FISMA and OPM Awareness and Training Requirements and Related NIST Guidelines

Mark Wilson, CISSP

Computer Security Division, ITL

National Institute of Standards and Technology

- March 12, 2007 -

mark.wilson@nist.gov

(301) 975-3870

http://csrc.nist.gov/

NIST

NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's primary mission is to promote economic growth by working with industry to develop and apply technology, measurements, and standards.

NIST carries out its mission through a portfolio of four programs:

Measurement and Standards Laboratories provides technical leadership for the Nation's measurement and standards infrastructure, and assures the availability of essential reference data and measurement capabilities

Advanced Technology Program stimulates U.S. economic growth by developing high risk and enabling technologies through industry-driven cost-shared partnerships

Manufacturing Extension Partnership strengthens the global competitiveness of smaller U.S.-based manufacturing firms by assisting in the adoption of advanced technologies, techniques, and business practices

National Quality Program enhances U.S. competitiveness, quality, and productivity, manages the Malcolm Baldrige National Quality Award, and provides global leadership in promoting quality awareness

Today's Menu . . .

- FISMA awareness and training requirements
- OPM awareness and training requirements
- NIST SP 800-50 highlights
- NIST SP 800-16 highlights
- Possible changes to SP 800-16
- NIST SP 800-53 awareness and training (AT) control family

FISMA Says . . .

- Agencywide information security program shall include . . . ***security awareness training to inform personnel, including contractors, and other users of information systems*** . . . of information security risks . . . and their responsibilities in complying with agency policies and procedures . . .

NIST SP 800-50 Says . . .

- “Users” does not mean only employees
- Users Include:
  - Employees
  - Contractors
  - Foreign or domestic guest researchers
  - Other agency personnel
  - Visitors
  - Guests
  - Other collaborators or associates requiring access

FISMA Says . . .

- The head of each agency shall . . . delegate to the agency Chief Information Officer . . . training and overseeing personnel with ***significant responsibilities for information security*** . . .

NIST Says . . .

Who has significant responsibilities?
Each agency must determine, but:

- CIO
- SAISO/CISO and Security Staff
- System Owners
- Information Owners
- Network Administrators
- System Administrators
- Security Administrators

. . . will usually be identified

FISMA: Train People with Significant Responsibilities . . .

What about contractors? The FAR says:

- "*Have the necessary organization, experience . . . and technical controls, or the ability to obtain them* . . ."
- "*Be otherwise qualified and eligible* . . ."
- Allowable cost: "*Costs of training and education that are related to the field in which the employee (e.g., contractor's employee) is working* . . ."
- Savvy contracting specialist: "*Yes, the contractor personnel should show up trained to perform the requirements of the contract*."

OPM (June 2004) Says . . .

- Develop awareness and training plan
- All users of federal information systems must be exposed to awareness materials at least annually
- Identify employees with significant information security responsibilities and provide role-specific training in accordance with NIST standards and guidance

NIST SP 800-50 Says . . .

- Conduct needs assessment
- Develop awareness and training plan
- Entire workforce should be exposed to awareness material annually
- A continuous awareness program, using various methods of delivery throughout the year, can be very effective
- Identify employees with significant information security responsibilities

OPM Also Says . . .

Train

- Executives
- Program and functional managers
- CIOs, IT security program managers, auditors, and other security oriented personnel (e.g., system and network administrators, and system/ application security officers)
- IT function management and operations personnel

NIST SP 800-50 Says . . .

- Sources of training courses and material: use existing courses/material, develop in-house, contract out?
- Off-the-shelf suitable or customize
- Maximize partnerships with agency training function, with other agencies
- Use the training methodology in NIST SP 800-16 to build courses

Training Programs Derive from . . .

FISMA Requirements

NIST Materials
(Special Publication 800 Series and Federal Information Processing Standards)

