Improving the Cyber Workforce

IA Training, Certification and Workforce Management in DoD

George Bieber

Defense-wide IA Program (DIAP)

george.bieber@osd.mil

Outline

- Background
- Status of IA Workforce Improvement Program
- Awareness (ISS LOB)
- Training & Exercises
- Challenges

Landscape circa 2005

ASD/C3I & USD/P&R memo: *IA Training & Certification (6/98)*

- **Unknown size/composition of the IA workforce**
  - People, positions not "tagged" for IA
  - No military IA career path, skill indicators
  - Personnel, manpower databases lacked fields to track
  - Unknown number of personnel performing IA functions part time as "additional duty"
  - Unknown number of personnel outside IT career fields performing IA functions
- **Wide variation in training content (Depth & Breadth)**
  - Inconsistent implementation across the Department
  - Inconsistent implementation within Components (military, civilian, contractor, local nationals – globally deployed)
  - Internal certification not recognized Department-wide
- **Schools struggling to keep pace with the challenge**
- **No visibility into spending on IA training & certification**
- **Minimal exercise or evaluation of IT/IA training**

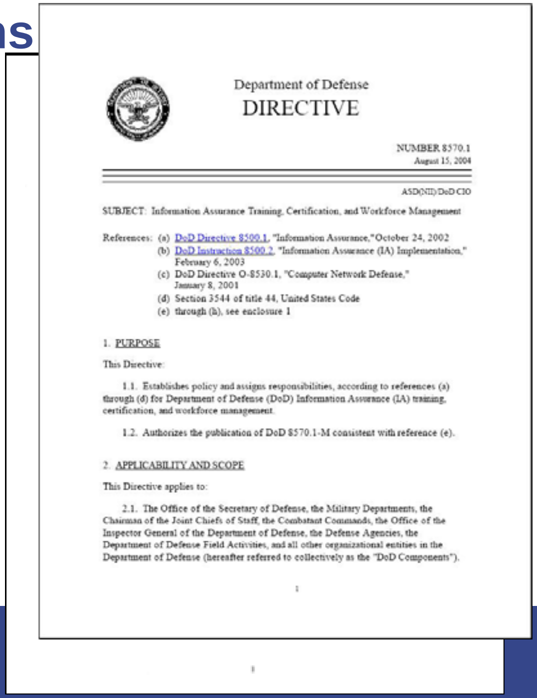
Component "certification" -- largely undefined

Strategy

Objectives	*Impact*
Certify the Workforce	◆ Improved IA posture (“raise the floor” on baseline skills) ◆ Foundation of a professional IA workforce ◆ Mechanism “raise the bar” on future skills
Manage the Workforce	◆ Ability to assign trained/certified personnel to IA positions ◆ Ability to conduct manpower studies; establish standards
Sustain the Workforce	◆ Elevates priority of IA for training dollars ◆ Enables personnel to hone IA skills, keep current with technology, threats and vulnerabilities, tools, techniques
Extend the Discipline	◆ Leaders at all levels understand impact of IA on mission accomplishment ◆ A model Allies, coalition partners can emulate ◆ IA literacy for critical non-IT disciplines
Evaluate the Workforce	◆ Leadership visibility into the IA workforce ◆ IA WIP “product improvement” ◆ Measure impact on IA posture

Policy (DoD 8570.1 and DoD 8570.01-M)

- Assign position specialty code/skill identifiers
- Identify positions in manpower databases
- Record, track contractors certification status
- Require IA in all levels of professional military education
- Applies to civilian, military, local national, contractor; full time or "as assigned"; regardless of job series/ occupational specialty
- Defines IA workforce categories, levels, functions
- Mandates use of commercial certifications to validate DoD baseline knowledge and skills
- Requires certifications be accredited under ISO/IEC 17024, *General requirements for bodies operating certification of persons*
- Specifies reporting requirements
- Provides for oversight, "product improvement"



Department of Defense
DIRECTIVE

NUMBER 8570.1
August 15, 2004

ASD(NII)/DoD CIO

SUBJECT: Information Assurance Training, Certification, and Workforce Management

References: (a) DoD Directive 8500.1, "Information Assurance," October 24, 2002
(b) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(c) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
(d) Section 3544 of title 44, United States Code
(e) through (h), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities, according to references (a) through (d) for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.

1.2. Authorizes the publication of DoD 8570.1-M consistent with reference (e).

2. APPLICABILITY AND SCOPE

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the Department of Defense Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

1

17024 defines "certification". Focuses on processes, presence of job task analysis (link to jobs; defines the work and skills), validation study (EEO), security and construction of test, continuous learning/ periodic retest

IA Workforce Improvement Program: Current Status and Initiatives

Current Status

- Met first year goal to certify 10% of the workforce; collectively, COCOMs have up to 40% of their workforce certified
- All mandated certifications have met or are well into the process of meeting ISO/IEC 17024 requirements to be ANSI accredited
- Renewed focus on personnel: e.g., AF cyber corps with IA career path; Army WO career path
- IA beginning to be taken to non-IT/IA leadership through professional military education, IA “boot camps” etc.
- 8570 compliance validation plan in place; first on-site review conducted by OSD
- NDU/IRMC courses support learning for CISSP, CISM certifications
- Certification corporate memberships, self-assessments, annual fees for individuals paid for by DoD
- Change 1 to the 8570 Manual published

Change 1 to 8570 Manual *(15 May 2008)*

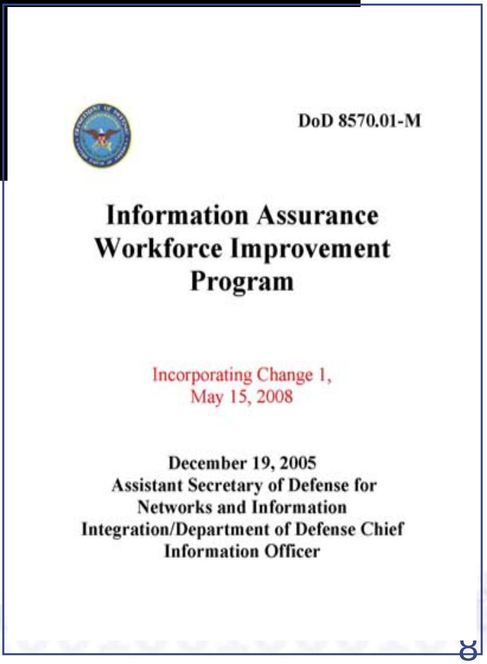
Computer Network Defense Service Providers (CND SP)

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND-SP Manager
GCIA	SSCP	CSIH GCIH	CISA GSNA	CISSP-ISSMP CISM

Information Assurance System Architects and Engineers (IASAE)

