Certification in DoD

George Bieber

March 17, 2011

Agenda

- Background
- 2011 IA WIP Results
- Commercial Certifications

IA Workforce Landscape circa 2003

- **No specific IA workforce management policy** (show me where it says I have to do it)
- **Unknown size/composition of the IA workforce**
  - 170,000 w/IT/IT management designators (military and civilian)
  - No military IA career path, skill indicators
  - Unknown number of personnel w/IA as "additional duty" in and/or outside IT designators
  - Wide year to year fluctuation in DoD FISMA report re personnel w/*significant IT security responsibilities** (doubled from 44,000 in FY03 to 89,000+ in FY04)
- **DOD IG Findings:** DoD lacks ability to verify/validate self-reported FISMA data (databases)
- **Schools unable to keep pace with the challenge**
  - Instructor knowledge & currency
  - Curriculum currency
- **Recognition of rapid change; but no requirement for continuous learning**
  - Components funding training for certifications, and often for tests as part of training
  - Didn't know how many of which certifications
- **Previous effort to implement a meaningful internal certification had failed**
  - MCEB: certify the workforce (1997)
  - DEPSECDEF memo (2001): certify the workforce
- **Concern over lack of training, but relatively few training courses available**
  - Minimal exercise at individual or unit level; no evaluation of IT/IA training
  - Personnel trained in IA -- then used in non-IA positions

** Not defined by OMB*

Strategic Objectives

Objective	*Impact*
Train & 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	◆ Elevate priority of IA for training dollars ◆ Enable personnel to hone IA skills, keep current with technology, threats and vulnerabilities, tools, techniques
Extend the Discipline	◆ Leaders understand impact of IA on mission accomplishment ◆ A model others can apply ◆ IA literacy for critical non-IT disciplines (Legal, LE)
Evaluate the Workforce	◆ Leadership visibility into the IA workforce ◆ "Product /process improvement" ◆ Measure impact on IA posture

2010 IA WIP Annual Report Results

Overall DoD Score

Yellow

Workforce Management	Trained	Certified	Qualified
Green	**Green**	**Yellow**	**Red**
90% of identified IA positions have been filled	**91%** of IA personnel have been trained	**67%** of IA personnel have obtained an IA baseline certification	**26%** of IA personnel are fully qualified

Filled: % of civilian & Military IA positions that are occupied & the number of IA contractors employed
Trained: % of IA personnel who either completed training in the last 3 years that included IA content related to their position and/or are certified (as defined below)
Certified: % of IA personnel who hold an IA certification that corresponds to the appropriate 8570 category and level.
Qualified: % of IA personnel who meet all the qualifications listed in AP3.T1 of 8570.01-M

Workforce Management	Training	Certification	Qualified
< 50% filled - Red 50 – 80% filled – Yellow > 80% filled - Green	< 50% trained – Red 50 – 80% trained – Yellow >80% trained – Green	<40% certified – Red 40 – 69% - Yellow >69% Green	<40% certified – Red 40 – 69% - Yellow >69% Green

