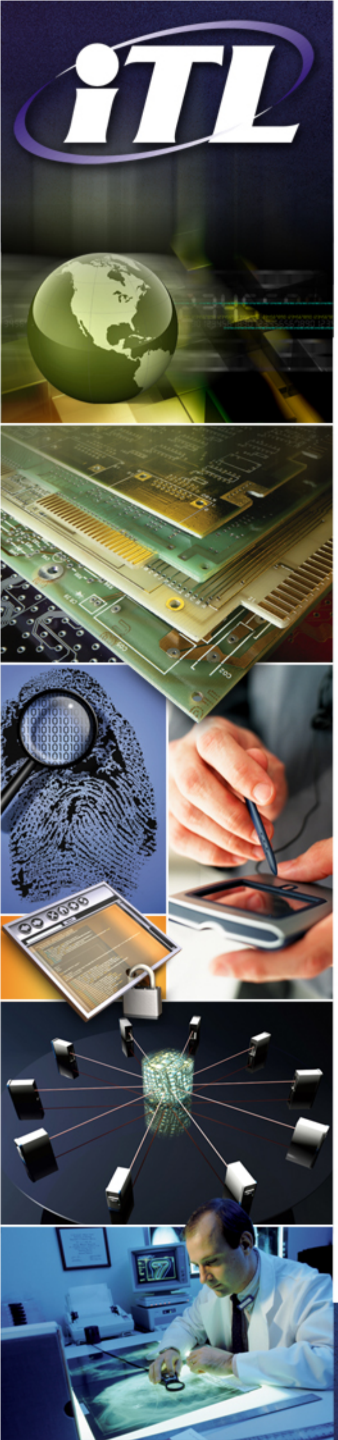


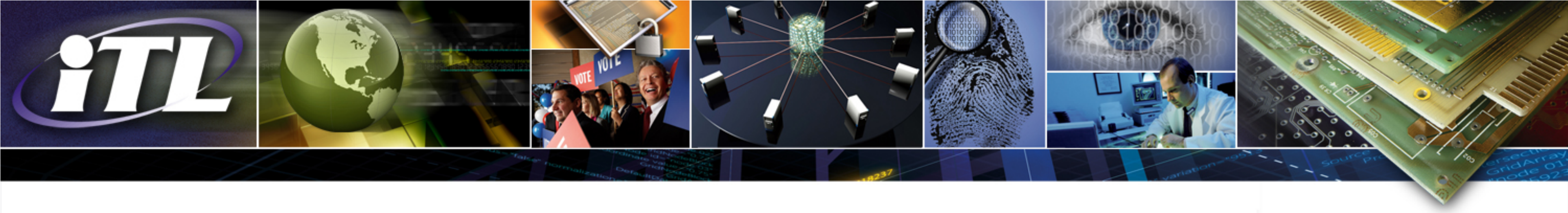
Cybersecurity Center of Excellence Concept Plan

Donna F. Dodson

Chief, Computer Security Division

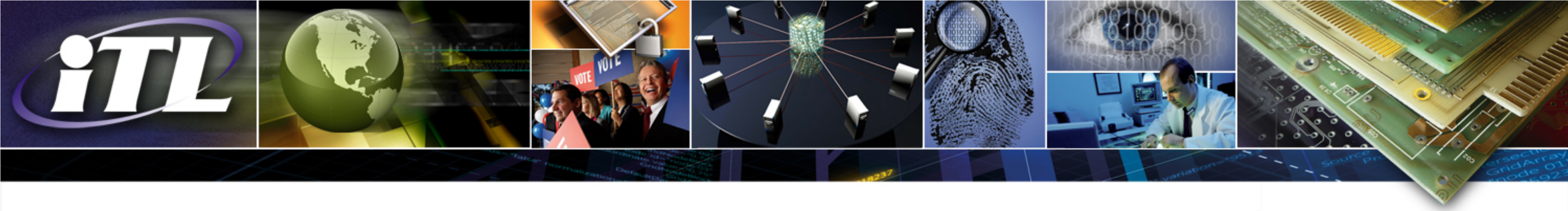
February 8, 2012

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



CCoE Mission

To foster development and rapid adoption and broad deployment of comprehensive cybersecurity platforms that support automated and trustworthy government and industry business operations and e-commerce.



