Defense Information Systems Agency

A Combat Support Agency

DoD IA Training Products, Tools Integration, and Operationalization

Roger S. Greenwell, CISSP, CISA, CISM
Technical Director / Capabilities Implementation Division
DISA Field Security Operations

July 2010

DISA
A Combat Support Agency

Agenda

- IA Training Mission Overview
- Challenges
- Training Mediums
- Available Courses
- Operationalization Goals

A Combat Support Agency

DISA Training Team Mission

- Support the development and maintenance of online resources correlating DoD IA training products and classes, to requirements defined in law, executive orders, and DoD issuances.
- Support correlating IA functions as defined in DoD 8570.1M to workforce categories, specialties, and levels to core IA training curriculum
- Serve as the DoD shared service center for the Office of Management and Budget (OMB)-directed Information System Security Line of Business (ISS LoB) for Tier I Awareness training
- Support the sharing of IA related information to include training materials through the use of the Information Assurance Support Environment (IASE)

DISA
A Combat Support Agency

Functions/Roles Supported

- System Administrators (SAs)
- Computer Network Defense (CND) Personnel
- Information Assurance Officers/Managers (IAOs/IAMs)
- Designated Accrediting Authorities (DAAs)
- System Architects
- Everyday System Users

DISA
A Combat Support Agency

Challenges

- Different people learn in different ways
- Ability for people to schedule out-of-office time to address training
- Availability of training when it's needed
- Shifting mindset of users from "just another required course"
- Need for more operational focused training
  - Training must evolve from basic IA concepts and tool "mechanics" to a functional perspective that enables tools and techniques

Need for the right training, at the right time, using the right medium!

DISA
A Combat Support Agency

Mediums Used for IA Training

- **Computer-based Training/Web-based Training (CBT/WBT)**
  - **Primarily Hosted on IASE**
  - **CD versions**
- **Instructor Led Training**
  - **Typical classroom based (face to face)**
  - **Interactive means such as Defense Connect Online (DCO)**
- **Virtual Training Environment (VTE)**
  - **Supports virtual asynchronous training using lessons and labs**
  - **Government hosted capability to expand range of coverage in both a unclassified and classified environments**
- **IA Range**
  - **Envisioned to support training, exercises, and testing in a mocked up environment; providing more real-world like experiences**

A Combat Support Agency

Online IA Training Products

- *Supports certification of DoD IA professionals (DoD 8570.01-M)*
- *Compliant with Section 508 of the Rehabilitation Act*
- *Most are cleared for "Open Release" by DoD*
- *Order free CD-ROMs or take online at http://iase.disa.mil*

- **New Products**
  - IA Briefing for Senior Operational Leaders v.1
  - CyberProtect v.2
  - Information Sharing v.1
- **Updated Products**
  - DOD IA Awareness v.8
  - DAA v.7
  - Using PKI v.1 (includes using PKI certificates)
  - IA for DoD Auditors and IGs v.2
  - IAP&T WBT v.5
- **Upcoming Products**
  - DOD IA Awareness v.9
  - DAA v.8
  - Introduction to Intrusion Detection Systems (IDS) Analysis v.1

