NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

What the National Initiative for Cybersecurity Education (NICE) is doing for you!

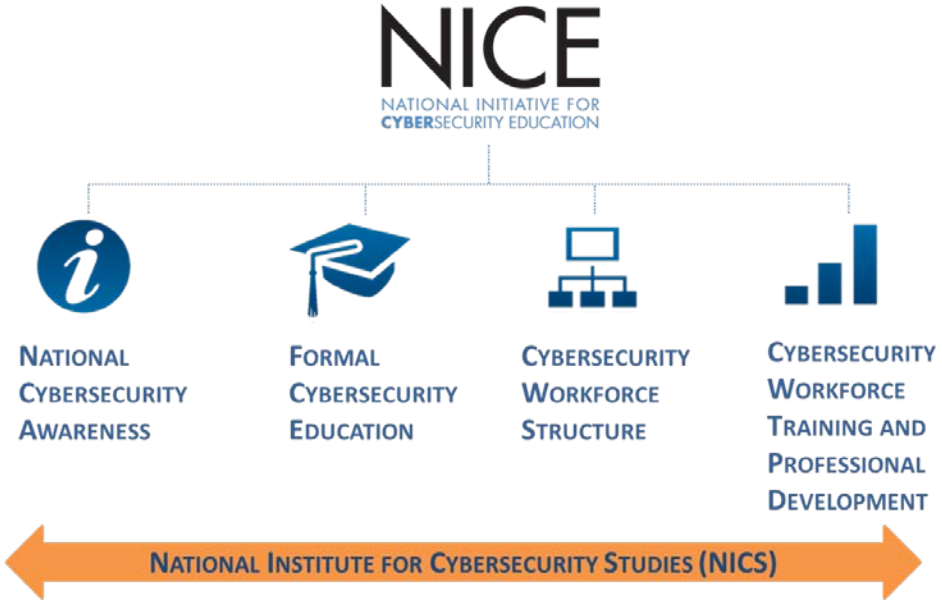
Margaret “Peggy” Maxson
Director, National Cybersecurity Education Strategy, DHS

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

A National Problem

- The Nation needs greater cybersecurity awareness and more cybersecurity experts.
- There is a lack of communication among government, private industry, and academia.
- Many cybersecurity training programs exist but there is little consistency among programs, and potential employees lack information about the skills needed for jobs.
- Cybersecurity career development and scholarships are available but uncoordinated, and the resources that do exist are difficult to find.

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort created following the recognition in two Presidential directives of the need for a robust, competent cybersecurity workforce.



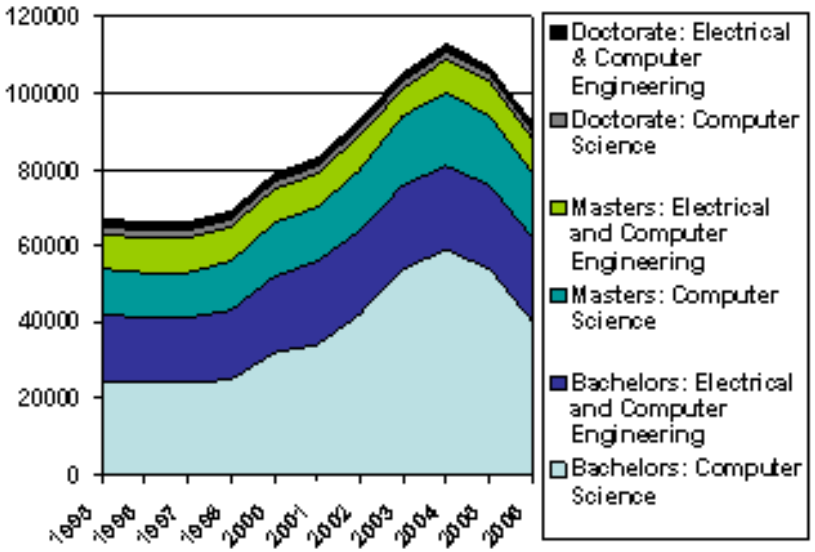
For more information on NICE, visit www.nist.gov/nice.