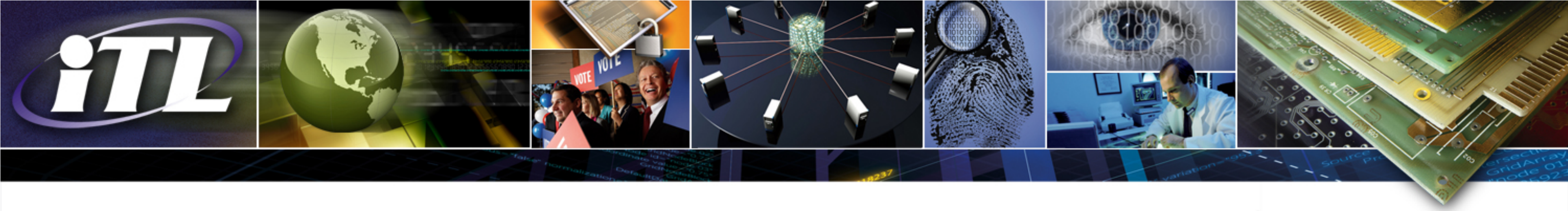
Strategy

Work as partners across the commercial, academic, and government sectors to develop and deploy cybersecurity platforms for innovative business solutions.

Approach

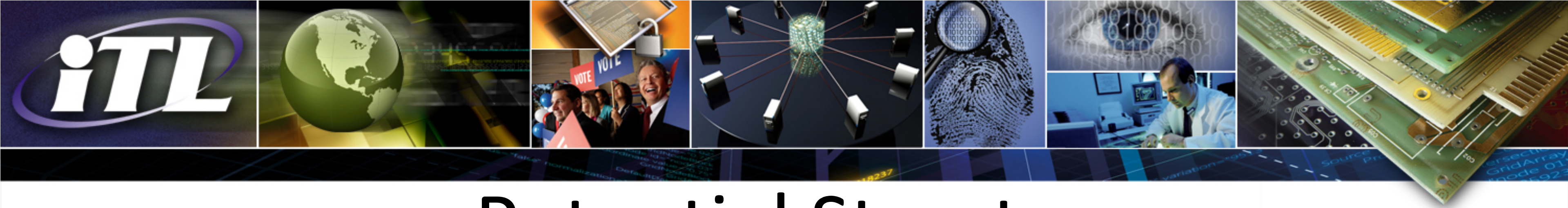
The CCoE strategy will be pursued through public-private-sector team research, development, and deployment acceleration efforts including:

- The development of multi-institutional, collaborative programs to foster the composition of secure IT platforms;
- A modern development facility that promotes frequent and direct interaction among experts;
- A team environment;
- Project objectives that are jointly identified and shared regarding deployment of comprehensive cybersecurity principles and platforms; and
- Creation of opportunities for collaborative leadership among technologist and business communities.