IA WIP Qualifications

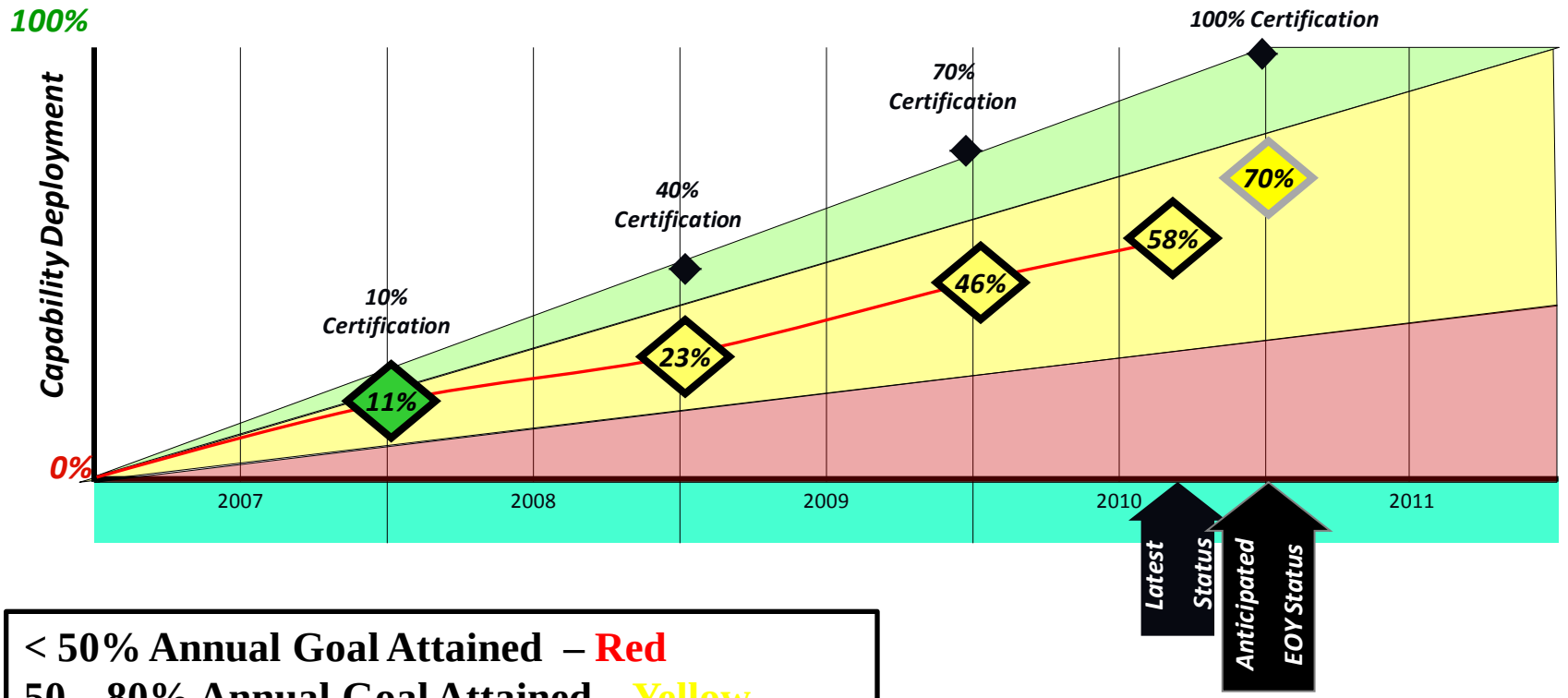
(DoD CIO Memo 30 April 2010)

	IAT I-III	IAM I-III	IASAE I-III	CND-A, CND-IS, CND-IR, CND-AU and CND-SPM
Initial Training*	Yes	Yes	Yes	Yes
IA Baseline Certification	Yes (within 6 months)	Yes (within 6 months)	Yes (within 6 months)	Yes – IAT and CND (within 6 months)
OJT Evaluation	Yes (for initial position)	No	No	Yes (except CND-SPM)
CE Certification	Yes	No	No	Yes (except CND-SPM)
Maintain Certification Status	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)	Yes (as required by certification)
Continuous Education	Yes (as required by Component and certification)	Yes (as required by Component and certification)	Yes (as required by Component and certification)	Yes (as required by Component and certification)
Background Investigation	As required by IA level and Reference (b)	As required by IA level and Reference (b)	As required by IA level and Reference (b)	As required by CND-SP level and Reference (b)
Sign Privileged Access Statement	Yes	n/a	n/a	Yes (except CND-SPM)
Experience	IAT I: Normally 0 to 5 or more years of experience in IA technology or a related field.	IAM I: Usually an entry level management position w/ 0 to 5 + years of management experience.	IASAE I: Usually entry level IASAE position w/ 0 or more years of IASAE experience.	Recommended years of experience in CND technology or a related field: CND-A: at least 2; CND-IR: at least 5 CND-AU: at least 2
	IAT II: Normally has at least 3 years in IA technology or related area.	IAM II: Usually has at least 5 years of management experience.	IASAE II: Usually has at least 5 years of IASAE experience.	CND-IS: Recommend at least 4 years of experience supporting CND and/or network systems and technology
	IAT III: Normally has at least 7 years experience in IA technology or a related area.	IAM III: Usually has at least 10 years of management experience.	IASAE III: Usually has at least 10 years of IASAE experience.	CND-SPM: Recommend at least 4 years of experience in CND management or a related field

*Classroom, distributive, blended, government or commercial provider

Implementation Progress

Stated Objective: Certify 100% of the DoD IA Workforce (DoDD 8570)



