High Impact Initiatives Redefine the Federal Information Security Workforce

Lynn McNulty, CISSP

Director of Government Affairs, (ISC)²

March 12, 2008

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®
ANSI
ISO/IEC 17024

(ISC)²®

SYSTEMS SECURITY CERTIFIED PRACTITIONER
SSCP®
ANSI
ISO/IEC 17024

SECURITY TRANSCENDS TECHNOLOGY®

Participants

Moderator

Lynn McNulty, CISSP, Director of Government Affairs, (ISC)²

Panelists

- Patrick Howard, CISSP, CISM, Chief Information Security Officer, U.S. Nuclear Regulatory Commission
- Mark Wilson, CISSP, IT Specialist, Computer Security Division, National Institute of Standards and Technology
- Brenda Oldfield, Director, Education, Training & Workforce Development, National Cyber Security Division, U.S. Department of Homeland Security
- George Bieber, Chief of the Information Assurance Education, Training, Awareness and Products Branch of the INFOSEC Program Management Office (IPMO), Defense Information Systems Agency (DISA)

An Agency Perspective of Workforce Training Requirements

Patrick D. Howard, CISSP, CISM
Chief Information Security Officer
U.S. Nuclear Regulatory Commission

Security Training Needs for Non-Professionals

- General Users
  - Social Engineering and other Threats
  - Incident Identification and Reporting
  - Security Policy and Procedures
- System Owners and ISSOs
  - Responsibilities
  - Security Planning
  - Data & System Categorization
  - Risk Management
  - Business Impact Analysis & Contingency Planning

Security Training Needs for IT Security Professionals

- FISMA and Compliance
- Threats and Vulnerabilities
- Security Controls & Technologies
- Risk Management
- Certification & Accreditation
- Security in the System Development Lifecycle
- Contingency Planning & Incident Response
- Customer Service

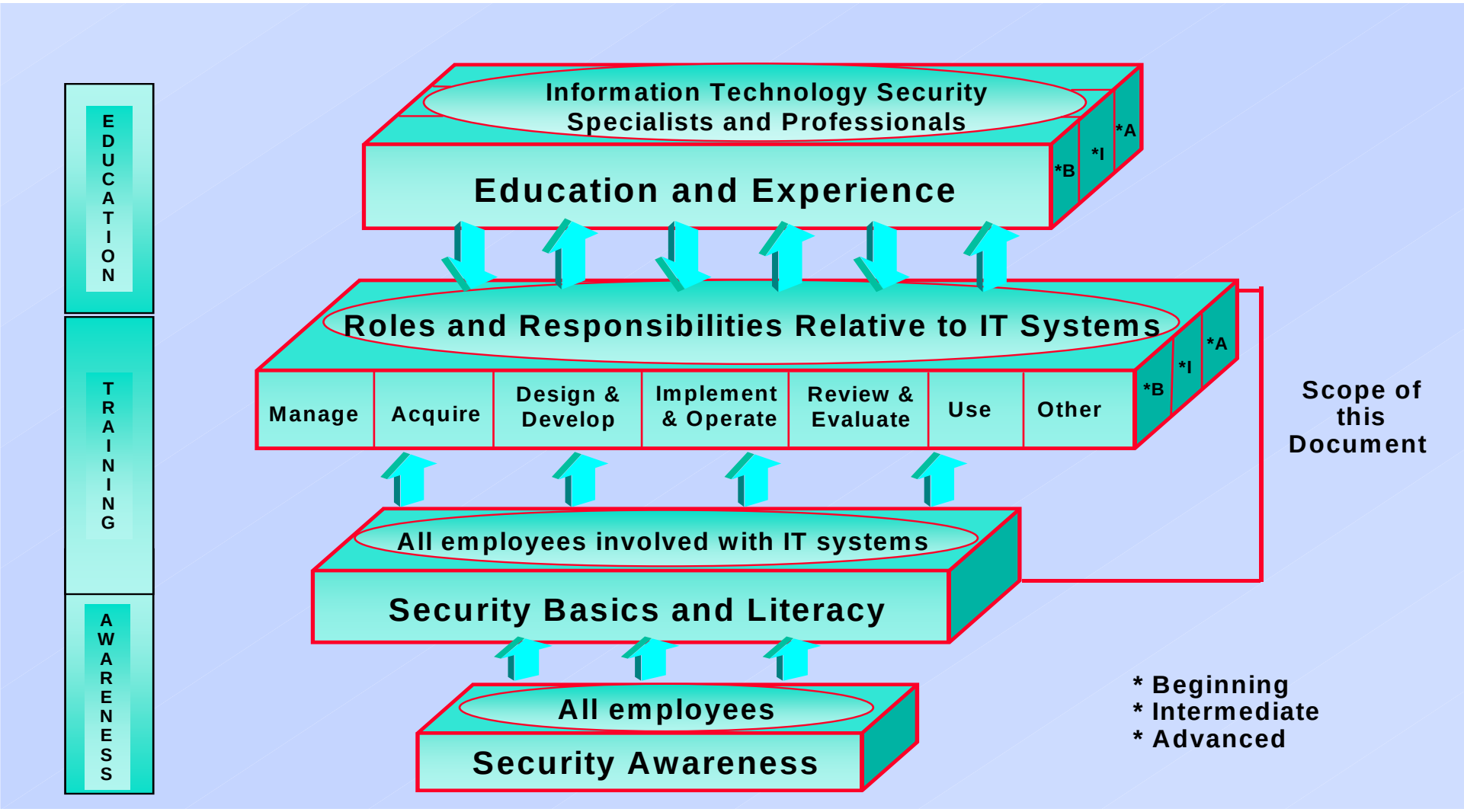
NIST Role-Based Training Guidelines and Other Related Stories

