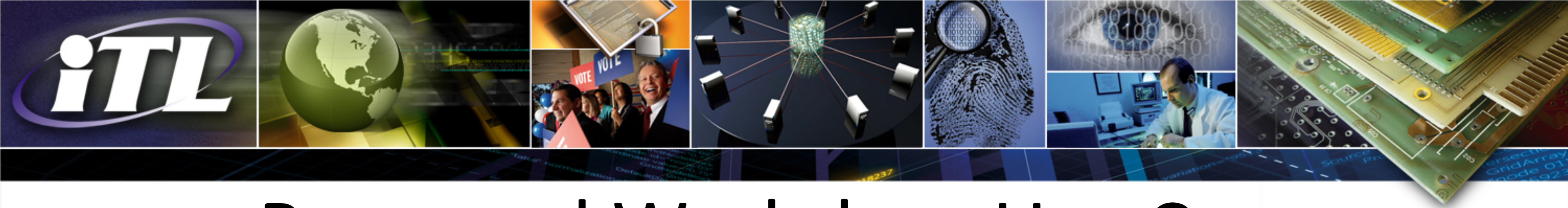
- June 26th. Initiate public engagement

Start Open Business Community Engagement

- Identify next communities and solicit requirements for Use Case development
- Solicit business drivers for ongoing participation with the NCCoE

Solicit Feedback and Comment

- Publicize the business engagement plan and operations process for comment and feedback



Proposed Workshop Use Case

Business Need

- Security platform to enable exchange of electronic health information by small healthcare providers

Data and Information

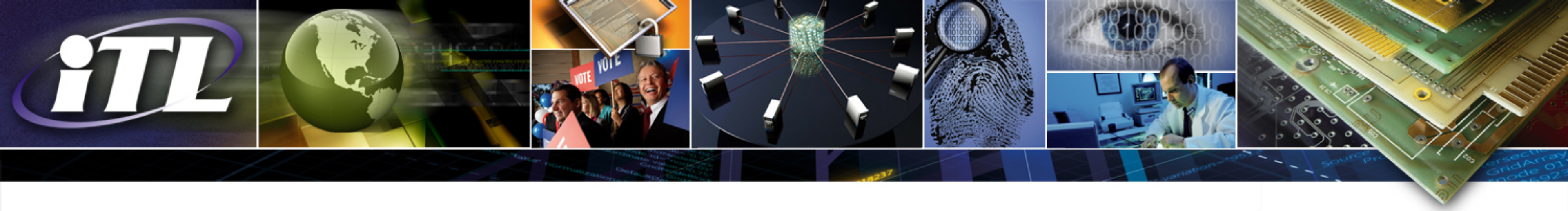
- Electronic Health Information

Sectors

- U.S. Federal government and health IT community

Relevant IT Technology, Standards, and Security Infrastructure Services

- Electronic Health Record (EHR) Systems
- Healthcare data exchange standards (e.g., HL7, DICOM, IHE)
- Desktop, laptop, and mobile devices (hardware root of trust)
- Operating systems and applications (secure configuration baselines)
- Security management and configuration (security automation specifications, continuous monitoring, health check)
- Data protection, identity, and key management (endpoint encryption, directory services, multi-factor authentication)
- Secure infrastructure (DNSSEC, IPv4, and IPv6)



NCCoE Update: Next Steps

Establish Communication Mechanisms

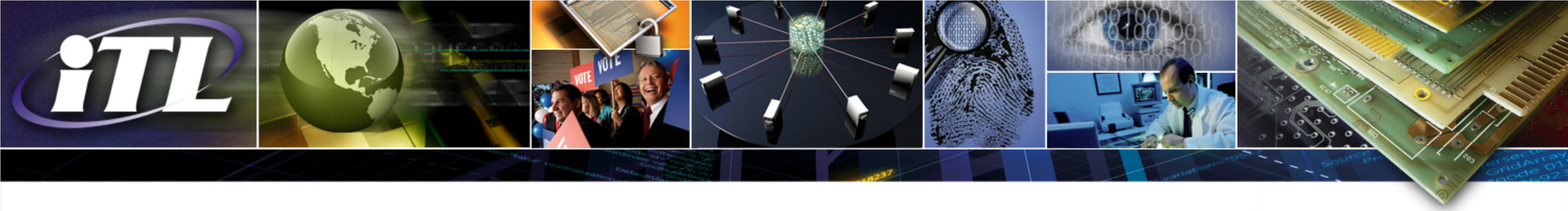
- Use Advisory Board, Business leader groups, consortia for inputs
- Open public involvement through social media and next workshops
- Participate in business sector events

