# Update of NIST SP 800-16

## "Information Security Training Requirements: A Role- and Performance-Based Model"

Mark Wilson, CISSP
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology (NIST)
mark.wilson@nist.gov
(301) 975-3870

- March 11, 2008 -

# Policy Drivers

- FISMA (Federal Information Security Management Act) [2002]
- OMB Circular A-130 Appendix III [2000]
- OMB Reporting Instructions for FISMA and Agency Privacy Mgmt. [Annually]
- OMB Memoranda [Ongoing]
- OPM 5 CFR Part 930 [June 2004]
- *Not NIST FIPS or SPs*

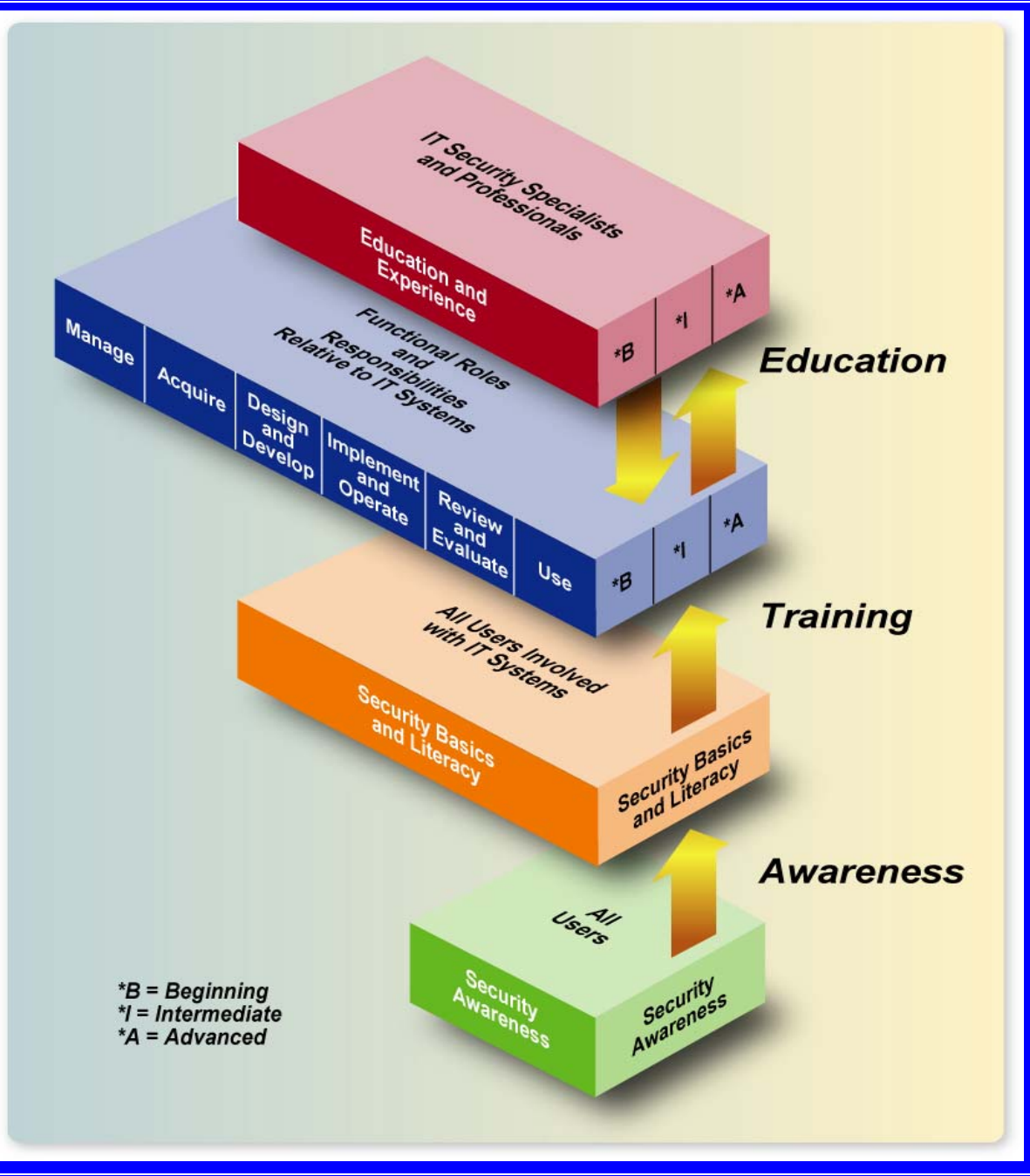
# Document Drivers

- "Harmonization" Efforts:
  - NSA's CNSS Training Standards
  - DHS' EBK
- NIST FISMA Implementation Project (Phase I) Documents
- OMB's ISS LOB Tier 2 Role-based Training Working Group