A Combat Support Agency

CBT/WBT Training Courses

General IA	***IA Training for IA Professionals***	***IA Technical Training***
Personal Electronic Devices (PED's) - Dated 12/08 - Version 1.1	Information Assurance Policy and Technology (IAP&T) - Dated 03/10 - Version 5.0	Domain Name System (DNS) Basic Concepts Overview - Dated 04/09 - Ver 1.0
Using Public Key Infrastructure (PKI) - Dated 12/09 - Version 1.0	Information Assurance for Professionals Shorts - Dated 12/09 - Version 5.0	Domain Name System (DNS) Advanced Concepts - Dated 10/09 - Ver 1.0
Phishing Awareness - Dated 04/08 - Version 1.0	IA Hot Subjects - Dated 11/06 - Version 1.1	Windows Server 2003 Incident Preparation & Response (IP&R): Part 1 - Dated 02/06 – Version 1.0
DoD Information Assurance Awareness (For DoD Personnel) - Dated 10/09 - Version 8.0	Physical Security for SIPRNet - Dated 05/09 - Ver 1.0	Windows Server 2003 Incident Preparation & Response (IP&R): Part II - Dated 10/07 – Version 1.1
Information Systems Security Awareness (For Non-DoD Personnel) - Dated 09/09 - Version 3.0	Computer Network Defense (CND) - Dated 12/06 - Version 2.0	UNIX Security for System Administrators - Dated 12/04 - Version 2.0
IC Information Assurance Awareness (for Intelligence Community Personnel) Dated 12/09	DoD Information Assurance Certification and Accreditation Process (DIACAP) - Dated 01/09 - Version 1.0	System Administrator Incident Preparation & Response for UNIX (SAIPR UNIX) - Dated 05/05 - Version 2.01
Personally Identifiable Information (PII)- Dated 10/07 - Version 1.0	Securing the Mobile Network - Date 02/06 - Version 1.2	Internet Protocol Version 6 (IPv6) - Dated 10/07 – Version 1.0
Information Operations (IO) Fundamentals - Dated 10/07 - Version 2.0	Enhancing Information Assurance through Physical Security - Dated 10/07 – Ver 1.0	
Information Assurance Awareness Shorts - Dated 01/09 - Version 3.0	Information Assurance for DoD Auditors and IGs - Dated 03/10– Ver 2.0	***IA Training for IT Managers***
	CyberProtect - Dated 03/10 – Ver 2.0	Designated Approving Authority (DAA) - Dated 03/10 - Version 7.0
Cyberlaw	CyberOps: NetWarrior - Dated 01/09 - Ver 1.0	Active Defense: An Executive's Guide to Information Assurance - Dated 02/03 - Version 1.0
Cyber Law 1 - Dated 10/04 - Version 1.0		
Cyber Law 2 - Dated 11/06 - Version 1.0	***NETOPS***	
	NetOps 100: An Overview	
	NetOps 200: NetOps Applied to GIG Operations	

DISA
A Combat Support Agency

Classroom Instruction

- DOD IA Boot Camp
- Security Readiness Review Walkthrough Training
  - Windows
  - Unix
  - Database
  - Web
  - Applications
  - DNS
  - Network
  - Retina
- NetOps Training
- Rapid Experience Builder (RaD-X) courses

DISA
A Combat Support Agency

Rapid Experience Builder (RaD-X)

- Training courses that deliver hands-on CND scenarios focused on:
  - Firewall Log Review
  - IDS analysis and configuration
  - Anomaly Detection among CND Tools
- Exposes students to a large number of attacks in a safe, non-production, environment
- Instructs students in recent attack signatures
- Delivered to McNOSC, ARCERT, PACOM, EUCOM, TNC Europe, NORTHCOM, JFCOM, DISA GNSC

DISA
A Combat Support Agency

NetOps Training

- **Four NetOps courses exist today**
  - **NetOps 100 Overview ***
  - **NetOps 200 NetOps Applied to GIG Operations ***
  - **NetOps 300 Evolving the DoD Enterprise Through Policy, Process and Culture**
  - **NetOps 400 delivering the NetOps- Enabled GIG**
- **Emphasis on formalizing the NetOps training and certification program**
- **Evolution of the program as a whole looking at the broader set of skills addressing NetOps**
- **Considerable updates during the next 18-24 months as program analysis gets underway**
- **Potential impacts as USCYBERCOM is stood up**