Establish Metrics and Measure

- Set baselines for success measures for business communities, IT industry, and consumers
- Establish data gathering techniques
- Measure – Report – Adjust

Provide Value

- Publish reference materials output from builds
- Gather feedback on use of reference materials



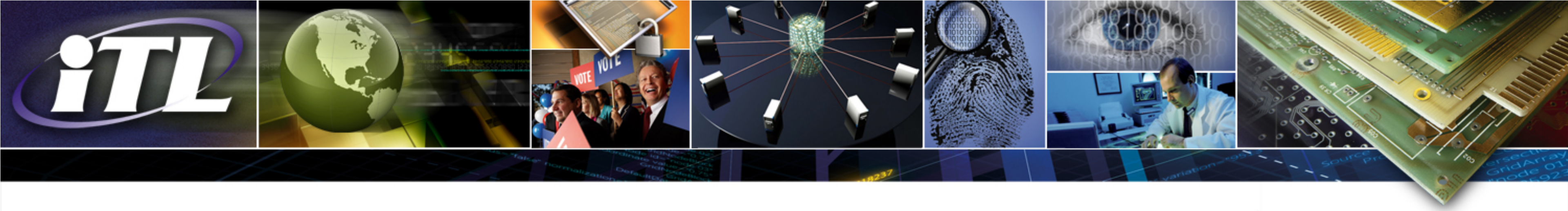
NCCoE: Operational and Business Model

Business sectors have real business needs:

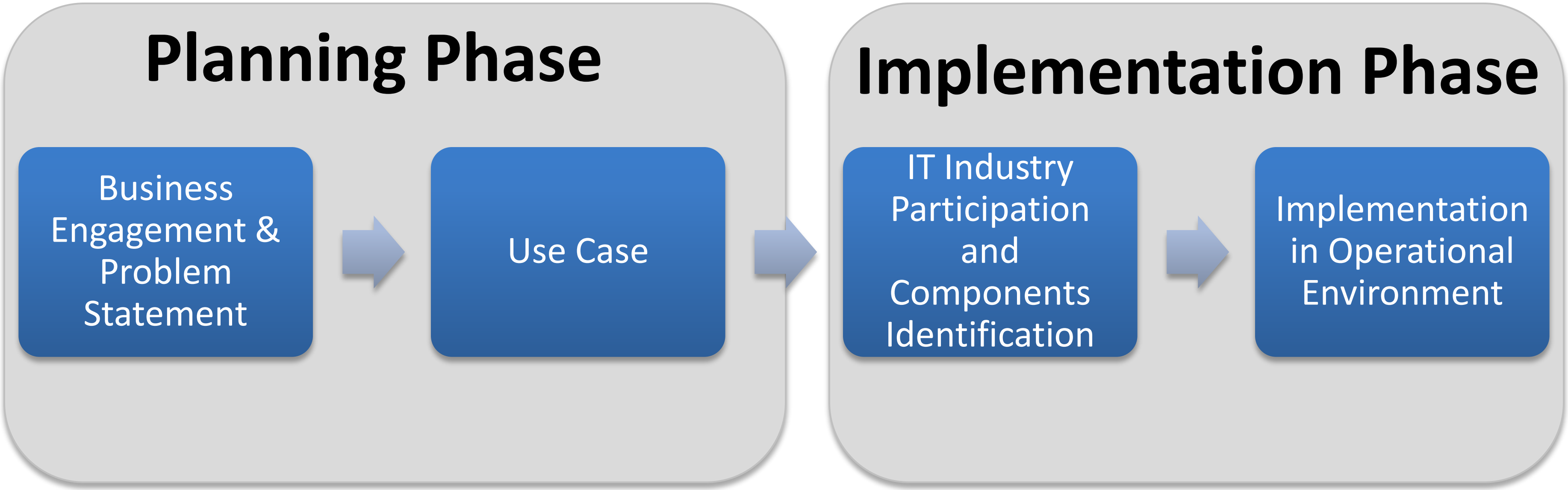
A physician in a small clinic uses a preferred mobile device to assist with patient care during a visit. However, there is no secure, consistent means to transfer electronic health information from the physician's device to the clinic's main server.

