

# IA Training, Certification and Workforce Management in DoD

---

**George Bieber**  
**Defense-wide IA Program (DIAP)**  
**(703)-602-9980**  
**george.bieber@osd.mil**

*Dec 2004 - ISPAAB*



# Outline

Department of Defense  
**DIRECTIVE**



NUMBER 8570.1  
August 15, 2004  
ASD(ISA)/DoD CIO

SUBJECT: Information Assurance Training, Certification, and Workforce Management

- References: (a) DoD Directive 8500.1, "Information Assurance Policy," February 6, 2003  
 (b) DoD Instruction 8500.2, "Information Assurance Policy," January 8, 2001  
 (c) DoD Directive O-8530.1, "Information Assurance Policy," 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 responsibility for the Department of Defense (DoD) information assurance training, certification, and workforce management.
- 1.2. Authorizes the publication of DoD 8570.1-M.

**2. APPLICABILITY AND SCOPE**

This Directive applies to:

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



DoD 8570.1-M

## DoD Information Assurance Training, Certification and Workforce Management

Draft

10 October, 2004  
Assistant Secretary of Defense for  
Networks and Information  
Integration/Department of Defense Chief  
Information Officer

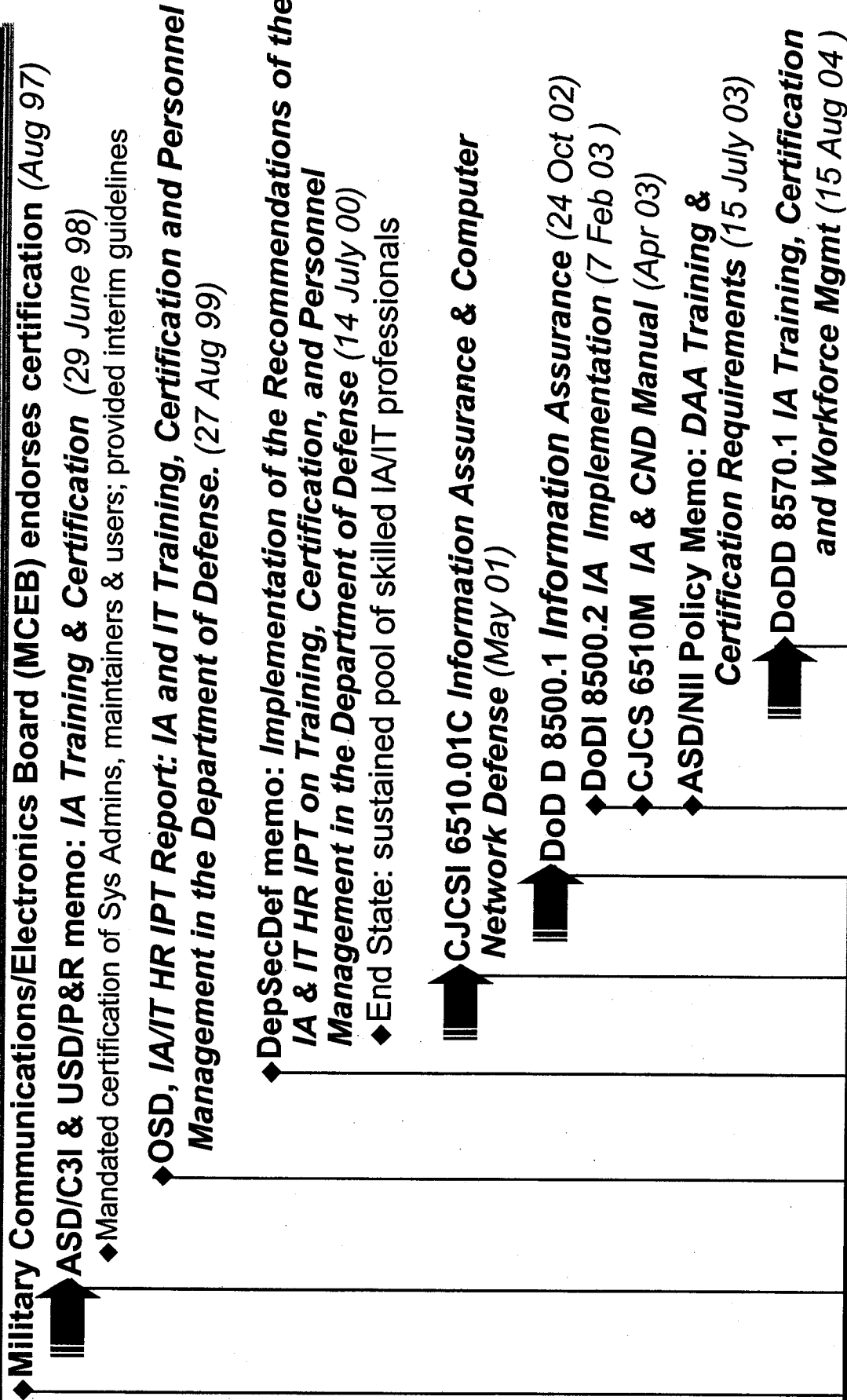
◆ Background

◆ Policy Overview

◆ Next Steps



# Background of IA Training & Certification in DoD

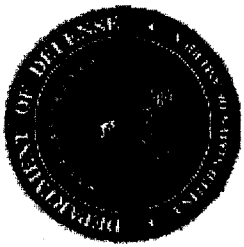


1997 1998 1999 2000 2001 2002 2003 2004 2005



# Where we are Today

- ◆ Component “certification”
  - ◆ Undefined
  - ◆ Varied content (Depth & Breadth)
  - ◆ Inconsistent implementation w/in Components and across Department
- ◆ Unknown size/composition of the IA workforce
  - ◆ 170,000 w/IT/IT management designators (military and civilian)
  - ◆ DoD Federal Information Security Management Act (FISMA) report re personnel w/*significant IT security responsibilities*:
    - ◆ Total number doubled: from 44,000 in FY03 to 89,000+ in FY04
    - ◆ DODIG: Department lacks enterprise-wide means to identify, track IA personnel
  - ◆ Personnel, manpower databases currently lack necessary fields
  - ◆ Positions, people not “tagged” for IA
  - ◆ No military IA career path, skill indicators (except Marine Corps)
  - ◆ Unknown number of personnel performing IA functions part time
  - ◆ Unknown number of personnel outside IT career fields performing IA functions
- ◆ Personnel trained in IA -- then used in non-IA positions



