Role-Based Security Training

Department of Veterans Affairs

Training and Policy Management Service

Rosa C Ayer, MBA, CISSP

Table Of Contents

- Background
- Overview of the Program
- Choosing Roles
- Designing the Message
- Shared Topics and Themes
- Recommendations

Background

In the past two years VA has developed several sets of awareness courses customized to specific key roles within our organization.

The intent of each of these role-based courses is to increase awareness and develop a culture throughout VA where it is proactively recognized that information security is everyone's business.

The courses enable individuals to recognize information security concerns and how to respond accordingly.

Overview of the Program

- The course framework and design are web-based training (WBT).
- The content is based on widely-accepted best practices in cyber security, as set forth in federal law, regulation, and the full set of NIST cyber security guidance.
- All courses are mandatory to meet the annual awareness training for role-specific staff as required by NIST SP 800-16.
- Courses are accessible through VA Learning Management System (LMS)
- Learners are given a pre-test, varied knowledge checks between lessons and a post-test, which they must achieve a 80% or better to receive credit.

Each course uses a unique story specific to the responsibilities of that role.

- We wanted to immerse learners in real-world situations that related to their role.
- They could experience the risks and benefits of information security.
- Supporting, anecdotal, and peripheral information is provided through a Flash-animated “smart learning aid.”

All courses include common topics and themes.

- How security affects the mission of the VA
- Managing the risk of security
- Integrating security needs into the capital planning process
- Resources and people involved to ensure the success of security programs

We used four primary techniques to develop the courses.

- Consistent message is communicated about the importance of information security.
- Consulted with subject-matter experts within VA
- Used guidance in NIST 800-16
- Mapped NIST to VA Policy identifying roles and responsibilities

Choosing the Roles

VA has identified the following specific roles as the target audience:

- IT Project Managers – levels 101, 201 and 301
- Executives and Chief Information Officers (CIOs) –levels 101 and 201
- IT Acquisition Personnel (Contracting Officers and Contraction Officers Technical Representatives (COTRs)) level 101 and 201
- Research and Development staff - level 201
- Human Resources Staff – level 201
- Health Care Professionals – level 201
- IT Staff and Software Developers – levels 101, 301 and 401
- More to come…


Information Security for Executives and CIOs 201
Measuring
Security Improvements
Across VA
HELP
PRINT
LIBRARY
GLOSSARY
MENU
AUDIO
REPLAY
CAPTION
Page 1 of 2