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.



NCCoE Business Model



Planning Phase

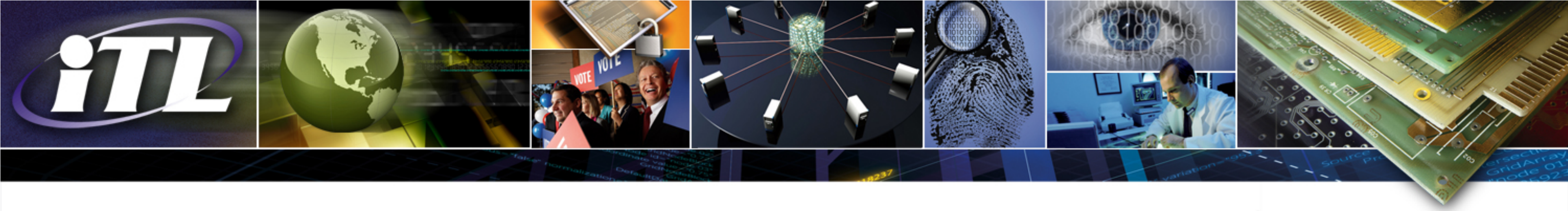
Business Engagement & Problem Statement

Use Case

Implementation Phase

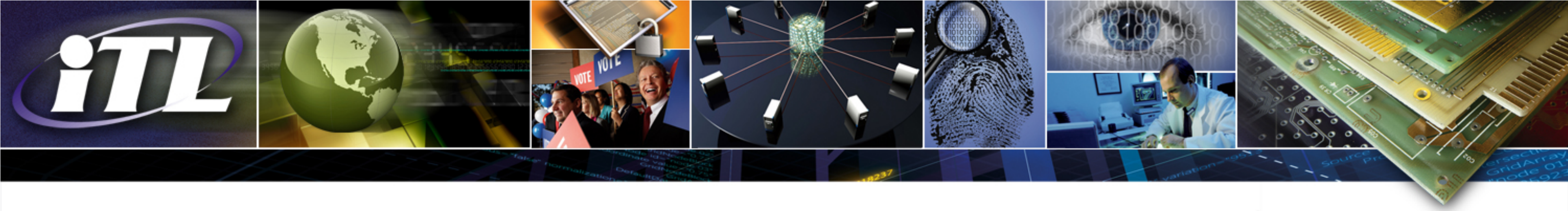
IT Industry Participation and Components Identification

Implementation in Operational Environment



NCCoE Business Model: Business Engagement & Problem Statement Selection

- Problem Identification
  - Potential Sources:
    - Advisory Board
    - Business Community, Consortia
    - Product Users
- Problem Selection
  - Open Discussions:
    - Threat Situation
    - Community Collaboration

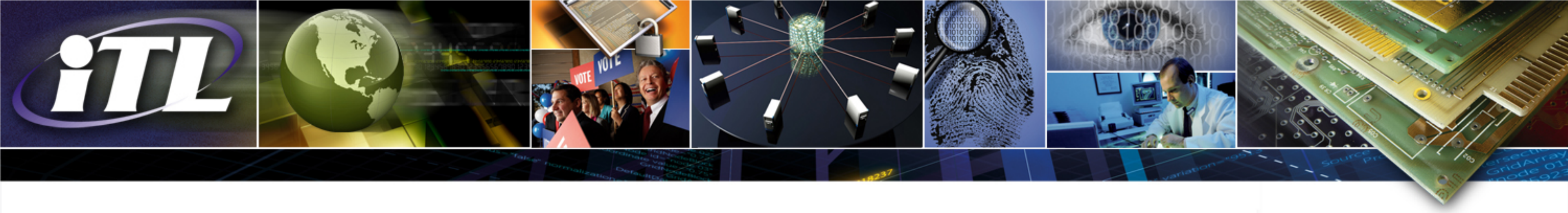


NCCoE Business Model: Use Case Selection

Articulate and scope the business problem

Open Discussions

- Relevance of existing technologies
- Impact to current threat models
- Collect proposed Use Cases
- Review in an open, transparent manner, solicit participation
- Select and refine Use Case