# Where we are Today

---



- ◆ Schools struggling to keep pace with the challenge
  - ◆ Instructor knowledge & currency
  - ◆ Curriculum currency
- ◆ We don't know what we're spending on IA training & certification
  - ◆ Funds managed @ major commands
  - ◆ Components fund training for certifications, but not tests
  - ◆ Corporately, don't know how many of which certifications
- ◆ Minimal exercise or evaluation of IT/IA training
  - ◆ Don't know effectiveness of training
  - ◆ Awareness seldom evaluated for impact on user behavior
  - ◆ Few training exercises (except Air Force Black Demon)



# Key DoD IA Strategy



## Objectives

### Goal 5: Create an IA Empowered Workforce

A sustained IA professional workforce with the knowledge, skills and tools to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures, AND the ability to put the right people with the right skills in the right place at the right time

### Objectives

**Certify the Workforce**

◆ Personnel performing IA functions trained & to a recognized standard

**Manage the Workforce**

◆ Positions identified & occupied by trained personnel; ensuring the commitment from top leadership

**Sustain the Workforce**

◆ Training funds available to enable personnel maintain currency of their IA skills

**Extend the Discipline**

◆ Local commanders understand the importance of IA training

*What personnel in the trenches want*



# Certification Targets



System Administrator Operators

Certification

Joe Kelly

Issued: 10-04-03

Expires: 10-03-06



Network Security Certified Professional

## IA Workforce Structure

Professional Level

DAA

Functional Levels

Certification

Enclave/  
Network  
Computer/  
Environment  
IA Mgmt

Network/  
Computer  
Environment IA Mgmt

Computing Environment IA

Enclave/  
Advanced  
Network &  
Computer IA

Network & Advanced  
Computer IA

Computing IA

Enclave (Level III)

Network

Environment (Level II)

Computing

Environment (Level I)

Entry Level

Sys Admin  
Network Admin

IA Officer  
IA Manager

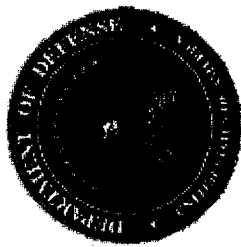
Levels & Functions align with 8500.2



# DoDD 8570.1 Policy Overview

- ◆ Train and certify privileged users & IA managers to DoD baseline requirements
- ◆ Assign position specialty code/skill identifiers to personnel with privileged access or performing IA management functions
  - ◆ Track key data in Component personnel/manpower database
- ◆ Identify positions in manpower databases
- ◆ Require certification status of contractors w/privileged access be recorded and tracked via DEERS/CAC
- ◆ Require initial IA awareness orientation as a condition of network access
- ◆ Require Annual IA awareness refresher training as condition for continued network access
- ◆ Require annual report by Components to document IA training and certification policy compliance
- ◆ Require insertion of IA in all levels of professional military education (PME)



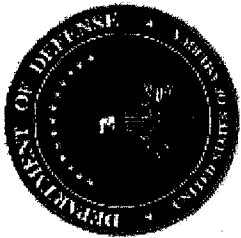


## 8570.1 Policy Overview

---



- ◆ Applies to
  - ◆ Civilians
  - ◆ Military
  - ◆ Contractors
  - ◆ Foreign Nationals (Civilian, Military, & Contractors)
  
- ◆ Applies to personnel performing IA functions
  - ◆ Regardless of job series or occupational specialty
  - ◆ Whether full time or “another duty as assigned”



# Draft Manual 8570.1M: Key Requirements



- ◆ Defines IA categories (technical, management), levels w/in categories (I, II, III), and functions w/in levels.
- ◆ Identifies specific vendor neutral commercial certifications as the DoD baseline for each level
- ◆ Requires IA certifications used by DoD to be accredited under the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17024, *General requirements for bodies operating certification of persons* (April 2003)
- ◆ Allows for “equivalent” certifications if they are:
  - ◆ Approved by OSD
  - ◆ Accredited to ISO/IEC 17024 by an authorized body (e.g., ANSI)
- ◆ Requires 80 hours continuing education over two-years -- or the # of hours specified by IA certification provider to maintain certified status... *whichever is more*
- ◆ Establishes DoD IA Certification Review Board under the DoD CIO/NIJ
- ◆ Requires a privileged user agreement outlining responsibilities, legal and policy limitations of their authority



# IA Training and Certification Requirements



Training & Certification Requirement	Technical Category	Management Category
Initial Training	Level I - III	Level I - III
IA Certification (From approved list)	Yes	Yes
OJT/Familiarization	Yes (within 6 months)	Yes (within 6 Months)
Local OS Cert	Yes (for initial position)	No
Refresher Training/ Continuing Ed	Yes	No
Re-certification	Yes (as required by Certification)	Yes (as required by Certification)
	Yes (as required by Certification)	No
	Yes (as required by Certification)	N/A

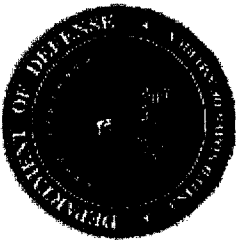
◆ Contractors: requirements to be stated in the contract

◆ IA/IT Training: Classroom/Distributive/Blended; DoD schools, vendor provided<sup>1</sup>