Executives & CIOs 201

High Level Outline

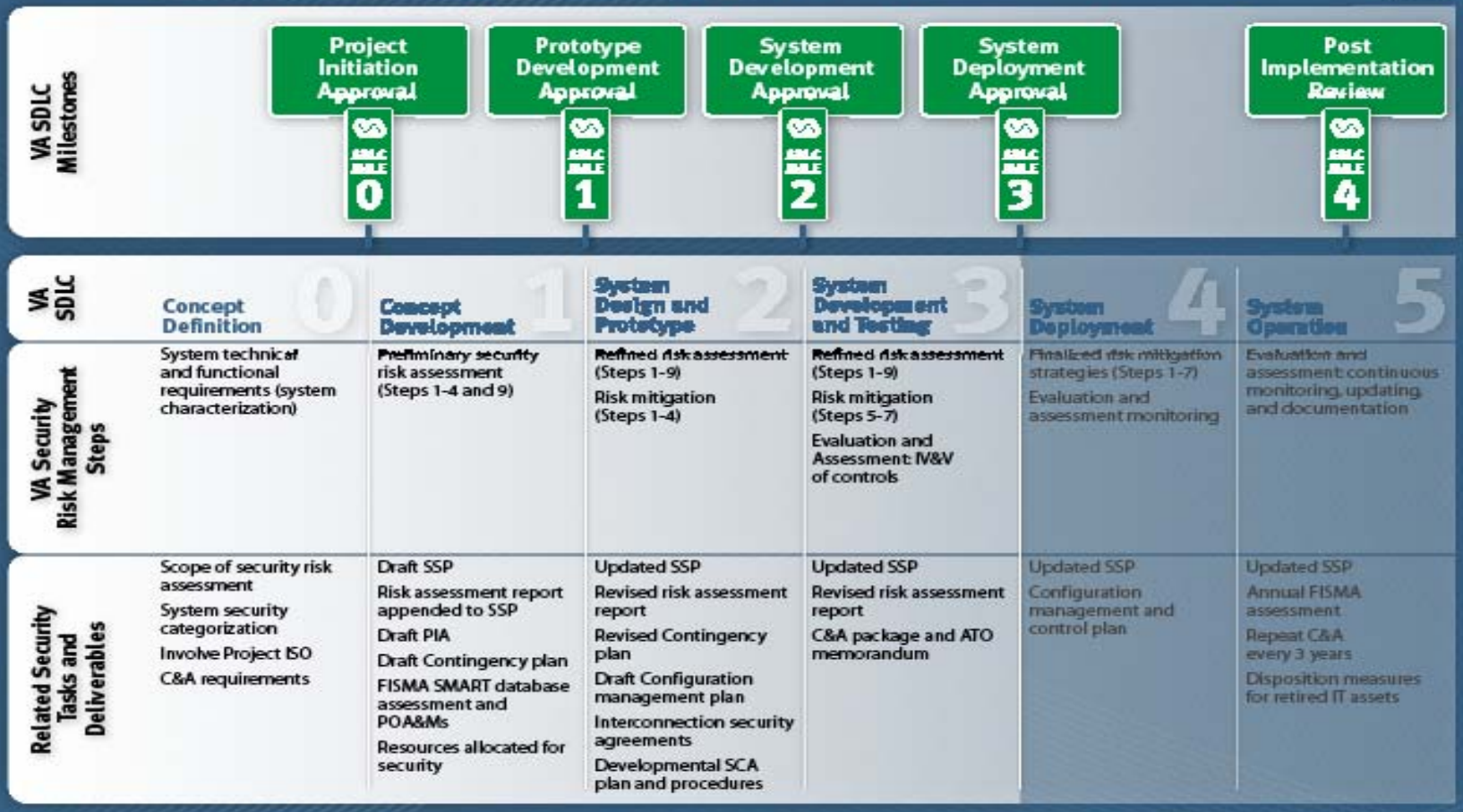
- COURSE WELCOME AND NAVIGATION
- CONTEXT: SECURING FEDERAL INFORMATION ASSETS
- VA'S FISMA REPORT CARD – MEASURING PROGRESS IN PROTECTING VETERANS AND PRESERVING VA'S IT ASSETS
- RECURRING DEFICIENCIES IN VA'S FISMA SCORE
- BEST PRACTICES FOR ADDRESSING IT SECURITY DEFICIENCIES AND IMPROVING FISMA SCORE
- PUTTING AWARENESS INTO ACTION
- COURSE SUMMARY


Information Security for Project Managers: Level 200
Introduction > Opening Animation
Risk Management
in the
System Development Lifecycle
DETOUR
ROUGH ROAD
SDLC MILE 0
SDLC MILE 1
SDLC MILE 2
SDLC MILE 3
SDLC MILE 4
HELP
PRINT
LIBRARY
GLOSSARY
MENU
AUDIO
REPLAY
CAPTION
Page 1 of 2

IT Project Managers
High Level Outline

- INTRODUCTION
- SETTING THE GOLD STANDARD IN INFORMATION SECURITY
- OVERVIEW OF RISK MANAGEMENT IN THE VA SDLC
- STEP 0 - RISK MANAGEMENT FOR CONCEPT DEFINITION
- STEP 1 - RISK MANAGEMENT FOR CONCEPT DEVELOPMENT
- STEP 2 - RISK MANAGEMENT FOR SYSTEM DESIGN AND PROOF OF CONCEPT
- STEP 3 - RISK MANAGEMENT FOR SYSTEM DEVELOPMENT AND TESTING
- COURSE SUMMARY

Risk Management in the System Development Lifecycle



VA Policy: All VA operating units must follow NIST SP 800-30 risk management methodology including risk assessment, risk mitigation, and ongoing evaluation and assessment processes.


