# Department of Veterans Affairs Role-Based Training: Information Security Toolkit for Managers

FISSEA
March 2009

Rosa Ayer

# VA is customer-service oriented and delivers a wide range of products and services to meet diverse needs

▶ External customers

- Veterans and their families
- DoD services and other federal agencies
- Universities and other research entities

▶ Internal customers

- Information Protection & Risk Management (IPRM)
- Office of Information & Technology (OI&T)
- The Administrations (VHA, VBA, NCA)
- Secretarial Staff and Program Offices

# Mission: Playbook

▸ *FISMA* states that agency wide Information Security programs are required and shall include "security awareness *training*

▸ *NIST SP 800-50* (2003): Building an *Information* Technology *Security* Awareness and *Training* Program

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

▸ *VA Directive 6500* requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems

# The VA OI&T Training Education Awareness Professionalization (TEAP) Mission:

▸ Continuous training of all Office of Information and Technology (OI&T) workforce on current IT topics

▸ Develop a highly skilled and motivated OI&T workforce

▸ Professionalize OI&T staff through training and certification programs

# VA is implementing 37 training & awareness projects to support our IT Strategic Plan, reduce risk, and comply with FISMA

| LMS Competency Model | Role-Based Training | Awareness Campaign |
|---|---|---|
| - Information Security Officers<br><br>- Chief Information Officers<br><br>- IT Staff<br><br>- GS 2210 specialties | - Law Enforcement<br><br>- Facilities Managers<br><br>- Software Developers<br><br>- Records Management | - Annual courses for security and privacy<br><br>- Multi-media: posters, newsletters, handouts, videos<br><br>- Computer Security Day |
| CSP 100 (versions 2 & 3) | ePO 4 WBT | ePO 4 ILT |
| Certification Program (CISSP, Net+, Sec+) | Rescue Users WBT | Rescue Administrators  ILT |
| CIO and Privacy Professionalization | Regional Training Centers | IP Portal |
| CBTs: ISA, PIA, FISMA, FOIA | **Toolkit for Managers** | and 17 other projects |

# Information Security Brown Bag Series

**2009 Brown Bag Series Topics**

- JAN    **Data Leakage Through Peer to Peer Networks**
- FEB    **FISMA Changes for 2009**
- MAR    **Social Security Number (SSN) Reduction**
- APR    **Software Assurance**
- MAY    **Voice Over Internet Protocol (VoIP)**
- JUNE   **Wireless Security**
- JULY   **Cybercrimes/ Hacking**
- AUG    **Federal Desktop Core Configuration (FDCC)**
- SEPT   **Personally Identifiable Information (PII)**
- OCT    **Phishing Statistics**
- NOV    **Security Content Automation Protocol (SCAP)**
- DEC    **Cloud Computing/ Virtualization Security**

- Strengthens the competencies of OI&T personnel by providing a monthly, brown bag series on hot security and operations topics

- Delivered as a 50 minute presentation, utilizing Windows Live Meeting and VANTS teleconference lines

- Complements IPRM's initiatives in creating and executing current Workforce Development and Professionalization programs

- Provides OI&T personnel, who wish to add these courses into their learning development plan, with awareness credit

**The needs of the workforce require a broader and deeper program with aggressive timelines to fill gaps in worker's knowledge and skills and achieve the IT Strategic Goals**

▸ More certifications

▸ More WBTs

▸ More Role-Based training courses

▸ Expanded Competency Model to include all job specialties of 2210

▸ Expanded Regional Training Centers

▸ Expanded CIO Professionalization to include CAP certification and coaching and mentoring

▸ Additional tools and resources, e.g., Managers Toolkit

# We provide multi-media rich programs and services to support the VA workforce in meeting their security responsibilities

▸ : Over 25 Web-based security courses are offered via the LMS

▸ Communicate via IP portal and various conference calls, workgroups, etc.

