



IA Personnel Readiness: Training, Certification and Workforce Management

George Bieber

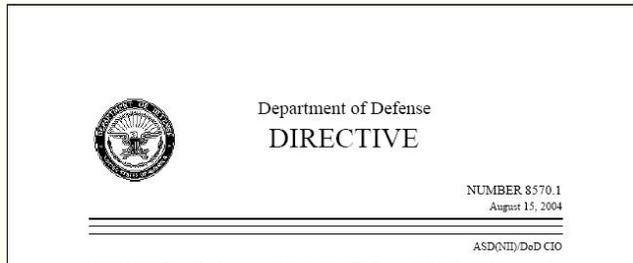
Defense-wide IA Program (DIAP)

(703)-602-9980

george.bieber@osd.mil



Outline



SUBJECT: Information Assurance Training

References: (a) [DoD Directive 8500.1](#)
(b) [DoD Instruction 8500.1](#)
February 6, 2003
(c) DoD Directive O-853
January 8, 2001
(d) Section 3544 of title 48, U.S.C.
(e) through (h), see enclosure

1. **PURPOSE**

This Directive:

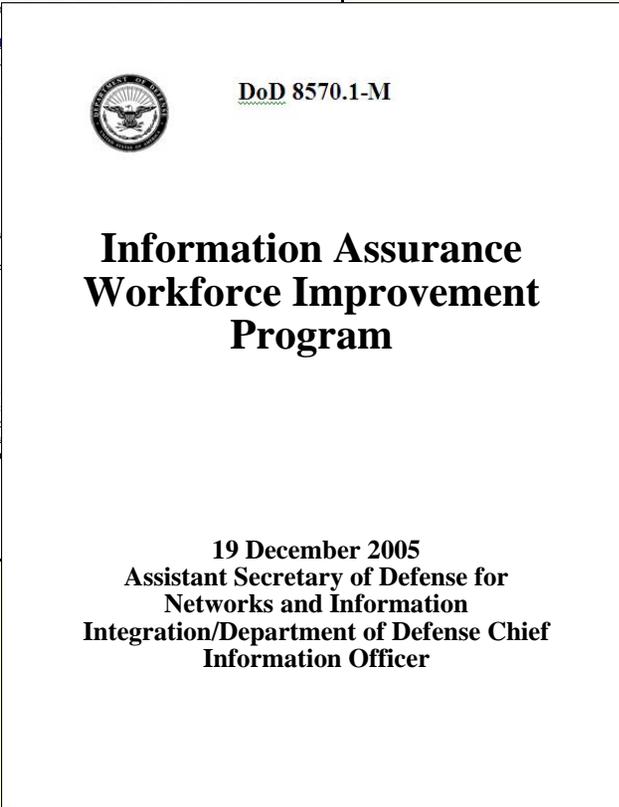
1.1. Establishes policy and assigns responsibility for information assurance certification, and workforce management for information assurance through (d) for Department of Defense information assurance certification, and workforce management.

1.2. Authorizes the publication of this Directive.

2. **APPLICABILITY AND SCOPE**

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Office of the Chairman of the Joint Chiefs of Staff, the Office of the Inspector General of the Department of Defense, the Department of Defense Field Activities, and the Department of Defense (hereinafter referred to as "DoD").



- ◆ Policy
- ◆ Objectives & Impact
- ◆ Governance & Oversight
- ◆ Making it Work
- ◆ Schedule
- ◆ Near Term Actions
- ◆ Moving Forward



IA Training & Certification in DoD

◆ Military Communications/Electronics Board (MCEB) endorses certification (Aug 97)

HR

HR

◆ ASD/C3I & USD/P&R memo: *IA Training & Certification* (29 June 98)

System Administrators, maintainers and end users

◆ OSD, *IA/IT HR IPT Report: IA and IT Training, Certification and Personnel Management in the Department of Defense*. (27 Aug 99)

HR

◆ DepSecDef memo: *Implementation of the Recommendations of the IA & IT HR IPT on Training, Certification, and Personnel Management in the Department of Defense* (14 July 00)

End State: sustained pool of skilled IA/IT professionals

◆ CJCSI 6510.01C *Information Assurance & Computer Network Defense* (May 01)

◆ DoD D 8500.1 *Information Assurance* (24 Oct 02)

◆ DoDI 8500.2 *IA Implementation* (7 Feb 03)

◆ CJCS 6510M *IA & CND Manual* (Apr 03)

◆ ASD/NII Policy Memo: *DAA Training & Certification Requirements* (15 July 03)

HR

◆ DoDD 8570.1 *IA Training, Certification and Workforce Mgmt* (15 Aug 04)

HR

◆ DoD 8570.1M *IA Workforce Improvement Program (IA WIP)* (19 Dec 05)

1997 1998 1999 2000 2001 2002 2003 2004 2005



IA Personnel Readiness

Vision

A professional, **efficiently managed** IA workforce with knowledge and skills to **securely configure** information technology, **effectively employ** tools, techniques and strategies to defeat adversaries, and **proactively identify and mitigate** the full spectrum of rapidly evolving threats and vulnerabilities in order to **protect the network**

