National Information Assurance Education and Training Program


Sherry Borror s. borror@ radium. ncsc. mil
INFOSEC Training and Education

• Documented Need
• Partnerships address long time problem
• NSA’s Response:
  • NIETP
  • NIST-CNSS-NSA Linkage/Partnerships
• Future Initiatives
Let’s Take Advantage of Work Already Done, and Work In Progress.
Many full/part-time personnel not trained for the job they hold.

- Self Taught.
- One the Job Training.
- Peer-to-peer exchange.
- Conferences, Vendor, and Govt.

"You Figure it out"
"Learn by mistake"
"Security Guides and INFOSEC Lore"
"If funds Available"
To Demonstrate Existence of a Career Field

- 1. Distinct Body of Knowledge
   EDACUMS have documented
- 2. Body of Literature
   Nat’l Conference & UC-Davis Project
- 3. Career Progression
   Already exists in several agencies
   Proposed in NCSC Pub #27
- 4. Sufficient Numbers of Personnel
   (Dedicated to that Profession)
   OPM study nearly completed
INFOSEC/IA Personnel Shortfalls

- Many security tasks not being adequately performed due to lack of personnel, training, and tools
- Critical security responsibilities assigned as additional duties
- Lack of comprehensive, consistent training for ISSOs security engineers, certifiers, accreditors
• NSTI SSC 1993 report
  – INFOSEC Education and Training listed in top three priorities
“Education, training, and awareness are countermeasures that effectively reduce exposure to a variety of known risks. In order to achieve this end, it is essential to have a federal work force that is aware of, and educated about, the problems of information systems security (INFOSEC).”

Charles A. Hawkins, Jr.
Acting Chairman, NSTISSC
25 Feb. 1993
• Redefining Security 1994 report

  “Uniformity in skills and knowledge taught security professionals is needed not only to ensure the quality of work, but also to foster a common understanding and implementation of security policies and procedures.”
• OTA 1994 Report

  To be comprehensive, however, the generally accepted practices must be defined at several levels of detail, and different sets of the standards would apply to different users and applications.”
“Some experts estimate that over one-half of the total financial and productivity losses in information systems is the result of human errors…”

Information Security and Privacy in Network Environments
Office of Technology Assessment. Sept. 1994
• President’s Commission on Critical Infrastructure Protection

  - “NIST, NSA, and the U.S. Department of Education work in collaboration with the private sector to develop programs for education and training of information assurance specialists and for the continuing education as technologies change. This effort should also support “training the trainers” to provide an adequate cadre of qualified instructors to teach technicians.”

Mission

Be a leading advocate for improving information system security (INFOSEC) education and training nationwide.
NIETP Activities Related to PDD63

*Highlights at a glance*

  - National Training Standards
  - National Colloquium for Information Systems Security Education
  - Centers of Academic Excellence in Information Assurance Education
  - Courseware Evaluation Program for Certification
  - Support to Military Services
  - Academic Outreach
  - Products
  - Support to President’s Critical Infrastructure Protection Board
Assistant Secretary of Defense
Command, Control, Communications and Intelligence
MEMO Dated July 2, 2001

“\nI hereby delegate to the Director, National Security Agency, the authorities and responsibilities of the Secretary of Defense under the following statute:
Public Law 106-398

Department of Defense Scholarships for Service Program
NSTISSC redesignated CNSS

Committee on National Security Systems

“The CNSS provides a forum for discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems through the CNSS issuance system”.
A method of involvement and consensus building to determine training needs as identified by skilled workers and professionals.

A joint NSA and ISU venture for producing CNSS Training Standards
EDACUM

A consortium of over 1000 INFOSEC Professionals from:

<table>
<thead>
<tr>
<th>Government</th>
<th>Academia</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSA</td>
<td>Idaho State University</td>
<td>ISI</td>
</tr>
<tr>
<td>NIST</td>
<td>Navy PGS</td>
<td>ISSA</td>
</tr>
<tr>
<td>DISA</td>
<td></td>
<td>ISC</td>
</tr>
<tr>
<td>SERVICES</td>
<td></td>
<td>ARCA</td>
</tr>
<tr>
<td>EDUCATION</td>
<td></td>
<td>MIS</td>
</tr>
<tr>
<td>COMMERCE</td>
<td></td>
<td>Rockwell</td>
</tr>
<tr>
<td>HHS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TREASURY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>House of Reps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EDACUM Principle

Strength Through Diversity

SMEs

Policy Specialists

“Outside” Experts

Managers/Supervisors

Educators

Stakeholders and Partners in Change
• **KNOWLEDGE**: Broad comprehension of a subject that cannot necessarily be applied
• **SKILL**: Comprehension of a subject that is/can be specifically applied to a job
• **ATTRIBUTE (ABILITY)**: Personality characteristics which are/can be developed to enhance job performance
KSA, to...BEHAVIORAL OBJECTIVE: PROGRESSION

