# NIST Role-based Training Guideline:  SP 800-16, Rev. 1

Mark Wilson, CISSP

Computer Security Division

National Institute of Standards and Technology

-  February 25, 2010  -

mark.wilson@nist.gov

(301) 975-3870 (voice)

http://csrc.nist.gov/

# Document Drivers

- Two Audiences: Information Security Professionals and Instructional Design Professionals

- "Harmonization" / "Transformation" Efforts:
  - NSA's CNSS training standards
  - DHS' Essential Body of Knowledge
  - OPM's 2210 Series Training Topics/Competencies/Behaviors
  - CIO Council's IT Workforce Committee (Matrix Project)
  - DOD's 8570 Training and Certification Program
  - ODNI's Cyber Training Subdirectory
  - ISS LOB Tier 2 Role-based Training Initiative
  - CNCI Cyber Education Efforts (Initiative 8 / "8-Plus")
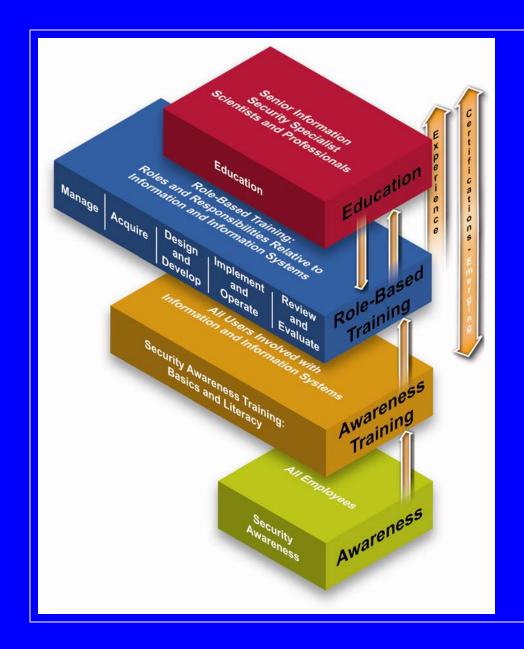
# Training Requirements Vs. Options

- Requirements:
  - Identify people with significant responsibilities for information security
  - Train them

- Options:
  - Number of roles to use
  - Build a course or module
  - Presentation mode (e.g., instructor-led, technology-based, incorporate avatars)
  - Order of content in course or module
  - Topics and elements

# The Rules

- Rule #1: Identify people with significant responsibility for information security

- Rule #2: Do not open SP 800-16, Rev. 1 until organization has identified people with significant responsibility for information security

- Rule #3: The list of roles in SP 800-16, Rev. 1 is a catalog; use what you need and do not use what you do not need

The "Learning Continuum" In Draft Special Publication 800-16, Rev. 1

# Awareness and Training Relationships

| Role-Based Training: CIO | Role-Based Training: SAISO | Role-Based Training: System Admin. | Role-Based Training: System Owner | Role-Based Training: Info. Owner | Role-Based Training: System Security Officer | ISS LOB Tier 2 Efforts |
|---|---|---|---|---|---|---|

**Information Security Awareness Training:  Basics and Literacy
Target Audience = All Users Of Information and Information Systems**

ISS LOB Tier 1 Efforts

**Information Security Awareness:  Target Audience = All Employees**
Posters, Lanyards, Badges, E-mail Advisories, Log-in Screen Warnings,
Computer Security Day, Trinkets, Newsletters, "Awards" from Mgmt.

# Draft Rev. 1 Key Thoughts/Goals

- Final document expected this FY
- SP 800-16, Rev. 1 to be supported by:
  – web-based "reference model" [on our CSRC]
  – 2 SOPs: information security professionals and instructional design professionals
- Eventual "Rev. 2" could be – should be?!?! – the product of the current harmonization/ transformation effort

# - Thank You -

Mark Wilson, CISSP

Computer Security Division

National Institute of Standards and Technology

mark.wilson@nist.gov

(301) 975-3870 (voice)