

# NICE Webinar Series

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



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**.

## 2008 CNCI (Continued)

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.**

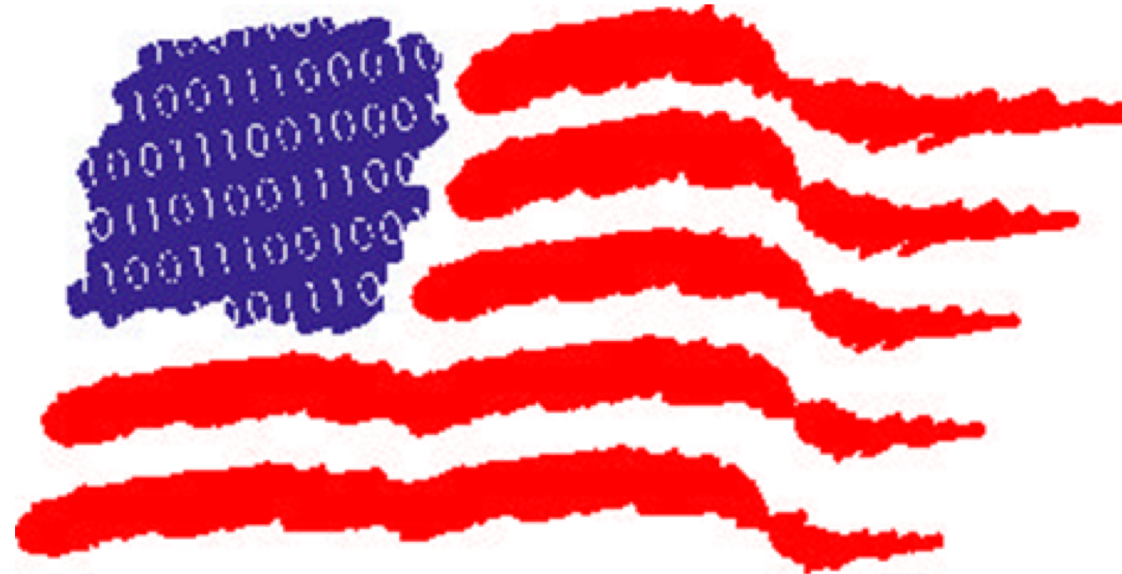
## 2017: Executive Order 13800 (Continued)

- **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<sup>®</sup> Scholarship For Service (SFS)



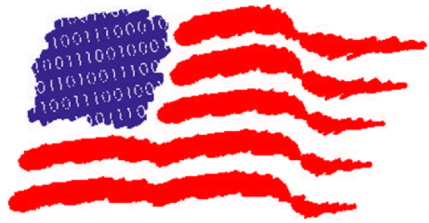
## '90s bombings

- 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**
- Presidential Decision Directive 63, May 1998
  - 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.)