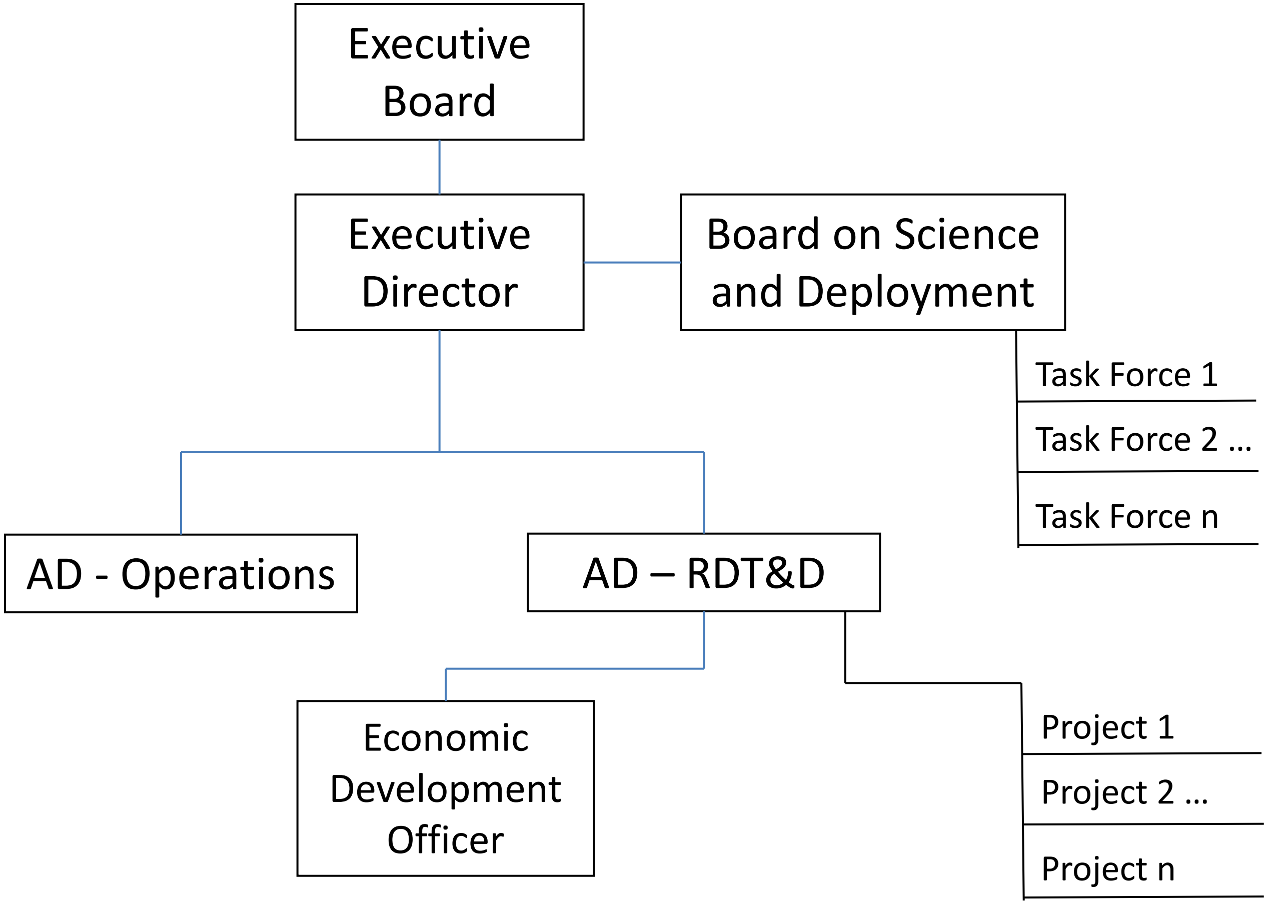


Goals

- Dissemination of new principles and mechanisms underlying security standards, metrics, and best practices for secure and privacy preserving information technologies;
- New and tested methods for composing, discovering, monitoring, and measuring the security posture of systems and enterprises; and
- Broad adoption of practical, affordable, and useful cybersecurity capabilities and practices across the full range of commercial and government sectors.



