TECHNOLOGY ★ COLLABORATION ★ EDUCATION
OI&T
NATIONAL IT TRAINING ACADEMY

# How Information Security Competency Models Drive Security Integration

Terri Cinnamon
VA OI&T, Director National IT Training Academy

March 24, 2010

# Compliance is Key

- FISMA requires agency personnel with significant security responsibilities to receive role-based training
- To be compliant with FISMA, NIST mandated that agencies implement role-based security training
- Government agencies categorize staff by positions, not roles
- Agencies must determine a process to match role-based security criteria to their positions

# Implementation of Roles at VA

- Match occupational codes in VA’s HR PAID system to roles defined by NIST
- The Learning Management System (LMS) “pushes” the right course to the right security professional utilizing competency models based upon GS 2210 positions that are mapped to specific training events

# VA Competency Model Advances Security Efforts

- Security knowledge traverses numerous core competencies
- Each competency identifies proficiency levels utilizing behavioral indicators
- All training is mapped to competencies at specific proficiency levels
- Aligning security competencies to learning events ensures staff receives proper role-based training

# Tracking Compliance

- Competency modeling provides a means to assign and track training
- VA utilizes its Learning Management System (LMS) to track this training
- LMS provides tracking and report creation to monitor training progress and verify training requirements are met

# VA’s Benefits from Competency Models

- Training is developed and assigned consistent with the requirements for role-based training
- Responsible spending of training funding because the right training is assigned to the right staff members
- The LMS tracks training progress and has reporting capabilities which enables VA to provide proof of completion
- IG approved ISO Security Training