# CyberCorps®: Scholarship for Service (SFS)

## 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](https://SFS.opm.gov)



# CyberCorps® (SFS) Students and Placements

## Top 15 Student Enrollments, 2011-2015

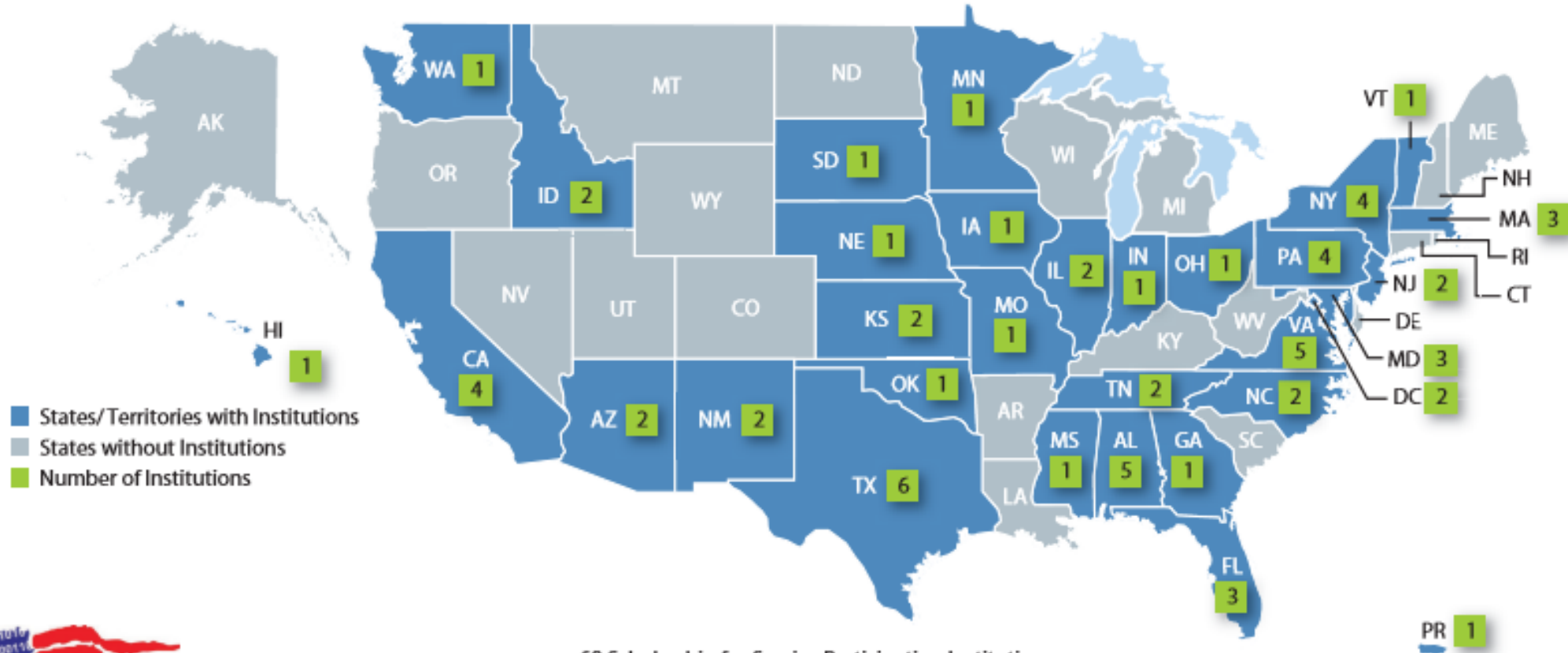
U of Tulsa (OK)	82
Carnegie Mellon U (PA)	63
Mississippi State U (MS)	48
Naval Postgraduate School (CA)	47
Cal State San Bernardino (CA)	45
Dakota State U (SD)	44
New York U (NY)	39
U of North Carolina at Charlotte (NC)	37
Northeastern U (MA)	36
U of Ill. at Urbana-Champaign (IL)	36
North Carolina A&T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

## Top 15 Placements of Graduates, 2011-15

National Security Agency	79
MITRE Corporation	44
US Navy	38
State, Local, Tribal	37
Federal Reserve System	32
US Army	28
Department of Homeland Security	26
Department of Justice	20
Johns Hopkins U Applied Physics Lab	20
Sandia National Laboratories	19
MIT Lincoln Laboratory	17
CMU Software Engineering Institute	15
US Air Force	11
Central Intelligence Agency	10
Pacific Northwest Laboratory	8



# 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](https://www.sfs.opm.gov) or contact: [sfs@opm.gov](mailto:sfs@opm.gov)



# National Capacity - GenCyber

GenCyber

HOME / CAMP MAP / CAMP LIST / ABOUT / FAQ

INSPIRING THE NEXT  
GENERATION OF  
CYBER STARS

ABOUT GENCYBER

2015 CAMP MAP

2015 CAMP LIST

FAQ

USER LOGIN

# Capacity Building - WiCyS





# Cybersecurity Enhancement Act of 2014



# 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.**



# Cybersecurity Enhancement Act of 2014

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](#)

# COMMUNITY COLLEGE CYBER PILOT PROGRAM AND ASSESSMENT

**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.



# COMMUNITY COLLEGE CYBER PILOT PROGRAM AND ASSESSMENT

**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.



# FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM UPDATES

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**;



# FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM UPDATES

(...) **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.