IASAE I	IASAE II	IASAE III
CISSP (or Associate)	CISSP (or Associate)	ISSEP ISSAP

- Clarifies local operating system certification includes security related tools/devices
- Adds IRMC 4012 certificate courses & Information System C&A course (Catalog #6209) for DAAs
- Changes report accounting from FY to CY
- Provides a year for implementation of Change 1
- Adds "*or Associate*" to IAT and IAM CISSP



DoD 8570.01-M

Information Assurance
Workforce Improvement
Program

Incorporating Change 1,
May 15, 2008

December 19, 2005
Assistant Secretary of Defense for
Networks and Information
Integration/Department of Defense Chief
Information Officer

http://www.dtic.mil/whs/directives/

Implementation/Process Improvement Initiatives (1)

Workforce Management Support Systems

- **DCPDS (Defense Civilian Personnel Data System)**
- **PCSS (Personnel Certification Support System) –** http://www.dodpcss.com
- **DoD Defense Workforce Certification Interface (DWCI)-** *authoritative data source for individual's certification status - allows automated transfer of select data on individual's certification status* **https://www.dmdc.osd.mil/dwc**
- **Contractor certification verification database –** *Track contractors with IA responsibilities category/level and certification status: under development*

DFARS Clause

- **Defense Federal Acquisition Regulation (DFAR) formally updated to reflect 8570 certification requirement for contractors** (Federal Register (Vol. 73, No. 7 / Thursday, January 10, 2008)

Implementation/ Process Improvement Initiatives (2)

FY08 Funding Provided for Certification Test Vouchers

DoD IA Skill Standards (IASS) Survey (Job Task Analysis)

◆56 IA functions performed by DoD IA personnel

◆Demographics of personnel performing IA functions

Interest by Civilian Departments and Agencies?

Other Activities

◆DoD on the ANSI Personnel Certification Accrediting Committee

◆DoD SMEs participating on Certification Provider advisory boards, certification review committees and test writing working groups

◆DIAP support to Performance Testing Council (PTC); bring more performance testing into certification

◆Continue to examine commercial certifications against functional requirements in the DoD Manual 8570.01-M "*Information Assurance Workforce Improvement Program*" for applicability to DoD

Implementation/ Process Improvement Initiatives (3)

Certification Self-Assessments

- *Determine personnel "readiness to test"*
- *Identify knowledge gaps; areas to focus training*

- ***CompTIA:*** **Self-assessments are available for each DoD approved CompTIA Certification including the CompTIA A+, CompTIA Network+ or CompTIA Security+ certifications through 28 February 2009**
- ***GIAC:*** **"short-assessments" for GISF, GSEC, GSLC and Security + are available through 31 December 2008**
- ***(ISC)2:*** **Self-assessments are available for the CISSP and SSCP certifications through 31 December 2008**
- ***ISACA:*** **has developed CISA and CISM self-assessment tools to help exam candidates assess their knowledge of the exam job practice areas and determine their strengths and weaknesses.**

New and Revised Security Controls

Existing Controls

- PRTN – 1 Information Assurance Training
- DCSD – 1 IA Documentation

New Controls

- **PRWF -1 Workforce Management Policy**
  …positions required to perform Information Assurance (IA) functions are established in writing and identified in the appropriate manpower table of organization or manning document…designated by IA category and level…. People…are identified in…personnel databases… The… manning document identifies all IA positions by specific IA category, level, and functions….
- **PRCT – 1 Personnel Certification Policy**
  …all personnel are certified to perform their assigned Information Assurance (IA) responsibilities, to include certification of baseline security and Operating System (OS) skills….

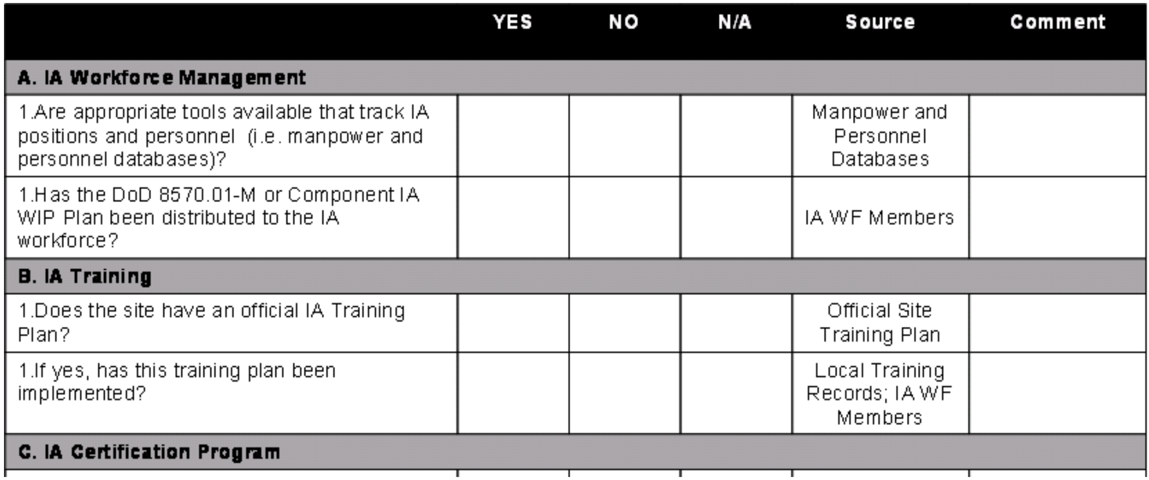
Assessing Compliance

DoD CIO Compliance Program

- Verify compliance w/security regulations; DoD IA policy as it pertains to people.
  - Review materials submitted by Components in response to DoD & FISMA requirements
  - On-site review at Component location to verify documentation & determine compliance status

DoD Information Awareness Site Review Checklist

Critical Element	Have IA and HR management personnel at the site level developed and implemented IA Workforce Improvement Program (IA WIP)?
Purpose	To assess the capability, performance and compliance against the policies and requirements of DoDD 8570.1 and DoD 8570.01-M.
Core Review Areas	IA Workforce Management, IA Training, IA Certification
Method	Site level review of IA WIP program plans, including documentation and procedures review.