Mark Wilson, CISSP
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology (NIST)
mark.wilson@nist.gov
(301) 975-3870

Policy Drivers

- FISMA (Federal Information Security Management Act) [2002]
- OMB Circular A-130 Appendix III [2000]
- OMB Reporting Instructions for FISMA and Agency Privacy Mgmt. [Annually]
- OMB Memoranda [Ongoing]
- OPM 5 CFR Part 930 [June 2004]
- *Not NIST Publications (FIPS or SPs)*

The NIST Learning Continuum



Risk Management Framework

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

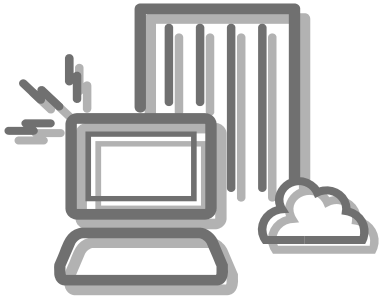
Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements



SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

Timeline

- Internal NIST Review: Oct. 2007
- Public Review and Comment: By April 2008? (for how long?)
- Second Draft Public Review: TBD (or not)
- Publish Date: . . . FY2008
- Then Begin Update of SP 800-50 “Building an IT Security Awareness and Training Program” [Pub. October 2003]

Free NIST Resources

- Division Website: http://csrc.nist.gov/
  - Final and Draft Publications – FIPS, SPs, NISTIRs
  - Federal Agency Security Practices (FASP)
  - Federal Computer Security Program Managers' Forum (aka, The Forum)
  - National Vulnerability Database (NVD)
  - Federal Desktop Core Configuration (FDCC)
  - Security Content Automation Protocol (SCAP)
  - FISMA Implementation Project
  - Federal Information System Security Educators' Association (FISSEA)
  - Awareness, Training, and Education (ATE)
  - Role-based Training Reference Model (planned)

OVERVIEW: Information Systems Security Line of Business (ISS LoB)

- Chartered to support the President's Management Agenda for Expanded E-Gov
- Value Proposition: to improve the level of IS Security across government:

  - Eliminate duplication of efforts;
  - Increase aggregate expertise; and,
  - Reallocate resources for missions

- Initially identified common IS Security needs across all branches of government

Overview: Information Systems Security Line of Business (ISS LoB)

Common Solutions address 4 areas:

- FISMA Reporting:
  - SSC - DOJ, EPA;
  - 90% implementation expected by Q4FY08
- Security Training:
  - Tier 1 Awareness Training – SSCs: DoD, OPM, DOS
  - Tier 2 Role-Based Training - WG in progress
- Situational Awareness and Incident Response
  - Tier 1 - aggregated purchase (SmartBUY)
  - Tier 2 - WG in progress; addressing specialized products
- Security Solutions Lifecycle (Certification and Accreditation): phased approach for shared services, using both government and industry providers

Overview: IT Security EBK

IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development:

Objectives:

- Ensure a qualified and appropriately trained IT security workforce
- Establish a national baseline representing the essential knowledge and skills that IT security practitioners must possess to perform
- Advance the IT security landscape by promoting uniform competency guidelines

IT Security EBK: Straw Man

Contributing Resources:

- DoD 8570.1 WIP JTA: *56 Critical Work Functions*
- Committee on National Security Systems (CNSS) Training Standards: *40XX series*
- National Institute of Standards and Technology:

  SP-800 Series
- FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems
- Federal Acquisition Regulations
- ISO/IEC Standards
- Industry Models (COBIT, SSE-CMM, CMMi)

IT Security EBK: The Framework

- 14 IT Security Competency Areas
- 4 Functional Perspectives: D,I,M,E
  - Design
  - Implement
  - Manage
  - Evaluate
- Key Terms and Concepts
- 10 IT Security Roles

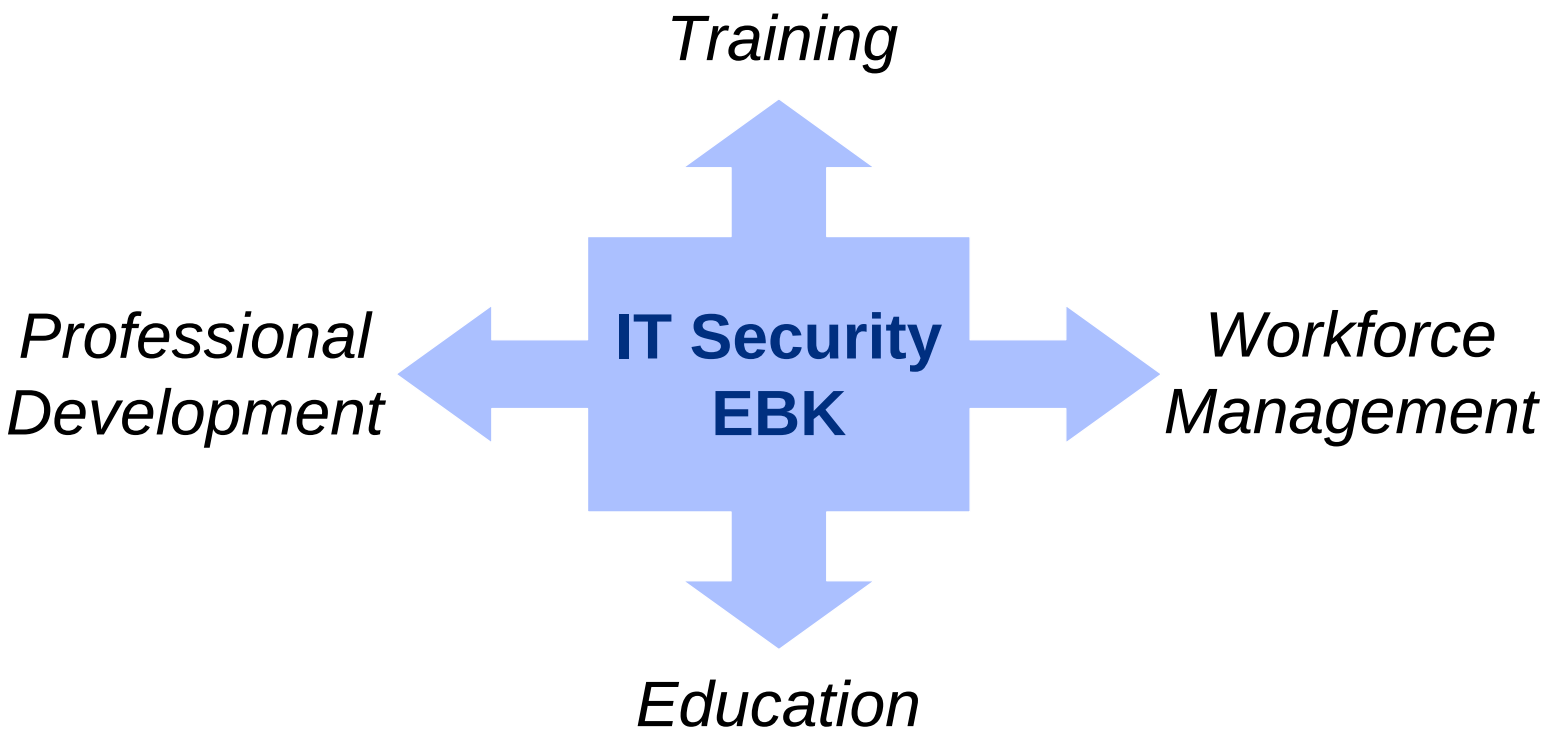
IT Security EBK:

