NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The President's Executive Order on Cybersecurity Workforce: Next Steps and How to Engage

June 5, 2017

Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

- Signed by the President on May 11, 2017
- Four Workstreams
- Thirteen Deliverables
- Range between 60-150 days

Four Workstreams

- Cybersecurity of Federal Government
- Cybersecurity of Critical Infrastructure
- Deterrence and International Cooperation
- Cybersecurity Workforce

Cybersecurity for the Nation: Policy

To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, **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.**

Workforce Development Provision

Purpose: In order to ensure that the United States maintains a long-term cybersecurity advantage . . .

Three Deliverables:

- Report to the President in 120 Days with Findings and Recommendations on Growing and Sustaining the Cybersecurity Workforce
- International Competiveness
- National Security Advantage

Deliverable #1: Public and Private Sector Workforce

- **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.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Who

The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security

Consultation with Appropriate Stakeholders

- State and Local Governments and Tribal Territories
- Academia
  - K-12 (Elementary, Middle, High)
  - Collegiate (2Y, 4Y, R, Prof)
- Training and Certification Organizations
- Non-Profit Organizations
- Private Sector Companies (Small, Medium, Large)
- Trade Associations
- International Organizations

Process for Addressing Deliverable

- Webinar
- Research Study
- Request for Information
- Workshop #1 – Synthesis of Research and RFI Responses
- Workshop #2 – Tentative Findings and Recommendations

Research Study

- Literature Review
- Scope of Effort ~ Environmental Scan
  - Domains:
    - K-12 Education
    - Postsecondary Education
    - Apprenticeships
    - Training
- Sufficiency of Effort ~ Evaluation Criteria
  - Based on Existing Metrics
  - Identification of Additional Metrics Desired

Request for Information (RFI)

- Federal Register Notice
- Deadline: 30 days after RFI is Issued
- Broad Set of Questions
  - Scope & Sufficiency of Cybersecurity Education and Training
  - Findings and Recommendations
- Comments Publicly Available
- Results Analyzed and Synthesized
- Results Shared at First Workshop

Workshop #1

- Host: Private Sector Organization
- Location: To Be Determined
- Date: Mid/Late July
- Time: 1-5 p.m.
- Format: Plenary Sessions with Speakers and Panels
- Focus: Research Study and RFI Results

Workshop #2

- Host: Academic Organization
- Location: To Be Determined
- Date: Late July/Early August
- Time: 1-5 p.m.
- Format: Plenary Sessions with Speakers and Panels
- Focus: Socializing Findings and Recommendations

Timeline

- Report Due: September 8th
- Final Draft of Report: August 9th
- Webinar #2: Early August
- Webinar #1: Late July
- RFI Closes: July TBD
- RFI Opens: June TBD
- Webinar: June 5th
- Research Study Begins: May 12th
- Executive Order Signed: May 11th

For more information:

- Website: nist.gov/nice/cybersecurityworkforce
- Email: cybersecurityworkforce@nist.gov

Question and Answer

Deliverable #2: International Competitiveness

- Review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and
- Within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review.

Who

The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence

Deliverable #3: National Security Advantage

- Assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and
- Within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out.

Who

The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence

Classification Status of Reports

The reports may be classified in full or in part, as appropriate.

Question and Answer

NICE Cybersecurity Workforce Framework – Draft NIST SP 800-181

Cybersecurity Work Categories (7)

- Specialty Areas (33) – Distinct areas of cybersecurity work;
  - Work Roles (52) – The most detailed groupings of IT, cybersecurity or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks.
    - Tasks – Specific work activities that could be assigned to a professional working in one of the NCWF's Work Roles; and,
    - Knowledge, Skills, and Abilities (KSAs) – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.

- Audience:
  - Employers
  - Current and Future Cybersecurity Workers
  - Training and Certification Providers
  - Education Providers
  - Technology Providers

- Reference Resource for cybersecurity workforce development

nist.gov/nice/framework

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cybersecurity Education and Awareness Portal

- Training Catalog
- Workforce and Development Toolkit
- Sample Curriculum
- Federal Virtual Training Environment (FedVTE)

www.niccs.us-cert.gov

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Advanced Technological Education Centers