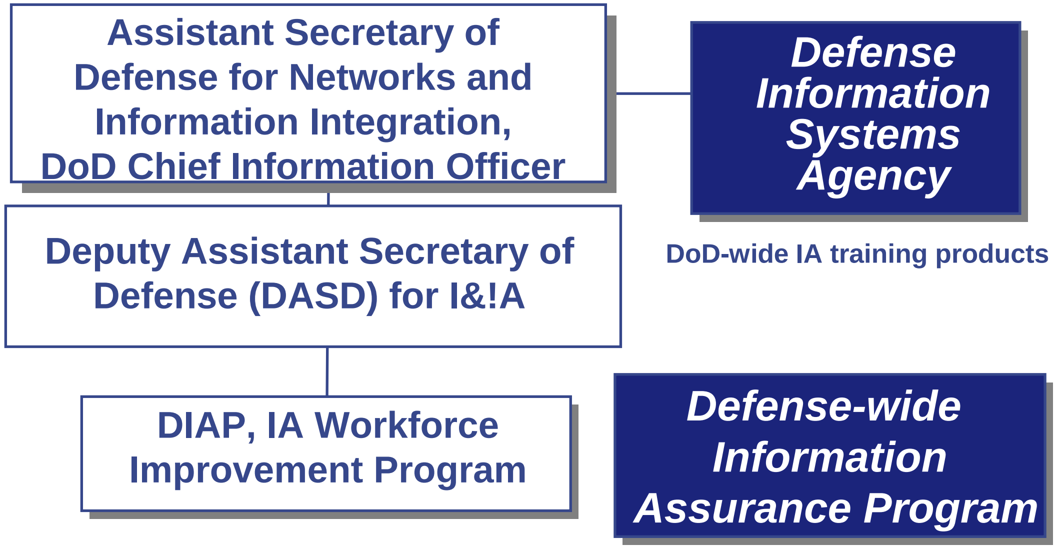


	YES	NO	N/A	Source	Comment
A. IA Workforce Management					
1.Are appropriate tools available that track IA positions and personnel (i.e. manpower and personnel databases)?				Manpower and Personnel Databases	
1.Has the DoD 8570.01-M or Component IA WIP Plan been distributed to the IA workforce?				IA WF Members	
B. IA Training					
1.Does the site have an official IA Training Plan?				Official Site Training Plan	
1.If yes, has this training plan been implemented?				Local Training Records; IA WF Members	
C. IA Certification Program					

- Is policy implemented as intended
- Is compliance resulting in the intended outcome (Operations)
- What is else is needed to achieve the desired end state (Programs)

Annual Awareness

DoD Shared Service Center (SSC) for Awareness



Assistant Secretary of Defense for Networks and Information Integration, DoD Chief Information Officer

Defense Information Systems Agency

DoD-wide IA training products

Deputy Assistant Secretary of Defense (DASD) for I&!A

DIAP, IA Workforce Improvement Program

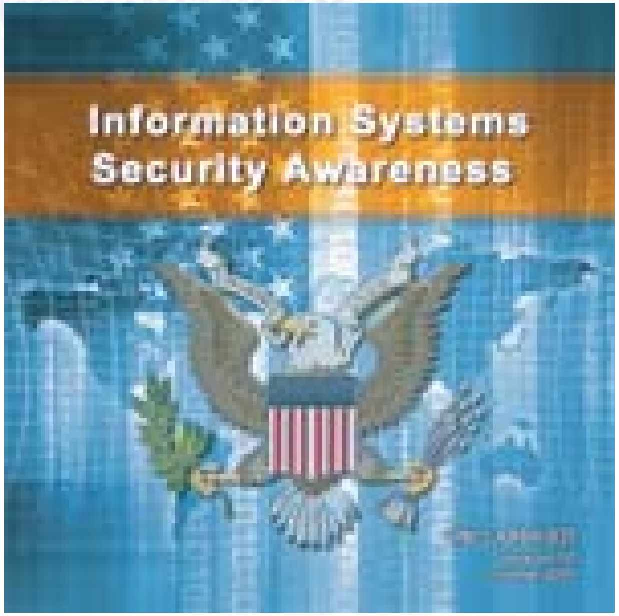
Defense-wide Information Assurance Program

- OMB designated ISS LoB SSC for IA awareness training
- Developing baseline at no cost to Components
- “Customers” implement, track, & report; fund unique requirements
- Reducing duplicate efforts
- Oct 2007: Components required to use “DoD IA Awareness”
- Meets FISMA and DoD 8570 requirements
- DoD CIO management review item.

Federal Customers

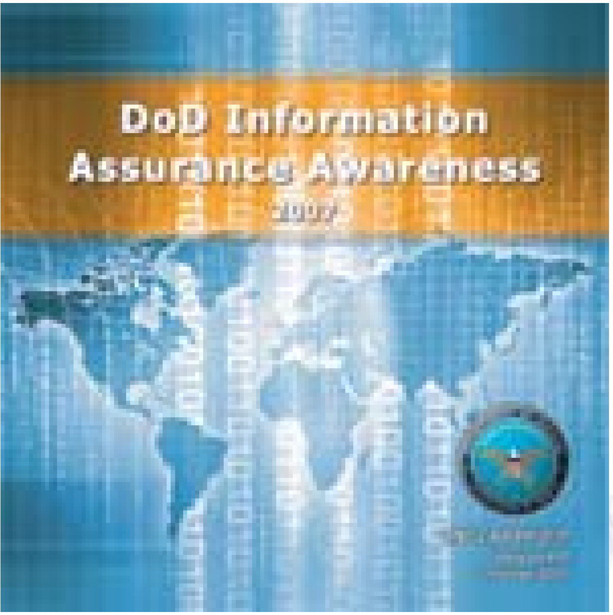
- Commodity Futures Trading Commission
- Defense Nuclear Facilities Safety Board
- Director of National Intelligence
- Education
- Energy
- Equal Employment Opportunity Commission
- Export Import Bank
- Federal Bureau of Investigation
- Federal Communications Commission
- Federal Reserve Bank
- Health and Human Services
- Housing and Urban Development
- Labor

Federal ISS Awareness

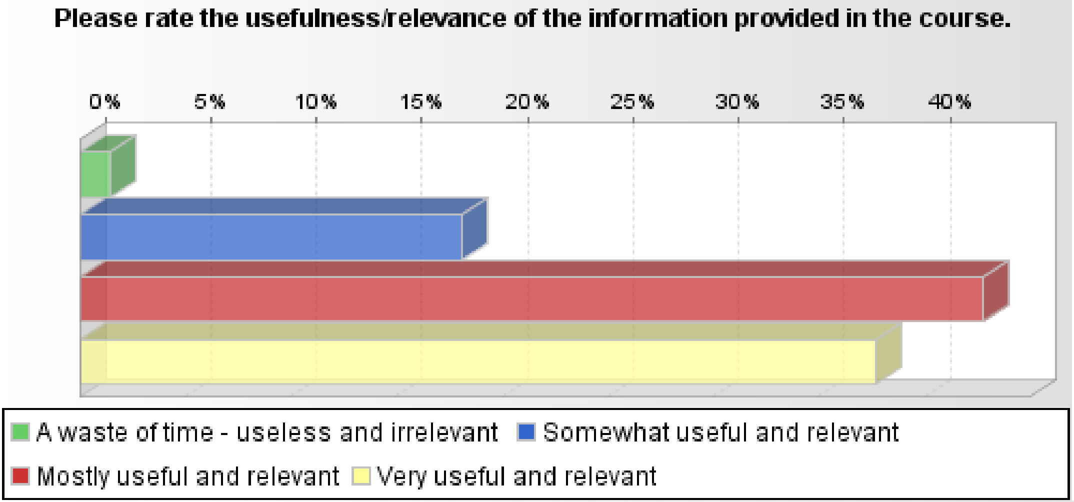


- Merit Systems Protection Board
- National Aeronautics and Space Administration
- National Mediation Board
- Nuclear Regulatory Commission
- Nuclear Waste Technical Review Board
- Office of Government Ethics
- Railroad Retirement Board
- Small Business Administration
- Transportation
- Treasury