## **Benefits of Certifications**

- ◆ **For Individuals**
  - ◆ **Pay**
  - ◆ **Prestige**
  - ◆ **Marketability**
- ◆ **For Organizations**
  - ◆ **Provide the common test(s) to validate a minimal level of knowledge in the functions required for a specific IA level (within each category)**
  - ◆ **Increased confidence that workforce can do the job**
  - ◆ **Create a “critical mass” of expertise to make a difference in IA posture**
  - ◆ **Attract and retain the best and brightest**
    - ◆ **Motivated**
    - ◆ **Knowledgeable**

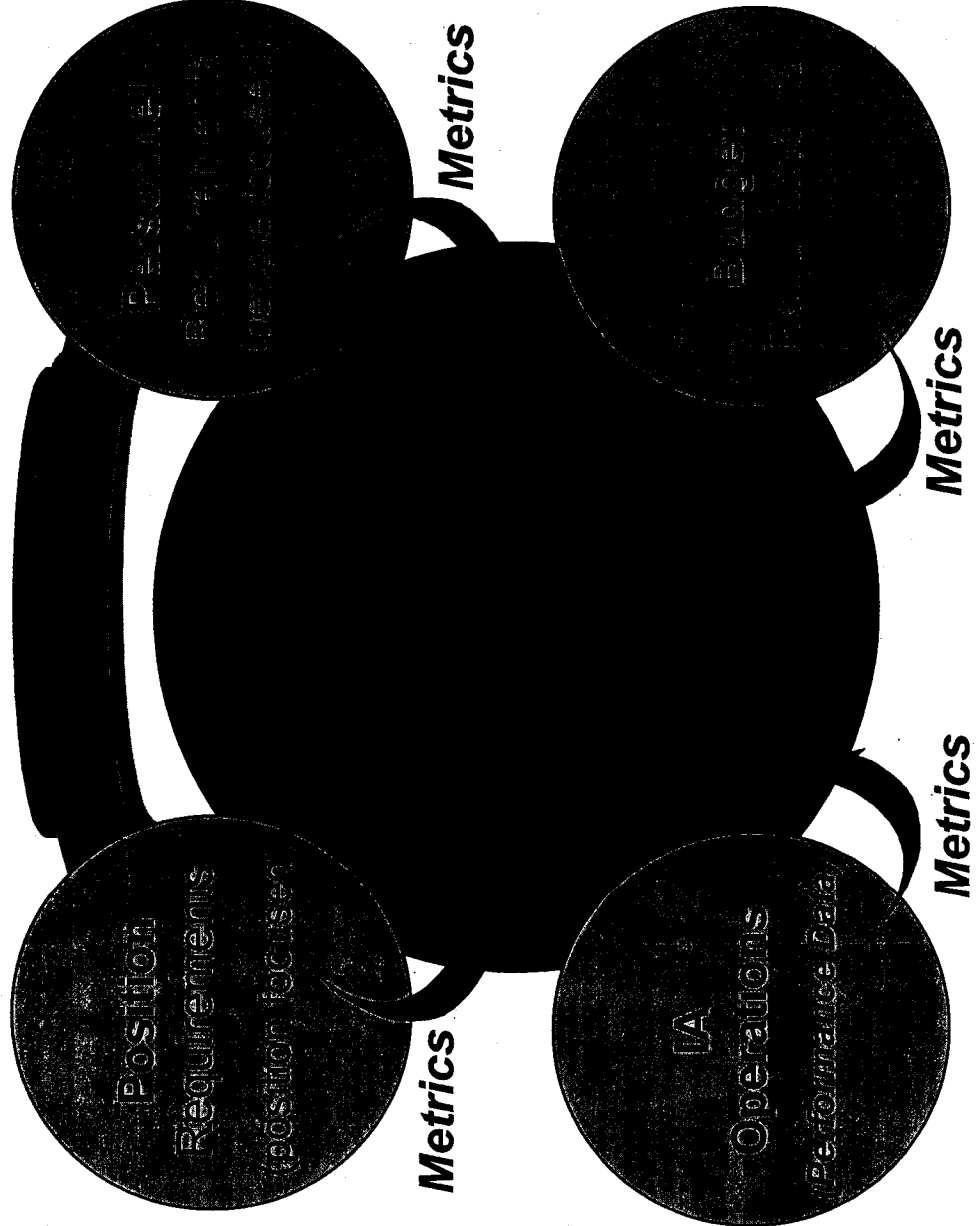


# Benefits of Accreditation

- ◆ Publicly recognized badge signifying excellence and commitment to highest standards
- ◆ Helps develop confidence by attesting in an *independent, measured, and documented manner* that an institution meets or exceeds current professional standards based upon a periodic thorough review and “site” inspection conducted by...experts
- ◆ Guides agencies that need expert opinion as a basis for qualitative judgment in connection with grants, contracts, etc.
- ◆ Could cut red tape (exemption from certain government requirements)
- ◆ Provides impartial evaluation on a periodic basis by professional colleagues
- ◆ Promotes professional recognition that industry standards are being met
- ◆ Promotes excellence within...by causing...[an industry] to continuously evaluate itself in light of ever-rising...industry standards
- ◆ Helps distinguish “institutions” from “road side stands”



# IA Certification Program Relationships



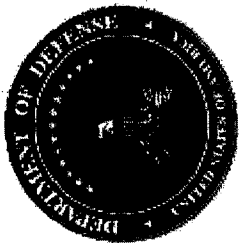


# Implementation Schedule (Notional)



	FY05	FY06	FY07	FY08	FY09
Upgrade Databases					
Identify Personnel; Develop & Apply Skill Codes					
Program, Planning, Budgeting & Execution (PPBE)					
<b>Certify Personnel</b>	<b>10,000</b>	<b>30,500</b>	<b>32,000</b>	<b>33,500</b>	

A bracket above the bottom row of the table spans from FY08 to FY09, labeled "DoD 8570.1M".  
 A bracket above the bottom row of the table spans from FY05 to FY09, labeled "DoD 8570.1".  
 A dotted triangle with a question mark is located in the cell for "Program, Planning, Budgeting & Execution (PPBE)" in FY07.  
 A solid triangle labeled "POM" is located in the cell for "Identify Personnel; Develop & Apply Skill Codes" in FY08.  
 The number "08" is located in the cell for "Identify Personnel; Develop & Apply Skill Codes" in FY08.