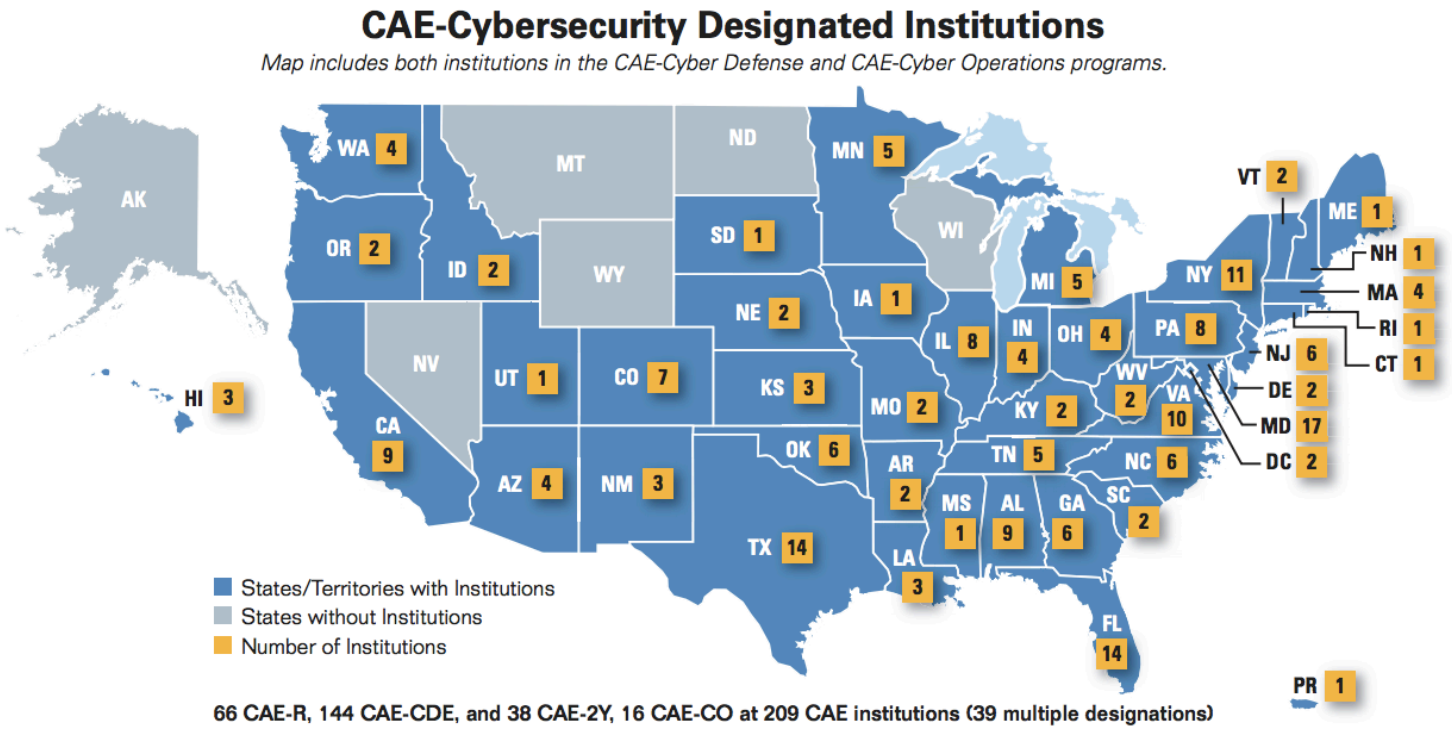
- Faculty development through online courses
- Cybersecurity Curricula
- Virtual Teaching and Learning Environment
- Simulated Environment with content aligned to industry certifications