The Challenge

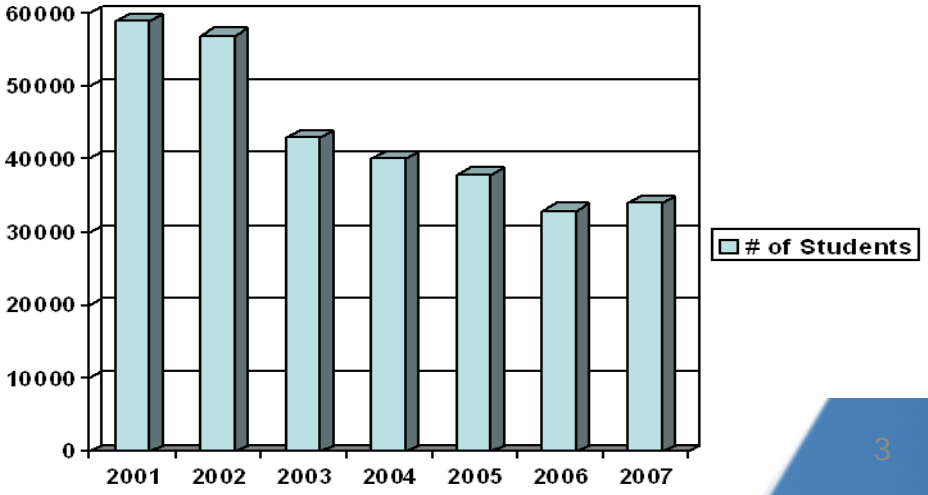
***TIMSS* Mathematics Test Score Comparison (2007): Avg. = 500 Source: *TIMSS* (2007)**

Grade	Four		Grade	Eight
Country	Score		Country	Score
Hong Kong	607		Chinese Taipei	598
Singapore	599		Rep. of Korea	597
Chinese Taipei	576		Singapore	593
Japan	568		Hong Kong	572
Kazakhstan	549		Japan	570
Russian Federat.	544		Hungary	517
England	541		England	513
Latvia	537		Russian Federat.	512
Netherlands	535		**United States**	**508**
Lithuania	530		Lithuania	506
United States	**529**		Czech Republic	504

Supply of Traditional NIT Graduates (1995-2000) (NCES)