- KSA
  - “Password Protection”

- PERFORMANCE ITEM
  - “Construct password protection schema”

- BEHAVIORAL OBJECTIVE
  - CONDITION: “Given password protection algorithm”
  - BEHAVIORAL: “Construct password instruction set for a Windows NT network”
  - STANDARD: “Which provides minimum 6 letter character and 30 day expiration date per new password”
Audit Function (Entry Level)

Work Closely with ISSO to ensure the AIS or network is used securely

• **Policy and Procedures**
  – Explain the purpose of a system audit
  – State logging policies
  – Reproduce documentation required in event of a detected intrusion to the system
  – Explain Electronic Records Management policy by monitoring notification
  – Describe the need for separation of duties
  – Explain Audit
  – State audit trails and logging policies
  – Reproduce documentation
Example INFOSEC Standard
System Administrator:

Competency # 2: Access Control
KSA # 2.a Policies/Administration (*9)

Performance Item # 2.a.1

“Use network access change controls as designed”

Competency # 4: Audit
KSA # 4.c Tools (*7)

Performance Item # 4.c.6

“Identify two intrusion detection systems”

* = Number of associate Behavioral KSAs  Total # KSAs for Systems Admin = 292
INFOSEC Electronic DACUMs to date

DACUM I: Establishing the basics
- Aug '92: Define A, T, & E levels/
  produce awareness materials.

DACUM II: Creation of new AT&E Matrix
- Aug '93: Build Nat’l. AT& E Model

DACUM III: Unified Taxonomy for ISS Professors
- Nov '93: Define and categorize KSAs.

DACUM IV: From Theory to Instruction
- Apr '94: Defined 3 operational level training Reqs.

DACUM V: National Training Standards
- Sept '94: Producing 3 draft NSTISSI 40XX.

DACUM VI: System Certifier Standard
- June '95: Define Trng. Std. for Certifier.
INFOSEC Electronic DACUMs to date
Cont.

**DACUM VII:** Completing A Picture
- June ‘98; Integrating DITSCAP

**DACUM VIII:** Defining Risk Analyst
- March ‘99: An emerging career

**DACUM IX:** Updating the Previous Work
- June 2000, Transforming standards from INFOSEC to IA

**DACUM X:** Putting IA into all of the standards
- March 2002 – Using Govt., Industry and Academia to transform the standards.
National Training Standards


Information Systems Security Professionals - No. 4011

Designated Approving Authority - No. 4012

System Administrators (INFOSEC) - No. 4013

Information Systems Security Officers - No. 4014

System Certifiers - No. 4015

Risk Analyst - No. 4016

Under Development
Quality of Training
Information Assurance Courseware Evaluation Project

Departments
Agencies & Institutions

Certified Training Provider

Delivery

Notification

Certification
Electronically Submit to Web

ACADEMIA

GOVERNMENT

COMMERCIAL
100% MAPPING

National Standards

Curriculum

Certification
Certified Organizations

AIR FORCE INSTITUTE OF TECHNOLOGY - 4011
ARC INFORMATION ASSURANCE INSTITUTE – 4011, 4012, 4015
GEORGE MASON UNIVERSITY – 4011
GEORGE WASHINGTON UNIVERSITY - 4011
FLORIDA STATE UNIVERSITY – 4011
IDAHO STATE UNIVERSITY – 4011, 4013, 4014, 4015
INDIANA UNIVERSITY OF PENNSYLVANIA - 4011
INFORMATION RESOURCES MANAGEMENT COLLEGE – 4011
IOWA STATE UNIVERSITY – 4011
JOHN HOPKINS UNIVERSITY - 4011
NAVAL POST GRADUATE SCHOOL – 4011
NORWICH UNIVERSITY – 4011, 4014
Certified Organizations

NEW MEXICO TECH - 4011
NORTHEASTERN UNIVERSITY - 4011
PURDUE UNIVERSITY - 4011
STATE UNIVERSITY OF NEW YORK AT BUFFALO – 4011
STATE UNIVERSITY OF NEW YORK AT STONY BROOK - 4011
TOWSON UNIVERSITY - 4011
UNIVERSITY OF CALIFORNIA, DAVIS - 4011
UNIVERSITY OF IDAHO – 4011
UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE – 4011
UNIVERSITY OF NEBRASKA AT OMAHA – 4011
UNIVERSITY OF TEXAS AT SAN ANTONIO - 4011
UNIVERSITY OF TULSA – 4011, 4012, 4013, 4014, 4015
Certified Organizations

SANS INSTITUTE – 4013
UNIVERSITY OF WISCONSIN, MILWAUKEE - 4011
UNIVERSITY OF FINDLAY - 4011
ACADEMIA
Emerging Role of Academia

• The number of colleges teaching INFOSEC is increasing.
• Integrated & stand alone courses.
• Whole degree programs.
• Good geo-locations.
The Not So Good News*

• Today there are only **four** declared, dedicated computer security research centers in degree granting departments at universities in the United States.