***Also available at http://iase.disa.mil**

A Combat Support Agency

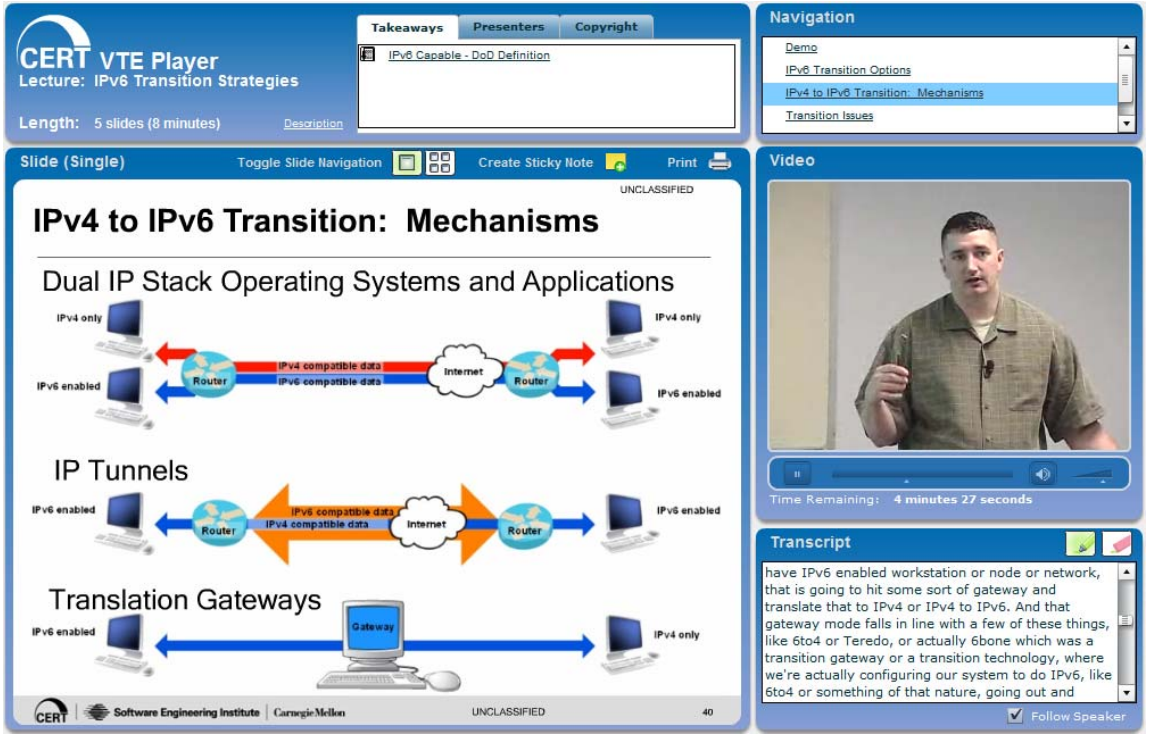
Virtual Training Environment (VTE)

- **Web-based training platform and knowledge library for Information Security, Forensics, and Incident Response material**
  - **20+ courses**
  - **Numerous courses supporting DoD 8570.01-M requirements**
  - **75+ Hands-on Labs**
  - **CMU Library material available as refresher training**
  - **CERT instructor support through 'virtual office hours'**
  - **Currently supported at CMU**
    - **Unclassified instantiation being stood up by DHS**
    - **Classified instantiation being stood up by DISA**

A Combat Support Agency

VTE Feature: Video Lecture

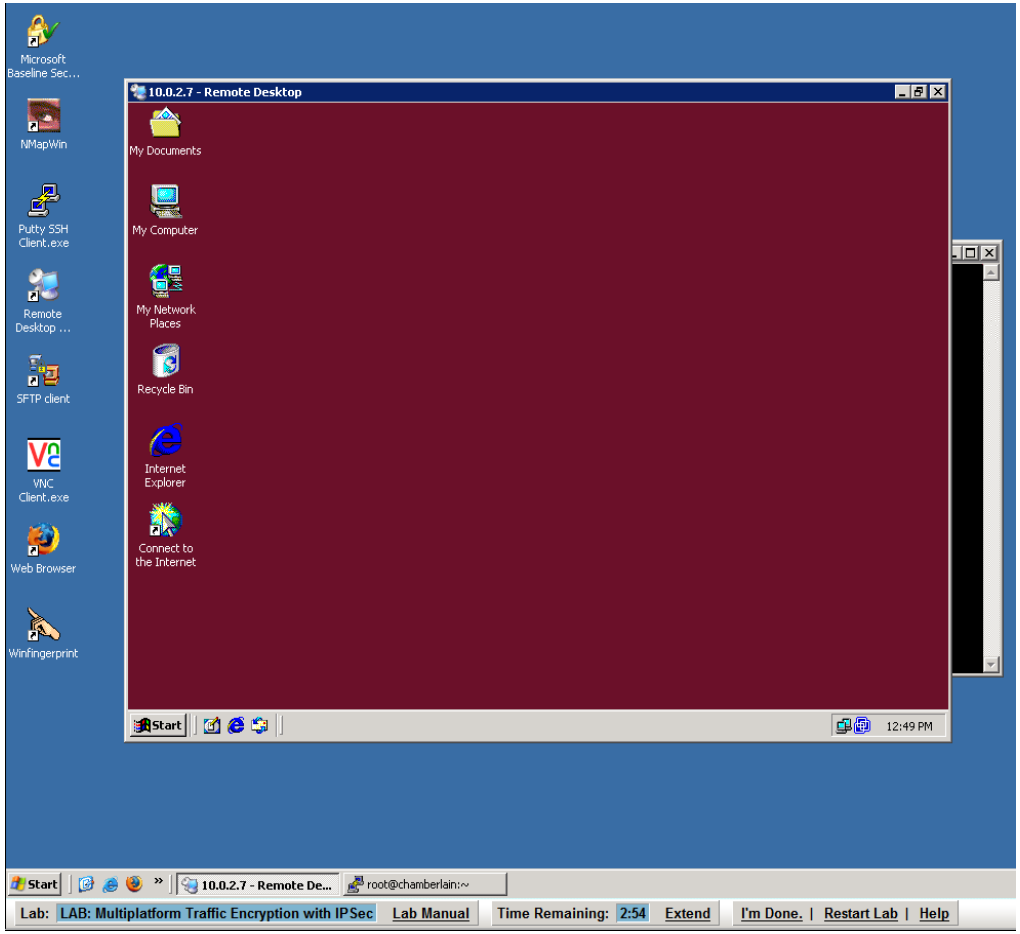
- Synchronized video, slide, transcript
- Searchable
- Remembers where you left off
- Linked takeaways (slides, transcript) from the interface
- Online note-taking