The Road Ahead

- ◆ Provide Components the capability to identify, tag, track and manage their IA workforce
- ◆ Establish a DoD enterprise-wide baseline IA certification requirement to validate knowledge, skills of IA personnel
- ◆ Leverage private sector capabilities to facilitate training; raising the bar for IA knowledge and skills needed by DoD
- ◆ Provide corporate oversight and enforcement capability
- ◆ Extend the discipline to non-IA/IT leadership at all levels

"Operational controls are IT security methods that are primarily implemented and executed by people – not systems...." Naval Audit Service



Policy

DoDD 8570 (signed 15 Aug 04)

- ◆ Identify, train and certify privileged users & IA managers to DoD baseline requirement
- ◆ Assign position specialty code/skill identifiers to personnel with privileged access; track key data in Component personnel/manpower databases of record
- ◆ Identify positions in manpower databases
- ◆ Record, track contractors IA certification status in DEERS
- ◆ Require IA in all levels of professional military education
- ◆ Applies to civilian, military, local national, contractor; full time or "as assigned"; regardless of series

DoD 8570.1M (signed 19 Dec 05)

- ◆ Defines IA workforce categories, levels, and 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*
- ◆ Requires continuous learning or re-test necessary to maintain certification status
- ◆ Specifies reporting requirements
- ◆ Establishes Oversight Advisory Council



Objectives and Impact

Objectives

Impact on DoD

Certify the Workforce

- ◆ Improved IA posture
- ◆ Foundation of a professional IA workforce
- ◆ Mechanism to rapidly “raise the bar” on IA skills

Manage the Workforce

- ◆ Ability to place trained/capable personnel in IA jobs
- ◆ Basis for defining standard IA personnel requirements

Sustain the Workforce

- ◆ Elevate priority of IA for training dollars
- ◆ Enable personnel to hone IA skills, keep current with latest technology, threats and vulnerabilities, tools and techniques

Extend the Discipline

- ◆ Leaders at all levels who understand the impact of IA on mission accomplishment
- ◆ A model for Allies and coalition partners
- ◆ IA literacy for other critical workforces (e.g., acquisition)

“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	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)



What's Changed Due to SD106 Process

- ◆ Stronger OSD oversight:
 - ◆ *Review and validate/approve* Component plans for implementing 8570/DoD baseline
 - ◆ **Methodologies** used to identify employees performing IA functions
 - ◆ **Tracking processes** used to determine specialized training received
 - ◆ **Impact** of using particular methodologies/processes
 - ◆ **Reliability and relevance** of Component reported metrics & information
 - ◆ **Components to provide a plan (POA&M)** for implementing 8570
 - ◆ Components to provide plan to track, monitor completion of security awareness training
 - ◆ Components to report on Component specific training and certification activities
- ◆ Continuous learning linked to requirement to maintain certification
- ◆ Waivers permitted in combat zone (except Level I)
- ◆ DAA re-certification requirement; IRMC/CNSS 4012 certificate as alternative



H.R.1815

National Defense Authorization Act for Fiscal Year 2006



Amends Chapter 101 of title 10, United States Code, to allow Services to use appropriated funds to pay for commercial certifications

Subtitle C – Education and Training

Part IV – Other Matters

SEC. 538. PAYMENT OF EXPENSES OF MEMBERS OF THE ARMED FORCES TO OBTAIN PROFESSIONAL CREDENTIALS.

(a) In General- **Chapter 101 of title 10, United States Code, is amended** by adding at the end the following new section:

Sec. 2015. Payment of expenses to obtain professional credentials

(a) Authority- The Secretary of Defense and the Secretary of Homeland Security, with respect to the Coast Guard when it is not operating as a service in the Navy, **may pay for--**

(1) expenses for members of the armed forces to obtain professional credentials, including expenses for professional accreditation, State-imposed and professional licenses, and professional certification; and

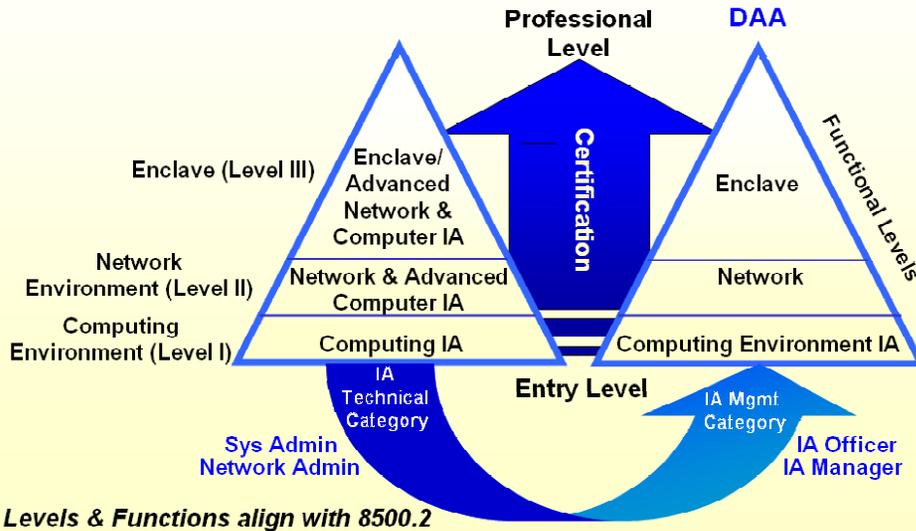
(2) examinations to obtain such credentials.

