



# Requirements Traceability

## High Level Security Requirements

*Derived from Legislation, Executive Orders, Policies, Directives, Regulations, Standards*

**Examples: HIPAA, Graham-Leach-Bliley, Sarbanes-Oxley, FISMA, OMB Circular A-130**



**Security Controls  
FIPS 200 / SP 800-53**

**Security Controls  
FIPS 200 / SP 800-53**

**Security Controls  
FIPS 200 / SP 800-53**

***Enterprise #1***

***Enterprise #2***

***Enterprise #3***

*What set of security controls, if implemented within an information system and determined to be effective, can show compliance to a particular set of security requirements?*



# Involvement in HIPAA Security

## What are we doing?

- To provide an understandable and usable methodology for Health Business Managers and HIPAA Security Officers to apply real security, we are
  - Updating NIST Special Publication 800-66 (*An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005)
  - Developing a HIPAA-centric Risk Management Framework (RMF)
  - Developing a HIPAA Risk Assessment Assistance Guide
- To enable a baseline of “known security” to be established to foster trust relationships between systems/organizations, we are
  - Mapping HIPAA required and addressable implementation specifications to NIST SP 800-53 security controls
  - Producing SCAP\* content based on this mapping, which will allow for initial automation of HIPAA compliance validation and implementation of technical requirements
- - \* Security Content Automation Protocol (SCAP) – A joint initiative by NIST, NSA, and DISA that provides a public free repository of security content to be used for automating technical control compliance activities, vulnerability checking (both application misconfigurations and software flaws), and security measurement.



# Deliverables

## What will we deliver?

- Update NIST Special Publication 800-66
  - Develop a HIPAA-centric Risk Management Framework (RMF)
  - Develop a HIPAA Risk Assessment ( RA) assistance guide
  - Create SCAP content specific to HIPAA
  - Architectural design methodology for establishing an HIE

***Our focus is on technical implementation assistance of the Security Rule, not on Security Rule Policy!***