A Combat Support Agency

VTE Feature: Virtual Labs

- Synchronized video, slide, transcript
- Real networks and computers
- Accessible directly in browser
- Deployed on demand
- Isolated training network
- 75+ Available configurations
  - Firewalls
  - Web
  - Exchange
  - Attack/Defend



DISA
A Combat Support Agency

VTE System Requirements

- Broadband (>200kbps) Internet connection (for video streaming)
- AJAX-capable browser (Microsoft Internet Explorer 6+, Mozilla Firefox 2.0+ for Windows, Firefox for Mac OS X and Linux variants, Google Chrome)
- Adobe Flash 9+ browser plug-in for access to lecture videos (Flash 10 recommended)
- Java Virtual Machine 1.5+ for access to Lab environments
- Adobe Acrobat Reader (for viewing PDF downloads)

Verified on FDCC and DoD systems, networks and firewalls!

A Combat Support Agency

VTE Course Highlights

- DOD 8570 Preparation
  - CompTIA Security+ Prep
  - CompTIA Network+ Prep
  - CompTIA A+ Prep (Summer 2010)
  - $(ISC)^2$ CISSP Prep
  - Cisco CCNA
  - Cisco Security (Summer 2010)
  - Certified Ethical Hacker (Summer 2010)
- DOD Sponsored Training Products
  - HBSS 3.0
  - HBSS Manager's Course

DISA
A Combat Support Agency

IA Range

- **Simulated GIG**
  - **Simulated Internet; Tier I**
  - **Allows for plug-in of Tier 2 and below**
  - **Contains tools used in the real world**
- **Supports multiple use cases**
  - **Exercise support**
  - **Red Teaming / product testing**
  - **Training**

DISA
A Combat Support Agency

Information Assurance Support Environment (IASE)

- **Web-based environment providing IA information to the community on various subject matter areas**
  - **Security Technical Implementation Guides (STIGS)**
  - **DoD Enterprise IA tools (SCCVI, SCRI, HBSS)**
  - **Online IA Training**
  - **DoD Policies, PPSM, CDS, CND, PKI, DIACAP/DITSCAP, Wireless Security, etc.**
- **Supported on NIPRNet and SIPRNet**
  - **Publicly accessible (http://iase.disa.mil)**
  - **PKI Restricted (https://powhatan.iiie.disa.mil)**
  - **SIPRNet (https://iase.disa.smil.mil)**
- **Request for new content area**
  - **Send request to IA-Web@disa.mil to receive Welcome Packet**

DISA
A Combat Support Agency

Operationalization

- **Operationalizing tools within the infrastructure**
  - **Mechanics of how to use the tools are important**
  - **Tactics, Techniques, and Procedures (TTPs) on how to integrate tool usage into the operational environment is critical**
  - **FSO and PEO-MA are jointly working to better operationalize tools as they're being deployed**
  - **Leveraging combination of mechanics and TTPs to develop operationally focused training**

DISA
A Combat Support Agency

Summary

- **IA Education, Training, and Awareness is a challenge everyone faces**
- **Leveraging the right medium is important**
- **Using a synchronous distance-learning based approach for complex training necessary for operational community**
- **Must balance the requirements for training products that address concepts, mechanics, and operations**

DISA

A Combat Support Agency