A Competency and Functional Framework for IT Security Workforce Development

Functional Perspectives
M - Manage
D - Design
I - Implement
E - Evaluate

IT Security Competency Areas	IT Security Roles																	
	Executive						*Functional*								*Corollary*			
	Chief Information Officer		Information Security Officer/ Chief Security Officer		IT Security Compliance Officer		Digital Forensics Professional		IT Security Engineer		IT Security Operations and Maintenance Professional		IT Security Professional		Physical Security Professional		Privacy Professional		Procurement Professional	
1 Data Security	M		M	D						D			M	D				D		
				E		E				E	I	E		E				E		
2 Digital Forensics			M	D			M	D												
						E	I	E			I									
3 Enterprise Continuity	M		M									D				D				
				E		E					I			E	I					
4 Incident Management	M		M	D								D		D			M	D		
				E		E	I				I	E		E	I		I	E		
5 IT Security Training and Awareness	M		M											D				D		
				E		E							I	E				E		
6 IT Systems Operations and Maintenance								D		D	M	D								
						E	I	E	I		I	E								
7 Network Security and Telecommunications								D		D	M	D								
						E	I		I		I	E								
8 Personnel Security														D				D		
						E								E		E	I			
9 Physical and Environmental Security	M		M											D	M	D				
				E		E								E	I	E				
10 Procurement	M	D	M	D															M	D
				E		E		E				E				E			I	E
11 Regulatory and Standards Compliance	M		M	D		D											M	D		
		E		E	I	E							I				I	E		
12 Risk Management	M		M	D										D			M	D		
		E		E	I	E	I		I		I		I	E	I		I	E		
13 Strategic Management	M	D	M	D																
		E	I	E		E														
14 System and Application Security	M		M							D										
				E		E			I	E	I									

IT Security EBK:
Strengthening the IT Security Workforce



IT Security EBK

- Review Document:
  http://www.us-cert.gov/ITSecurityEBK

- Contact:

Brenda Oldfield
Director - Education, Training & Workforce Development
National Cyber Security Division
U.S. Department of Homeland Security

(703) 235-5184
brenda.oldfield@dhs.gov

DoD's IA Workforce Improvement Program (IA WIP)