Information Security 201 for Acquisition Personnel
Introduction
Information Security
for
Acquisition Managers
ROUGH
ROAD
DETOUR
ACHIEVING THE
GOLD
STANDARD
BUILDING AND
STRENGTHENING
OUR CAPABILITIES
HELP
PRINT
LIBRARY
GLOSSARY
MENU
AUDIO
REPLAY
CAPTION
Page 1 of 4

Acquisition Personnel 201

High Level Outline

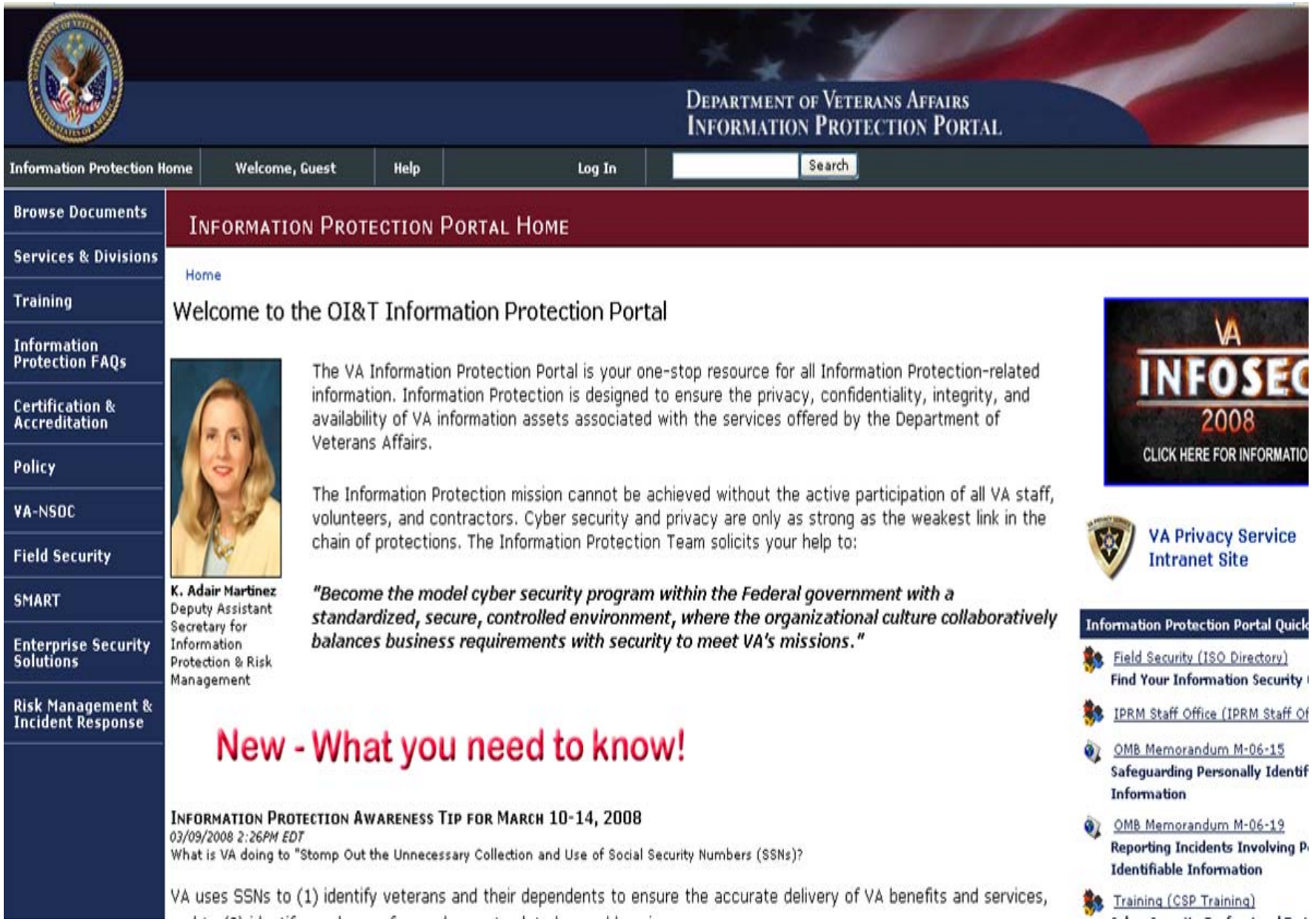
- INTRODUCTION
- SETTING THE GOLD STANDARD IN INFORMATION SECURITY
- THE ACQUISITION AND SYSTEM DEVELOPMENT LIFE CYCLES
- PLANNING PHASE
- CONTRACTING PHASE
- POST-AWARD AND MONITORING PHASE
- FOLLOW-ON PHASE
- COURSE SUMMARY

