Federal Cyber Security
Training, Education & Workforce Development

Brenda Oldfield
Director, Cyber Education and Workforce Development (CEWD)
National Cyber Security Division
U.S. Department of Homeland Security

July 27, 2009
Foster effective cybersecurity education and workforce by facilitating the availability of qualified IT security professionals to support the Nation’s cyber security needs

**Improve** cyber security education/training for IT professionals

**Increase efficiency/enhance quality** of existing cyber security workforce development programs

**Invigorate the pipeline** of skilled cyber security employees
CEWD Program Activities:

- National Centers of Academic Excellence in IA Education
- Federal Cyber Service: Scholarship for Service
- IT Security Essential Body of Knowledge (EBK)
- Information Systems Security Line of Business (ISS LOB) Role-Based Training Working Group Lead
- **Comprehensive National Cyber Initiative:** Expand Cyber Education, Co-Lead/DHS & DoD/NSA
National Centers of Academic Excellence in IA Education
National CAEs – “Partnerships with Academia”

Co-Sponsored: National Security Agency and DHS

NSA/Information Assurance Directorate
National IA Education and Training Program

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

http://www.nsa.gov/ia/academia/acade00001.cfm
National CAEs – “Academic Recognition”

A Three Tier Program

- Meet 9 Criteria
- PhD Research
- CAE – R
- CAE/IAE
- Map to CNSS Standards
- CNSS Certification
CAE Criteria for Measurement - 2009

2. IA treated as multidisciplinary science
3. Practice of IA encouraged throughout the university
4. Student based IA Research
5. Faculty active in IA research and practice
6. IA Resources
7. IA Academic Program is robust and active
8. Declared center for IA education
9. Number of faculty members and course loads

Prerequisite: Use of CNSS Training Standards

website: http://www.nsa.gov/ia/academia/acade00001.cfm
Goal: Proactively increase our understanding of robust IA technology, policy, and practices that will enable our Nation to effectively prevent and respond to a catastrophic cyber event. This program will contribute significantly to the advancement of state-of-the-art IA knowledge and practice.

Vision is to establish a process that will:
1. Recognize schools with programs that integrate research activities into the curriculum and into the classroom setting.
2. Provide NSA, DHS, and other federal agencies with insight into academic IA programs (with their reach into industry) that can support advanced academic, research, and development capabilities.
3. Serve as potential source and facilitator for government-academia researcher exchanges.
4. Present opportunities for IA research centers to drill deeper into much needed solutions for securing critical information systems and networks.
40 CAE-Rs, 104 CAE/IAEs, total of 106 altogether, covering 36 States, District of Columbia and Puerto Rico
Federal Cyber Service:

Scholarship for Service (SFS)
Information Assurance Scholarship Program (IASP)
Federal Cyber Service Program Goals

- To increase national capacity for educating information technology (IT) specialists in IA disciplines
- To produce new entrants to the Federal IA workforce
- To increase national R&D capabilities in IA
- To strengthen partnerships between institutions of higher learning and relevant employment sectors

- SFS Co-Sponsored by the National Science Foundation and DHS
- IASP, Sponsored by DoD
Institution Eligibility:
• NSA/DHS CAE/IAE designation (or equivalent)
• Full-time program of study in IA field(s)
• Institutions must submit a grant proposal in response to an annual solicitation

Student Eligibility:
• US Citizen
• Full-time student in IA program, within 2 years of graduation
• Eligible for federal employment (must acquire security clearance)
• Awardee institutions set additional selection criteria

Scholarship Component:
• Funding: tuition, room/board, fees, and stipends - $8,000/yr (undergraduate), $12,000/yr (graduate)
• Length: 2 year scholarship for final 2 years of undergraduate or graduate (master’s or doctoral) work
• Obligation: Summer internship, post-graduation service requirement equal to scholarship length in a Federal Agency
More than 1000 SFS scholarship recipients, of these ~close to 200 are still in their academic programs

Government placement rate >92%

Capacity building grants to more than 60 institutions are strengthening capacity

28 institutions currently participating
SFS Participating Institutions

1. Air Force Institute of Technology
2. Auburn University
   Alabama State
   Tuskegee University
3. Carnegie Mellon University
4. Florida State University
5. George Washington University
   Marymount University
6. Georgia Institute of Technology
7. Idaho State University
8. Iowa State University
9. Mississippi State University
10. Naval Postgraduate School
11. New Mexico Institute of Mining/Tech
12. Norwich University
13. North Carolina A&T State
14. Polytechnic University
15. Purdue University
16. Stoneybrook SUNY
17. Syracuse University
18. University at Buffalo, the State University of New York
19. University of California at Irvine
20. University of Idaho
21. University of Illinois @ Urbana at Champaign
22. University of Nebraska – Omaha
23. University of North Carolina – Charlotte
24. University of Tulsa
25. University of Pittsburgh
An umbrella framework, linking competencies & functional perspectives to IT security roles fulfilled by personnel in the public and private sectors:

- 10 Notional IT Security Roles
- 14 Competency Areas
- 4 Functional Perspectives

- Promotes uniform competency guidelines to increase overall efficiency of IT security training and education;
- Facilitates cost-effective professional development, including skills training and certifications, or other affiliated human resource activities (recruiting & career path planning)

**Current Implementations/Projects:**

- State Government IT Security Workforce Development model
- Department of Energy
- Federal CIO Council IT Workforce Committee
NSPD-54/HSPD:

Provide the USG with a technically adept cyber workforce capable of achieving the goals of the CNCI.