# Next Steps: 8570.1 Manual

◆ Enter draft manual into formal SD106 coordination

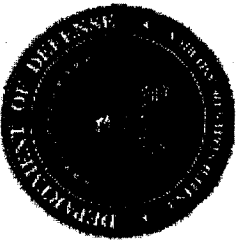
◆ NII respond to SD106 comments

◆ NII respond to Union comments

◆ ASD/NII signature

Dec	Jan05	Feb	Mar	Apr
-----	-------	-----	-----	-----

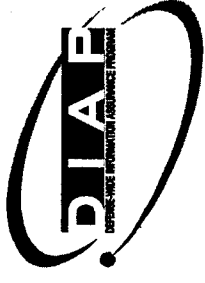
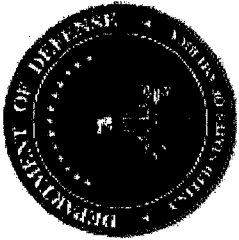




# The Year Ahead

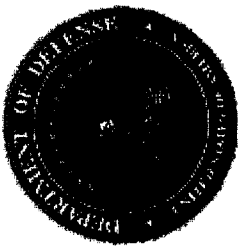
---

- ◆ Use of appropriated funds to pay for commercial certifications (tests) for uniformed personnel.
  - ◆ Navy proposing congressional language to amend Chapter 101 of title 10, United States Code
- ◆ Role of DoD schools, CNSS standards, and certificates
  - ◆ Source of training for certifications (A+, Security+, CISSP etc)
  - ◆ DoD/Component layer of a comprehensive certification/professional program
  - ◆ DoD/Component level policy, processes and procedures
  - ◆ Satisfy DoD certification continuous education requirement
- ◆ Rigor and content of commercial certifications
  - ◆ Obtain ISO 17024 accreditation
  - ◆ Add performance-based element to testing (vice multiple choice)
  - ◆ Add continuing learning requirement/re-test requirement
  - ◆ Incorporate DoD IA best practices (DISA STIGS, NSA Guidelines)
- ◆ Adequacy of Service “legacy” databases to meet 8570 requirements
  - ◆ Services reluctant to make changes pending transition to DIMHRS
  - ◆ Jump start personnel/manpower database upgrades (\$2M)
    - ◆ Initial estimate: \$500-\$600K/Service



# The Year Ahead

- ◆ Undertake formal SD106 staffing of 8570.1 Manual
- ◆ Publish language in DFARS for contractors to meet requirements
- ◆ Develop internal DoD IA certification review process
  - ◆ Categories, Levels and Functions
  - ◆ Certifications
- ◆ Provide foundation for DHS definition of national IA skills standards
  - ◆ Define a common language of IA-related work & worker requirements
  - ◆ Enable: ◆ Consistent description of the scope of individual certifications
    - ◆ Mapping of certifications against job functions
    - ◆ A common basis for accreditation
- ◆ Pursue initiatives with enterprise-wide potential to
  - ◆ Reduce cost of training/testing (e.g., DANTES)
  - ◆ Enhance training outcomes (e.g., SAST)
- ◆ Support establishment of “Black Demon-like” IA combat training exercises for COCOMs
- ◆ Engage stakeholders – OPS, HR, RM – at COCOMs/Services/Agencies
  - ◆ Facilitate 8570 implementation at the grass roots level



# Observations... Questions

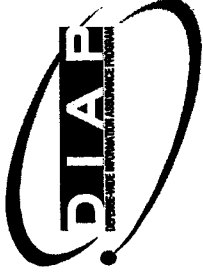
---



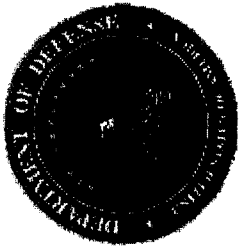


# Backup

---



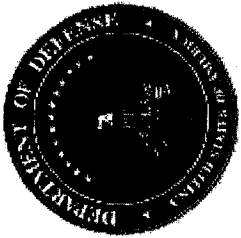
- ◆ **DoD IA Certification Selection Process**
- ◆ **Skills Standards Development/Job Task Analysis**
- ◆ **Appropriated Funds Issue for Military**
- ◆ **DoD IA Strategy: Goal 5 and Initiatives**



## Certification Criteria

---

- ◆ **Relevant to DoD** – Address functions performed by DoD IA workforce
- ◆ **Meaningful** -- Recognized by a broad audience outside DoD & government;  
Career enhancing in government; portable across organizations
- ◆ **Verifiable** -- Validated, standard test
- ◆ **Periodic renewal** -- Continuous learning/retest to maintain certification
- ◆ **High security content** -- Linked to nationally recognized best practices  
e.g., NSA guidelines/DISA STIGS/Center for Internet Security benchmarks
- ◆ **Multiple training sources** *nation/world-wide; multiple delivery media*  
--traditional classroom, web, CD, blended, other
- ◆ **Multiple Certification Levels** – e.g., Entry/Intermediate/advanced
- ◆ **Test out feature** – but rigorous test to reflect “experience” factor
- ◆ **Pre-test/self assessment feature** -- tailor training to gaps in knowledge
- ◆ **DoD participation in process** -- initial security guidelines; exercise  
certifying test(s); conduct follow-up evaluations of learning outcomes;  
provide feedback to industry
- ◆ **Reduced cost** -- Enterprise-wide costing
- ◆ **Use of blended solution to minimize time in class** -- especially to meet  
continuous education requirement



# Types of Certifications

Certification	Description	Exam/result
Product specific training	Offered by vendors or others, for example, on firewalls, operating systems, and other IT components	Some have exams; knowledge of specific products
General certifications	Cover the breadth of IT security issues such as principles and terms, but are of varied depth on technical issues, e.g., CISSP	Typically written but not practical; validates broad but not practical knowledge.
Technical certifications	Vendor neutral courses that go into great depth in a single technical subject area; e.g., management of firewalls.	Require a peer graded practical exam as well as a written exam; qualifies students in a narrow technical area.
Training and education course certificates or diplomas	Courses or sets of courses in a variety of topics that offer a certificate or degree at the end. The certificate merely validates that the person took the course	May have testing, but not a certification exam at end; resulting knowledge variable, depends on student.
Emerging general operational certifications	Organizations are beginning to establish general certifications, typically at the entry level	May require a written and practical exam at a basic level.