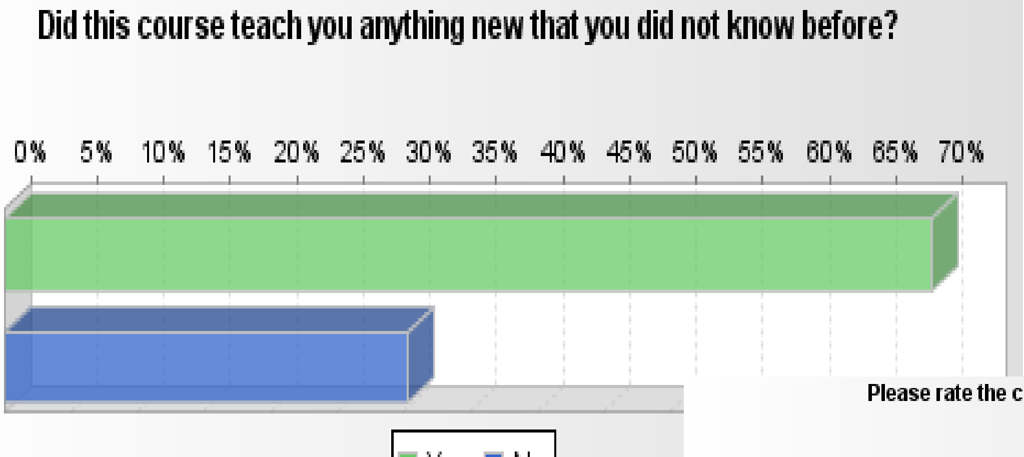
DoD IA Awareness



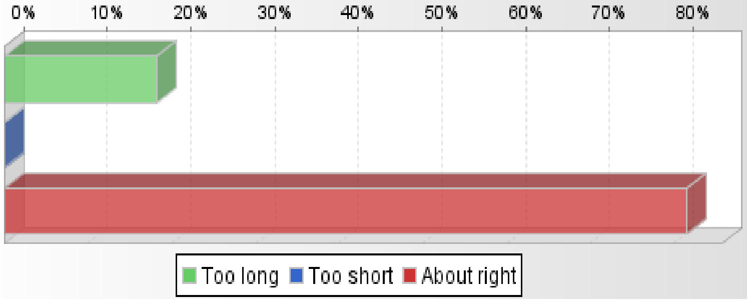
INFOSEC Awareness Training


Please rate the usefulness/relevance of the information provided in the course.

Useful/relevant information


Did this course teach you anything new that you did not know before?

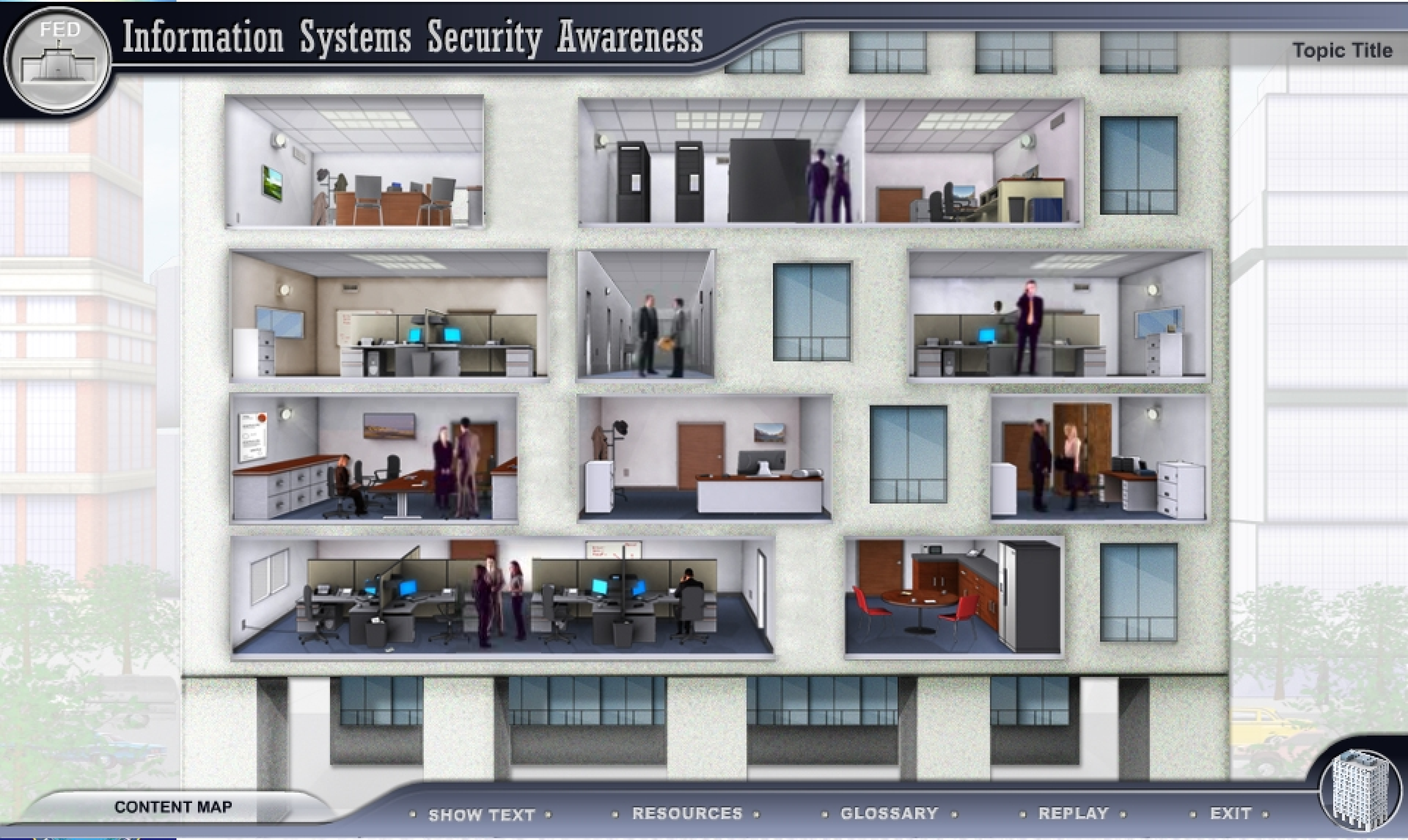
Teaches something new


Please rate the course length. Was the course?