# Key Thoughts/Goals

- Document to be Slimmer (or not)
- To be Supported by Follow-on Web-based “Reference Model” [on CSRC]
- Initial Course Outline on Web = Baseline
- “Scoping Guidance” [From SP 800-53]
  - ADDIE Model
  - Needs Assessment
  - Job Task Analysis

# The NIST Model



# "Awareness" Versus "Awareness Training"

- **Current NIST Guidelines: Awareness Equals Awareness Training**
- **In SP 800-16, Rev. 1:**
  - **Awareness is Limited to . . .**
  - **Awareness Training Equals Basics and Literacy**
- **Impact of OMB's ISS LOB Tier 1 Awareness Training Initiative**

# Information Security Training Matrix

| Role: Information Owner | | | | | | |
|---|---|---|---|---|---|---|
| | | Responsibilities | | | | |
| Training Areas | Reference | A Manage | B Acquire | C Design & Develop | D Implement & Operate | E Review &Evaluate |
| **1. Laws & Regulations** | | **1A** | **1B** | **1C** | **1D** | **1E** |
| 1.1 Federal | Appendix | | | | | |
| 1.2 Departmental | Local | | | | | |
| 1.3 Agency/Bureau | Local | | | | | |
| **2. Security Program** | | **2.1A** | **2.1B** | **2.1C** | **2.1D** | **2.1E** |
| 2.1 Planning | SP 800-100 | ALL | | | | |
| | | **2.2A** | **2.2B** | **2.2C** | **2.2D** | **2.2E** |
| 2.2 Management | SP 800-100 | | | | ALL | |
| **3. System Life Cycle Security** | | | | | | |
| 3.1 Initiation | | **3.1A** | **3.1B** | **3.1C** | **3.1D** | **3.1E** |
| 3.1.1 Needs Determination | 800-100 (Ch 5) | 2,5,6,8,9 | 2,3,4,5, 6,9,10,12 | 2,3,4,5, 6,9 | | 2,3,4,5, 6,7,8,9, 10,11,12 |
| 3.1.2 Security Categorization | 800-60 FIPS 199 | | | | | |
| 3.1.3 Prelim. Risk Assessment | FIPS 199 800-100 (Ch 10,11) | | | | | |
| 3.1.4 Security Planning | 800-18 800-65 | | | | | |
| **3.2 Development/Acquisition** | | **3.2A** | **3.2B** | **3.2C** | **3.2D** | **3.2E** |
| 3.2.1 Requirements Analysis | 800-65 | 4,5,6, 7,8,9 | | | | 7,8,9, 10,12 |
| 3.2.2. Security Control Development | FIPS 200 800-53 | | | | | |
| 3.2.3 Developmental ST&E | 800-53A (M&O) | | | | | |
| 3.2.4 Risk Assessment | 800-30 800-100 (Ch 10,11) | | | | | |
| 3.2.5 Cost Considerations & Reports | 800-65 | | | | | |
| 3.2.6 Security Planning | 800-18 800-65 | | | | | |
| 3.2.7 Other Planning Components | ALL | | | | | |
| **3.3 Implementation/Assessment** | | 3.3A | **3.3B** | **3.3C** | **3.3D** | **3.3E** |
| 3.3.1 ST&E | 800-53A | 3,4,5,8, 9,10,12 | 9,10,12 | | | 3,4,6,8, 9,10,12 |
| 3.3.2 Inspection & Acceptance | Functional Specifications | | | | | |
| 3.3.3 System Integration/Installation | Config. Guide | | | | | |
| 3.3.4 Security Certification | 800-37 | | | | | |
| 3.3.5 Accreditation | 800-37 | | | | | |
| **3.4 Operations/Maintenance** | | 3.4A | **3.4B** | **3.4C** | **3.4D** | **3.4E** |
| 3.4.1 Configuration Management | 800-100 (Ch 14) | 4,5,8,9, 10,11,12 | 8,9,10, 12 | | | |
| 3.4.2 Continuous Monitoring | 800-53 800-53A 800-37 800-100 | | | | | |
| **3.5 Disposal** | | **3.5A** | **3.5B** | **3.5C** | **3.5D** | **3.5E** |
| 3.5.1 Information Preservation | Federal Departmental Agency | 1,5,6,7 | | | | |
| 3.5.2 Media Sanitization | | | | | | |
| 3.5.3 Hardware & Software Disposal | | | | | | |