## Selection Process



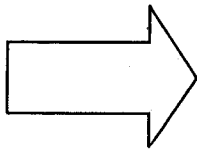
- ◆ Identified baseline DoD IA functions
- ◆ *Mapping by Certification Providers:* Certification providers were requested to map their certifications to the DoD IA functions
- ◆ *Site Visits to DoD Schools/Commands:* input on which certifications were considered valuable and their alignment to current DoD IA training program
- ◆ *Mapping by the Institute for Defense Analysis (IDA):* Certifications to functions
- ◆ *SMEs input from within and outside government:* on the IA functions and their alignment to commercial certifications.
- ◆ *Independent survey by the Center for Internet Security (CIS):* to identify which certification best matched the DoD levels and functions.
- ◆ *Integration:* to specify certifications by IA Levels



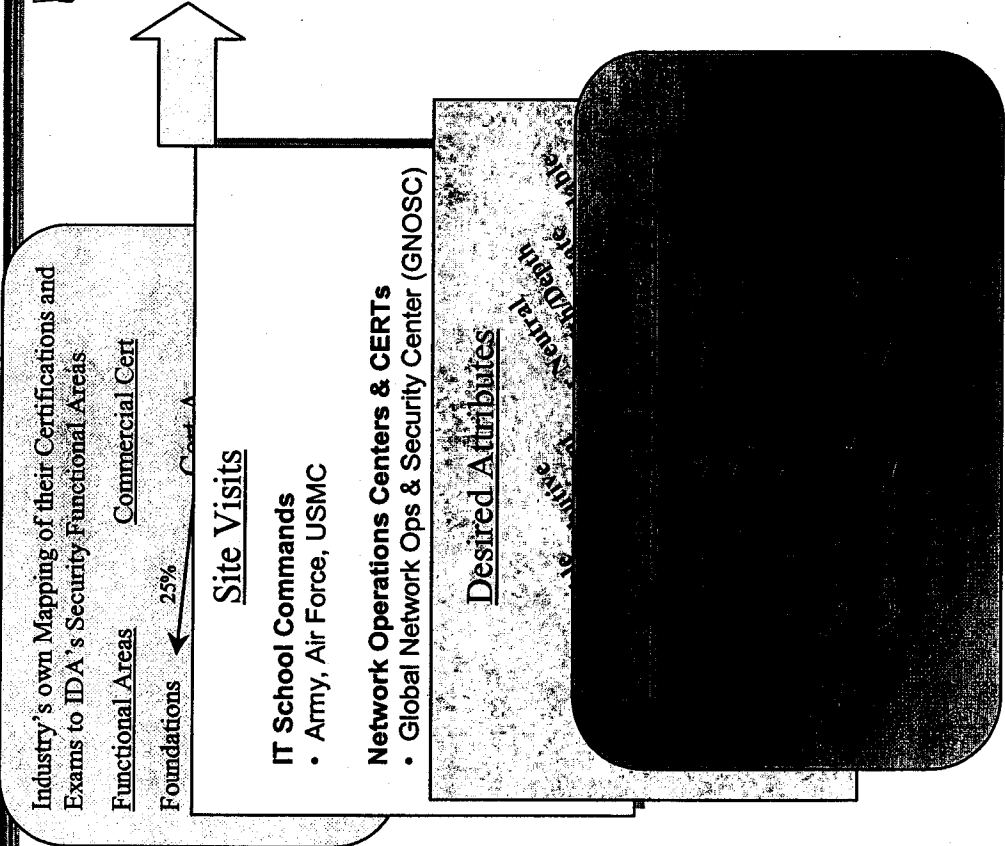
# Process & Criteria



110 "IA"  
Certifications



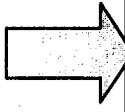
99 Certifications  
were viewed as  
candidates



## Review Panel

### Experience

- Computer science
- Business Management
- Information Science
- Training & Readiness
- Operations Research
- Military Service



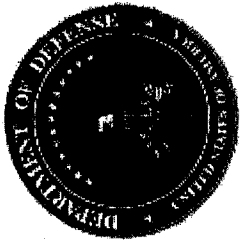




# Mapped Construct

IA Tech Level 3	General Operations	Cert D Cert F Cert B	Cert K Cert C Cert Y	Cert T Cert R Cert Q
	Focused	Cert A		
	Region Specific	Cert M Cert W Cert X	Cert G	Cert S Cert P Cert Z

Mapped for IA Management Levels as well



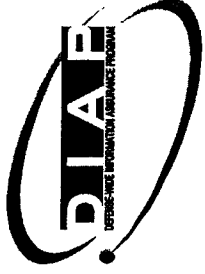
# Validation



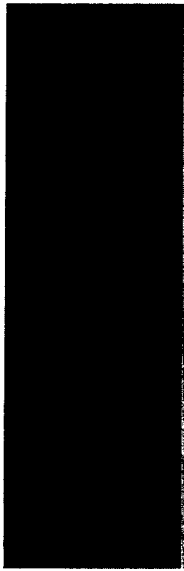
- ◆ **Army Credentialing Opportunities On-Line (COOL)**  
(<https://www.cool.army.mil/>)
  - ◆ Relates commercial certifications to Army-specific IT occupational specialties
  - ◆ A primary focus is Information Systems Operator-Analyst: "74B"
  - ◆ *Excellent correlation to IDA findings (added 2 more certifications to set)*
- ◆ **CompTIA Tech Career Compass**
  - ◆ Commercial undertaking; relates commercial certifications to industry:
    - ◆ Job Titles (*network analyst, network administrator, project manager*)
    - ◆ Experience Levels (*entry, intermediate, senior*)
  - ◆ IA certifications fully support IDA findings
- ◆ **SPAWARS (San Diego, CA) Analysis**
  - ◆ Conducted analysis of its Sys Admin personnel certification requirements
    - ◆ 90% correlation with IDA's research
    - ◆ SPAWARS analysis included specification of technical training as well<sup>26</sup>



