FISSEA WORKSHOP:
Developing Role-Based Training for Managers and System Administrators
September 25, 2003

In a small-group exercise, workshop participants developed training solutions for the role-based tasks defined in NIST SP 800-16. Six tasks were selected from the cells in the IT Security Training Matrix in 800-16: three from the A column (Manage) and three from the D column (Implement and Operate).

Participants in each group identified learning objective, presentation mode(s), individual or group learning/practice activity, and learning measurement strategy for the assigned task. The training solution was summarized for presentation to the group.

The summary information for each training solution follows:

MANAGER TASKS
CELL 1A Laws and Regulations

Objective:

- At end, managers will be able to identify key IA federal laws and regulations and directives pertaining to managerial responsibilities.

Presentation Mode:

- Instructor led training
  - Focus on key requirements (and identify the mandate)
  - Consequences (benefits/adverse impacts)

Practice Activity:

- Presentation of scenarios for discussion (e.g. Is Hurricane Isabel covered under regulations?)

Learning Measurement Strategy:

- Identify areas where they might be weak in meeting requirements and what they will do in response.

MANAGERS TASKS
CELL 3.1A System Life Cycle Security: Initiation

Training Area:

- Manager system life cycle

Objective:

- The manager will recognize the need for and benefits of security planning at the <u>“beginning”</u> of the system life cycle.

Target:

- FGA-Department Program Manager – “Line of Business”

Method:

- ILT- Instructor led training
- 2-hour module including practical exercises (scenario basis including Federal regulations, and risk matrix –HML)
- Materials to include handouts and overhead slides

K, S, & “A”:

- Why?
    - Legal
    - Business Impact

Measurement:

- Undefined

SYSTEM ADMINISTRATOR (Level 2)
CELL 3.3D System Life Cycle Security: Test and Evaluation

Learning Objectives:

- Conduct tests; assess performance and operations of security controls and safeguards.

Presentation Mode:

- Illustrated lecture training – instructor explains the objectives
- Hands-on demonstration
- Individual training

Learning Strategy:

- Inform of test plan and procedures.
- Means to conduct the test.

Learning Measurement:

- Group: Compare class solution against student results.
- Individual: Students report back with results.

SYSTEM ADMINISTRATOR
CELL 3.4D System Life Cycle Security: Implementation

Learning Objectives:

- Describe the major DSS vulnerabilities and how to harden IIS against attacks.

Presentation Mode:

- Lecture training
- Computer practice or simulation
- Handouts, quick reference cards
- Demonstrations

Learning Strategy/Measurement:

- Small group exercises.
- Students will describe how to apply safeguards against assigned vulnerabilities.

SYSTEM ADMINISTRATOR (Beginning Level)
Cell 3.6D: Systems Life Cycle: Archiving and Termination

Learning Objectives:

- Define a termination plan

- List the steps to properly archive or dispose of assets (unclassified)

Presentation Mode:

- Illustrated lecture – instructor explains the objectives

- Hands-on demonstration with actual equipment (hard drive, degausser, utility to verify that material has been removed).

Individual Learning Activity:

- Students follow the steps in the process to degauss a hard drive and verify the results.

Learning Measurement:

- Results of hands-on learning activity:

- Did the student correctly: define a termination plan, follow the procedures for degaussing a hard drive, and use the verification utility?

MANAGER TASKS
CELL 3.6E Termination

Assumptions:

- High Level Managers with limited time
- Working with sensitive/unclassified systems
- Termination plan is available (from SLC)

Learning Objectives:

- Be familiar with retirement requirements both legal and operational
- Where to find a checklist
- Know resources needed to retire system and augment if necessary
- Verify sanitization-software/hardware
- Know archival requirements

Presentation Mode:

- One on one Instruction
  - Written resources
  - SISOP present
  - ISSO present

- Unique in terms of briefing for individual requirements

Practice Activity:

- Case study with scenarios tailored to the organization
- Question and answer session

Evaluation:

- Short term:
  - Does retirement of system happen?

- Long Term:
  - No adverse outcomes
  - Not in the news
  - Audit agencies are satisfied
  - External IG paper trail