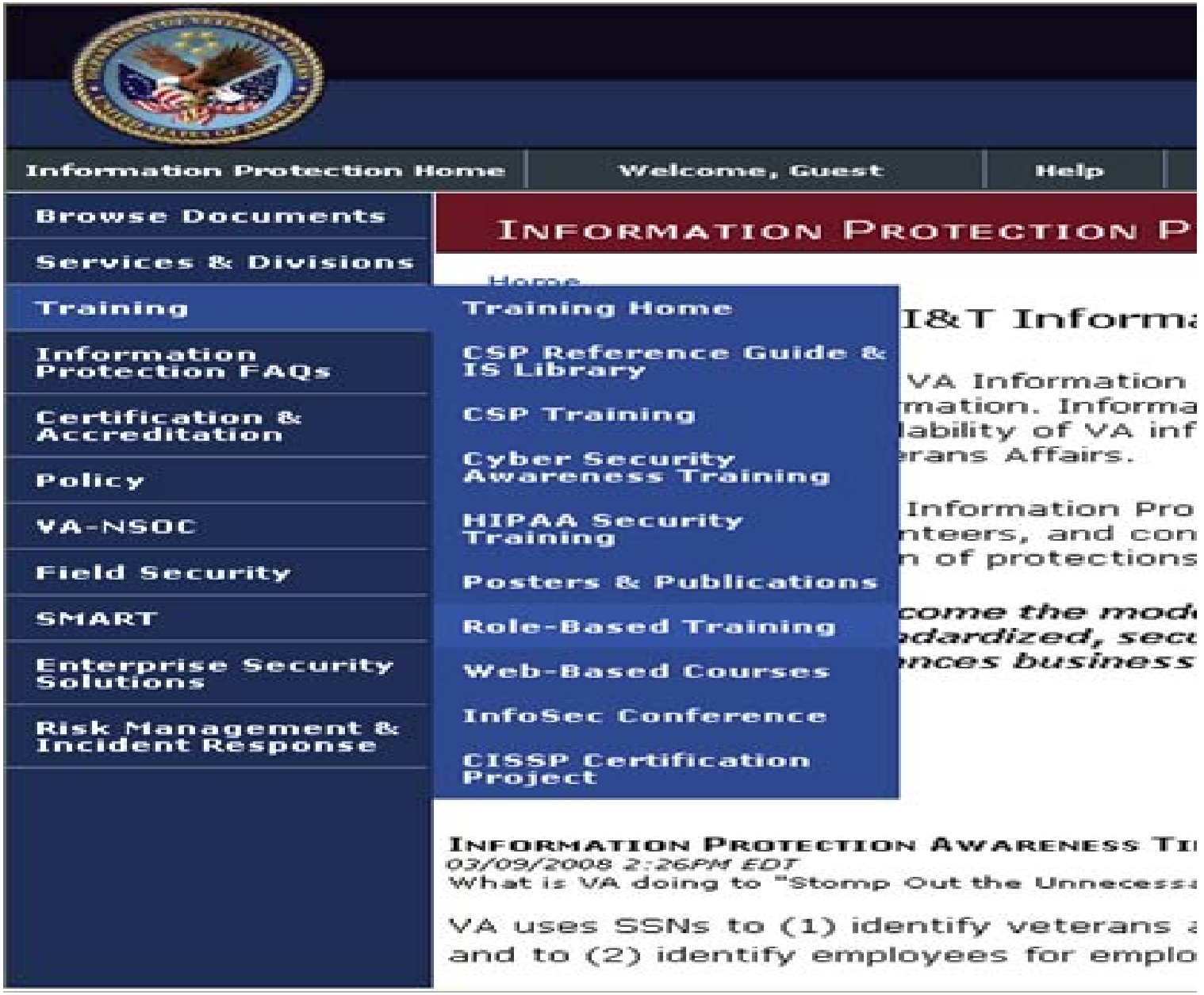
The messaging goals of all courses are consistent.

