The Evolution of Federal Government Cybersecurity Education and Scholarship Programs

March 21, 2018
2003 National Strategy to Secure Cyberspace

National Cyberspace Security Priorities: A National Cyberspace Security Awareness and Training Program

• Foster Adequate Training and Education Programs to Support the Nation’s Cybersecurity Needs
• Increase the Efficiency of Existing Federal Cybersecurity Training Programs
• Promote Private Sector Support for Well-Coordinated Widely Recognized Professional Cybersecurity Certifications
2008 Comprehensive National Cybersecurity Initiative (CNCI)

Initiative #8: Expand cyber education

While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field.
Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950’s, to meet this challenge.
2009 Cyberspace Policy Review

Subtitle: Assuring a Trusted and Resilient Information and Communications Infrastructure

• Increase Cybersecurity Education: The Federal government, with the participation of all departments and agencies, should expand support for key education programs and research and development to ensure the Nation’s continued ability to compete in the information age economy. Existing programs should be evaluated and possibly expanded, and other activities could serve as models for additional programs.
2009 Cyberspace Policy Review (Continued)

• Expand Federal Information Technology Workforce: The President’s cybersecurity policy official, in coordination with the ICI-IPC, should consider how to better attract cybersecurity expertise and to increase retention of employees with such expertise within the federal service.
2014 Cybersecurity Enhancement Act

• Title III – Education and Workforce Development
  – Section 301. Cybersecurity competitions and challenges
  – Section 302. Federal cyber scholarship-for-service program

• Title IV – Cybersecurity Awareness and Preparedness
  – Section 401. National cybersecurity awareness and education program
Title III, Section 301
Cybersecurity Competitions and Challenges

The Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, shall

(1) support competitions and challenges

(A) to identify, develop, and recruit talented individuals to perform duties relating to the security of information technology in Federal, State, local, and tribal government agencies, and the private sector; or

(B) to stimulate innovation in basic and applied cybersecurity research, technology development, and prototype demonstration that has the potential for application to the information technology activities of the Federal Government; and

(2) ensure the effective operation of the competitions and challenges
Title IV, Section 401
National Cybersecurity Awareness & Education Program

The Director of the National Institute of Standards and Technology (referred to in this section as the “Director”), in consultation with appropriate Federal agencies, industry, educational institutions, National Laboratories, the Networking and Information Technology Research and Development program, and other organizations shall continue to coordinate a national cybersecurity awareness and education program.
Section 401 - That Includes Activities Such As

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Director;
(2) efforts to make cybersecurity best practices usable by individuals, small to medium-sized businesses, educational institutions, and State, local, and tribal governments;
(3) increasing public awareness of cybersecurity, cyber safety, and cyber ethics;
Section 401 Activities (Continued)

(4) increasing the understanding of State, local, and tribal governments, institutions of higher education, and private sector entities of—

   (A) the benefits of ensuring effective risk management of information technology versus the costs of failure to do so; and

   (B) the methods to mitigate and remediate vulnerabilities;

(5) supporting formal cybersecurity education programs at all education levels to prepare and improve a skilled cybersecurity and computer science workforce for the private sector and Federal, State, local, and tribal government; and

(6) promoting initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government and develop strategies for recruitment, training, and retention.
Section 401 Strategic Plan

• The Director, in cooperation with relevant Federal agencies and other stakeholders, shall **build upon programs and plans in effect** as of the date of enactment of this Act **to develop and implement a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and education program**

• Not later than 1 year after the date of enactment of this Act, and **every 5 years** thereafter, the Director shall transmit the strategic plan under subsection (c) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.
2015 Federal Cybersecurity Workforce Assessment Act

The head of each Federal agency shall

(1) identify all positions within the agency that require the performance of information technology, cybersecurity, or other cyber-related functions; and

(2) assign the corresponding employment code, which shall be added to the National Initiative for Cybersecurity Education’s Cybersecurity Workforce Framework
2017: Executive Order 13800

Title: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure Cybersecurity for the Nation: Policy

... the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.
2017: Executive Order 13800 (Continued)

- **Assess the scope and sufficiency of efforts** to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education.

- Provide a report to the President within 120 days with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.
Q & A
CyberCorps®
Scholarship For Service (SFS)
‘90s bombings

- World Trade Center Bombing, 1993
- Oklahoma City Bombing, 1995

- Executive Order 13010 - Commission on Critical Infrastructure Protection (PCCIP) (July 1996)

- PCCIP Final Report (October 1997)
  - Public-private sector communication
  - Real-time attack warning capability
  - Comprehensive education and awareness programs
  - Legal structures for assurance
  - Research and development efforts

  - NSA Centers of Excellence 1998
  - National Science Foundation CyberCorps Scholarship for Service (SFS) Program 2000
CyberCorps® Scholarship for Service (SFS)

- **Scholarship** grants support students earning degrees in cybersecurity in exchange for commitment to work for a federal, state, local, or tribal government agency after graduation.