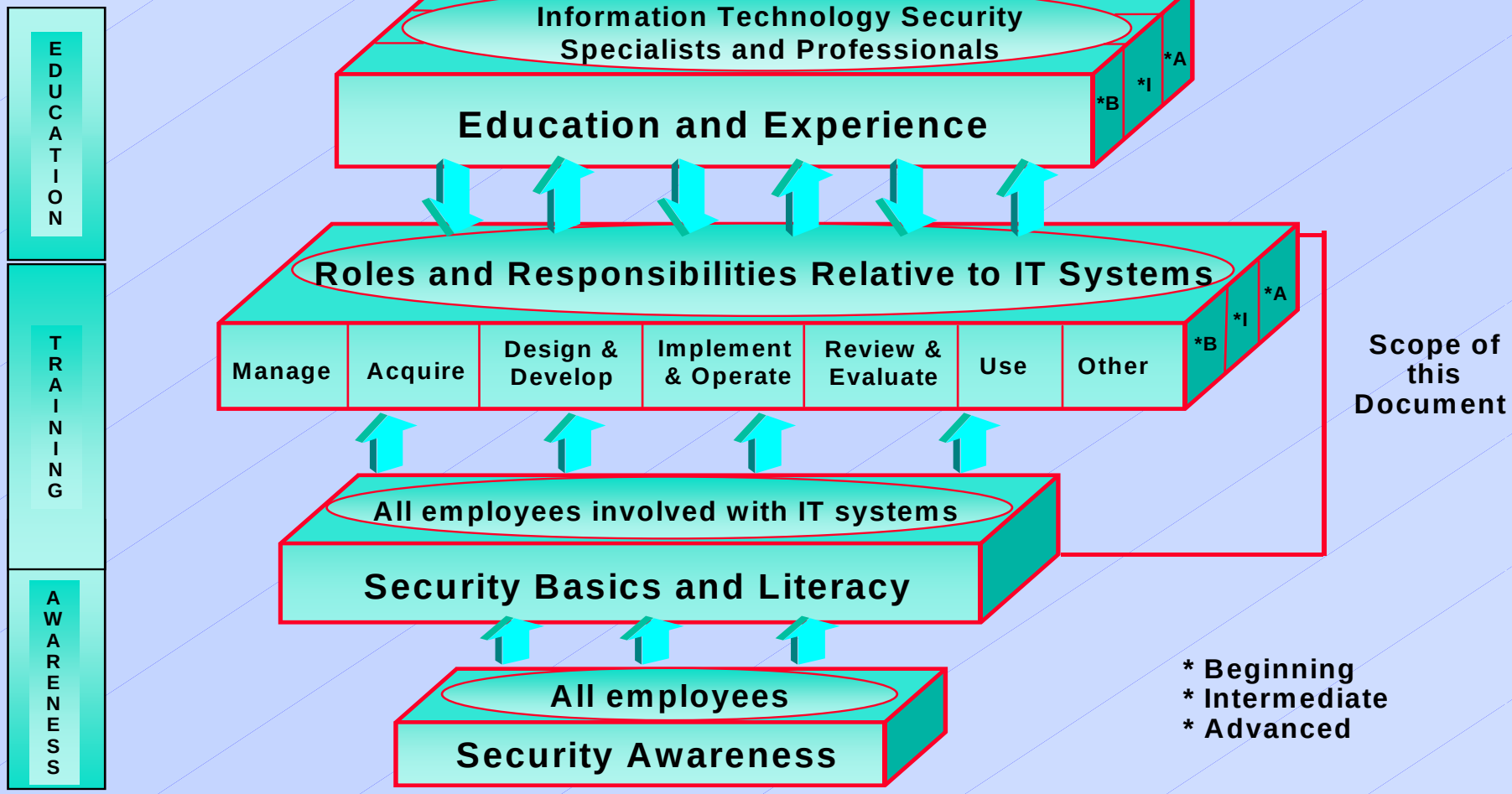
Information Security Body of Knowledge

Agency Policy & Procedures

SP 800-16 Background

- Published in April 1998
- Written in mid-1990s
- Written by a FISSEA workgroup
- Pre-FISMA
- Pre-OPM 2004 requirements
- Language is dated

The NIST Model



“NIST Model” Highlights

Learning Continuum

- Awareness
- Training
- Education

Basics and Literacy

- Bridge between awareness and training
- ***Does this help you?***

IT Security Training Matrix

TRAINING AREAS	FUNCTIONAL SPECIALTIES						
	A MANAGE	B ACQUIRE	C DESIGN & DEVELOP	D IMPLEMENT & OPERATE	E REVIEW & EVALUATE	F USE	G OTHER
1 LAWS & REGULATIONS	1A	1B	1C	1D	1E	1F	
2 SECURITY PROGRAM							
2.1 PLANNING	2.1A	2.1B	2.1C	2.1D	2.1E		
2.2 MANAGEMENT	2.2A	2.2B	2.2C	2.2D	2.2E		
3 SYSTEM LIFE CYCLE SECURITY							
3.1 INITIATION	3.1A	3.1B	3.1C		3.1E	3.1F	
3.2 DEVELOPMENT	3.2A	3.2B	3.2C	3.2D	3.2E	3.2F	
3.3 TEST & EVALUATION			3.3C	3.3D	3.3E	3.3F	
3.4 IMPLEMENTATION	3.4A	3.4B	3.4C	3.4D	3.4E	3.4F	
3.5 OPERATIONS	3.5A	3.5B	3.5C	3.5D	3.5E	3.5F	
3.6 TERMINATION	3.6A			3.6D	3.6E		
4 OTHER							

Six Functional Specialties (Roles)

Manage

Acquire

Design & Develop

Implement & Operate

Review & Evaluate

Use

Do these work for you?