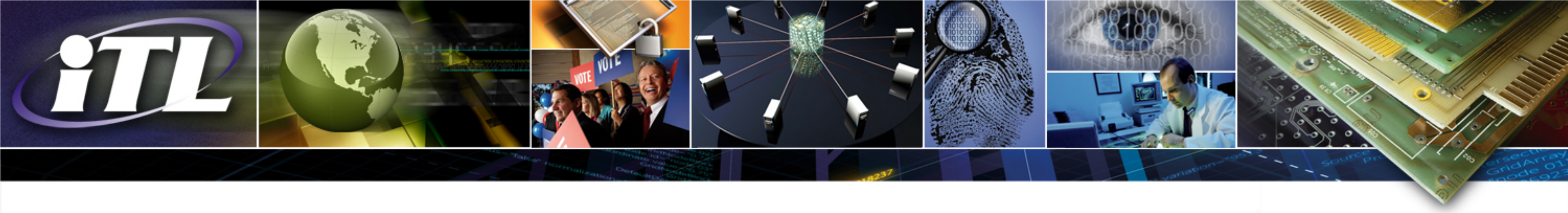


NCCoE Business Model: IT Industry Participation

Open Call to Participate

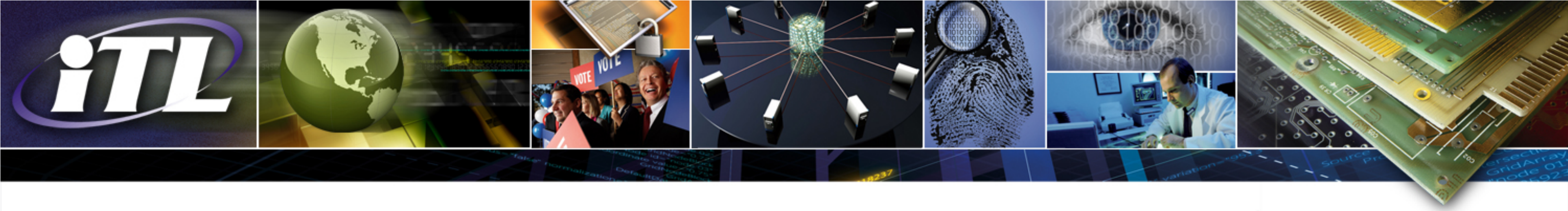
Industry, Agencies, Academia, Consortia

- Each provides technology, knowledge, abilities mapped to Use Case
- All work to a common build reflecting an instance of the Use Case
- Identify gap areas in technologies, innovation and standards
- Maintain the Use Case, update, or sunset



NCCoE Business Model: Implementation in Operational Environment

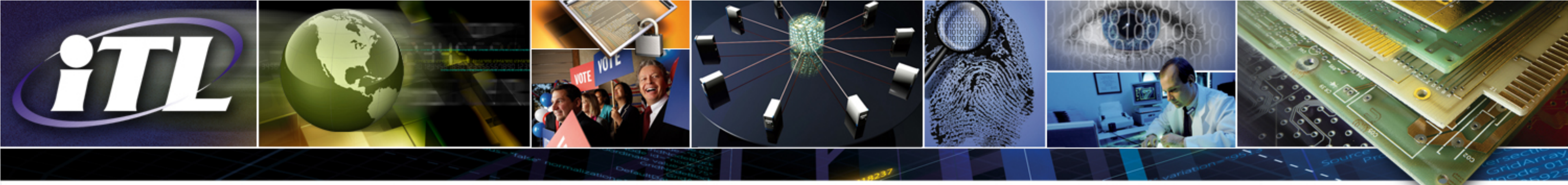
- Solution is documented with enough detail that it can be reproduced, independently of the NCCoE (i.e. published results available to the public)
- Traced to standards, guidelines and best practices
- Traced back to business problem statement
- Metrics evaluated on benefits to customer, industry, public, Maryland constituency, etc…
- Allows for other IT industry participants to repeat and contribute to references
- Host technical sessions extending the Use Case implementation in specific, high value areas based on technology, threats, needs, and/or assets



NCCoE Business Model: Why do we Care?