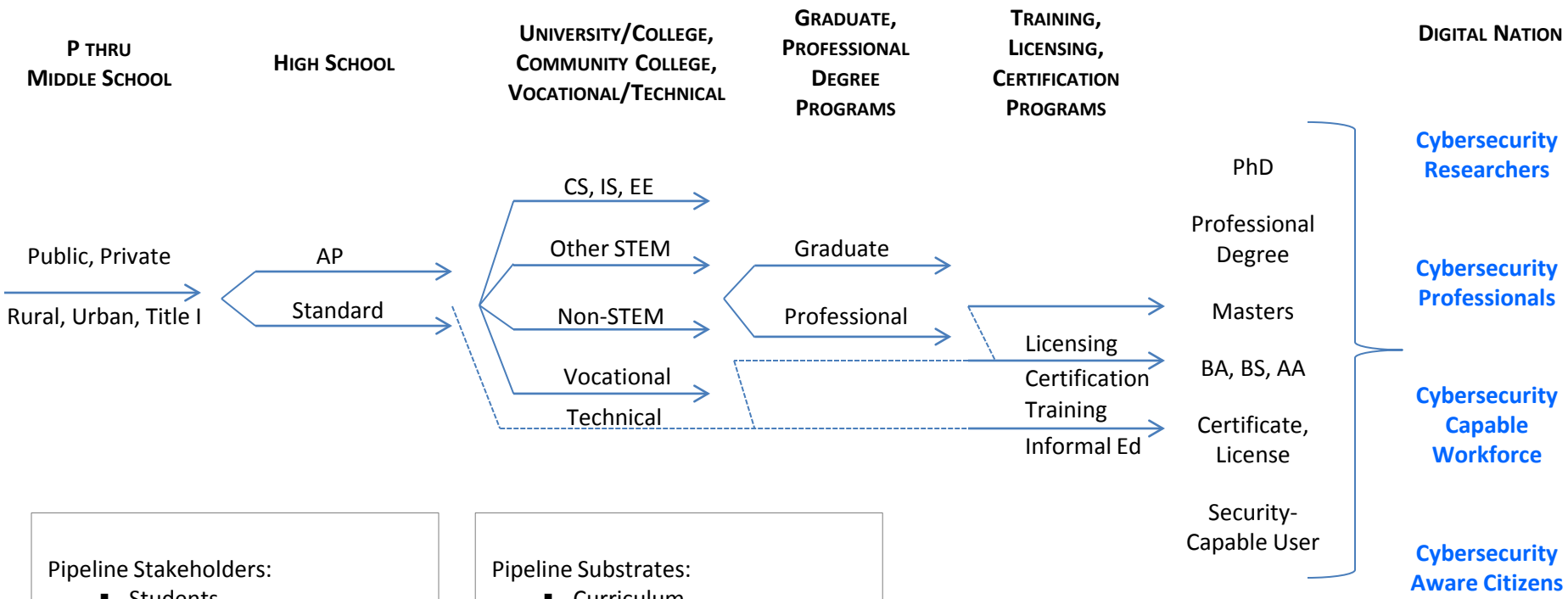


Computing and Information Sciences as Intended Major on SAT



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The Pipeline



Pipeline Stakeholders:

- Students
- Parents
- Teachers
- Educational Institutions
- State, Local Government
- Federal Government
- Professional Organizations
- Commercial Sector

Pipeline Substrates:

- Curriculum
- Ontologies, Taxonomies
- Standards
- Teacher Preparation
- Public Awareness
- Education Technologies
- Science and Practice of Learning

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

National Cybersecurity Workforce Framework

The Framework, version 1.0 published 22 August 2012, outlines 31 functional work specialties within the cybersecurity field and is the foundation of the effort.

Framework Use: Numerous efforts are underway to incorporate the Framework in education related activities nation-wide:

- K-12 and beyond cyber competitions are mapping their objectives to the KSA's in the Framework.
- K-12 cyber camps are focusing their activities on the KSA's.
- Higher learning institutions are mapping their curriculum to the framework.
- Find the framework @ http://www.nist.gov/nice/framework/

CYBERSECURITY WORKFORCE FRAMEWORK

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Human Capital Managers: Effective Strategies to Build Your Cybersecurity Workforce

What's your HC Strategy? Hiring, retaining and sustaining an effective, proactive Cybersecurity function presents challenges to HCMs, learn what you need to do to develop a successfully strategy...

Information for

- The Nation
  - General Public
  - Students
  - Educators
  - Parents
- Industry
  - Cybersecurity Professionals
  - Human Capital Managers
  - Cyber Managers
- Government
  - Cybersecurity Professionals
  - Human Capital Managers
  - Cyber Managers
  - Policy Makers
- Veterans

STOP | THINK | CONNECT™

Cybersecurity is a shared responsibility. For additional tips and resources for all age groups, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign.

STAY SAFE

Cybersecurity is for everyone. Awareness is the first step, explore tips & strategies to keep yourself and your family safe.

EXPLORE CAREERS

Explore the 31 Cybersecurity Specialty Areas defined within the National Cybersecurity Workforce Framework

FIND TRAINING

Our automated tool can match you with the professional training you need to keep up with changing threats.

WORKFORCE DEVELOPMENT

Learn about skills gap analysis, training strategies, and other activities to keep your Cyber workforce on top.

DISCOVER EDUCATIONAL OPPORTUNITIES

A Cybersecurity career can begin at different stages. From grade school to graduate school, explore educational opportunities on the CYBER HIGHWAY.

UPCOMING EVENTS

- JUN 11 — CISSE, June 11 - 13, Lake Buena Vista, FL
- JUN 18 — Cyber Discovery Camp 1.0, Jun 18 – 23, Baltimore, MD
- JUL 9 — Cyber Discovery Camp 2.0, Jul 9 – 14, Ruston, LA
- AUG 19 — GFIRST, Aug 19-24, Atlanta, GA
- AUG 28 — Information Assurance Exposition, August 28-30, Nashville, TN
- SEP 10 — ISC2 Security Congress, Sept 10 - 13, Philadelphia, PA
- OCT 1 — National Cyber Security Awareness Month, Oct 1 – Oct 30
- OCT 30 — NICE Workshop, Oct 30 – Nov 1, Gaithersburg, MD
- NOV 11 — CAE Principles Meeting, Nov 11 – 13, Atlanta, GA

VIEW CALENDAR
SUBMIT AN EVENT

Education Resources

Information for Students and Educators, from P-12, Undergrad to Doctoral Candidate:

- Discover Innovative Programs
- Explore Degree Programs
- Find Cyber Competitions
- Find Scholarships

Training Resources

Tools to connect Cybersecurity Professionals and Training Opportunities:

- Find Training Opportunities
- Explore the Workforce Framework
- Explore Professional Certificaitons
- Map & Submit Training Opportunities

Talent Management

Career development and HR Resources for Cyber Professionals and HR Professionals:

- Understanding Professionalization
- Explore Career Roadmaps

Research

Whitepapers, studies and other research promoting Cybersecurity education and the Profession.