• Over the past five years, approximately 5,500 PhDs in computer science and engineering were awarded by universities in the US. Only 16 of those were awarded for security-related research at these major centers (only **8 of the 16 were U.S. Nationals**).

Dr. Eugene Spafford
Testimony to House Science Comm.
Feb. 11, 1997
Defending America’s Cyberspace

“In developing the Federal Cyber Service initiative, we can leverage existing Federal education, training and awareness programs. In education, the NSA has a program to designate universities as Centers of Academic Excellence in Information Assurance Education based on established criteria rooted in the National Security Telecommunications and Information Systems Security Committee (NSTISSC) training standards.”
Partnerships with Academia

Centers of Academic Excellence in Information Assurance Education

Reducing the vulnerability of our NII by promoting higher education in information assurance, and producing a growing number of professionals with IA expertise in various disciplines.

http://www.nsa.gov/isson/programs/coeiae/index.htm
Centers Of Academic Excellence in Information Assurance Education (Graduate and Undergraduate Levels)

Criteria for Measurement


1. Use of NSTISSC Training Standards
2. IA treated as multidisciplinary
3. Demonstration of use of IA within the university
4. Encourages research in IA
5. IA curriculum reaches beyond normal geographic borders
6. Faculty active in IA research and practice
7. State of the art IA reference system/materials
8. Declared concentrations in IA
9. Declared center for IA education
10. More than one faculty member
Geo location is very good.
Centers of Academic Excellence in Information Assurance Education

**Academic Years 1999-2002**
- James Madison University
- George Mason University
- Idaho State University
- Iowa State University
- Purdue University
- University of California at Davis
- University of Idaho

**Academic Years 2000-2003**
- Carnegie Mellon University
- Florida State University
- Information Resources Management College, National Defense University
- Naval Postgraduate School
- Stanford University
- University of Illinois at Urbana Champaign
- University of Tulsa

**Academic Years 2001-2004**
- Drexel University
- Georgia Institute of Technology
- Mississippi State University
- Norwich University
- Syracuse University
- United States Military Academy, West Point
- University of Maryland, Baltimore County
- University of North Carolina, Charlotte
- West Virginia University
Centers of Academic Excellence in Information Assurance Education

Academic Years 2002-2005

New Designations:
- Air Force Institute of Technology
- George Washington University
- Indiana University of Pennsylvania
- New Mexico Tech
- North Carolina State University
- Northeastern University
- Polytechnic University
- State University of New York, Buffalo
- State University of New York, Stony Brook
- Towson University
- University of Maryland, University College
- University of Nebraska, Omaha
- University of Texas, San Antonio

Re-Designations:
- James Madison University
- George Mason University
- Idaho State University
- Iowa State University
- Purdue University
- University of California, Davis
- University of Idaho
Major DoD Military Installations

- Army
- Navy
- Air Force
- Joint/Dual
- USMC
- Gov’t
Gov’t/DoD Bases/Agencies w/ INFOSEC Training
NSA Centers of Academic Excellence in IA Education
Service Academies
Institutions with NSTISSC IA Certified Courseware
MAP TO CUSTOMER SITES!

Geolocation is very good.
University Based Web Sites

George Mason: Center For Secure Information Systems
http://www.isse.gmu.edu/~csis

Purdue University: Center for Education and Research in Information Assurance and Security
http://www.cerias.purdue.edu

University of California, Davis: Security Lab

James Madison University
http://www.infosec.jmu.edu
http://cob.jmu.edu/mba/MBAPgms.htm#TheInformationSecurity MBA

Colloquium for Information Systems Security Education
http://www.infosec.jmu.edu/ncisse
Partnerships with Business, Academia, & Government

National Colloquium for Information Systems Security Education

**Purpose:** The Colloquium provides a forum for leading figures in government, industry and academia to work in partnership to define current and emerging requirements for information security education and to influence and encourage the development and expansion of information security education, especially at the graduate and undergraduate levels.

http://www.infosec.jmu.edu/ncisse
In Summary
National Security Agency
ATTN: I2
9800 Savage Road
Fort Meade, Maryland  20755-6000

Dr. Vic Maconachy, Program Manager:
w.macona@radium.ncsc.mil

Phone: (410) 854-6206
FAX: (410) 854-7043