- Sharing expertise through collaboration with industry

www.atecenters.org/st

National Centers of Academic Excellence (CAE)
in CyberSecurity

Cyber Defense: 200+ Cyber Offense: 16



www.nsa.gov/resources/educators/centers-academic-excellence

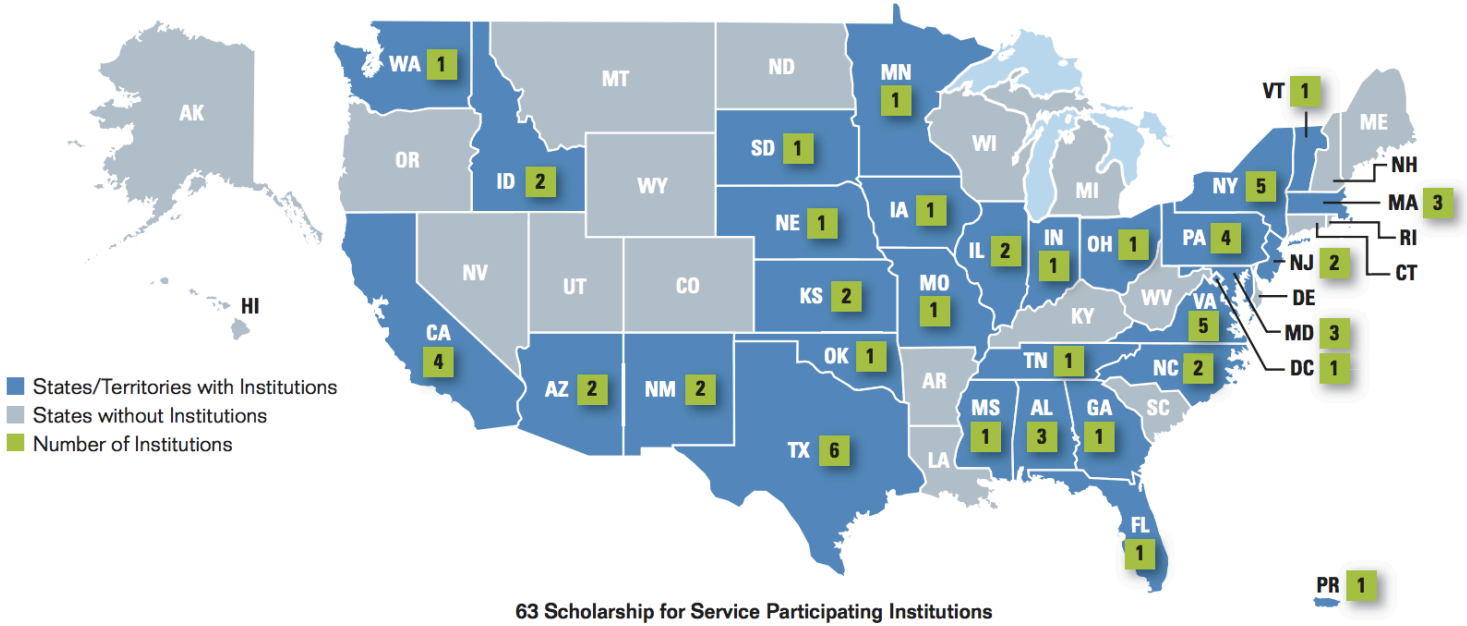
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Scholarship for Service (SFS)

- Scholarships
- Capacity Building

CyberCorps®
Defending America's Cyberspace

CyberCorps®: Scholarship for Service (SFS) Participating Institutions



63 Scholarship for Service Participating Institutions
in 29 states + District of Columbia and Commonwealth of Puerto Rico

www.sfs.opm.gov

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

GenCyber

www.gen-cyber.com

NICE Engagement

Inform

NICE Working Groups and Interagency council

Quarterly e-Newsletter

Events:

- Monthly Webinars
- NICE Conference & Expo – Nov. 7-8 in Dayton, OH
- NICE K-12 Cybersecurity Education Conference – Dec. 4-5 in Nashville, TN

Influence

NICE Workforce Framework

Cybersecurity Jobs Heat Map

RAMPS Federal Funding Opportunity

Innovate

NICE Challenge Project

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

nist.gov/nice

Join the NICE Working Group

- K 12
- Collegiate
- Competitions
- Training and Certifications
- Workforce Management

nist.gov/nice/nicewg

Participate in our events

- NICE Conference and Expo
- NICE K-12 Cybersecurity Education Conference
- NICE Webinars

Subscribe to the NICE eNewsletter

Featured Article

Using an Apprenticeship Model to Meet Industry Needs for Secure Software Development

by Julie Howar, Illinois Central College; Nancy Mead, Software Engineering Institute, Carnegie Mellon University; and Girish Seshagiri, Ishpi Information Technologies, Inc.

In many countries, including the U.S., there is a growing "skills gap" between the kinds of jobs offered and the skills qualifications of job seekers, resulting in adverse consequences to employers and job seekers alike. The German apprenticeship dual model has successfully helped match jobs and skills in several European countries. The dual model is structured such that time spent in a vocational school for theoretical training is complemented by simultaneous practical training and experience at a partnering company. The apprentices receive a salary as they gain work-related skills. There is growing evidence that the U.S. could reap substantial benefits from this model. Read More

Key Dates

Community College Cyber Summit
July 22-24, 2016

Information Assurance Symposium
August 16-18, 2016

National K-12 Cybersecurity Education Conference
October 6-7, 2016

more dates

NICE SPOTLIGHT ON

Academia

20 Years of CISSE: Past, Present, Future

by Vic Maconachy, Vice President for Academic Affairs, Capitol Technology University and CISSE President, and Dan Shoemaker, Professor and Graduate Program Director, University of Detroit Mercy Center for Cyber Security and Intelligence Studies, CISSE Treasurer

The Colloquium for Information Systems Security Education (CISSE) turns 20 this year. Given how ubiquitous computers have become, it is probably hard to recall what things were like when CISSE was formed. In 1996, anything called "the cloud" was in the sky, "big data" and "mobile security" still lay in the domain of science fiction. Read More

Industry

Talent Pipeline Management

by Carrie Samson, Manager of Programs, U.S. Chamber of Commerce Foundation Center for Education and Workforce

As the demand for talent continues to rise, 12 IT companies in Northern Virginia joined forces to tackle this challenge like never before using a new strategy called Talent Management Pipeline (TPM) to create demand-driven solutions. Read More

nist.gov/nice/enewsletter

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Question and Answer