(b) Limitation- The authority under subsection (a) may not be used to pay the expenses of a member to obtain professional credentials that are a prerequisite for appointment in the armed forces.

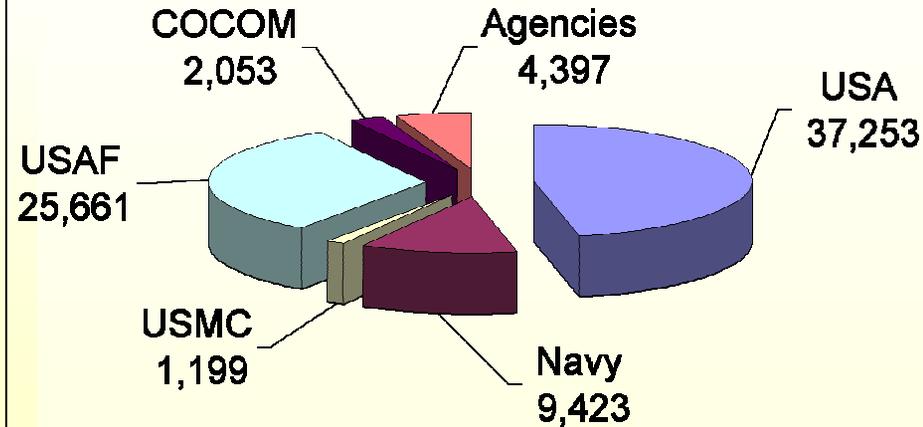


IA Workforce Focus

Defining the IA Workforce Structure



Identifying Workforce Size, Distribution*



* Based on 05 FISMA Report; excluding NSA, DIA;

Equating Certification to Personnel "Authority to Operate"