- **Capacity** grants support innovative approaches to increase the ability of the U.S. higher education enterprise to produce cybersecurity professionals.

- FY2018 budget: $55M (est.)
Scholarship Track

- Tuition, fees, and stipends for up to 3 years of study.
- Managed by NSF in collaboration with OPM and DHS.
- Approximately 25% of graduates go to NSA
- About 64% at the master’s level and 34% undergraduates
- Over 3,300 scholarships have been awarded since the inception of the program and currently there are 69 participating universities with about 720 students in school.
- Over 94% of graduates go to work for the government.
- Website: SFS.opm.gov
### CyberCorps® (SFS) Students and Placements

#### Top 15 Student Enrollments, 2011-2015

<table>
<thead>
<tr>
<th>Institution</th>
<th>Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>U of Tulsa (OK)</td>
<td>82</td>
</tr>
<tr>
<td>Carnegie Mellon U (PA)</td>
<td>63</td>
</tr>
<tr>
<td>Mississippi State U (MS)</td>
<td>48</td>
</tr>
<tr>
<td>Naval Postgraduate School (CA)</td>
<td>47</td>
</tr>
<tr>
<td>Cal State San Bernardino (CA)</td>
<td>45</td>
</tr>
<tr>
<td>Dakota State U (SD)</td>
<td>44</td>
</tr>
<tr>
<td>New York U (NY)</td>
<td>39</td>
</tr>
<tr>
<td>U of North Carolina at Charlotte (NC)</td>
<td>37</td>
</tr>
<tr>
<td>Northeastern U (MA)</td>
<td>36</td>
</tr>
<tr>
<td>U of Ill. at Urbana-Champaign (IL)</td>
<td>36</td>
</tr>
<tr>
<td>North Carolina A&amp;T State U (NC)</td>
<td>36</td>
</tr>
<tr>
<td>Florida State U (FL)</td>
<td>35</td>
</tr>
<tr>
<td>U of Texas at Dallas (TX)</td>
<td>30</td>
</tr>
<tr>
<td>U of Nebraska at Omaha (NE)</td>
<td>29</td>
</tr>
<tr>
<td>James Madison University (VA)</td>
<td>28</td>
</tr>
</tbody>
</table>

#### Top 15 Placements of Graduates, 2011-15

<table>
<thead>
<tr>
<th>Institution</th>
<th>Placements</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Security Agency</td>
<td>79</td>
</tr>
<tr>
<td>MITRE Corporation</td>
<td>44</td>
</tr>
<tr>
<td>US Navy</td>
<td>38</td>
</tr>
<tr>
<td>State, Local, Tribal</td>
<td>37</td>
</tr>
<tr>
<td>Federal Reserve System</td>
<td>32</td>
</tr>
<tr>
<td>US Army</td>
<td>28</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td>26</td>
</tr>
<tr>
<td>Department of Justice</td>
<td>20</td>
</tr>
<tr>
<td>Johns Hopkins U Applied Physics Lab</td>
<td>20</td>
</tr>
<tr>
<td>Sandia National Laboratories</td>
<td>19</td>
</tr>
<tr>
<td>MIT Lincoln Laboratory</td>
<td>17</td>
</tr>
<tr>
<td>CMU Software Engineering Institute</td>
<td>15</td>
</tr>
<tr>
<td>US Air Force</td>
<td>11</td>
</tr>
<tr>
<td>Central Intelligence Agency</td>
<td>10</td>
</tr>
<tr>
<td>Pacific Northwest Laboratory</td>
<td>8</td>
</tr>
</tbody>
</table>
CyberCorps*: Scholarship for Service (SFS) Participating Institutions

69 Scholarship for Service Participating Institutions
in 31 states, the District of Columbia and Commonwealth of Puerto Rico
https://www.sfs.opm.gov/ContactsPl.aspx

For more information, visit: sfs.opm.gov or contact: sfs@opm.gov
National Capacity - GenCyber
Capacity Building - WiCyS

Women in Cybersecurity
Cybersecurity Enhancement Act of 2014

One Hundred Thirteenth Congress
of the
United States of America

AT THE SECOND SESSION
Begun and held at the City of Washington on Friday,
the third day of January, two thousand and fourteen

An Act

To provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.
(a) SHORT TITLE.—This Act may be cited as the "Cybersecurity Enhancement Act of 2014".
The Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management and Secretary of Homeland Security, shall continue a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments (…)