Course is the right length

Survey of 10,000+ users

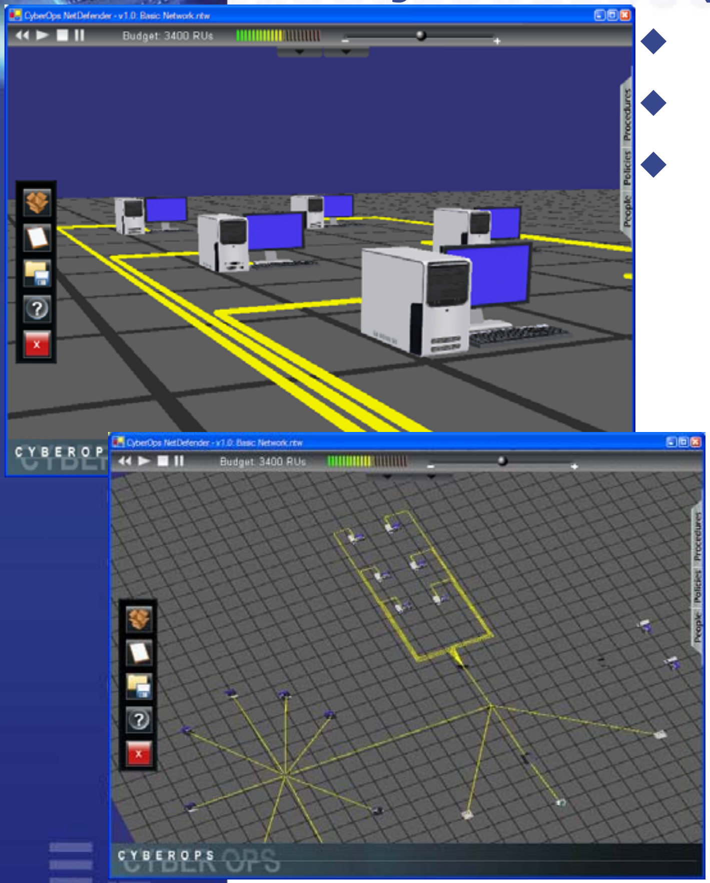
FY09 Awareness Product Design



CIO/NII
Enabling Net-Centric Operations

Training & Exercises

CyberOPs (DISA)



- Simple but powerful network layout presentation
- Realistic 3D models; accurate spatial representations
- Save & reuse networks as plain XML text – no binary data issues

  - Interactive 3D network configuration environment
  - Controllable discrete-event simulation engine
  - Automatic attack generation capability
  - Instructor-driven, customizable, scoring and performance measurement tools
  - Campaign play mode progressing from unsecured to MAC II, Sensitive networks
  - Customizable scenarios to target specific security issues
  - Printable performance reports
  - Complete tutorial and help modules

- Generates 10 different attack types in random sequences w/random levels of effectiveness: Data Modification – Jamming – Sniffer Programs – Data Theft – Malicious Code – Spoofing – Denial of Service – Peer-to-Peer – Social Engineering – Trusted Insider

Other Products

NetOps
NetOps: An Overview
Start Back Home Next End
Phishing Awareness
DAA
Designated Approving Authority
Information Assurance for DoD Auditors and IGs
PII
Personally Identifiable Information
IPv6
Internet Protocol version 6
IA Hot Subjects
Web-Based Training
TCP Reset • DDoS Attack on Routers
Spoofing Attacks • Physical Security
Remote Access/Remote Control • SNMP
Version 1.1
Unclassified
November 2006
Enhancing Information Assurance through Physical Security
Web-Based Training
2007

CAC Required

- Intro to HBSS
- HBSS
- SCCVI
- SCRI

http://iase.disa.mil

FY 09 Planned Initiatives

Virtual Training Environment (VTE) https://www.vte.cert.org

On-demand technical training curriculum covering IA, DoD IA Tools, and DoD 8570 certifications

- Move to .mil domain; reduce per seat cost; increase capacity to ~100,000
- Mirror on SIPRnet to support deployed and afloat forces