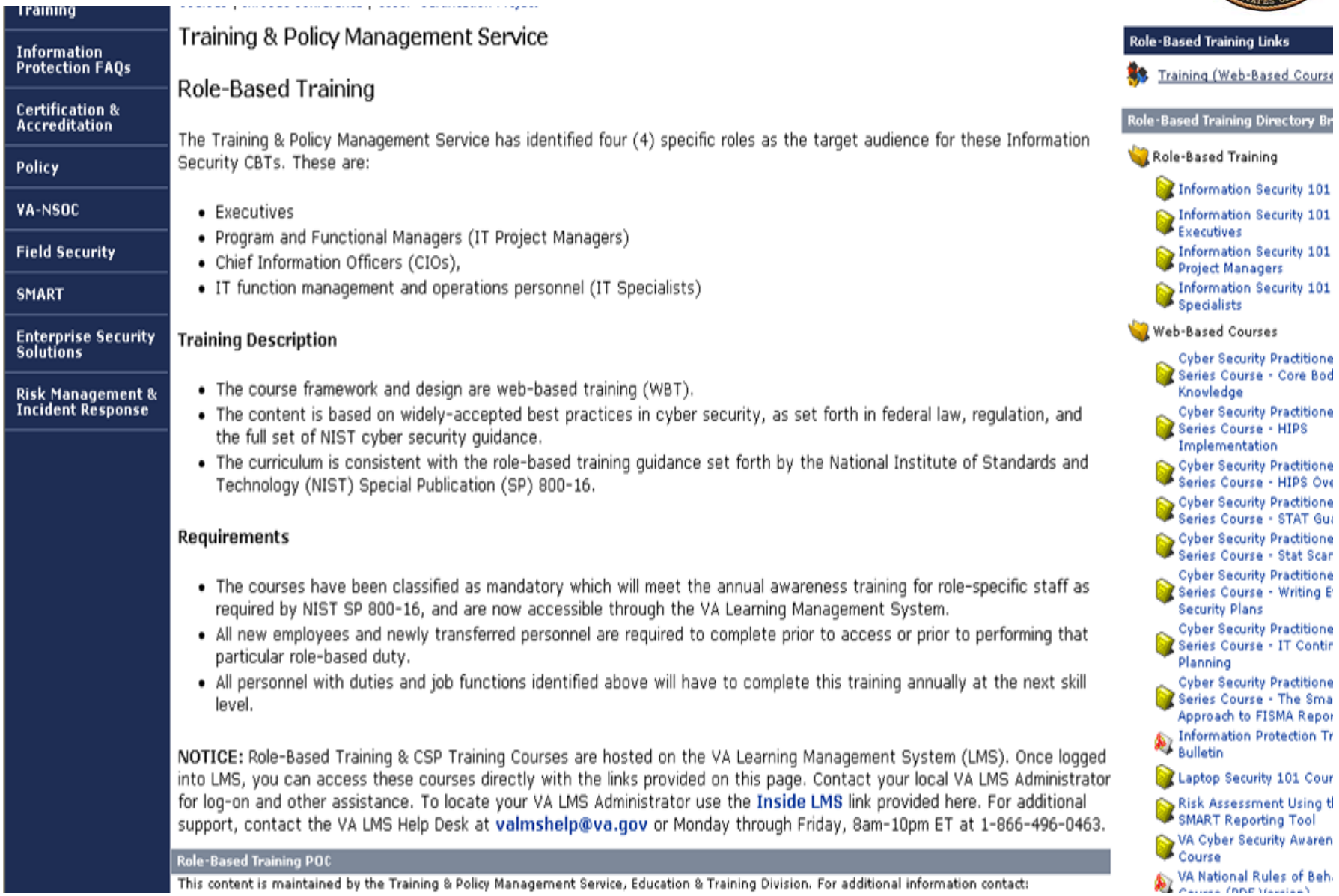
- Focused on changing the attitudes of the learners and developing a greater sense of appreciation for the impact of security on business results.
- Stressed the importance of security to support and strengthen the business of the VA.
- Discussed compliance as a management tool to achieve necessary security goals.