IA Training, Certification and Workforce Management in DoD

George Bieber

Defense-wide IA Program (DIAP)

(703)-602-9980

george.bieber@osd.mil

Landscape circa 2005

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

- **Unknown size/composition of the IA workforce**
  - **Personnel, manpower databases unable to track**
  - **Positions, people not "tagged" for IA**
  - **No military IA career path, skill indicators**
  - **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**

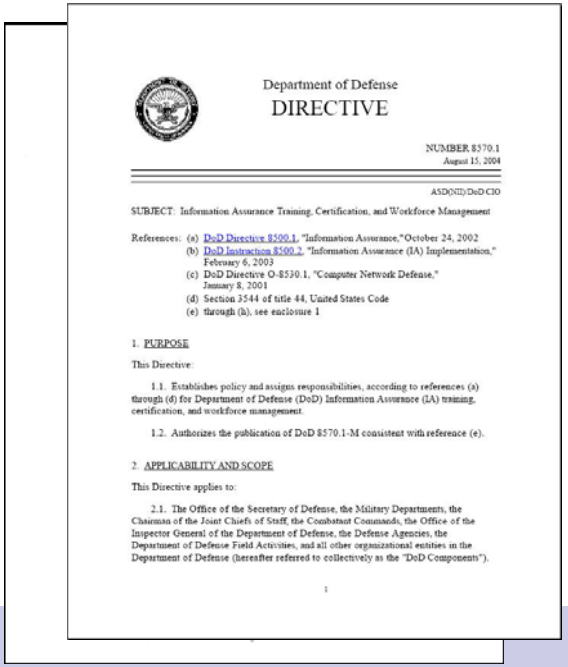
Component "certification" -- largely undefined

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

Baseline IA Certifications

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

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

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

Rationale for Private Sector Certifications

- **Standard test; community developed: serves as “baseline”**
- **Worldwide accessibility**
- **Meets an international standard (ISO/IEC 17024)**
- **Accredited by an independent 3rd party (ANSI)**
- **Continuous learning/periodic retest -- linked to the certification**
- **Portability across domains (NIST, DOD, IC; public and private sector)**
- **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)**
- **Work Related: Accreditation requires job task analysis (JTA)**
- **Providers track/report on individual’s certification status.**

Challenges

- **Identifying the workforce**
- **Ability to tag and track the workforce (databases)**
- **Educating leadership**
- **Fear of tests**
- **Managing expectations (of DoD, of certification providers)**
- **Personnel turnover (leadership & key staff)**
- **Bureaucracy**
- **Organizational: in garrison vs deployed**
- **Getting the information to the IA workforce (outreach)**
- **Funding (and retaining funding) for training**
- **Funding (allocating and retaining training funds)**
- **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.**

About (ISC)²

- **Established in 1989 - Non-profit consortium of industry leaders**
- **Global leaders in certifying and educating information security professionals with the CISSP® and related concentrations, CAP^CM & SSCP®**
- **Offer the first information technology-related credentials to be accredited to ANSI/ISO/IEC Standard 17024**
- **Track and report on the rapidly evolving information security workforce**
- **Global standard for information security – (ISC)² CBK®, a taxonomy of information security principles**
- **Board of Directors -- Top information security professionals worldwide**
- **Approximately 50,000 certified professionals in 122 countries**
- **Produce the only annual Global Information Security Workforce Study**

Questions for the Panelists

- What is your opinion of the current state of the federal IT/IA security workforce?
- Is there a requirement for a separate job series of government IT/IA professionals?
- A recent ITAA CIO survey indicated that CIOs are declining in agency hierarchies. What are the implications of this for IT security professionals?
- Is there one action you could recommend that would immediately improve the professionalism of the federal IT security workforce?

Questions?

Contact Information:

Lynn McNulty, CISSP

Director of Government Affairs

(ISC)²

Lynn.McNulty@verizon.net

703-448-8208