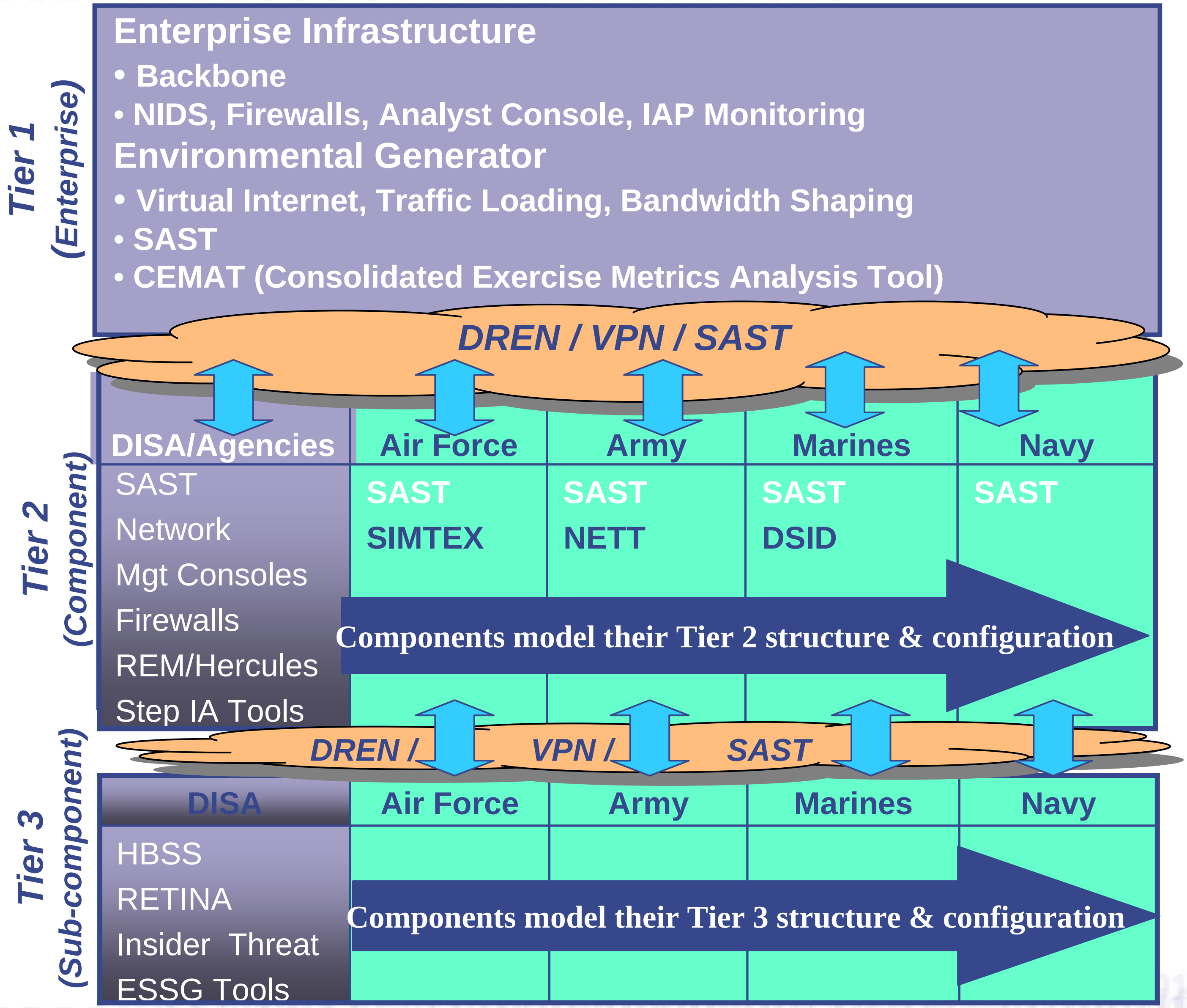
IA Range

A robust, “train as we fight” persistent virtual network operations environment:

- Exercise, test & measure personnel; rapidly build expertise
- Exercise, test & measure organizations
- Test & evaluate tools and techniques
- Access anytime, anywhere
- No risk to an operational network
- Service/agency autonomy/enterprise interoperability
- Build proficiency
  - Proactive intrusion prevention
  - Early detection of threat/attack
  - Accurate assessment of threat/attack
  - Rapid application of “best” defense

- ***NSDP-54/HSPD-23: Comprehensive National Cybersecurity Initiative***
- ***Need for personnel to get smarter faster to defeat all levels of threat***

Approach to an IA Range



Tier 1 (Enterprise)

Enterprise Infrastructure

- Backbone
- NIDS, Firewalls, Analyst Console, IAP Monitoring

Environmental Generator

- Virtual Internet, Traffic Loading, Bandwidth Shaping
- SAST
- CEMAT (Consolidated Exercise Metrics Analysis Tool)

DREN / VPN / SAST

Tier 2 (Component)

DISA/Agencies	Air Force	Army	Marines	Navy
SAST	SAST	SAST	SAST	SAST
Network	SIMTEX	NETT	DSID	
Mgt Consoles				
Firewalls				
REM/Hercules				
Step IA Tools				

Components model their Tier 2 structure & configuration

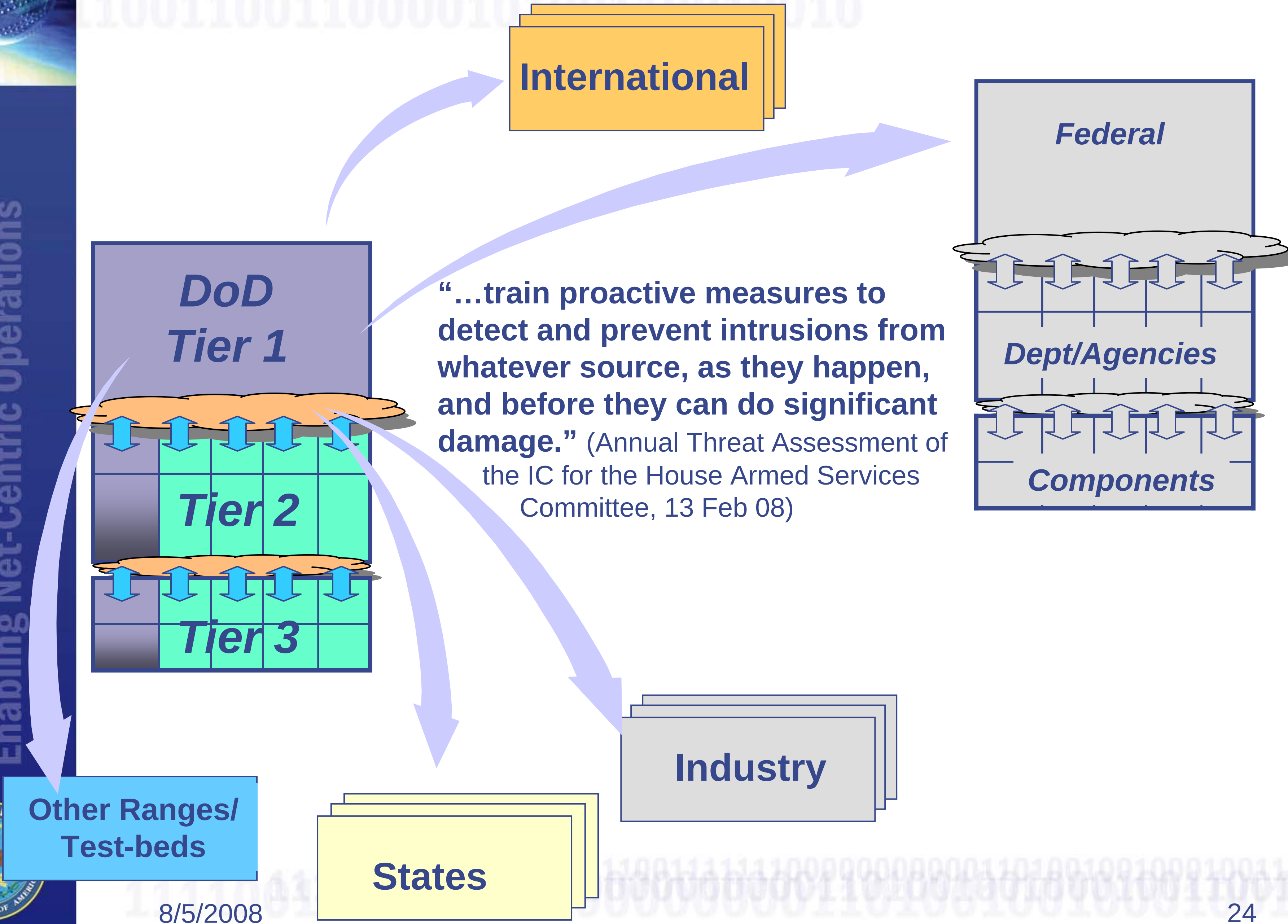
DREN / VPN / SAST

Tier 3 (Sub-component)

DISA	Air Force	Army	Marines	Navy
HBSS				
RETINA				
Insider Threat				
ESSG Tools				