< 50% Annual Goal Attained – Red
50 – 80% Annual Goal Attained – Yellow
>80% Annual Goal Attained – Green

Definitions

- **Certification**: Procedure by which a third party (e.g.,CISCO, CompTIA) gives written assurance that a…person conforms to specified requirements
  - **Accreditation**: Procedure by which an authoritative body (e.g., ANSI) gives formal recognition that a body is competent to carry out specific tasks (e.g., certification)
    - **Conformity Assessment**: Any activity concerned with determining…that relevant requirements are fulfilled (e.g., ISO/IEC 17024)

Certification

- Validation that at a point in time, you knew something
- Measure of career development and progress
- Indication of commitment to the discipline
- Driver for keeping knowledge and skills current
- Condition of employment

ISO/IEC17024

General Requirements for Bodies Operating Certification Systems of Persons

Requirements for Certification Bodies

- Development & Maintenance of Certification Scheme
- Organizational Structure
- Management System
- Subcontracting
- Records
- Confidentiality
- Security

Requirements for Certification Process

- Application
- Evaluation
- Testing
- Decision on Certification
- Survellance
- Re-certification

Extensions to address DoD/government Concerns

- Content/Skill Set: relationship; to the actual job
- Assessment instruments (tests); reflect experience
- Documentation of Psychometricc Procedures
- Continuous Learning/periodic re-test
- Maintaining accreditation

Types of Certifications

Certification	What	Result
Product Specific	Offered by vendors (e.g., Microsoft, CISCO) on their products	Knowledge of specific product; but not in context of a specific organization
General	Cover breadth of (IT/IA) domain; principles, lexicon; vary in depth on technical issues	Typically written/internet based testing; validates broad, but not practical knowledge
Technical	Vendor neutral; go into depth in a single technical area (e.g., management of firewalls, IDS analysis)	Requires peer graded practical & written exam in focused technical area
Training or Educational certificates/ diplomas	Courses or sets of courses on variety of topics; offer a degree or certificate at completion validating attendance	May have testing; resulting knowledge varies w/student. (Recent American National Standard for Assessment –Based Certificate programs
Operational	Organizational specific certifications, typically at the entry level	Written and practical exam at a basic level

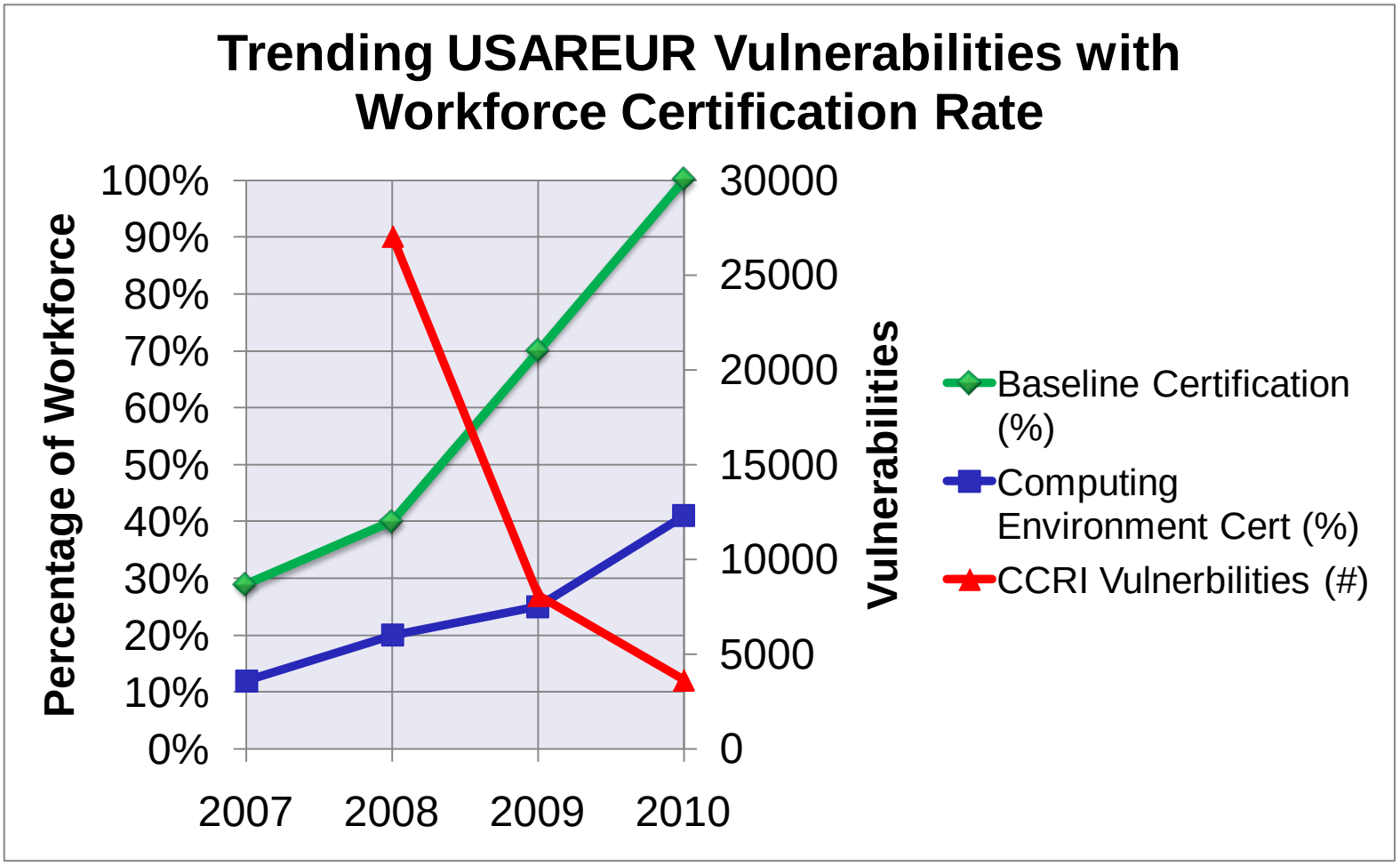
DoD Concerns with Commercial Certifications