Potential Structure



Executive Board

Executive Director

Board on Science and Deployment

Task Force 1

Task Force 2 …

Task Force n

AD - Operations

AD – RDT&D

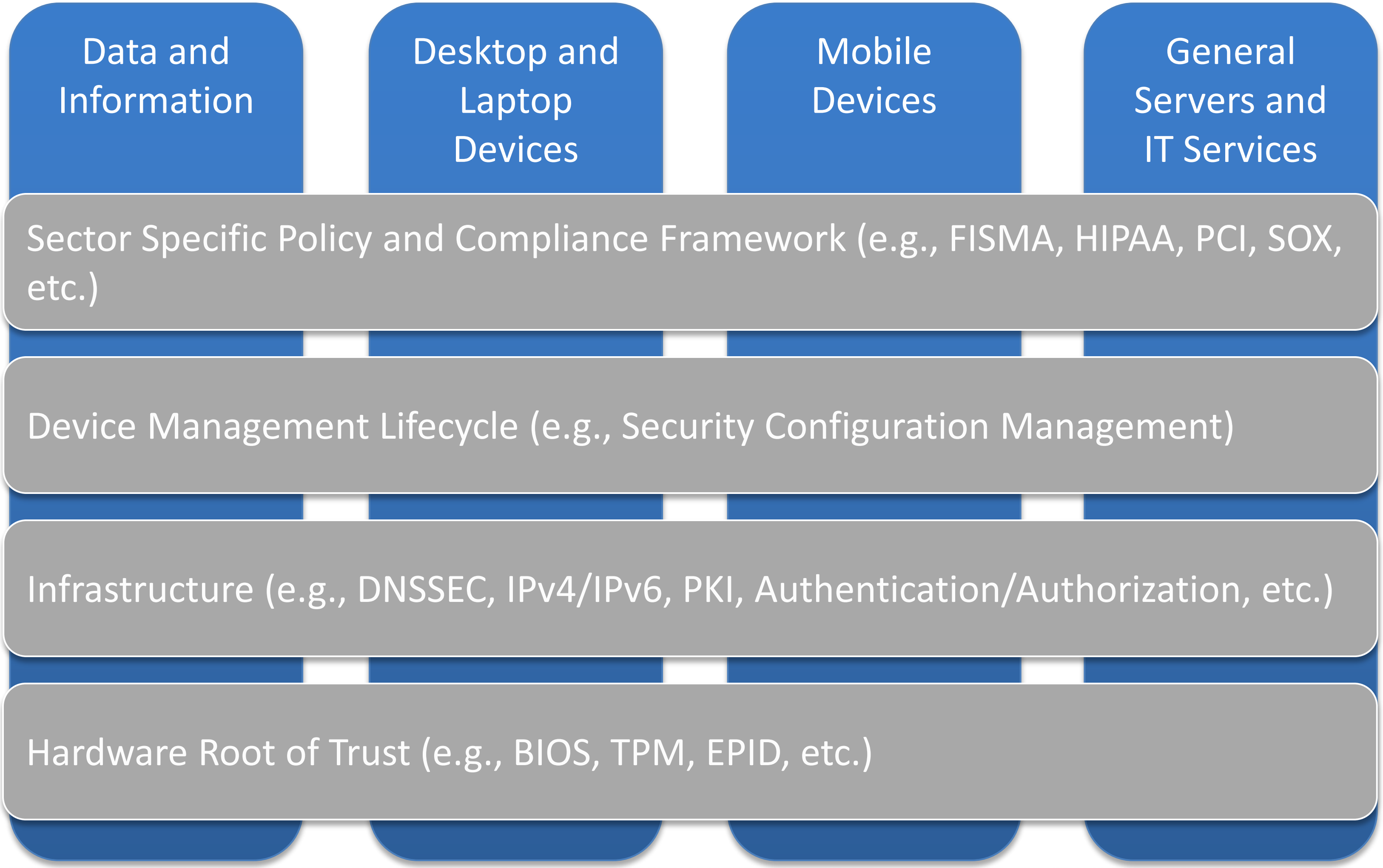
Economic Development Officer

Project 1

Project 2 …

Project n

Sketch of Use Case Framework



Data and Information

Desktop and Laptop Devices

Mobile Devices