Cyber Security Corps
Joe Kelly
Issued: 10-04-03
Expires: 10-03-06

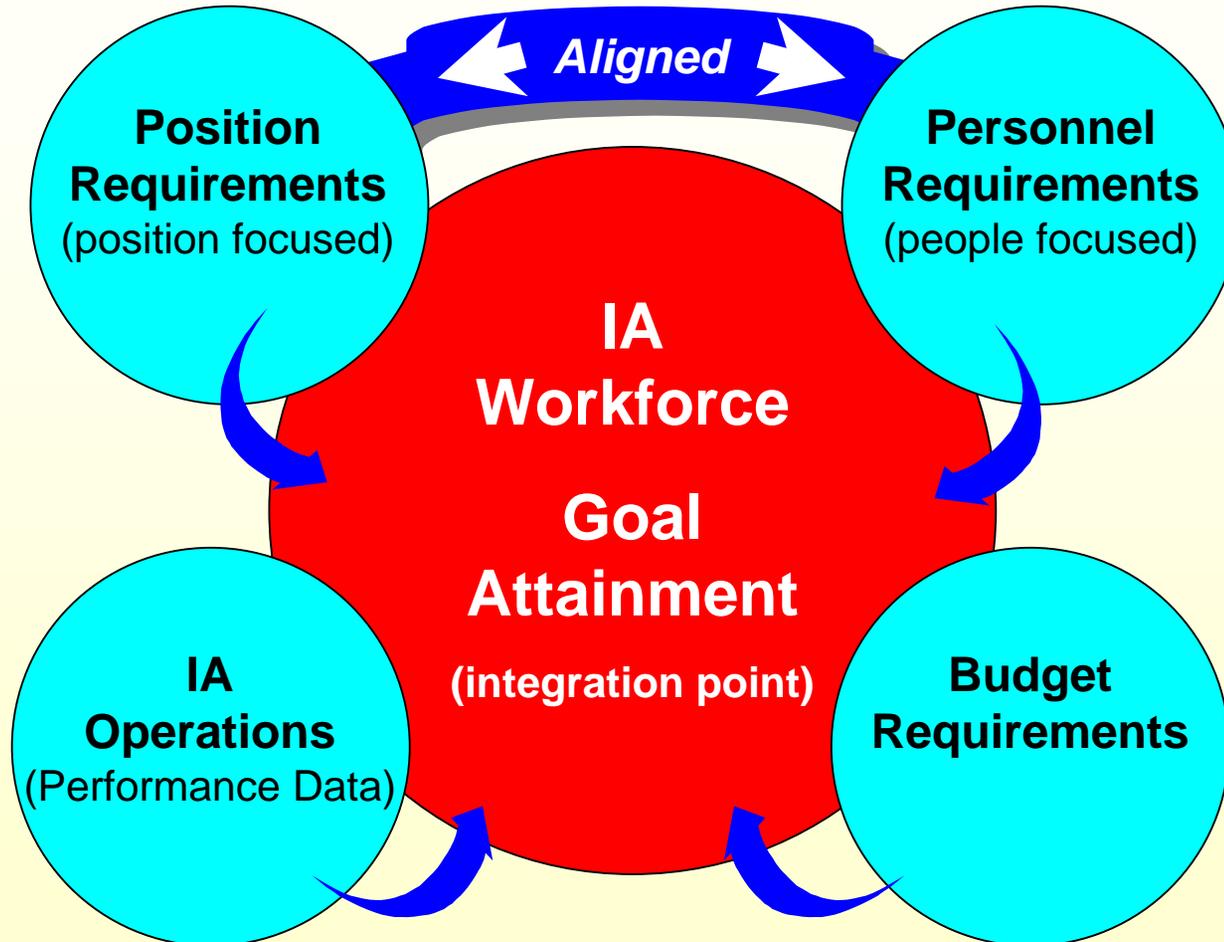
Network Security Certified Professional

Planning future areas for IA certification

- ◆ Certifiers and Accreditors
- ◆ IA architects, engineers
- ◆ Red Team members
- ◆ CND/SP members
- ◆ IDS analysts
- ◆ Auditors



Making it Work

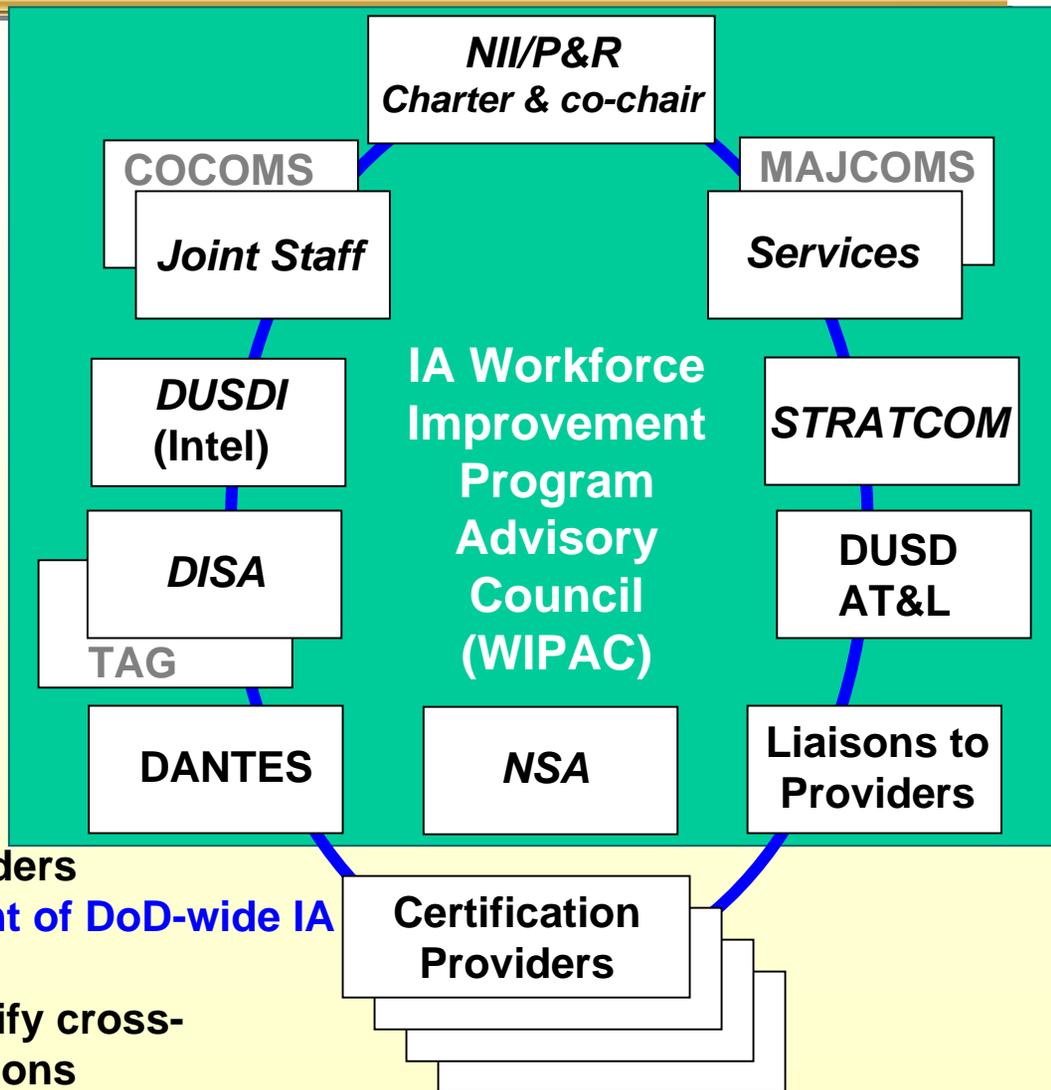


"Operational controls are IT security methods that are primarily implemented and executed by people – not systems...." Naval Audit Service