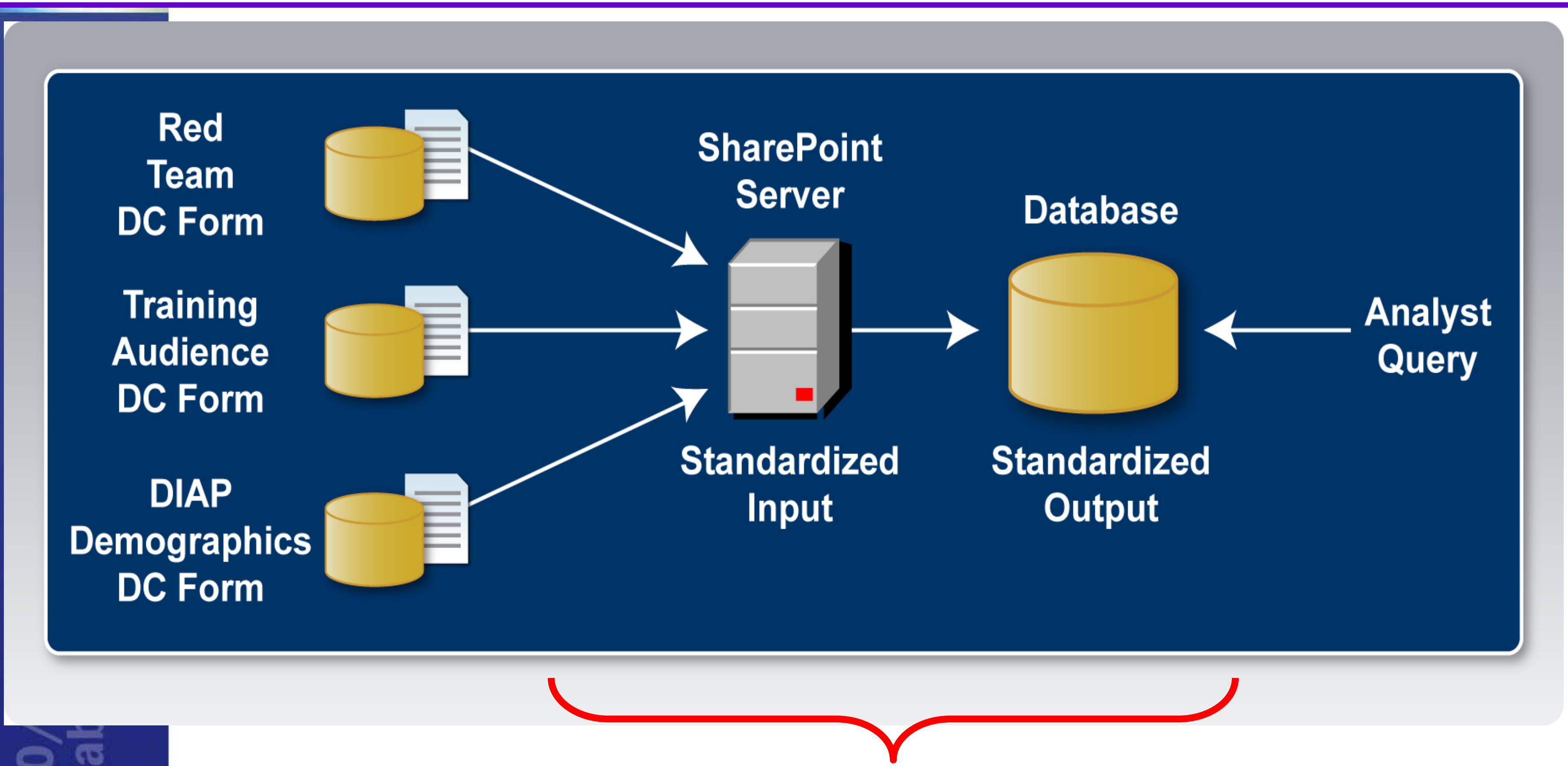
Components model their Tier 3 structure & configuration

IA Range Future/Potential Interfaces



"…train proactive measures to detect and prevent intrusions from whatever source, as they happen, and before they can do significant damage." (Annual Threat Assessment of the IC for the House Armed Services Committee, 13 Feb 08)

Data Collection Analysis



Consolidated Exercise Metrics Analysis Tool (CEMAT)

Trend Analysis Capability

Challenges

Challenges

- Identifying the workforce
- Ability to tag and track the workforce (databases)
- Educating leadership
- Personnel turnover (leadership & key staff)
- Fear of tests
- Managing expectations (of DoD, of certification providers)
- Bureaucrats
- Organizational: in-garrison vs deployed
- Outreach: Getting the information to the IA workforce
- Funding (and retaining funding) for training
- Metrics and evaluation
  - **Compliance** (Is the policy being implemented…as intended)
  - **Assessment** (Does it make a difference)

Parting Thoughts

- If I get my people certified they’ll quit and become contractors.
- I have a degree; I don’t need a certification.
- I’ve been doing the job for 15 years, I don’t need a certification.
- The certifications have no value; they don’t teach the DoD approach.
- I know people who passed the test but can’t do the job.
- I have money for training thru 2010…because of 8570
- I’m studying for the CISM. Its hard. But don’t water down the policy; there are too many people out here calling themselves IA professionals, but they don’t have a clue about security.
- Finally, I’ll be able to get rid of the [less than knowledgeable people] they assign to protect my network.
- Where commands got their people certified, retention was 80% or higher; commands that didn’t had retention rates of 10% and below.

AFCEA Solutions Conference: Information Assurance

- **<u>Awareness and Literacy for Government in the Cyber Age</u>**: Extending Cyber awareness and literacy to other disciplines beyond IT

- **<u>Growing Cyber Security Professionals for Tomorrow's Federal Workforce</u>**: Strengthening the cyber security workforce pipeline for the future?

- **<u>Building Cyber Security Professionals for Today</u>**: Improving the current USG Cyber security workforce to effectively defend our nation in cyberspace?

9-10 September 2008
Ronald Reagan International Trade Center

Active Government/Military and Academia $75
Industry (AFCEA Member) $295
Industry (Non-Member)$395

http://www.afcea.org/events/solutions

Detail

Baseline IA Certifications

Tech I	Tech II	Tech III
A+	GSEC	CISSP
Network+	Security+	SCNA
SSCP	SCNP	CISA
	SSCP	GSE

Mgmt I	Mgmt II	Mgmt III
GSLC	CISSP	CISSP
Security+	GSLC	GSLC
GISF	CISM	CISM

"Technical certifications are part of our personnel development and are considered… investment in our employees"
(private sector best practice)

IA Training and Certification Requirements

Training & Certification Requirement	Technical Category	Management Category	
	Level I - III	Level I - III	DAA **(US Gov't Employee only)**
Initial Training	Yes	Yes	Yes
IA Certification (From approved list)	Yes **(within 6 months)**	Yes **(within 6 Months)**	Yes **(DISA WBT or IRMC 4012)**
OJT/Familiarization	Yes **(for initial position)**	No	No
Local OS Cert; security tools/ devices	Yes	No	No
Refresher Training/ Continuing Ed	Yes **(as required by Certification)**	Yes **(as required by Certification)**	No
Re-certification	Yes **(as required by Certification)**	Yes **(as required by Certification)**	Yes **(every 3 years)**

Workforce Education, Training & Certification: A Snapshot

(Based on 482 respondents during one joint exercise)