General Servers and IT Services

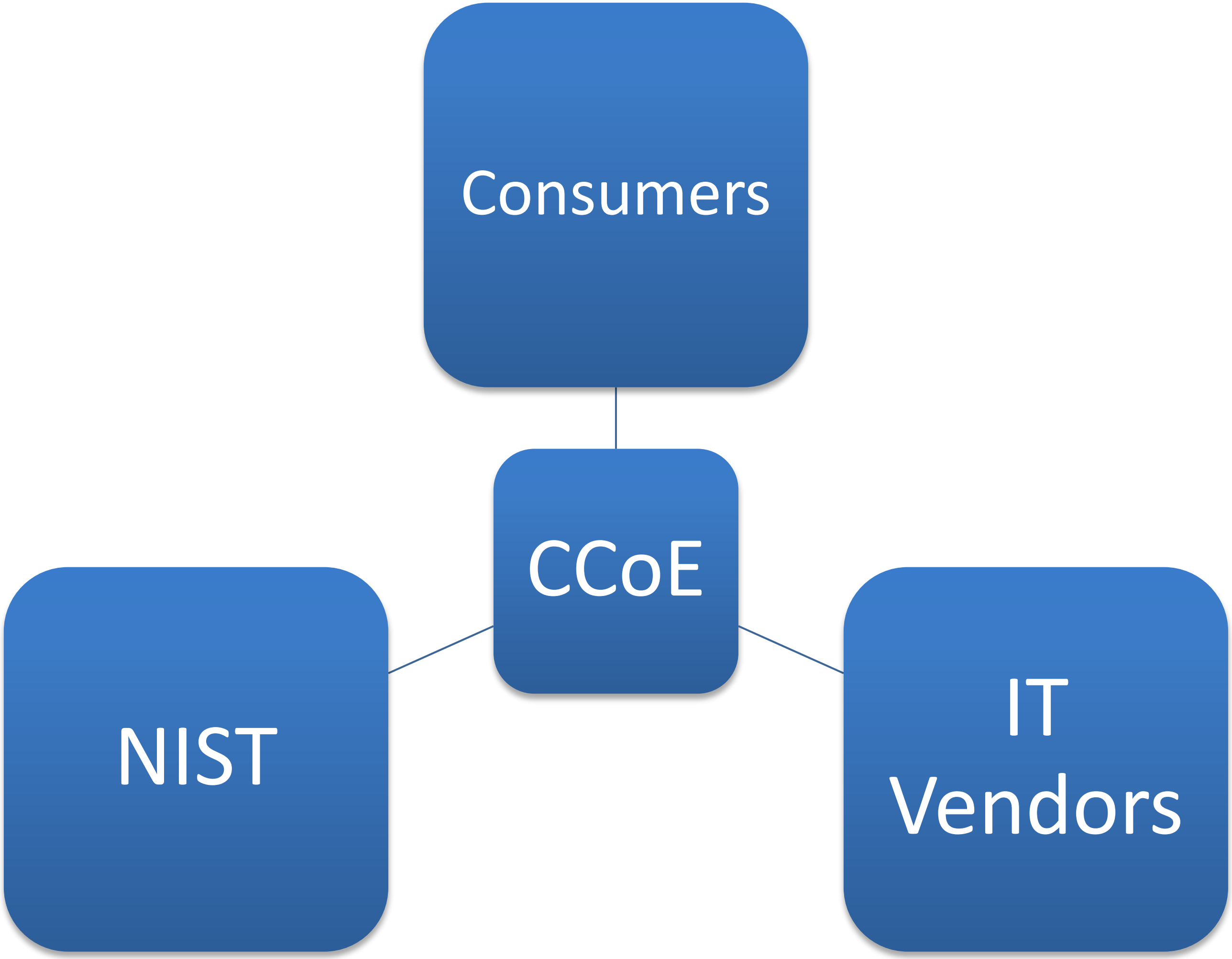
Sector Specific Policy and Compliance Framework (e.g., FISMA, HIPAA, PCI, SOX, etc.)

Device Management Lifecycle (e.g., Security Configuration Management)

Infrastructure (e.g., DNSSEC, IPv4/IPv6, PKI, Authentication/Authorization, etc.)

Hardware Root of Trust (e.g., BIOS, TPM, EPID, etc.)