▸ Provide instructor-led training

– Regional Training Center-Hub: Falling Waters

– LiveMeeting

– Satellite broadcasts

– InfoSec and other conferences venues

– IT Info. Protect. Certification Program by providing vouchers for industry certifications: CISSP (182), Network + (50), Security + (25)

# Role-Based Training

Today - Phase I

▸ Four roles were identified:
- – Executives
- – IT Project Managers (Program and Functional Managers)
- – Chief Information Officers (CIOs)
- – IT Specialists

**Total Personnel Trained 16,900+**

# Role-Based Training

Today - Phase II

▸ 201 IT Project Managers

▸ 201 Executives and Chief Information Officers

▸ 201 IT Acquisition Staff

▸ 201 Research and Development Staff

▸ 201 series courses were released to the field April 15, 2008

▸ **9,900 trained as of Sept 2008**

▸ 301 IT Project Managers

▸ 301 Health Care Providers

▸ 301 Human Resources Staff

▸ 301 Software Developers

▸ 301 courses to be released 2Q 2009

▸ **Target audience of 22,000 employees**

# Role-Based Training

<span style="color:blue">In Development - Phase II</span>

▸ 401 Law Enforcement

▸ 401 Facilities Managers

▸ 401 Software Developers

▸ 401 Records Management

▸ 401 courses to be released 4Q 2009

▸ **Target audience 22,000 employees**

# Information Security Toolkit for Managers

# Toolkit for Managers Project Background

Supports **executives, program/project managers, facility CIOs,** and others in supervisory roles in the understanding and implementation of VA's Information Security policies and procedures

**POLICY**

- VA Directive 6500
- FISMA
- OMB Directive A-130
- HSPD-12
- HIPAA
- Other Federal Laws (Clinger-Cohen, GRPA, etc.)

**VA INFORMATION SECURITY TOOLKIT** *for Managers*

**GUIDANCE**

- VA Directive 6500 Handbook
- VA IT Strategic Plan
- NIST SP 800-series
- GAO Reports
- IG findings and recommendations

**VA EXECUTIVES, PROGRAM / PROJECT MANAGERS, FACILITY CIOS**

**INFORMATION SECURITY PROGRAM IMPLEMENTATION ACROSS VA**

# *Why do Senior Managers need the Toolkit?*

▸ **Excellence in veteran care and services**:  We must ensure that our medical professionals, benefits administrators, and staff have accessibility to the information they need to continue providing excellent service to Veterans and their families.  At the same time, the privacy and security of veteran medical and personal data must be protected.  The Toolkit helps managers make risk-based decisions that balance service accessibility and information protection.

▸ **Information security starts at the top**:  Senior managers are ultimately accountable for security processes employed (or not employed) on their projects, by their employees, and within their organizations.  The Toolkit outlines senior management security responsibilities in a format that is concise, engaging, and focused on results.

▸ **Individual performance drives enterprise performance**: VA can only improve its FISMA score and overall security posture when managers step up to lead the charge.  The Toolkit provides practical guidance that addresses management challenges faced by VA leaders

# *What makes the Toolkit unique?*

▶ **Business-driven**: Information security is more than an IT problem, it is a business issue.  The Toolkit focuses on integrating information security practices into the daily project management tasks that managers perform to run their business.

▶ **Information Security Knowledge at Your Fingertips**:  The portability of these  training materials allow managers to keep information security references readily available while performing their duties.

# How is the Toolkit tied to VA's mission?

▸ **Seamless Service to our Veterans:** Part of achieving seamless service to our veterans is ensuring the confidentiality, integrity, and accessibility of the information entrusted to us. The Toolkit empowers managers to lead the charge in implementing measures that safeguard veteran data and motivates them to promote information security best practices across their organization.

▸ **Making VA a 21st century organization:** The president has made it clear that VA needs to modernize in order to meet the growing needs of a new generation of veterans. The Toolkit reminds managers that information security needs to be a consideration during the planning, design, development, and maintenance of these efforts.

# Project Scope

Phase 1: Production of Toolkit Training Products, Job Aids, and Checklists

| Toolkit Training Products | |
|---|---|
| **Training Component** | Security Tutorial for Managers presented in a 3-ring binder |
| **Job Aids (3)** | Security Calendar of Events; Visual 'folding cube' with 9 graphics; Quick Reference Desk Set |
| **Checklists** | Security Checklist Pocket Guide for Managers |
| **Supporting Items** | Pen/highlighter combo for note-taking |
| **Packaging** | Custom, reusable computer/brief bag |

Phase 2: Continued Training through Workshops and Web-based Courses

- Two workshops: Falling Waters and INFOSEC 2009
- Web-based courses deployed on VA Learning Management System
- Support CIO competency model and workforce development

# Toolkit Topics

**What do VA managers need to know?**

▸ **Policy:** Laws Are the Basis for Core Program Elements

▸ **Enterprise Security:** Filling the Gaps Across VA

▸ **Risk Management:** Securing VA's Mission and Operations

▸ **Capital Planning:** Budgeting for the Total Solution

▸ **Performance Measures:** Improving Performance Over Time

▸ **Critical Factors for Success:** Leading by Example

# Toolkit Product: Tutorial

The **Tutorial** is the main training component of the Toolkit and provides managers with a reference of **information security policy, procedures, processes, and best practices** to support consistent implementation of VA's Information Security program across the agency.