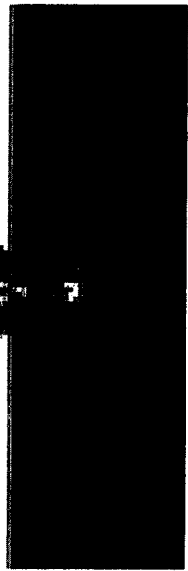
# National Strategy to Secure Cyberspace



*Promote Private Sector Support for Well-coordinated Widely  
Recognized Professional Cybersecurity Certifications*



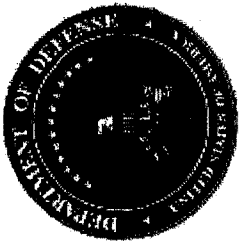
THE DEPARTMENT OF DEFENSE  
**SECURE  
CYBERSPACE**  
INITIATIVE



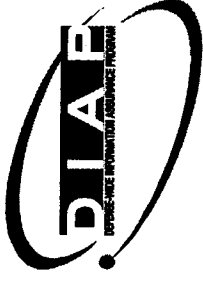
*Certification can provide employers and consumers with greater information about the capabilities of potential employees or security consultants*

*No one certification offers a level of assurance about a person's practical and academic qualifications*

*...explore approaches to developing nationally recognized certifications and guidelines for certification*



# Information Assurance Skill Standards Development



- ◆ **Purpose:**
  - ◆ Define a common language of IA-related work and worker requirements applicable to the DoD and other organizations
  - ◆ To enable:
    - ◆ Consistent description of the scope of certifications
    - ◆ Mapping of certifications against functions/skills
    - ◆ A common basis for accreditation
- ◆ **Process:**
  - ◆ Collect and integrate existing Job Task Analysis data to seed information: Use *"thought leaders"* in iterative interviews
  - ◆ Refine common language and link work to worker requirements: Use *subject matter experts (SMEs)* in focus groups
  - ◆ Define IA roles and verify linking of work/worker requirements: Use *additional SMEs* in focus groups
  - ◆ Collect data to determine occurrence of IA functions in different populations: Conduct *web-based survey*



# **Benefits of IA Skill Standards**

- ◆ **Serves as a common language for defining IA/IT security roles and competencies**
- ◆ **Provides a framework for
  - ◆ **mapping the IA/IT security certification landscape, and**
  - ◆ **identifying skills and performance gaps****
- ◆ **Provides information for use in HR applications**
- ◆ **Provides a foundation for strengthening IA education and training**
- ◆ **Provides a platform for developing Return on Investment measures**
- ◆ **Facilitates establishment of legal defensibility of certification use**

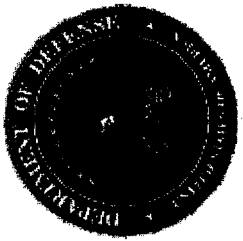


# **Why its Important**



***Certification is meaningless if it doesn't relate to actual work  
(functions/skills)***

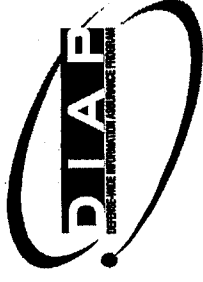
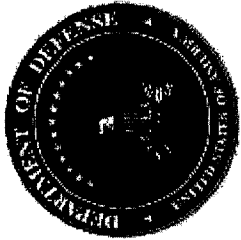
- ◆ **ISO/IEC 17024 General requirements for bodies operating certification schemes for persons (April 2003) requires certifications to map to jobs (functions/skills)**
- ◆ **Currently:**
  - ◆ **No common position standards**
  - ◆ **No common standard of position levels**
  - ◆ **No common standard of position categories**
- ◆ **Certification providers (e.g., ISC2) base certifications on their own Job Task Analysis (JTA) data/"common body of knowledge" ...or in some cases, on no JTA**
- ◆ **National/international standards will**
  - ◆ **Promote the National Cybersecurity vision**
  - ◆ **Promote rigor in commercial certifications**



# **Expected Outcomes**

---

- ◆ **Standard work categories (e.g., technical, management)**
- ◆ **Standard category levels**
  - ◆ **How many levels (3, 4, 7?)**
  - ◆ **Nomenclature (e.g., I, II, III; entry, intermediate, advanced)**
- ◆ **Standard functions within categories and levels**
  - ◆ **Nomenclature (what are the functions; what are they called)**
- ◆ **Skill Standards**
  - ◆ **By category and level: performance standards that delineate what a person must know and be able to do in order to successfully perform roles/functions related to a specific job, an occupational cluster, or across an industry sector**



## **Efforts to Date**

- ◆ **DoD Directive 8570.1 IA Training, Certification and Workforce Management signed (15 Aug 04); supporting Manual, identifying specific commercial certifications, completing informal coordination**
- ◆ **Contractor in place**
- ◆ **Sixteen existing “JTAs”/sources identifying IA work collected: Military Services, 2210, CNSS, Clinger-Cohen competencies (IT Security/IA), commercial certification providers**
- ◆ **DoD “Thought Leaders” identified for first round**
- ◆ **Commercial certification providers primed to go to their customers for private sector data**
- ◆ **DHS coordinating meetings with Associations to obtain their participation**