Three Fundamental Training Content Categories

Laws and Regulations

The IT Security Program

System Life Cycle Security

Changes . . . ?

Role-Based Training: 26 Job Functions

- Auditor, External
- Auditor, Internal
- Certification Reviewer
- Chief Information Officer (CIO)
- Contracting Officer
- Contracting Officer's Technical Representative (COTR)
- Data Center Manager
- Database Administrator
- Designated Approving Authority (DAA)
- Freedom of Information Act Official
- Senior IRM Official
- Information Resources Manager
- IT Security Program Officer/Manager
- Network Administrator
- Privacy Act Official
- Program Manager
- Programmer/Systems Analyst
- Records Management Official
- Source Selection Board Member
- System Administrator
- System Designer/Developer
- System Owner
- Systems Operations Personnel
- Technical Support Personnel
- Telecommunications Specialist
- User

Role-Based Training: 26 Job Functions

Too many job functions?

- Combine Internal and External Auditor
- Who has trained a Freedom of Information Act Official?

Any missing job functions?

- Law enforcement officials
- First responders
- Office of General Counsel

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

- Certification Reviewer/Cert. Agent
- CIO
- Contracting Officer
- COTR
- IT Function Management
- IT Operations Personnel
- (Other) Security-Oriented Personnel

Primary Consideration

- Authorizing Official
- Senior Agency Information Security Officer (includes security staff)
- Program and Functional Managers
- Information Owner
- System Owner

Secondary Consideration

- Freedom of Information Act Official
- Privacy Act Official
- Records Management Official
- Office of General Counsel Staff
- First Responders
- Contracting Officer

Secondary Consideration

- COTR
- Source Selection Board Member
- 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?

Semantics, Schemantics

- In SP 800-16:
  - "Job function" = titles like CIO, auditor, system administrator, COTR, etc.
  - "Role" = functional specialties like manage, acquire, design and develop, implement and operate, etc.

Semantics, Schemantics

- Does this work:
  - "Role" = "job function" = titles like CIO, auditor, system administrator, etc.
  - Are we using "role" and "job function" interchangeably?
  - "Responsibilities" = manage, acquire, etc.
  - Does this map better to "roles and responsibilities" as we usually use the words?

Information Security Body of Knowledge Topics and Concepts – Currently in SP 800-16

- Laws and Regulations
- IT Security Program
- System Environment
- System Interconnection
- Information Sharing
- Sensitivity
- Risk Management
- Management Controls
- Acquisition/ Development/ Installation/ Implementation Controls
- Operational Controls
- Awareness, Training, and Education Controls
- Technical Controls

Information Security Body of Knowledge Topics and Concepts - Proposed

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Topics and Concepts

- Currently 12 topics and concepts
- Proposed 17 topics and concepts - these map to the 17 families of controls in NIST SP 800-53
- Plus several of the original 12 that are not system-level, control-focused:
  - Laws and Regulations
  - Information Security Program

IT Security Training Matrix

TRAINING AREAS	FUNCTIONAL SPECIALTIES						
	A MANAGE	B ACQUIRE	C DESIGN & DEVELOP	D IMPLEMENT & OPERATE	E REVIEW & EVALUATE	F USE	G OTHER
1 LAWS & REGULATIONS	1A	1B	1C	1D	1E	1F	
2 SECURITY PROGRAM							
2.1 PLANNING	2.1A	2.1B	2.1C	2.1D	2.1E		
2.2 MANAGEMENT	2.2A	2.2B	2.2C	2.2D	2.2E		
3 SYSTEM LIFE CYCLE SECURITY							
3.1 INITIATION	3.1A	3.1B	3.1C		3.1E	3.1F	
3.2 DEVELOPMENT	3.2A	3.2B	3.2C	3.2D	3.2E	3.2F	
3.3 TEST & EVALUATION			3.3C	3.3D	3.3E	3.3F	
3.4 IMPLEMENTATION	3.4A	3.4B	3.4C	3.4D	3.4E	3.4F	
3.5 OPERATIONS	3.5A	3.5B	3.5C	3.5D	3.5E	3.5F	
3.6 TERMINATION	3.6A			3.6D	3.6E		
4 OTHER							

. . . And NIST SP 800-53

- 1 of 17 control families address awareness and training (AT)
- 4 controls in the AT family
  - AT1: Security Awareness and Training Policy and Procedures
  - AT2: Security Awareness
  - AT3: Security Training
  - AT4: Security Training Records

Questions? Comments?

- Thank You -

Mark Wilson, CISSP

Computer Security Division, ITL

National Institute of Standards and Technology

- March 12, 2007 -

mark.wilson@nist.gov

(301) 975-3870 (voice)