- **USSTRATCOM Cyber Analysis Campaign, 2010:**
  - **8570 certifications do not produce adequately qualified personnel for DoD networks**
  - **Too much time and resources dedicated to attaining and maintaining commercial certifications (compared with the time and resources spent learning DoD specific tools, techniques and best practices)**
  - **DoD has outsourced training and this has resulted in a further lack of control over the workforce**
  - **Need better cyber training that is interactive and threat based**
- **JROCM Manpower Study, 2010:**
  - **8570 viewed as a burden due to the difficulty in finding both the time and funds necessary to meet 8570 requirements.**
- **DISA Cyber Workforce Survey, 2010:**
  - **"We have seen no benefit in certifications. They are a paper drill"**

Feedback from the Field on Commercial Certifications

- **Personnel w/IA certifications better able to correctly identify incidents – impacts situational awareness** (JITC, BD09)
- **Personnel w/OS certifications better able to defend against Red Teams** (JITC, BD10)
- **Common lexicon provided by certifications improved communications between CND/SPs and help desks – enables issues to be resolved at lower level** (Agency CISO)
- **Certification *improves performance for all*, even those who failed test** (EUCOM study)
- **Training and certifying the military Cyber workforce improves retention** (INSCOM NCO)
- **Where commands got their people certified, retention was 60% or higher; commands that didn't had retention rates of 30% and below** (NETWARCOM)
- **Unions members can meet the requirement** (Agency CISO)
- **The greater the number of certified personnel, the lower the incidence of data "spillage"** (EUCOM Study)
- **Policy is helping drive availability of funding for IA training** (Agency IAM)
- **8570 is starting to have an impact on the quality of contractor personnel we're getting. Before we'd get anyone; now we get people who know something.** (AF Senior Chief)
- **Certification provided "big picture" perspective** (Navy Carrier IAM)
  - **Improved morale -- training relevant to the job**
  - **Re-energized interest in learning**
  - **Improved advancement scores compared to non-certified personnel**
  - **Personnel have *increased confidence* to use available tools and resources**