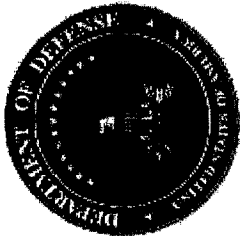




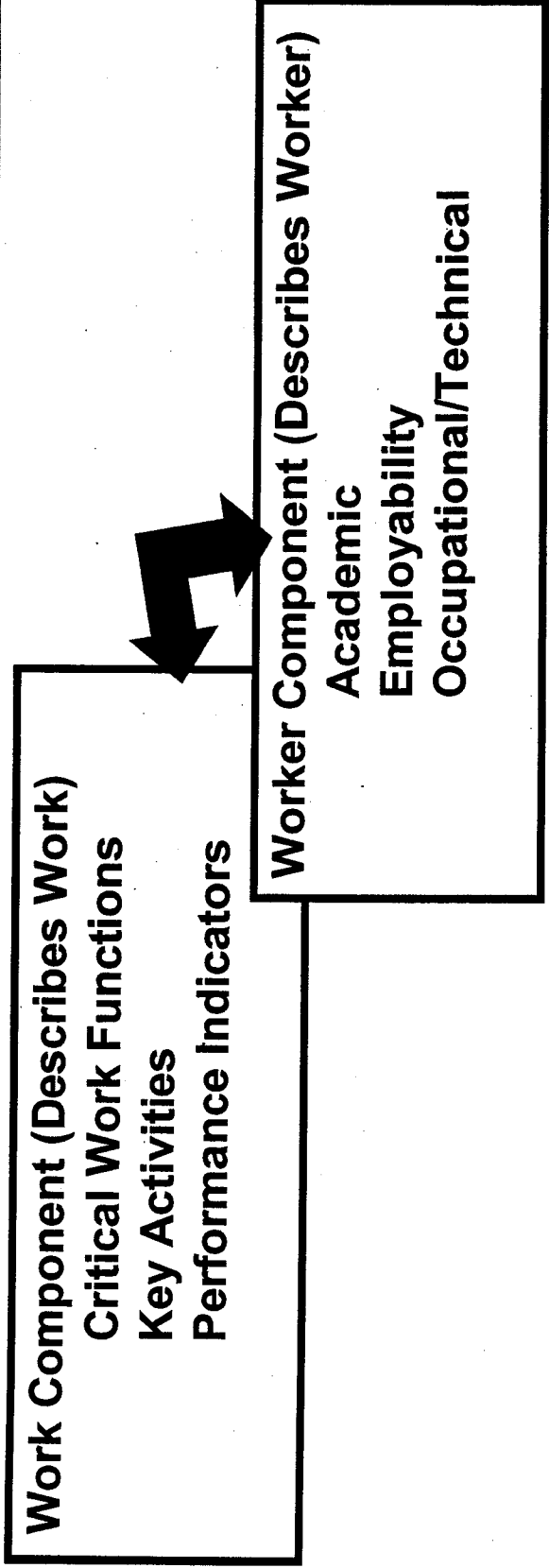
## **Next Steps**

---

- ◆ **Integrate available data**
- ◆ **Interview “Thought Leaders”**
- ◆ **Conduct focus groups**
- ◆ **Produce Initial Report – Strawman**
  - ◆ **Target: November-December 2004**
  
- ◆ **Governance – focus on the content side of certifications**
  - ◆ **DHS lead to bring in private sector**



# Approach to Get There



1. Scan the Environment
2. Frame the Landscape
3. Seed the Landscape
4. Review the Landscape
5. Map the Landscape
6. Verify the Landscape
7. Validate the Landscape

**Where are we now?**

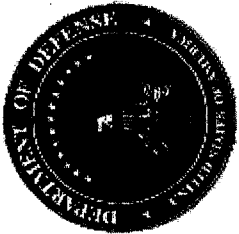


# Use of Appropriated Funds for Certification Tests



- ◆ Authority is in place for civilian employees
- ◆ Authority is not in place for uniformed personnel
- ◆ Navy, AF point to US Comptroller General opinion from the 1940s
  
- ◆ Navy is seeking legislation to grant authority
  
- ◆ Process
  - ◆ Navy's Office of Legislative Affairs circulated proposal to Navy and the Marine Corps for review and comment.
  - ◆ Navy General Counsel approved the proposal
  - ◆ SECNAV reviewed and approved
  - ◆ OSD Office of Legislative Counsel review (NLT15 October)
    - ◆ Review by other Services, Components
    - ◆ OMB/White House
    - ◆ Congress





# **Proposed Language**



## ***Amend Chapter 101 of title 10, United States Code***

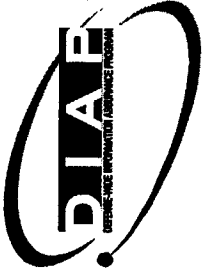
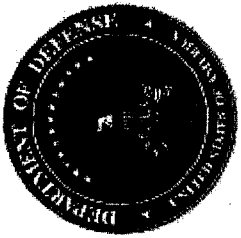
- ◆ Add the following new section:
  - ◆ *Payment of expenses for members of the armed forces to obtain professional credentials*
  - ◆ Use appropriated funds, or funds otherwise available...to pay for—
    - ◆ Expenses for members of the armed forces to obtain professional credentials, including expenses for professional accreditation...and professional certification
    - ◆ Examinations to obtain such credentials
  - ◆ Regulations...specify the types of professional expenses that may not be paid under this section



# Rational

## *Professional credentials, licenses and certifications*

- ◆ Essential element of transformation to performance-based training that is based on required, position-related knowledge, skills and abilities.
- ◆ Enable the use of existing, nationally accepted industry standards and associated training,
- ◆ Significantly reduce the cycle time of training delivery for the skill demands of those positions having significant similarities with private sector occupational specialties.
- ◆ Provide improved mechanism to verify and measure the attainment of knowledge, skills and abilities
- ◆ Outline criteria for career progression.
- ◆ Operate in an environment of rapidly expanding use of commercially available systems, products, and services that have certification standards corresponding to military occupation specialties.
- ◆ No need to duplicate standards where there is significant overlap of knowledge, skills and abilities between the civilian private sector and the services.
- ◆ Already recognized by legislative authority to fund civilian certifications for civilian employees of the Government (5 USC §5757).