Expected
NCCoE Benefits

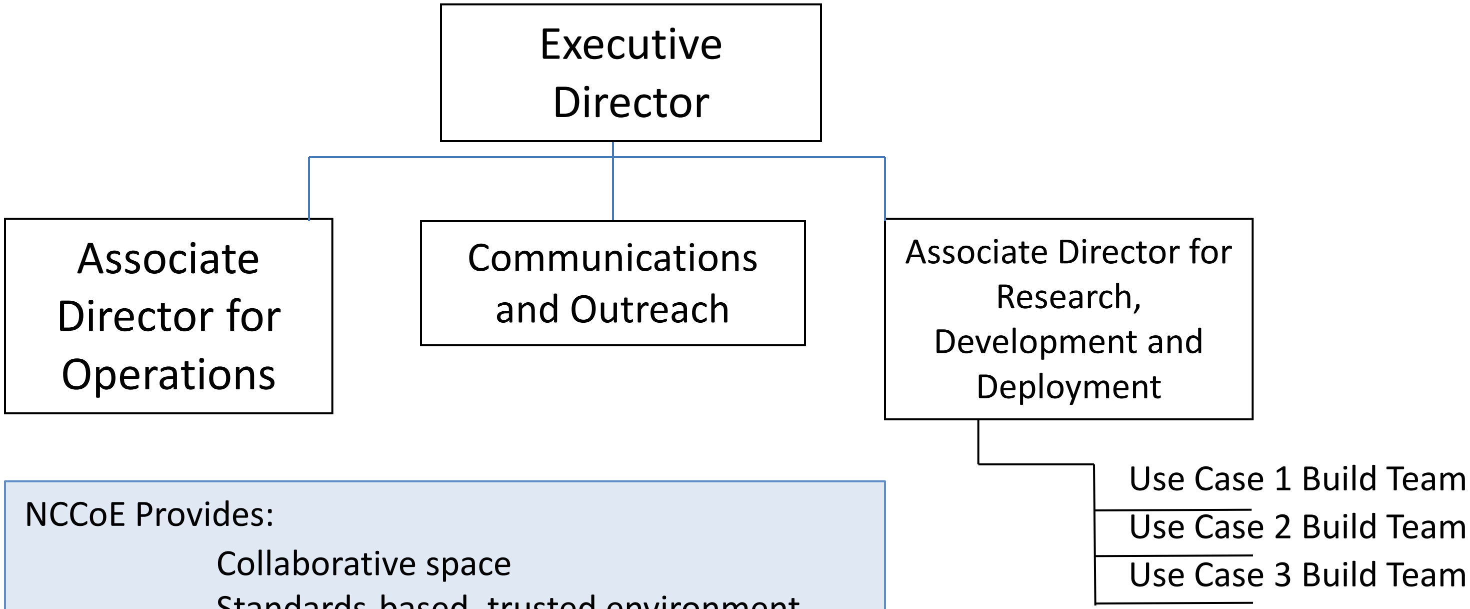
- Accelerated adoption of practical, affordable, and usable cybersecurity solutions
- Increased opportunities for innovation
- Trusted environment for interaction among businesses and solution providers
- Innovation resulting in possible new cybersecurity products, services, and businesses
- Further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



NCCoE: Operational Model

NIST Staff

- 8.25 FTEs
- 3 FTEs in hiring process
- 2 Details in process



Executive Director

Associate Director for Operations

Communications and Outreach

Associate Director for Research, Development and Deployment

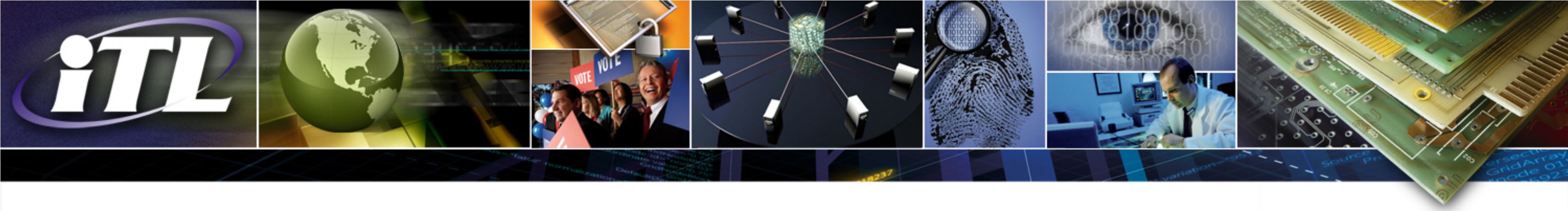
Use Case 1 Build Team

Use Case 2 Build Team

Use Case 3 Build Team

NCCoE Provides:

Collaborative space
Standards-based, trusted environment
Ability to draw expertise from across NIST



NCCOE Update, Business and Operational Model

Thank you