• provide scholarships through qualified institutions of higher education, including community colleges (…)
• prioritize the employment placement of scholarship recipients in the Federal Government.
ELIGIBILITY.—To be eligible to receive a scholarship under this section, an individual shall—

(1) be a citizen or **lawful permanent resident** of the United States;
(2) demonstrate a commitment to a career in improving the security of information technology;
(3) **have demonstrated a high level of proficiency in mathematics, engineering, or computer sciences**;
(4) be a **full-time student** in an eligible degree program at a qualified institution of higher education, as determined by the Director of the National Science Foundation;
2018 National Defense Authorization Act

NDAA

NDAA for Fiscal Year 2018

Conference:

- Conference Report Language
- FY18 NDAA Floor Summary
Pilot Program.--Not later than 1 year after the date of enactment of this subtitle, as part of the Federal Cyber Scholarship-for-Service program established under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall develop and implement a pilot program at not more than 10, but at least 5, community colleges to provide scholarships to eligible students who—

(1) are pursuing associate degrees or specialized program certifications in the field of cybersecurity; and
(2)(A) have bachelor's degrees; or (B) are veterans of the Armed Forces.
Assessment.--Not later than 1 year after the date of enactment of this subtitle, as part of the Federal Cyber Scholarship-for-Service program established under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, shall assess the potential benefits and feasibility of providing scholarships through community colleges to eligible students who are pursuing associate degrees, but do not have bachelor's degrees.
To be eligible to receive a scholarship under this section, an individual shall (...) be a full-time student in an eligible degree program at a qualified institution of higher education, as determined by the Director of the National Science Foundation, except that in the case of a student who is enrolled in a community college, be a student pursuing a degree on a less than full-time basis, but not less than half-time basis;
(...) provide awards to improve cybersecurity education at the kindergarten through grade 12 level—

(A) to increase interest in cybersecurity careers;  
(B) to help students practice correct and safe online behavior and understand the foundational principles of cybersecurity;  
(C) to improve teaching methods for delivering cybersecurity content for kindergarten through grade 12 computer science curricula; and  
(D) to promote teacher recruitment in the field of cybersecurity.
Dr. Victor Piotrowski  
Lead Program Director  
National Science Foundation  
vpiotrow@nsf.gov  

Information for students and hiring officials:  
http://sfs.opm.gov  

Information for universities to apply for Cybersecurity Education grants:  
https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991  
https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709
Q & A
NSA/DHS National Centers of Academic Excellence in Cyber Defense

Cybersecurity Workforce Development for the Nation

Lynne Clark, Chief, NSA/DHS CAE-CD Program, NSA College of Cyber
CAE-C and IASP

• Centers of Academic Excellence in Cybersecurity (CAE-CD and CAE-CO)

The goal of the CAE-CD program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in CD and producing a growing number of professionals with cyber defense expertise.

• Information Assurance Scholarship Program (IASP)
  o NSA Executive Agent for DoD/CIO, housed in CAE-CD program office
  o 2018 NDAA: changes name to Cyber Scholarship Program
  o Scholarships and Capacity Building Grants like SFS
  o Students owe DoD one year of service for each year of scholarship; up to 5 years
  o Only CAE-C designated schools eligible
  o DoD workforce (Departments, Agencies, Field Activities)
  o Must be US Citizen
  o Students assigned to hiring billets – scholarship and job are conjoined
IASP Process

NSA sends solicitation to CAE-CD and CAE-CO designated schools

Schools identify candidate students (rising Juniors & grad students) & prepare capacity building grant proposals

IASP Executive Agent compiles student applications

DoD CIO sends billet call to DoD organizations

DoD organizations identify hiring billets, establish availability

• No job fair; no internship search
• US Citizens up to 5 years
• Student is an employee as of first summer

Hiring organizations review applications and pick students

IASP EA & hiring organizations collaborate to reconcile assignments

Hiring organizations work clearances & hiring administration

IASP notifies schools; Students accept; IASP issues grants to schools

Hiring organizations work clearances & hiring administration

Students attend selected program

Employee of gaining organization in summers

Gaining organization after graduation
National Information (Assurance) Education & Training Program

- Cybersecurity Standards (CNSS)
- DoD Information Assurance Scholarship Program Administration
- Information Assurance Curriculum Evaluation (IACE)
- NSA/DHS CAE-CD Program
- NSA-IAD Outreach to Service Academies Summer Interns Visiting Professors
- Security Education Academic Liaison (SEAL)
- National CAE Program (CAE-IAE)

