SP 800-16 Update Project

FISSEA Conference
March 19, 2013

Pat Toth

Computer Security Division
Information Technology Laboratory

Background

- NIST SP 800-16 *"Information Technology Security Training Requirements: A Role- and Performance-Based Model"* April 1998

- NIST SP 800-16 Rev 1 DRAFT March 2009

Driving Forces

- Roles and responsibilities have greatly expanded
- Security roles, responsibilities, skills, and competencies for the federal cybersecurity workforce

Purpose

- Provide a comprehensive methodology for the development of training modules for roles identified as having significant information security responsibilities

Approach

- Landscape Analysis
- Draft Development
- Final Publication

Landscape Analysis

- Federal frameworks, models, publications, and policies intended to help agencies define roles, responsibilities, skills, and competencies for cybersecurity workforce
- Included:
  - SP 800-16
  - SP 800-16 Rev 1 Draft
  - SP 800-53
  - SP 800-37
  - SP 800-50
  - CIO Council Workforce Development Matrix Resource Guide
  - OPM Regulation 5 CFR 930 “Information Security Responsibilities for Employees Who Manage or Use Information Systems”
  - NICE Cybersecurity Framework
  - OMB A-130
  - OPM Competency Model for Cybersecurity
  - Committee on National Security Systems
  - DHS Essential Body of Knowledge
  - DOD Directive 8570
  - ODNI Cyber Training Subdirectory

Draft Development

- Internal Working Draft March 2013
- Internal Review April 2013
- Public Review and Comment June 2013

Internal Working Draft

- Competencies
  - Basic Knowledge
  - Advanced Network Technology and Protocols
  - Architecture
  - Compliance
  - Computer Network Defense
  - Configuration Management
  - Crypto and Encryption
  - Data Security
  - Database
  - Digital Forensics
  - Emerging Technologies
  - Enterprise Continuity
  - Identity Management/Privacy
  - Incident Management
  - Industrial Control Systems
  - Information Assurance
  - Web Security
  - Information Systems
  - IT Operations and IT Systems
  - IT Security Awareness and Training
  - Management
  - Modeling and Simulation
  - Network and Telecommunications Security
  - Personnel Security
  - Physical and Environmental Security
  - Procurement
  - Security Risk Management
  - Software
  - Systems and Application Security

KSA Example
Data Security

CPM-6 Skill in analyzing network traffic capacity and performance characteristics
DM-2 Knowledge of data administration and data standardization policies and standards
DM-3 Knowledge of data mining and data warehousing principles
DM-4 Knowledge of sources, characteristics, and uses of the organization's data assets
DM-5 Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information
DM-6 Knowledge of the characteristics of physical and virtual data storage media
DM-7 Skill in developing data dictionaries
DM-8 Skill in developing data repositories
DM-9 Skill in data mining techniques
DM-10 Knowledge of database theory
DM- 11 Skill in data reduction
DM-13 Ability to interpret and incorporate data from multiple tool sources
OT-1 Knowledge of complex data structures
OT-2 Knowledge of computer programming principles such as object-oriented design
OT-3 Skill in Data Loss Prevention technologies (DLP)

Sample Curriculum Models for Roles

Function Area: Operate and Maintain
Role Area: Data Administration

Roles:

- Data Security Analysis
- Data Management Systems Security
- Data Administrator
- Database Administrator

Responsibility — Develop and administer databases and/or data management systems that allow for the storage, query, and utilization of data.

Knowledge Unit:

- Data Security
- Digital Forensics
- Database
- Cryptography and Encryption
- Architecture
- Identity Management / Privacy
- Information Systems
- Modeling and Simulation
- Incident Management

Knowledge Unit

Data Security

- Manage
  - DM-2
  - DM-10
- Design
  - DM-3
  - DM-4
  - DM-7
  - DM-8
  - OT-1
  - OT-2
  - DM-5
- Implement
  - DM-5
  - DM-6
  - DM-9
- Evaluate
  - CPM-6
  - DM-11
  - DM-13
  - OT-3

Participate

Public Review and Comment

May 2013

– Send e-mail to ptoth@nist.gov

– Watch for announcement on www.csrc.nist.gov

Contact Information

Pat Toth
(301) 975-5140
patricia.toth@nist.gov