# Risk Management Framework

FIPS 199 / SP 800-60

**Security Categorization**

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

**Security Control Selection**

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

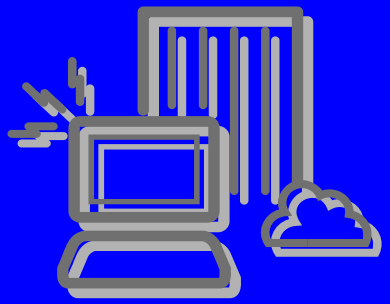
**Security Control Monitoring**

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

**Security Control Refinement**

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements



SP 800-37

**System Authorization**

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

**Security Control Documentation**

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

**Security Control Implementation**

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-37

**Security Control Assessment**

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

# Proposed Groupings of Job Functions in 800-16, Rev. 1

- **Job functions for *primary consideration*** – probably/possibly meeting FISMA and OPM "intent" of those having "significant responsibilities for information security"
- **Job functions for *secondary consideration*** – possibly, but not readily or usually identified as having . . .

# Primary Consideration

- Authorizing Official
- Certification Reviewer/Cert. Agent
- CIO
- IT Function Management
- IT Operations Personnel
- (Other) Security-Oriented Personnel
- Programmer/Systems Analyst
- Security Administrator

# Primary Consideration

- Auditor (Internal and External)
- Senior Agency Information Security Officer (or CISO / ISSM) (includes security staff)
- Program and Functional Managers
- Information Owner
- System Owner
- Data Center Manager
- Senior IRM Official
- Information System Security Officer

# Primary Consideration

- Information Resources Manager
- System Designer/Developer
- System Operations Personnel
- Technical Support Personnel
- Telecommunications Specialist
- Database Administrator
- System Administrator
- Network Administrator

# Secondary Consideration

- Freedom of Information Act Official
- Privacy Act Official
- Records Management Official
- Office of General Counsel Staff
- First Responders
- Contracting Officer
- COTR
- Source Selection Board Member

# Secondary Consideration

- User
  - If users receive exposure to security awareness material, should they also be trained? If so, how and to what depth? Basics and literacy?
  - Users with root access (Unix, XP, NT, Vista) – *uberusers* – are they "just" users or are they system administrators albeit "junior sysadmins" who should receive formal, role-based training?

# OPM 5 CFR Part 930 Says

- Train:
  - Executives
  - Program and Functional Managers
  - CIOs, IT Security Program Managers, Auditors, and Other Security-oriented Personnel
  - IT Function Management and Operations Personnel

# Caveats (Yeah, But . . .)

- No Departments/Agencies Will Identify All Roles as Having “Significant Responsibilities” (Wilson’s Bet)
- Organization Culture Must be Considered (see Job Task Analysis)
- Hybrid Courses/Roles Possible
- This Methodology is Flexible!!
- Add Your Own Detailed Information to Topics and Concepts

# Timeline

- Internal NIST Review: Oct. 2007
- Public Review and Comment: By @#$%^&*) 2008? (for how long?)
- Second Draft Public Review: TBD
- Publish Date: . . . FY2008 (or . . .)
- Then Begin Update of SP 800-50 "Building an IT Security Awareness and Training Program" [Pub. October 2003]

# NIST Free Resources

- Division Website: http://csrc.nist.gov/
  - Final and Draft Publications – FIPS, SPs, NISTIRs
  - Federal Agency Security Practices (FASP)
  - Federal Computer Security Program Managers' Forum (aka, The Forum)
  - National Vulnerability Database (NVD)
  - Federal Desktop Core Configuration (FDCC)
  - Security Content Automation Protocol (SCAP)
  - FISMA Implementation Project
  - Federal Information System Security Educators' Association (FISSEA)