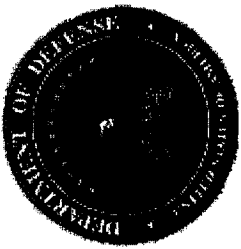


# Rational

## *Professional credentials, licenses and certifications*

### **In exercising authority:**

- ◆ **Military departments ensure payments limited to those directly associated with obtaining credentials and certifications**
- ◆ **Payments would not duplicate other educational benefits already available for military members under existing law**
- ◆ **Will not be used to pay for expenses to meet the basic qualifications for entry into specific officer communities and professions, e.g., bar examinations for lawyers and licenses for doctors and nurses**
- ◆ **Would enable armed forces to leverage training opportunities available from the private sector to potentially reduce the costs involved in providing essentially the same training exclusively within the military.**



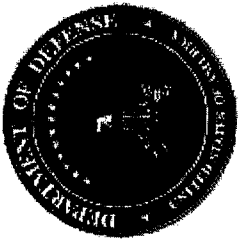
# Goal 5 Objective: Certify the Workforce



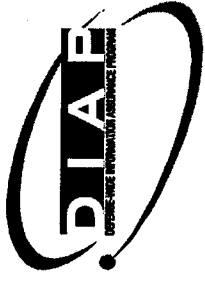
**5.1 Standardize**    **◆◆ Enterprise baseline certification(s)**  
**Baseline IA Skills**    **◆◆ Specify functions & levels**  
**Across the Enterprise**    **◆◆ Specify minimum Enterprise-wide requirements**

- ◆ What certification(s) for which function & levels?
- ◆ What will work; what won't work?

- ◆ *Incorporate IA training in Service and joint IA exercises (Red Teams, Joint Exercise Teams etc.); identify training gaps*
- ◆ *Raise the bar of Service school IA/IT training*
  - ◆ Document needs, issues
  - ◆ Identify commonalities
  - ◆ Support Service initiatives to enhance instructor IA skills
  - ◆ Assess training against selected commercial certifications
- ◆ *Engage certification providers; moving industry towards ISO accreditation*
- ◆ *Establish CND Service Provider certification & accreditation program*
- ◆ *Establish ISSE certification (NSA with ISC<sup>2</sup>)*



# Goal 5 Objective:



## Manage the Workforce

5.2 *Provide Trained/Skilled Personnel When and Where Needed* → ♦ Tag & track IA people, billers/certifications

- ♦ Provide tools to manage the workforce
- ♦ Promote flexibilities to recruit/retain

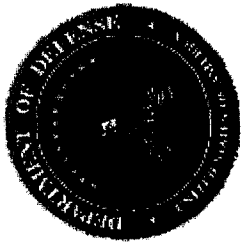
- ♦ What do we need to know to manage workforce?
- ♦ What's available to recruit/retain the best?

♦ *Identify requirements for upgrading IA personnel management tools*

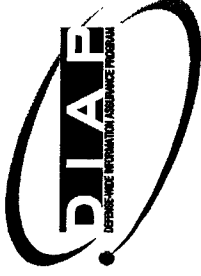
- ♦ DoD Civilian Personnel Data System (DCPDS)
- ♦ Defense Integrated Military Human Resources System (DIMHRS)
- ♦ DEERS/RAPID, Common Access Card (CAC)
- ♦ Existing Service military personnel/manpower databases

♦ *Enhance utility of the DoD IA Scholarship Program (IASP) for recruitment and retention*





# Goal 5 Objective: Sustain the Workforce



- 5.3 Continuously Enhance IA Skill Levels**
- ◆ Keep personnel current w/change
  - ◆ Rapid curriculum update
  - ◆ Deliver training when/where needed
  - ◆ Leverage technology



- ◆ How do we do rapid curriculum update?
- ◆ How do we deliver it when/where needed?
- ◆ What technology/methodology works?
- ◆ *E-learning and knowledge management portal (pilot)*
- ◆ *Leverage DISA's DoD IA training & awareness products and classes*
- ◆ *New products underway:*
  - ◆ *System Defender*
  - ◆ *CyberOps*
- ◆ *Exercises: Table-Tops to Component-wide; International CNDSP*
- ◆ *Utility/applicability of commercial vendor curriculum to DoD*



# Goal 5 Objective: Extend the Discipline



## 5.4 Infuse IA Into Other Disciplines

- ◆ Define what other disciplines should know about IA
- ◆ Ensure allies/coalition forces implement IA
- ◆ Support critical infrastructure/home and defense

- ◆ What training can our allies/coalition partners use?
- ◆ How do we support homeland defense?

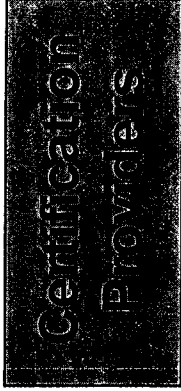
- ◆ IA for Program Managers WBT (Defense Acquisition University & DIAP)
- ◆ Cyber Law I WBT (DISA, Services, JTF CNO, others)
- ◆ DISA's DoD IA training & awareness products for allies, coalition partners (International CND Coordination WG)
- ◆ Certification Accreditation (Institute for Defense Analysis workshops with certification providers supporting DHS/national strategy for cyber security)
- ◆ Products funded/underway:
  - ◆ IA for Auditors, Evaluators and IGs
  - ◆ Cyber Law II
  - ◆ IA for SCADA (Supervisory Control and Data Acquisition) Systems
  - ◆ IA T&E



# Definitions

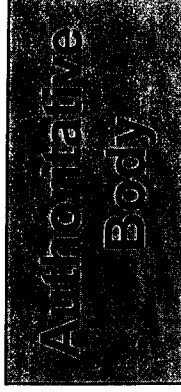
## ◆ Certification:

Procedure by which a third party (e.g., CISCO or 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 directly or indirectly that relevant requirements are fulfilled.