With an initial focus on role-based, specialized skills of current cyber personnel and the pipeline of future cyber recruits, this effort will expand the capabilities of today’s workforce and prepare the future USG workforce.
Mission Accomplished

Competencies (Knowledge/Skills/Abilities) to Perform the Mission

Mission Functions: WORK DEFINED
CNCI Education Strategic Drivers

1) Develop an educational framework that keeps pace with speed of technological change – both in content and delivery

3) Create a systematic approach and common taxonomy of cyber roles, skills sets and standards

5) Accelerate the availability of skilled workers in the pipeline for Federal employment:
Current DHS/Federal Cyber Education and Training Partnerships:

- Enterprise-wide Access to CMU/SEI Virtual Training Environment
- Software Assurance Education and Training Programs
- Federal Cyber Security Training Exercise Program
- Federal Virtual Worlds Trusted Source Hosting Project
Create A Systematic Approach and Common Language

- Build Foundations for a Cyber Security Competency Assessment Framework
- Federal Cyber Roles - Competency Synchronization Analysis
Cyber Competence Assessment Framework

- **Black Belts**
- **Brown Belts**
- **Green Belts**
  - General IT security skills, maintenance of networks
  - Awareness, basic literacy, all users
Enhance/Improve the Federal Cyber Service and CAE Programs

• IA Education Standards Review
• Enhance CAE/IAE Program Criteria
• IA in Community Colleges & Faculty IA Development
• SFS Mentorship Facilitation Program Pilot
60-Day Review: Expanded Focus

**CNCI**
- Federal Focus
- Federal Employee Awareness
- Federal Workforce Focus
- Federal Pipeline

**National Education**
- National Focus
- Public Awareness
- K-12 & Higher Education
- National Pipeline
Outreach & Awareness Program Activities

Cyber Security Awareness Volunteer Education Program (C-SAVE)

National Cyber Security Awareness Month: Our Shared Responsibility
Why is the program needed?

- National Cyber Security Alliance (NCSA) conducted a baseline study in 2008 on how cybersecurity was being taught in schools
- Major findings of the 2008 National Cybersafety, Cyberethics, Cybersecurity Baseline Study include:
  - Only 10% of educators received > 6 hours of professional development on cybersecurity
  - Only 22% are comfortable teaching about cyber bullying, identity theft and other types of cyber crime
  - Only 35% of curriculum covers viruses/malware
  - Only 185 of curriculum covers identity theft and phishing

- As evidenced by the study results, there is currently a gap in cybersecurity education in schools
Encourages cybersecurity professionals to:

- Visit local classrooms
- Educate students on cybersecurity issues and the importance of safe online practices
- Share their personal experiences in the cybersecurity field
- Promote interest in cybersecurity as a profession for young people
C-SAVE Materials:

- Guidance for approaching schools on setting up a visit
- Suggested lessons for all grade levels
- Tips for working in a classroom setting
- Tips for presenting to young people
National Cyber Security Awareness Month established by NCSD in 2004:

- Held every October in partnership with the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC)

- Designed to educate all citizens on cyber threats and how to safeguard themselves at home, work and school

- Throughout the month, public and private sector partners are actively engaged through events and initiatives aimed at increasing overall awareness
Contact Info:

Brenda Oldfield  
**Director, Cyber Education and Workforce Development**  
**National Cyber Security Division**  
**U.S. Department of Homeland Security**  

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

http://www.us-cert.gov/ITSecurityEBK
Online Training Resource - FREE

- Adaptive Cyber-security Training Online
- DHS / FEMA Sponsored
- U.S. Citizens Only
- Web-Based
  - Designed to utilize the latest online learning methodologies
    - Adapts to the user
    - Feature-rich Interface
- Robust, Adaptive Training
  - No more “Next->Next->Next->Certificate!”

ACT Online: www.act-online.net
# FREE - A Wide Array of Course Offerings!

<table>
<thead>
<tr>
<th>IA General/Non-Technical</th>
<th>IA Technical/IT Professional</th>
<th>IA for Business Professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Security for Everyone</strong></td>
<td><strong>Information Security Basics</strong></td>
<td><strong>Business Information Continuity</strong></td>
</tr>
<tr>
<td>TEI Course Number: AWR-175-W</td>
<td>TEI Course Number: AWR-173-W</td>
<td>TEI Course Number: AWR-176-W</td>
</tr>
<tr>
<td><strong>Cyber Ethics</strong></td>
<td><strong>Secure Software</strong></td>
<td><strong>Information Risk Management</strong></td>
</tr>
<tr>
<td>TEI Course Number: AWR-174-W</td>
<td>TEI Course Number: AWR-178-W</td>
<td>TEI Course Number: AWR-177-W</td>
</tr>
<tr>
<td><strong>Cyber Law and White Collar Crime</strong></td>
<td><strong>Network Assurance</strong></td>
<td><strong>Cyber Incident Analysis &amp; Response</strong></td>
</tr>
<tr>
<td>(Projected Release: August 09)</td>
<td>TEI Course Number: AWR-138-W</td>
<td>(Projected Release: August 09)</td>
</tr>
<tr>
<td><strong>Digital Forensics Basics</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEI Course Number: AWR-139-W</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[www.act-online.net](http://www.act-online.net)
Questions?

- Register @ [http://www.act-online.net](http://www.act-online.net)

- Contact:
  - Tammy Alexander
  - Project Coordinator, University of Memphis
  - tammy.alexander@memphis.edu
  - 901-678-1521