# Contact Information


Dr. Victor Piotrowski  
Lead Program Director  
National Science Foundation  
[vpotrow@nsf.gov](mailto:vpotrow@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=504991)  
[https://www.nsf.gov/funding/pgm\\_summ.jsp?pims\\_id=504709](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

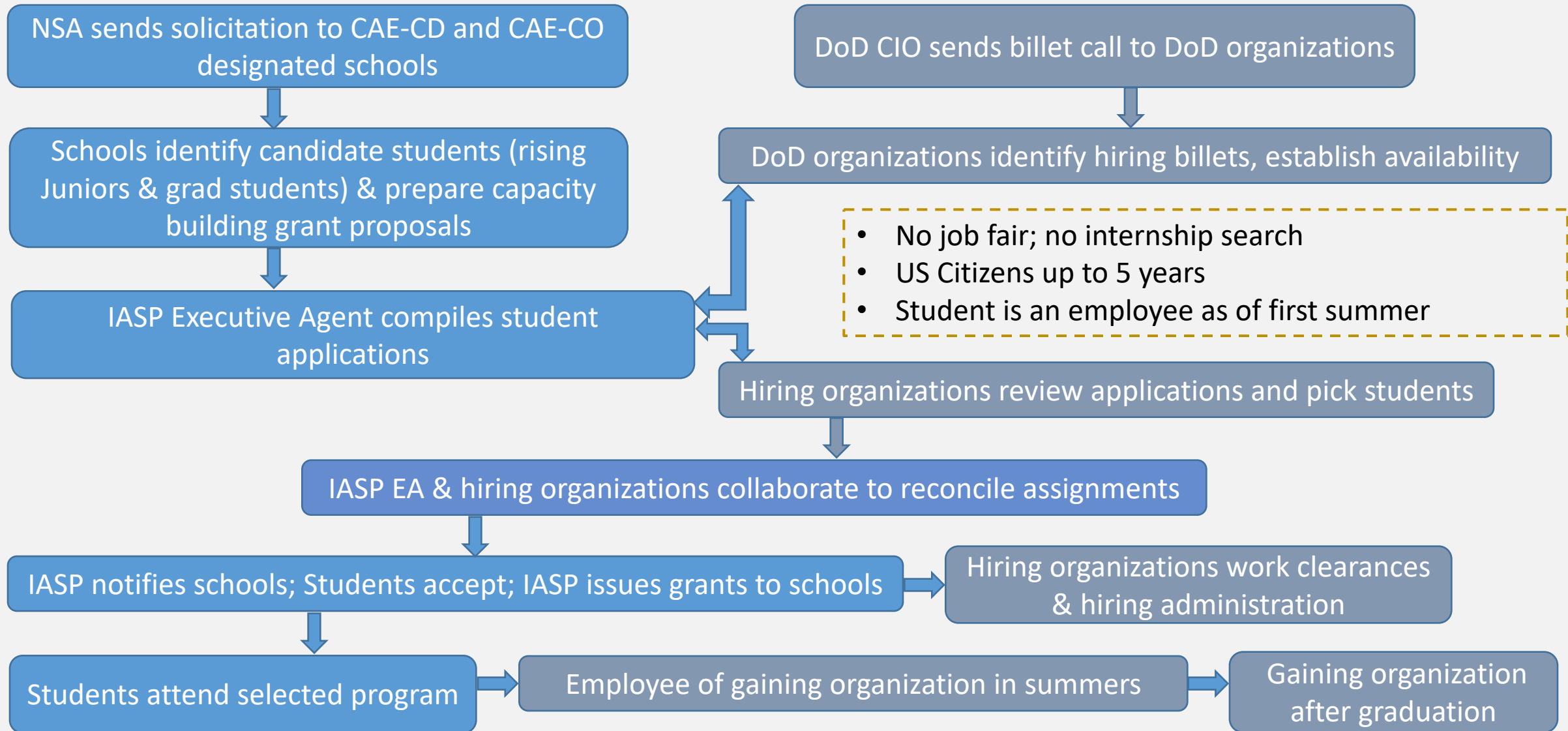
# CAE-C and IASP

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

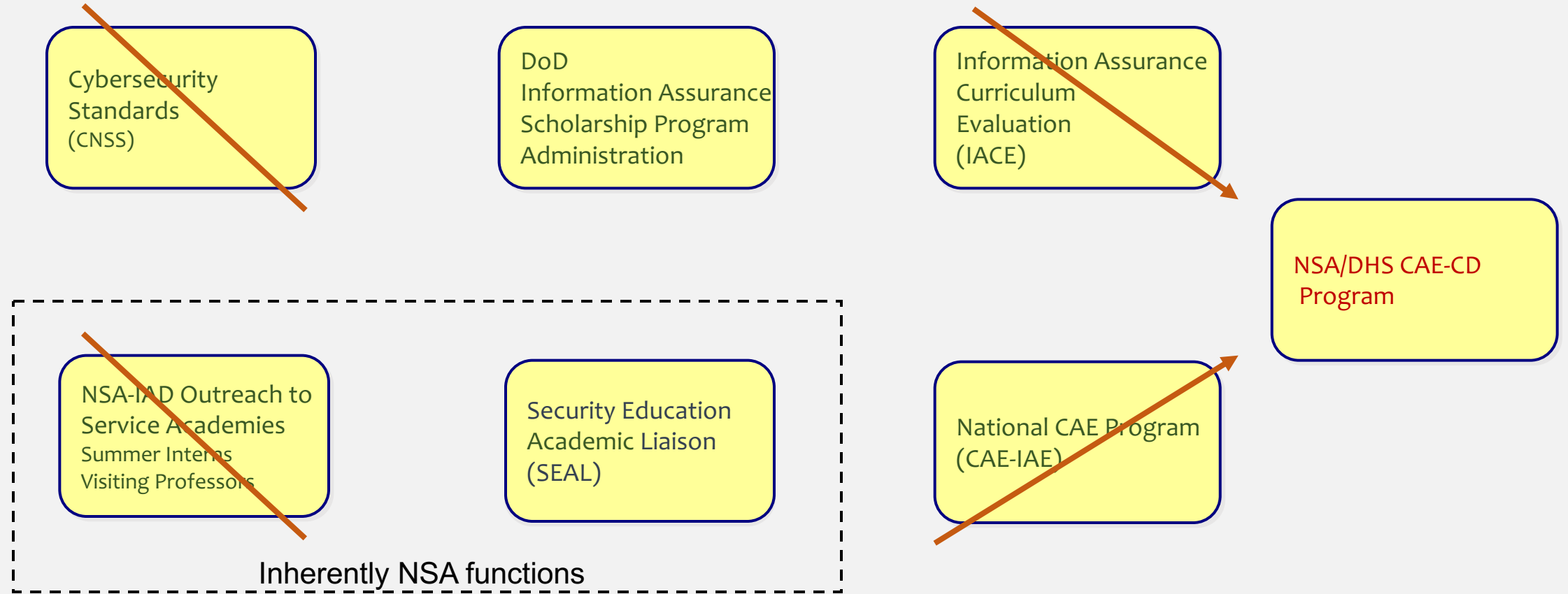
The goal of the CAE-CD program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in CD and producing a growing number of professionals with cyber defense expertise.