Governance and Oversight

- ◆ Establish process to add/delete certifications
- ◆ Review/update levels & functions
- ◆ Monitor program progress; impact on IA posture
- ◆ Review Component programs & plans to validate compliance
 - ◆ Implementation & sustaining plans
 - ◆ Plans, methodologies to track, monitor, document personnel awareness and training completion
- ◆ Conduct assessments to ensure validity of functions, training & certification requirements per 29CFR1607
- ◆ Provide feedback to certification providers
- ◆ Prioritize requirements for development of DoD-wide IA training content
- ◆ Engage IA training community to identify cross-Component IA training issues & solutions



*P&R: Defense Human Resources Activity TAG: Training Action Group



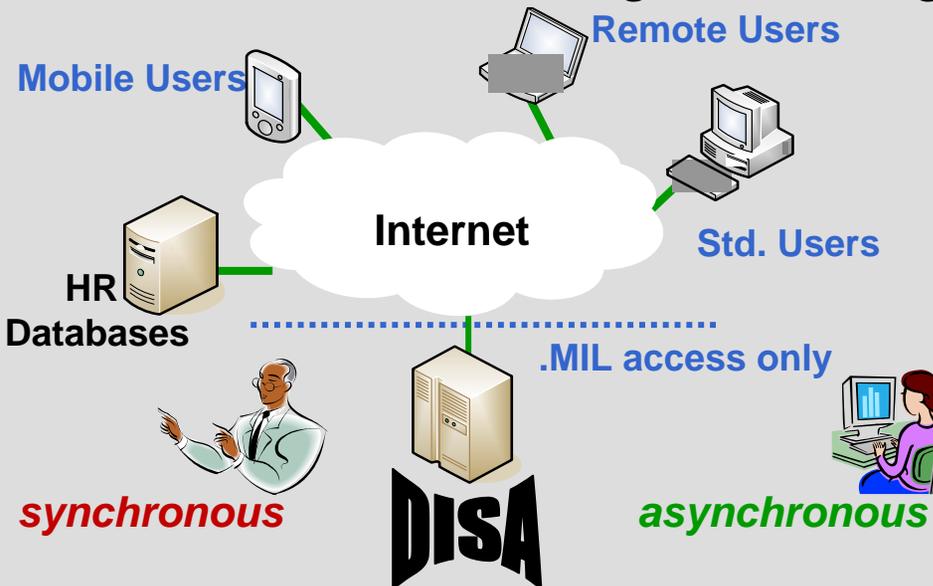
Robust Advanced Distributive Training

IA Training & Awareness (NII)

(Policy, Concepts, Procedures; Professionalization)



Distributive training & mentoring



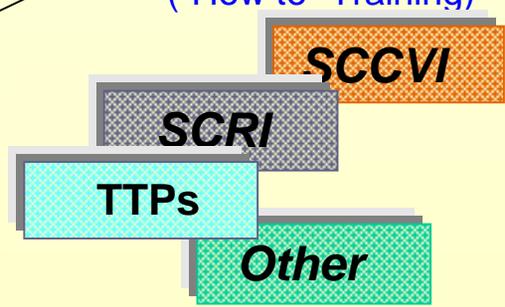
Rapid Experience Builder

System Administrator Simulation Trainer (SAST)

Filling the experience deficiency in cyber security staff through simulation



IA Tools ("How to" Training)