Use Case Participants

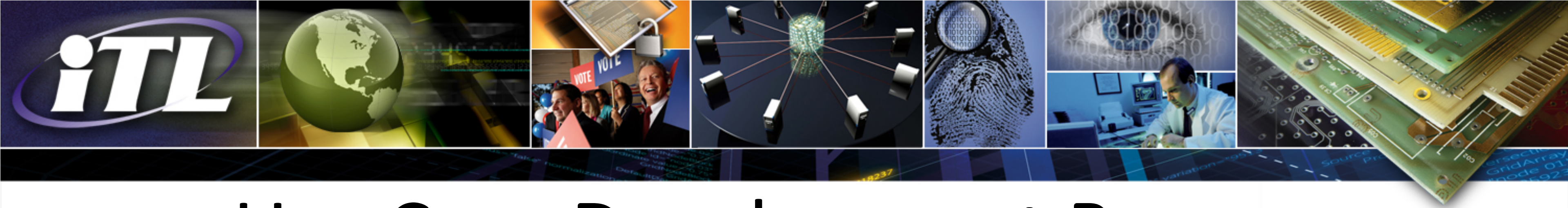


Consumers

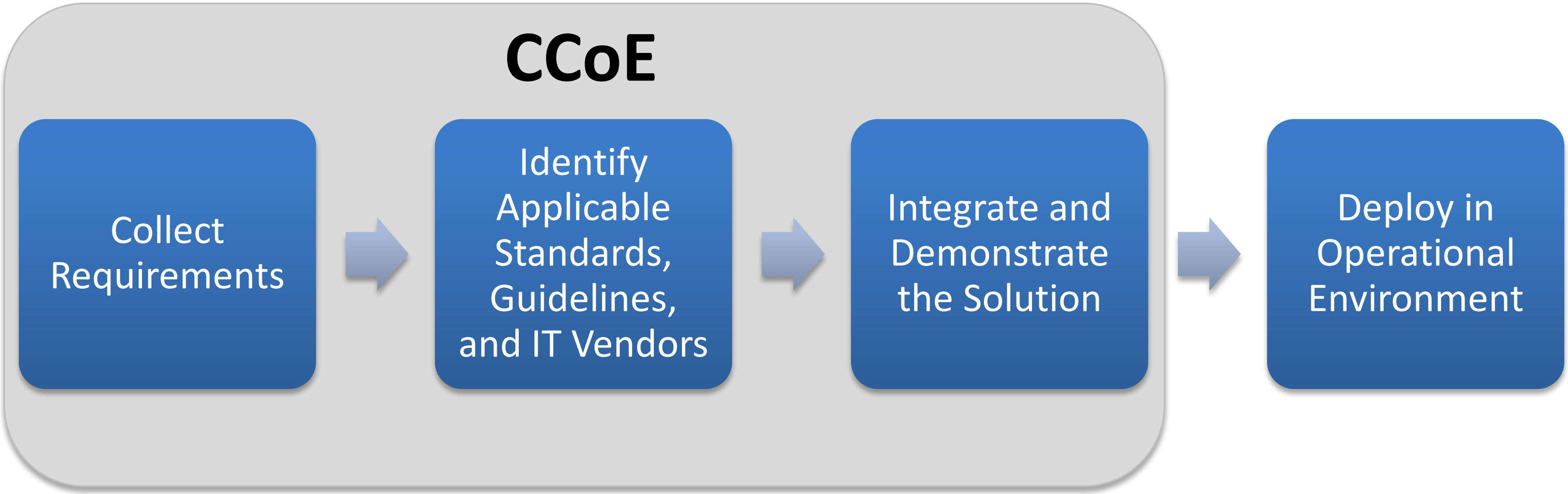
CCoE

NIST

IT Vendors



Use Case Development Process



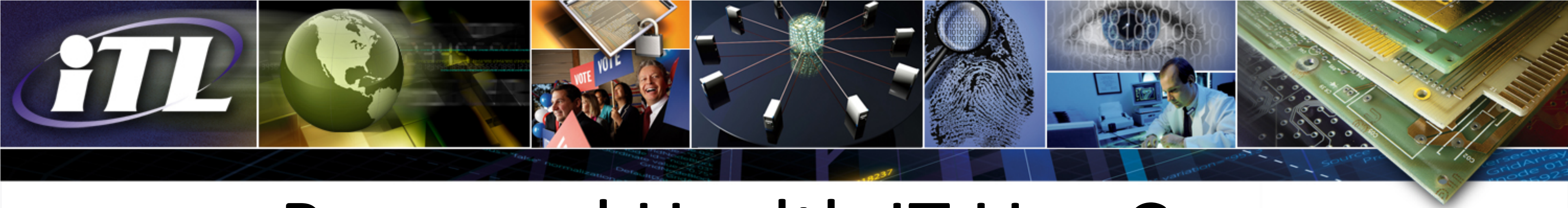
CCoE

Collect Requirements

Identify Applicable Standards, Guidelines, and IT Vendors

Integrate and Demonstrate the Solution

Deploy in Operational Environment



Proposed Health IT 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

IT Technology 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)