- Search NICE Research
- Submit Research

I Want To..

- Become a Cyber Professional
- Advance my Cyber Career
- Explore the NICE Framework
- Search for Training Courses
- Get my child involved
- Become a NICE Partner
- Become a Training Catalog Vendor

NICE Partners

AWARENESS

Promoting Cybersecurity Safety at Work and at Play

- Awareness Home
- How-to Guide
- Cyber Glossary
- NICE Initiatives

STOP | THINK | CONNECT

Cybersecurity is a shared responsibility. For additional tips and resources for all age groups, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign.

BEST PRACTICES

View our Cyber How-To Guide to learn safe online strategies and find additional Awareness resources.

CYBER TERMS

View our interactive Cyber Glossary to learn Cybersecurity Terminology and learn about DHS' effort to standardize terms.

PROMOTING SAFETY

Learn about NICE initiatives to promote Awareness at work and at home.

National Cyber Security Awareness Month

CELEBRATE AWARENESS

October is National Cyber Security Awareness Month, see what's going on.

Why Cybersecurity Awareness?

More than ever, people rely on the Internet for everything from basic communications, to making transportation reservations, to entertainment. With each click of the mouse, citizens risk their online security if they have not taken the proper precautions to protect themselves and their Personally Identifiable Information (PII). Cybersecurity involves protecting that information by preventing, detecting, and responding to attacks.

Cybersecurity is a growing issue. Our vulnerabilities threaten the safety and livelihood of our citizens' online safety and as such, it is paramount that the government work to increase the public's awareness of cybersecurity and make them active and involved cybercitizens. Learn about ongoing initiatives to promote Awareness for all Americans.

What Can I do to Protect Myself?

While there are no sure ways to protect yourself from a cyber attack, there are some simple steps you can take to help keep your PII private.

- Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly.
- Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.
- Verify the authenticity of requests from companies or individuals by contacting them directly. If you are being asked to provide personal information via email, you can independently contact the company directly to verify this request.
- Pay close attention to website URLs. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.
- For additional tips visit STOP.THINK.CONNECT and view our HOW-TO-GUIDE.

The government has a number of resources available to the public to learn more about protecting yourself. Get more cybersecurity tips from DHS specific to email, phone, and social media among others, at [http://www.dhs.gov/files/events/cybersecurity-tips.shtm]. Get additional tips through US-CERT at [http://www.us-cert.gov/cas/tips/]

AWARENESS TIPS

Provided by US-CERT

ST11-001: Holiday Traveling with Personal Internet-Enabled Devices

Tuesday, March 20, 2012, 10:00:00 AM

The Internet is at our fingertips with the widespread use of Internet-enabled devices such as smart phones and tablets. While traveling and shopping anytime, and especially during the holidays, consider the wireless network you are using when you complete transactions on your device.

ST08-001: Understanding Hidden Threats: Rootkits and Botnets

Tuesday, March 20, 2012, 10:00:00 AM

Attackers are continually finding new ways to access computer systems. The use of hidden, methods such as rootkits and botnets has increased, and you may be a victim without even realizing it.

ST04-024: Understanding ISPs

Tuesday, March 20, 2012, 10:00:00 AM

ISPs offer services like email and internet access. In addition to availability, you may want to consider other factors so that you find an ISP that supports all of your needs.

ST06-005: Dealing with Cyberbullies

Tuesday, March 20, 2012, 10:00:00 AM

Bullies are taking advantage of technology to intimidate and harass their victims. Dealing with cyberbullying can be difficult, but there are steps you can take.

ST05-002: Keeping Children Safe Online

Tuesday, March 20, 2012, 10:00:00 AM

Children present unique security risks when they use a computer—not only do you have to keep them safe, you have to protect the data on your computer. By taking some simple steps, you can dramatically reduce the threats.