COTS Training Products, Libraries



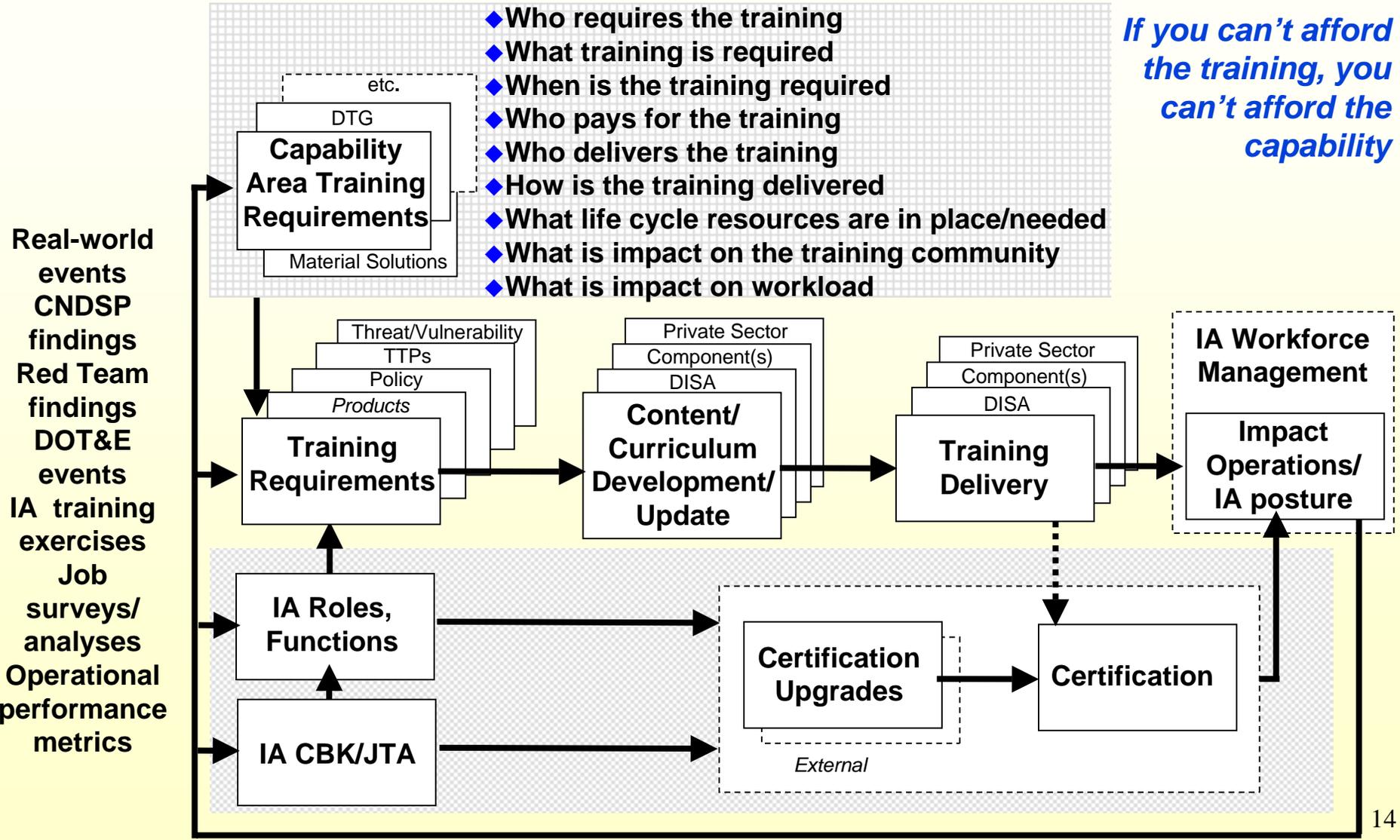
Certification Pre-Tests



A recognized global leader in IT governance, control and assurance.



Foundational Activities: Training





DANTES: Manage Certification Test Vouchers

Defense Activity for Non-Traditional Education Support

- ◆ Existing voluntary certification support program for military personnel
- ◆ Partnerships with critical players:
 - ◆ Education Centers on military bases
 - ◆ Test providers (Nat'l Test Centers)
 - ◆ Certification providers
 - ◆ OSD/NII and OSD/P&R

Certification Program

diploma

- ✦ DANTES test sites administer 15,000 to 20,000 certification exams each year.
- ✦ Certification examination fall into the basic categories listed below.

Medical	Electronics
Engineering	Automotive
Information Technology	Construction
Finance	Environmental
Food/Hotel Management	Physical Fitness

Tech I *	Tech II	Tech III
A+	GSEC	CISSP
Network+	Security+	SCNA
SSCP	SCNP	CISA
SSCP	SSCP	GSE
Mgmt I	Mgmt II	Mgmt III
GSLC	CISSP	CISSP
Security+	GSLC	GSLC
GISF	CISM	CISM

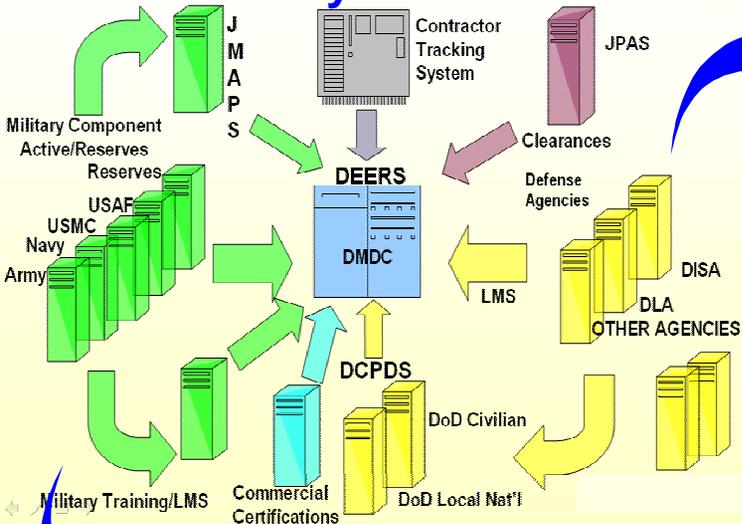
- ◆ Paperless voucher system
- ◆ Database to track, report voucher usage
- ◆ Facilitate re-distribution of expiring vouchers
- ◆ Ability to support civilian workforce