Inherently NSA functions
CAE in Cyber Defense


2001: ASD C3I memo


2001: 2 July 2001: Information Assurance Scholarship Program

2004: NSA/DHS Partnership

2007: CAE-R Designation

2008: CAE-CO Program

2012: CAE-2Y Designation

2014: CAE-CDE Designation

2016: NICE Cybersecurity Workforce Framework

2017: 2013: Introduction of CAE-CD Knowledge Units (KUs)

1999: 7 schools

2001: 50 schools

2007: 86 schools

2012: 4 schools

2013: 145 schools

2012: 195 schools

Total Schools: 232

CAE-IAE

CAE-CO Program

CAE-CD 232 schools
New Paradigm 2017

232 Total Institutions

CAE Regional Resource Centers (CRRCs):
- Build regional community
- Provide Faculty Professional Development
- Assist Candidate Institutions

Legend:
State - # of CAEs as of November 2017
States with designated Community Colleges

CAE National Resource Centers (CNRCs)
- Community - California State University, San Bernardino (CA)
- Mentors - Whatcom Community College (WA)
- Reviewers - Northern Virginia Community College (VA)
- Knowledge Units - University of Houston (TX)
CAE-CD Candidates Program

- Designed to provide support to schools pursuing designation
  - Program Development (building program)
  - Application Assistance (documentation)
- Schools helping schools
  - CRRCs
  - Advisors, Reviewers, Mentors
- Two application windows per year

https://www.caecommunity.org/cae-program-applicant-checklist
CAE Designation Requirements

Curriculum
- Mapped to Knowledge Units
- Student Path and Recognition
- Faculty Qualifications
- Program Maturity
- Interdisciplinary Focus Areas

Programmatic Criteria
- Cyber Center
- Robust Program
- Regional Accreditation
- Articulation Agreements
- Faculty in Cyber Defense Research
- Students in Cyber Defense Research
- Outreach (other Colleges or High School)

**Program Path**

**Program Choice**
- Optional KUs (3)
- Optional KUs (3)
- Optional KUs (14)
- Optional KUs (14)
- Optional KUs (7) + Thesis or institutional equivalent
- Optional KUs (7) + Thesis or institutional equivalent
- Optional KUs (3) + Dissertation or institutional equivalent
- Optional KUs (3) + Dissertation or institutional equivalent

**Objective Driven**
- Technical Core KUs (5)
- Non-technical Core KUs (5)
- Technical Core KUs (5)
- Non-technical Core KUs (5)
- Technical Core KUs (5)
- Non-technical Core KUs (5)
- Technical Core KUs (5)
- Non-technical Core KUs (5)

**Everyone**
- Cybersecurity Foundational KUs (3)
- Cybersecurity Foundational KUs (3)

**Program Type**
- Associates
- Bachelors
- Masters
- Doctoral

**Thesis/ Dissertation or Institutional equivalent in a Cyber Defense Topic**

**Knowledge Units (KUs)**

**Foundational:** Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components

**Technical Core:** Basic Scripting and Programming; Basic Networking; Network Defense; Basic Cryptography; Operating Systems Concepts

**Non-technical Core:** Cyber Threats; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis; Cybersecurity Planning & Mgmt

Graduate programs provide evidence their students are admitted with foundational and core knowledge or it is included in the program of study.

PhD program assumes MS degree in related field.

43
CAEs & the NICE Framework

NICE Framework
NIST SP 800-181: Categories

- Operate and Maintain: 7 Work Roles
- Oversee and Govern: 14 Work Roles
- Protect and Defend: 4 Work Roles
- Investigate: 3 Work Roles
- Collect and Operate: 5 Work Roles
- Analyze: 7 Work Roles
- Securely Provision: 11 Work Roles

Students completing an Associates or Bachelors Program could qualify for work roles in multiple categories.

Students completing a graduate program would be expected to qualify for a specialized work role tracking most closely with one or two categories.

- 2017/2018 Annual Report: Schools asked to map their program path to one or more NICE Framework categories
- 2019 Application Cycle: Applying schools will map their program path to one or more NICE Framework categories
2018 CAE-CD Imperatives

- Educator shortage/Faculty Professional Development
- Competency measurement/metrics
- Cooperative education/apprenticeship
- Community College to BA/BS; CAE to CAE articulation
- Peer assistance and evaluation
- K-12 pipeline

80% of national demand

Focus on Workforce Development
Contact Information

Lynne Clark, Chief, National CAE-CO Program
410-854-6206
askCAEIAE@nsa.gov
CAE-CO https://www.iad.gov/NIETP/
CAE-CO & CO https://www.caecommunity.org/
https://www.nsa.gov/
Q & A
Thank You for Joining Us!

Subscribe to receive NICE Webinar Notifications:

https://public.govdelivery.com/accounts/USNIST/subscriber/topics?qsp=USNIST_3

nist.gov/nice/webinars