Impact of Certification: USAREUR Perspective



Rationale for Commercial Certification

- **Standard test; community developed: "baseline" for organizational-specific training**
- **Worldwide accessibility**
- **Meet an international standard (ISO/IEC 17024)**
- **Accredited by an independent 3rd party (ANSI) (processes vice content)***
- **Continuous learning/periodic retest -- linked to maintaining certified status***
- **Portability across domains (NIST, DOD, IC; public and private sector; allies)**
- **Meaningful: community generally knows them**
- **Currency and Accountability: Test validates that at a specific point in time the individual demonstrated certain knowledge/skill; the certified status is verification that they have kept their knowledge/skills current.**
- **Validity: Accreditation requires validation study* (EEO/Legal)**
- **Privacy: Addresses individual privacy concerns***
- **Work Related: Accreditation requires job task analysis* (JTA)**
- **Administration: Providers track/report on individual's certification status*.**
- **Lexicon: Provides a common lexicon across multiple domains**

ISO/IEC 17024/ANSI requirement

Benefits of Certification to Organizations

- **Provides a baseline of tested knowledge/skills (validated minimal level of knowledge in the functions required for a specific job) upon which to build organizational-specific training**
- **National/international in scope, including training availability**
- **Leverage vice create processes**
- **Leverage vice maintain content (currency, relevance)**
- **Standards can be met by others (e.g., across government, among allies & coalitions, between businesses/industry)**
- **Independent 3rd party review of processes, procedures**
- **Cost pro-rated based on use**
- **Addresses validation issues (EEO/Legal)**
- **Addresses individual privacy concerns**
- **Provides tool for attracting/retaining the best and brightest**
- **Creates a "critical mass" of expertise to make a difference in overall security posture**

Certification Providers

What certification providers have done to accommodate government

- Changed/modified business practices to meet an ISO standard
- Incorporated a continuous learning element into their programs
- Changed delivery methods and/or schedules
- Invited government onto advisory boards
- Engaged government in certification updates/item writing

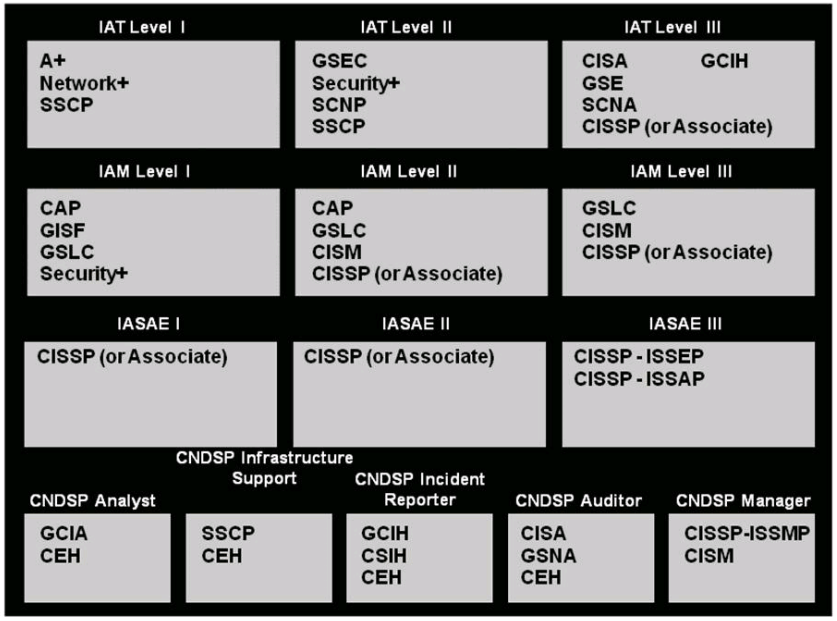
What certification providers are doing/need to do

- Add performance-based exams
- Drive associated training to incorporate interactive, threat based scenarios in curriculum
- Emphasis value to organizations (a certified staff will better secure your environment vice a certification will lead to increase in salary)
- Provide (independent quantitative) “evidence” that certification makes a difference in security
- Further augment business practices to accommodate organizations (e.g., bulk payment of annual fees, databases)
- Maintain ANSI accreditation; meet revised ISO 17024 standard
- Stay engaged with NICE

Future of Certifications in DoD

- **IA baseline certification table being removed**
  - Post on IASE.disa.mil
  - Reinforce qualification vice certification
  - Provide flexibility (update, coordination)

- **Priority**
  - OS certifications
  - Technical skills




CYBER
SECURITY
PROFESSIONALS
EDUCATED • AWARE • TRAINED • CERTIFIED
ADAPTIVE • AGILE • EFFECTIVE