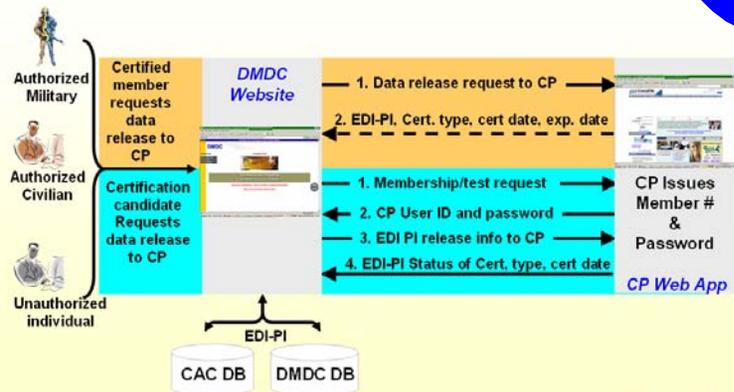
DMDC: Streamline IA Training & Certification Data Exchange



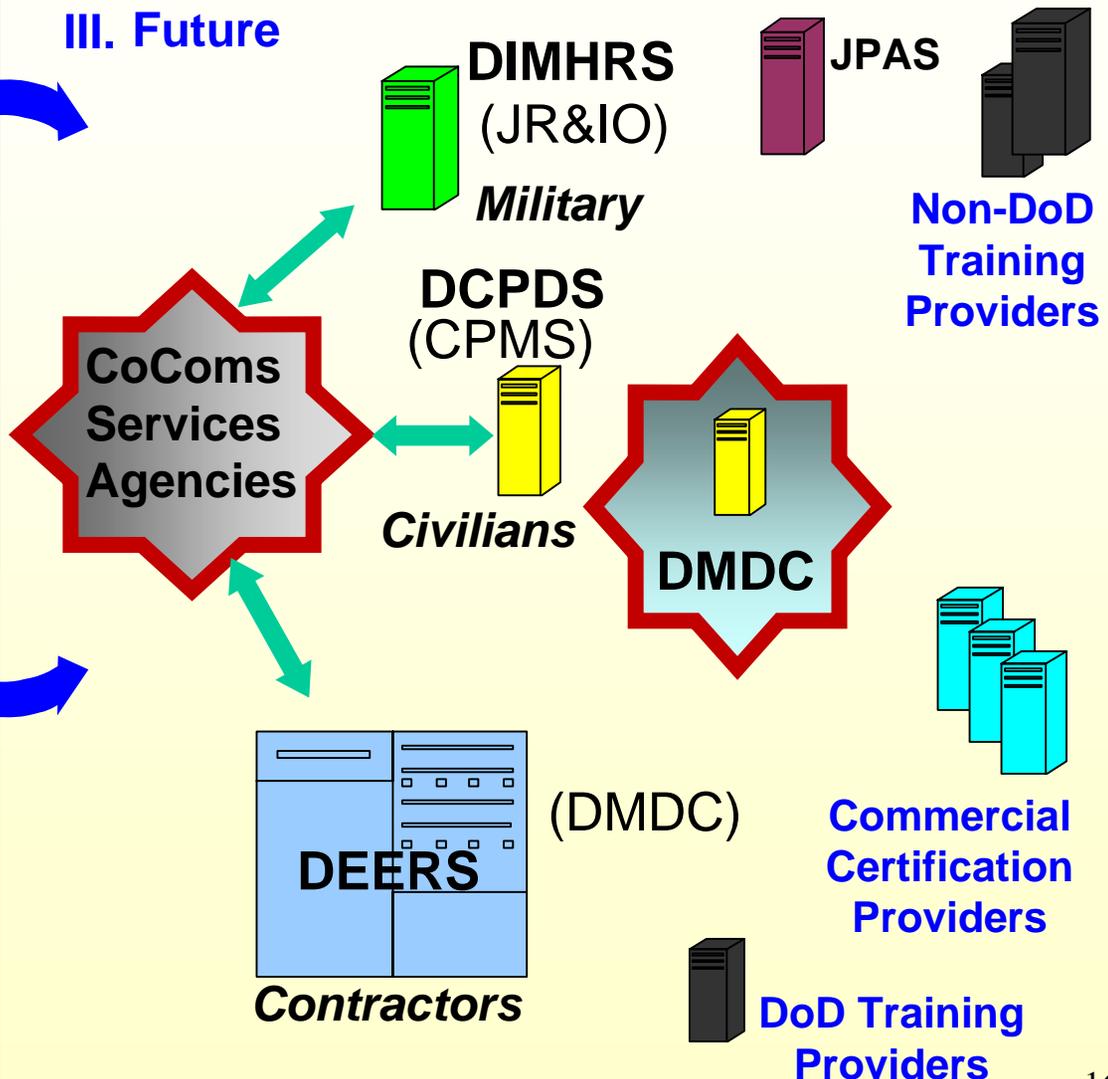
I. Today



II. Proposed Pilot



III. Future



UNCLASSIFIED//FOUO

Defense Manpower Data Center (DMDC)



Schedule (DoDD 8570.1; 8570.1M)

	<i>Startup</i>		<i>Implement</i>				<i>Maintain</i>		
	FY05	FY06	FY07	FY08	FY09	FY10	FY11	FY12	FY13
Databases		Upgrade			DIMHRS				
People		Identify, code							
Dollars		QDR	PDM III (20 Dec 06) \$ FY07-11						
		POM 08	PB08 FY08-13 (Components POM)						
Certification		?\$	8,000	24,500	25,500	27,000			