The tutorial also has the following features:

▸ <u>Manager's Challenge</u>: Common risks that managers face and practical solutions

▸ <u>Keys to Success</u>: Best practices in information security management

▸ <u>Spotlight On</u>: Special topics related to information security issues

▸ <u>Key Players</u>: Roles and responsibilities of critical personnel

▸ <u>Case Studies</u>: Highlights of successes and lessons learned in information security

Product Specifications

- 3-ring binder
- Approximately 200 pages
- Full color graphics
- Dimensions: 5.5 x 8.5 inches

# Toolkit Product: Calendar

The **Calendar** includes dates for performing enterprise-wide information security activities (such as POA&M remediation), completing quarterly and annual FISMA data collection activities, and submitting information security reports.

The calendar also has the following features:

- Monthly Awareness Messages: The left-hand page of the calendar highlights an information security topic of the month.

- Notes: Space is provided for managers to write notes and reminders

- Holidays and Pay Schedule:  Federal holidays, VA pay days, and military days of remembrance are also captured in the calendar.

Product Specifications

- Portrait notebook calendar
- Information Security awareness messages on the left
- Calendar entries on the right
- Dimensions: 8.5 x 11.5 inches

# Toolkit Product: Quick Reference Desk Set

The **Quick Reference Desk Set** contains seven quick guides that VA managers can rely upon to support their decision making process.

Topics covered by the Quick Reference Desk Set include:

- ▸ Overview of management responsibilities in VA 6500
- ▸ Enterprise security overview
- ▸ Information security priorities in the VA IT Strategic Plan
- ▸ Plan of Action and Milestone remediation
- ▸ Certification and Accreditation
- ▸ Product and Service Acquisitions
- ▸ The NIST Risk Management Framework

Product Specifications

- • Includes 7 standard tri-fold brochures
- • Clear plastic stand
- • Dimensions: 8.5 x 11.5 inches

# Toolkit Product: Checklist Pocket Guide

The **Checklist Pocket Guide** is a highly portable reference book that can easily is compact enough to fit in a briefcase, portfolio, suit coat, or handbag.  The checklists will provide actionable procedures to implement information security initiatives.

A sample of topics covered in the Checklist Pocket Guide include:

▸ Security activities across the System Development Lifecycle

▸ System security plan development

▸ Risk assessment

▸ Contingency planning

▸ Configuration management

▸ Asset management

▸ Certification and Accreditation

▸ POA&M management

Product Specifications

- Portable booklet of checklists
- Approximately 20 pages
- Saddle-stitch (stapled) binding
- Durable cover
- Dimensions: 4 x 9 inches

# Toolkit Product: Visual Folding Cube

The innovative **Visual Folding Cube** job aid provides a hands-on and tactile method of communicating security awareness messages.

The cube allows display of nine graphics to communicate security processes, themes, and objectives including:

- ▸ The POA&M process
- ▸ Integration of security across the SDLC
- ▸ The Risk Management Framework
- ▸ Security Control Classes

Product Specifications

- Nine full-color graphics
- Dimensions: 2.75 inches

# Summary of VA Projects Today & Tomorrow

▶ LMS Competency Model

▶ Role-Based Training

▶ Certification Program

▶ Regional Training Classrooms

▶ Toolkit for Managers

▶ CIO Professionalization

▶ Information Security Brown Bag Series

▶ Using social media, such as Web 2.0 technologies as a means for learning and meeting security missions

▶ Additional IS Training

▶ IT National Training Academy

# Questions on Department of Veterans Affairs Role Based Training : Information Security Toolkit for Managers?

**CONTACTS:**

▸ **Terri Cinnamon, ADAS, terri.cinnamon@va.gov**

▸ **Rosa Ayer, rosa.ayer@va.gov**