Easy Access to the Courses

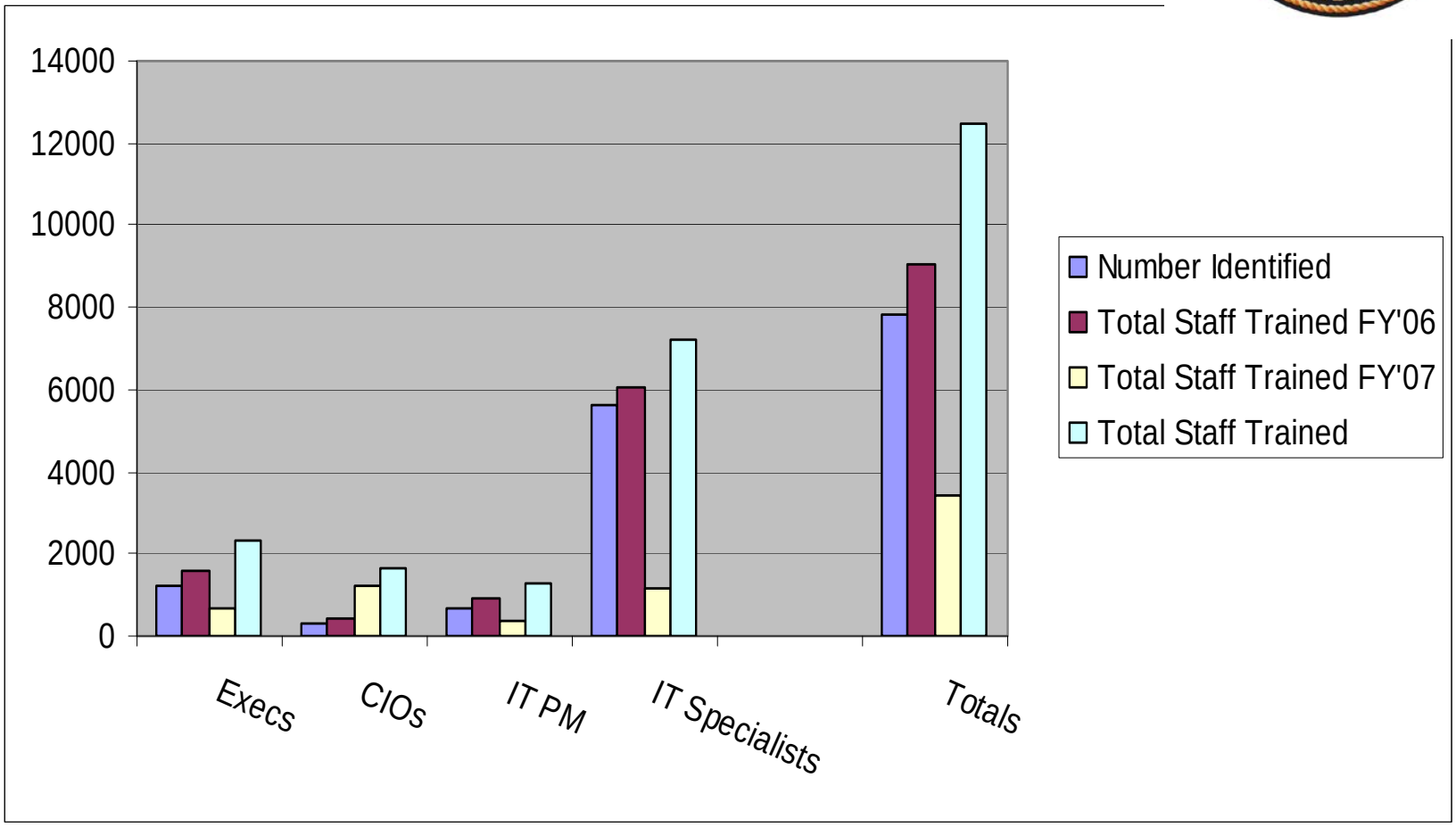
- All courses accessible through the Information Protection Portal
- Direct link to all training
- Direct link to Role-Based Courses