- ◆ Based on FISMA reporting: 80,000 total military & civilian IA personnel
 - ◆ Certify 10% first year; 30% each year for next 3 years
 - ◆ Assume 5% annual attrition rate
 - ◆ Average \$300/certification test; \$75/year for fees



Near-Term Actions

Due Date	Requirement	Explanation
04/14/06	Identify the Office of Primary Responsibility (OPR)	Identify the Office of Primary Responsibility (OPR) for implementing requirements of the references and a specific individual point of contact (POC). The OPR and its POC must be able to represent and integrate human resources/training, budget/finance, operations, as well as information assurance requirements of their Component.
04/30/06	Submit quarterly progress report	Submit the first quarterly progress report to DIAP
04/30/06	Identify IA WIPAC Representative	Components listed ...as members of the Information Assurance Training, Certification, and Workforce Management Advisory Council identify their representative. This Council's name will be changed in its Charter to the Information Assurance Workforce Improvement Program Advisory Council (IA WIPAC). Component representatives to the IA WIPAC must have sufficient authority to effectively represent their Component including human resources/training, budget/finance, operations, and information assurance matters. The Reference establishes the IA WIPAC and its responsibilities.
07/15/06	Submit draft Implementation Plan	Submit draft implementation plan to the IA WIPAC. Include plans for budget; work breakdown structure; milestones to identify, train, and certify the IA workforce; and plans for updating and populating personnel and manpower databases.
10/01/06	Initiate IA WF data solutions	Initiate solutions for tagging and tracking IA personnel status.
12/30/06	10% IA Workforce Certified	Complete certification of 10% of the IA Workforce.
12/30/06	Submit Final Implementation Plan	Submit updated implementation plan to the IA WIPAC to include progress in 2006 and planned actions for 2007.



The Year Ahead

- ◆ Publish language in DFARS for contractors to meet requirements
- ◆ Institutionalize IA workforce management capability
 - ◆ Existing database upgrades (personnel, manpower, training, other)
 - ◆ Data flow/processes between private sector and DoD and within DoD
- ◆ Charter the DoD IA workforce improvement program advisory council (WIPAC)
- ◆ Continue the DoD-wide Job-Task Analysis (JTA); document DoD IA skills
 - ◆ Define a common language of IA-related work and worker requirements
 - ◆ Enable better mapping of certifications against job functions
 - ◆ Enable a common basis for accreditation
 - ◆ Support validation studies per 29CFR1607
- ◆ Engage vendor specific certifications (e.g., Microsoft, CISCO)

It [getting the certification] REALLY wasn't a big deal once we got past the idea that it HAD TO BE DONE which was a bigger issue at the employee level than with the management. (COL, US Army)



More to Do

- ◆ Integrate DoD schools, CNSS standards & certificates, training exercises, conferences and other knowledge sharing into program as:
 - ◆ Source of training for certifications (A+, Security+, CISSP etc.)
 - ◆ DoD/Component layer of a comprehensive certification/professional program; address policy, processes & tactics & techniques
 - ◆ Satisfy continuous learning requirement
- ◆ Address training and certifications requirements of other portions of the IA workforce (e.g., CNDSP team members; engineering and architecture)
- ◆ Promote rigor and use of DoD best practices in commercial certifications to enhance DoD IA readiness
 - ◆ ISO 17024 accreditation is basic requirement imposed on IA certifications
 - ◆ Performance-based element to testing (vice multiple choice)
 - ◆ Continuing learning/re-test requirement to maintain certification status
 - ◆ Better define what is accepted for continuing learning credit
 - ◆ Incorporate DoD IA best practices (DISA STIGS, NSA Guidelines)

“Within...[our company’s] IT Security Office, credentials such as the CISSP are valued, acknowledged and celebrated.” (private sector best practice)



More to Do

◆ Pursue initiatives with enterprise-wide potential to increase ROI/Leverage capabilities/pool resources

- ◆ Expand performance-based training (e.g., Simulation Trainers, BULWARK DEFENDER IA combat training exercises)
- ◆ Provide access to on-line training/self-assessment/certification
- ◆ Manage test voucher usage

◆ Other considerations

- ◆ Structure (e.g., reduce personnel performing IA as an “other duty”)
- ◆ Who we assign (and train) (e.g., aptitude, skill); and who instructs
- ◆ What we train (e.g., content, currency, relevance)
- ◆ How we train (e.g., traditional classroom, web, simulation, **study time**)

On certification: “It...forced me to finally buckle down and do a bit of studying and focus on some areas where I was a bit lacking.” (Devin, US Army, Kwajalein)



Moving Forward

- ◆ Culture change -- leadership commitment and communication essential
- ◆ Governance and management crucial to success
- ◆ Human Resources (HR) needs to be a full partner
- ◆ Treat as opportunity to dramatically improve IA workforce/IA posture
- ◆ Protect dollars

We had bad luck with one CISSP class...and only 10% passed the exam That was a function of poor exam prep by the students, not a bad class or instructor. It took a while to get everyone over their fear of the exam, but as some passed, they started training the rest and it all fell in place.