	Total Players (%)	Players w/ Related Cert	Players w/ Related BA/BS, MA/MS	Players w/ Related AA/AS	Total w/ Related Degree	Received Military specific IA/CND Training	No IA/CND Training
Military (Active)	67%	18%	11%	16%	27%	82%	15%
Military (Guard)	7%	51%	12%	6%	18%	57%	3%
Military (Reserve)	1%	50%	50%	30%	80%	67%	16%
Gov't Civilians	7%	40%	20%	3%	23%	66%	9%
Contractor	18%	74%	27%	23%	50%	89%	6%
Totals	100%	31%	17%	16%	33%	78%	11%

For the exercise most sites had the "A" team on double shifts, Margin of Error is likely in the negative

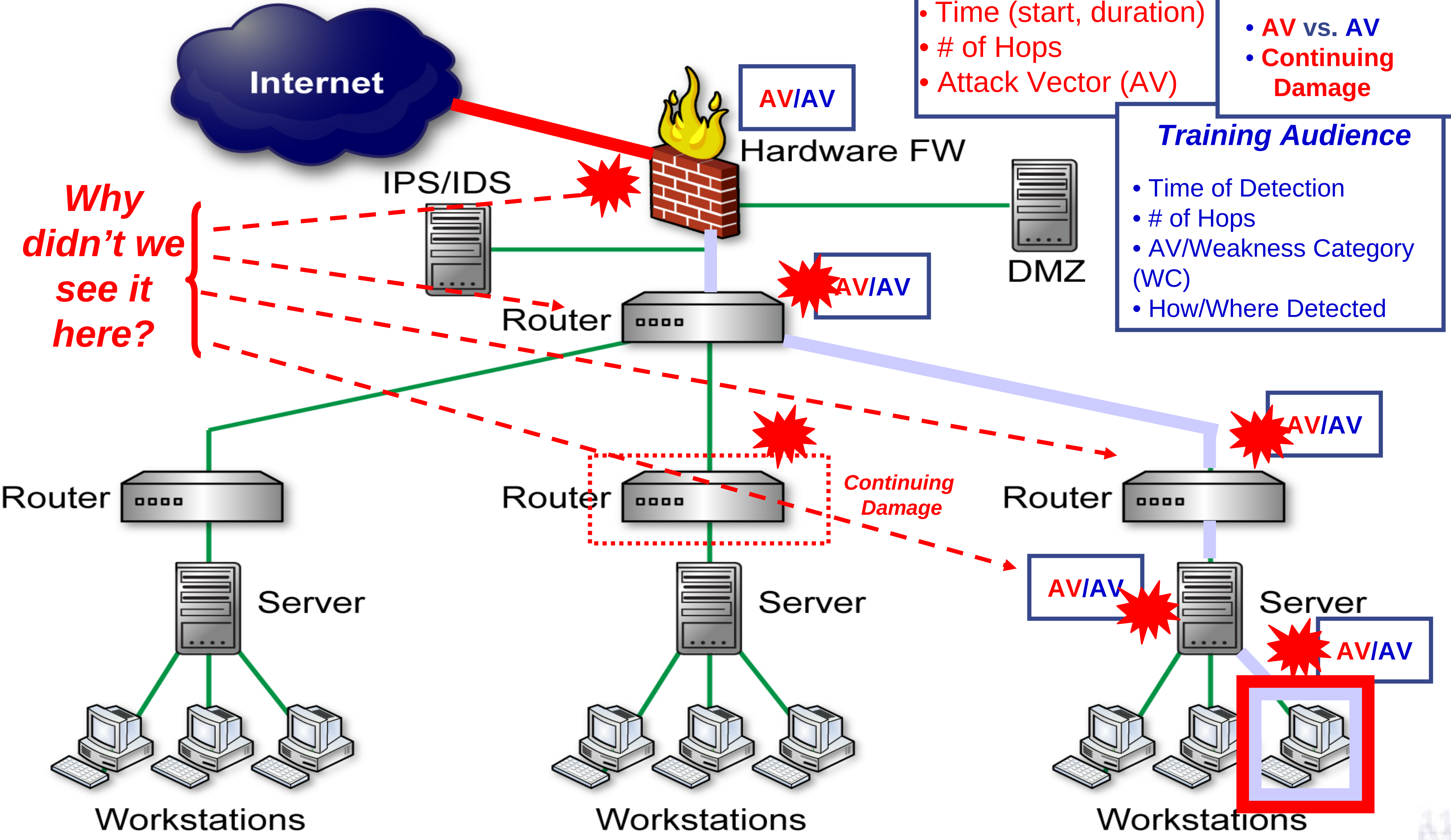
IA Range Drivers

- **DoD IA Strategy (Goal 5): An IA workforce able to…effectively employ IA tools, techniques and strategies to defeat adversaries, and proactively identify and mitigate the full spectrum of rapidly evolving threats to defend the Net**
- **National Military Strategy for Cyberspace Operations: more robust exercising w/increased realism in a combined cyberspace operations range**
- **NSDP-54/HSPD-23: Comprehensive National Cybersecurity Initiative**
- **Need for personnel to get smarter faster to defeat all levels of threat (1G, 2G, 3G)**
- **T&E of enterprise tool effectiveness individually and in combination with other tools and devices in a realistic operational environment, including impact of, and on, the human factor (training; workload)**
- **Automated T&E data collection and reduction, analysis capability to replace man-power intensive methods/reduce cost**
- **Rigorous, timely, standardized reporting across all exercises to address IA and workforce metrics and trends over time; impact real-world operations *(e.g., rapid detection of intrusions vs accuracy of assessment)***

User Requested Capabilities

- Availability 24/7/365
- Flexible / Scaleable
- Support Service/Component specific CND Exercises as well as Joint events
- Unclassified but closed network; w/ability to connect to higher classification networks
- Supports Service/Component specific equipment (HW/SW; simulators)
- Capable of repeat/replay/refresh scenarios
- Navigation and targeting down to the host level – Red Team Exploit
- Linked pre- post event training (e.g., via CBT/Web)
- Current architecture; but evolves as Enterprise evolves
  - Full suite of services – voip/im/mail/p2p
  - HBSS, PKI/CAC
  - Ipv6 (by FY10)
- Sufficient robustness to allow for JTF-GNO directives to be implemented
- Supports Wireless/Mobile devices
- Fake internet
  - thousands of sites; some with malicious content
  - Includes .com/ .org/ .gov/ .edu etc.
- Provides capability for Red Team attacks from fake internet (including “cover fire” to mask the attacks for range of threats

Anatomy of an Attack



Red Team

- Time (start, duration)
- # of Hops
- Attack Vector (AV)

Analysis

- **AV vs. AV**
- **Continuing Damage**

Training Audience

- Time of Detection
- # of Hops
- AV/Weakness Category (WC)
- How/Where Detected