Department of Veterans Affairs
Information Protection Portal
Information Protection Home
Welcome, Guest
Help
Log In
Search
Browse Documents
Services & Divisions
Training
Information Protection FAQs
Certification & Accreditation
Policy
VA-NSOC
Field Security
SMART
Enterprise Security Solutions
Risk Management & Incident Response
Information Protection Portal Home
Home
Welcome to the OI&T Information Protection Portal
The VA Information Protection Portal is your one-stop resource for all Information Protection-related information. Information Protection is designed to ensure the privacy, confidentiality, integrity, and availability of VA information assets associated with the services offered by the Department of Veterans Affairs.
The Information Protection mission cannot be achieved without the active participation of all VA staff, volunteers, and contractors. Cyber security and privacy are only as strong as the weakest link in the chain of protections. The Information Protection Team solicits your help to:
"Become the model cyber security program within the Federal government with a standardized, secure, controlled environment, where the organizational culture collaboratively balances business requirements with security to meet VA's missions."
K. Adair Martinez
Deputy Assistant Secretary for Information Protection & Risk Management
VA
INFOSEC
2008
CLICK HERE FOR INFORMATIO
VA Privacy Service Intranet Site
Information Protection Portal Quick
Field Security (ISO Directory)
Find Your Information Security
IPRM Staff Office (IPRM Staff Of
OMB Memorandum M-06-15
Safeguarding Personally Identif
Information
OMB Memorandum M-06-19
Reporting Incidents Involving P
Identifiable Information
Training (CSP Training)
New - What you need to know!
Information Protection Awareness Tip for March 10-14, 2008
03/09/2008 2:26PM EDT
What is VA doing to "Stomp Out the Unnecessary Collection and Use of Social Security Numbers (SSNs)?
VA uses SSNs to (1) identify veterans and their dependents to ensure the accurate delivery of VA benefits and services,


Information Protection Home
Welcome, Guest
Help
Browse Documents
Services & Divisions
Training
Information Protection FAQs
Certification & Accreditation
Policy
VA-NSOC
Field Security
SMART
Enterprise Security Solutions
Risk Management & Incident Response
Training Home
CSP Reference Guide & IS Library
CSP Training
Cyber Security Awareness Training
HIPAA Security Training
Posters & Publications
Role-Based Training
Web-Based Courses
InfoSec Conference
CISSP Certification Project
INFORMATION PROTECTION P
Home
I&T Informa
VA Information
mation. Informa
lability of VA inf
erans Affairs.
Information Pro
nteers, and con
n of protections
come the mod
dardized, secu
nces business
INFORMATION PROTECTION AWARENESS TI
03/09/2008 2:26PM EDT
What is VA doing to "Stomp Out the Unnecessa
VA uses SSNs to (1) identify veterans
and to (2) identify employees for emplo