ST06-001: Using Caution with USB Drives

Tuesday, March 20, 2012, 10:00:00 AM

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks.

MORE

Increase Your Awareness

STOP.THINK.CONNECT

Stay Safe Online

National Cyber Security Awareness Month

OnGuardOnline.gov

I Want To...

- Become a Cyber Professional
- Advance my Cyber Career
- Explore the NICE Framework
- Search for Training Courses
- Get my child involved
- Become a NICE Partner
- Become a Training Catalog Vendor

NICE Partners

EDUCATION

Furthering Learning in Cybersecurity & STEM

Education Home

For Students
- Degree Programs
- Scholarship Opportunities
- Hands On Learning Activities
  - Cyber Competitions
  - Cyber Camps

For Educators

NICE Initiatives
- STEM Improvement Efforts
- Common Evidence Standards
- Promoting Education
- Curriculum Resources
- Virtual Labs

Programs
- Software Assurance
- Centers of Academic Excellence (CAE)
- Regional Cyber Centers
- I-Corps
- Scholarship for Service (SFS)
- Integrated Cybersecurity Education Communities (ICEC)
- Cyber Competitions Investigation Project (CCIP)

CLASSROOM LEARNING

Get started with Cybersecurity. Learn about the exciting programs available at every level, from grade school to graduate school.

TEACHING

Get new ideas for brining technology into the classroom, find curriculum resources and strategies for making STEM accessible.

HANDS ON EXPERIENCES

Find camps, competitions and other after-school activities that extend learning beyond the classroom.

DRIVING INNOVATION

Learn about NICE initiatives and programs underway to connect Educators, Students and Technology.

Why promote Cybersecurity & STEM Education?

Personal digital security is critical to the Nation's economy and the security of our critical infrastructure. Improving the cybersecurity posture of the nation requires requires change and education at the individual level, from grade school to graduate school and beyond. We must build a digitally literate workforce that uses technology in a secure manner. To do so, we must teach science, technology, engineering and math (STEM) and other critical subjects to all students, and educate all students on the secure use of today's evolving technologies.

It is important to have the educational resources in place to make digital literacy and personal security reality. The Department of Education and the National Science Foundation (NSF) lead the Formal Cybersecurity Education efforts for NICE. Their mission is to bolster formal cybersecurity education programs encompassing kindergarten through 12th grade, higher education and vocational programs, with a focus on the STEM disciplines to provide a pipeline of skilled workers for the private sector and government.

EDUCATION NEWS

Provided by The National Science Foundation

NSF Releases Report Detailing Substantial Growth in Graduate Enrollment in Science and Engineering in the Past Decade
Released June 1, 2012
Press Release

Colorado State University Volunteer Precipitation Network Honored with National Land-Grant Organization Award
Released May 25, 2012
News From the Field

NSF Report Details Federal Science and Engineering Support to Colleges, Universities and Nonprofit Institutions
Released May 23, 2012
Press Release

National Science Foundation Hosts Inaugural Global Summit on Merit Review
Released May 16, 2012
Press Release

Cubesats "Land" at National Science Foundation on Thursday, May 24th
Released May 11, 2012
Media Advisory

NSF Honors Two Early Career Researchers With Alan T. Waterman Award
Released May 10, 2012
Press Release

Engineering Students Using Such Design Tools as SMART Boards Are More Successful
Released May 10, 2012
News From the Field

MORE

Education Opportunities

- Centers of Academic Excellence
- Advanced Technological Education (ATE) Centers
- Regional Cyber Centers
- Integrated Cybersecurity Education Communities (ICEC)
- National Cybersecurity Education Council (NCEC)

NICS Education Partners

- Stay Safe Online
- Cyber Security Education Consortium (CSEC)
- Center for Systems Security and Information Assurance (CSSIA)
- DHS NCSD Software Assurance

I Want To...

- Become a Cyber Professional
- Advance my Cyber Career
- Explore the NICE Framework
- Search for Training Courses
- Get my child involved
- Become a NICE Partner
- Become a Training Catalog Vendor

NICE Partners

NIST

Contact Information

Peggy Maxson Margaret.Maxson@hq.dhs.gov

Find the framework @ http://www.nist.gov/nice/framework/