Training
Information Protection FAQs
Certification & Accreditation
Policy
VA-NSOC
Field Security
SMART
Enterprise Security Solutions
Risk Management & Incident Response
Training & Policy Management Service
Role-Based Training
The Training & Policy Management Service has identified four (4) specific roles as the target audience for these Information Security CBTs. These are:
Executives
Program and Functional Managers (IT Project Managers)
Chief Information Officers (CIOs),
IT function management and operations personnel (IT Specialists)
Training Description
The course framework and design are web-based training (WBT).
The content is based on widely-accepted best practices in cyber security, as set forth in federal law, regulation, and the full set of NIST cyber security guidance.
The curriculum is consistent with the role-based training guidance set forth by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16.
Requirements
The courses have been classified as mandatory which will meet the annual awareness training for role-specific staff as required by NIST SP 800-16, and are now accessible through the VA Learning Management System.
All new employees and newly transferred personnel are required to complete prior to access or prior to performing that particular role-based duty.
All personnel with duties and job functions identified above will have to complete this training annually at the next skill level.
NOTICE: Role-Based Training & CSP Training Courses are hosted on the VA Learning Management System (LMS). Once logged into LMS, you can access these courses directly with the links provided on this page. Contact your local VA LMS Administrator for log-on and other assistance. To locate your VA LMS Administrator use the Inside LMS link provided here. For additional support, contact the VA LMS Help Desk at valmshelp@va.gov or Monday through Friday, 8am-10pm ET at 1-866-496-0463.
Role-Based Training POC
This content is maintained by the Training & Policy Management Service, Education & Training Division. For additional information contact:
Role-Based Training Links
Training (Web-Based Course
Role-Based Training Directory Br
Role-Based Training
Information Security 101
Information Security 101 Executives
Information Security 101 Project Managers
Information Security 101 Specialists
Web-Based Courses
Cyber Security Practitione Series Course - Core Bod Knowledge
Cyber Security Practitione Series Course - HIPS Implementation
Cyber Security Practitione Series Course - HIPS Ove
Cyber Security Practitione Series Course - STAT Gu
Cyber Security Practitione Series Course - Stat Scar
Cyber Security Practitione Series Course - Writing E Security Plans
Cyber Security Practitione Series Course - IT Contir Planning
Cyber Security Practitione Series Course - The Sma Approach to FISMA Repor
Information Protection Tr Bulletin
Laptop Security 101 Cour
Risk Assessment Using t SMART Reporting Tool
VA Cyber Security Awaren Course
VA National Rules of Beh

Compliance Results



Role-Based Training Compliance Results

Agency Totals	Number Identified	Total Staff Trained FY'06	Total Staff Trained FY'07	Total Staff Trained
Execs	1234	1618	697	2315
CIOs	299	449	1194	1643
IT PM	665	916	394	1310
IT Specialists	5606	6036	1150	7186
Totals	7804	9019	3435	12454

Follow these recommendations when developing role-based training.

1. Identify the organization's core messages for information security
2. Incorporate industry best practices (what *should* be done), not just what *is* currently done
3. Define and identify roles and responsibilities for Information security
4. Tie every action back to the "why am I doing this" – for VA, this is to **"protect the veteran"**
5. Use story!

Avoid these situations when developing role-based training.

1. Don’t just talk about “what you need to do” – make it real, answer the “why should I care?”
2. Don’t expect 100% buy-in even from those helping to develop the course; “that’s not the way we do things”
3. Don’t expect training alone to solve the problem; each *role* needs the proper incentives for doing right and disincentives for doing wrong

Role-Based Training

For additional information contact

- Rosa Ayer – (561) 753-2827
  rosa.ayer@va.gov