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

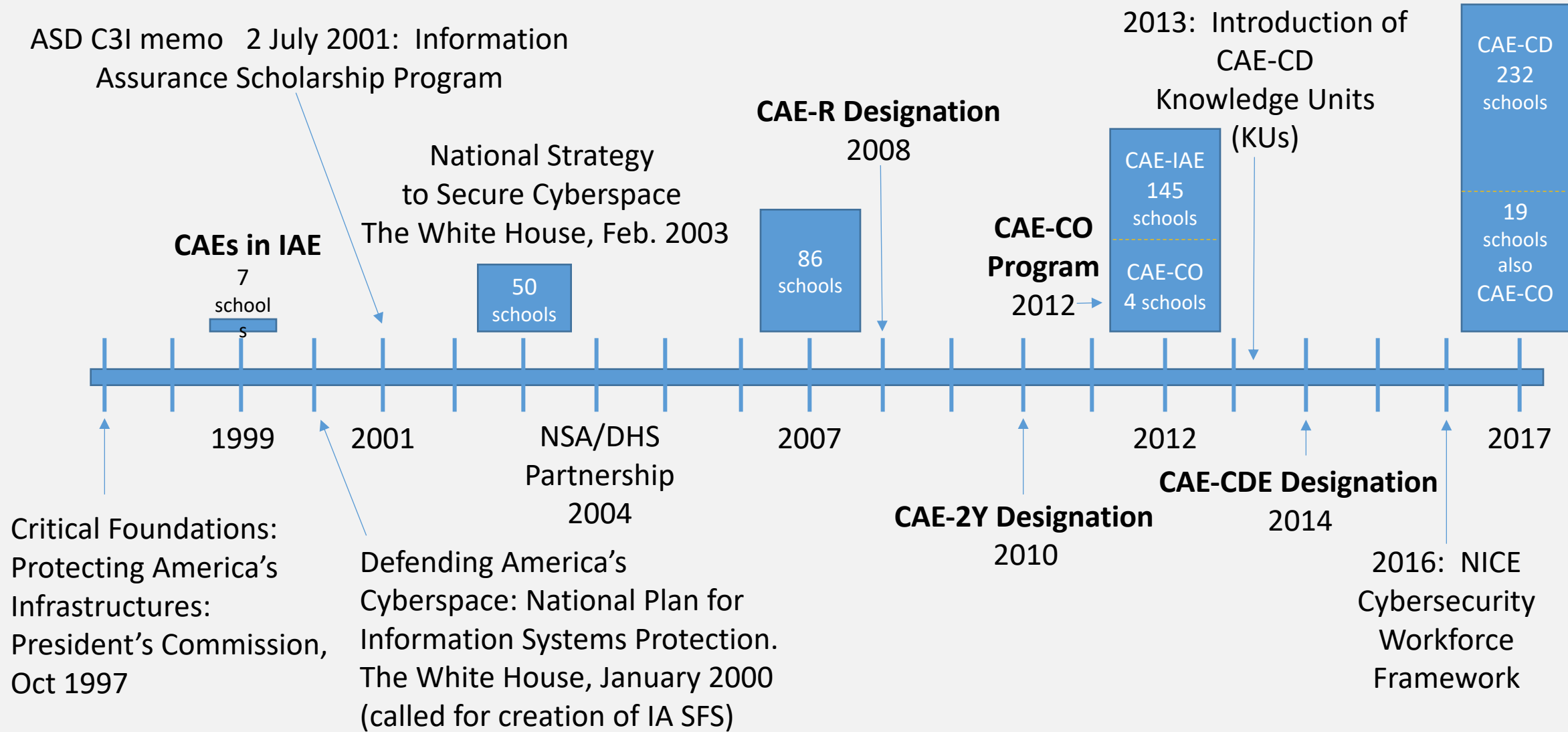
# IASP Process



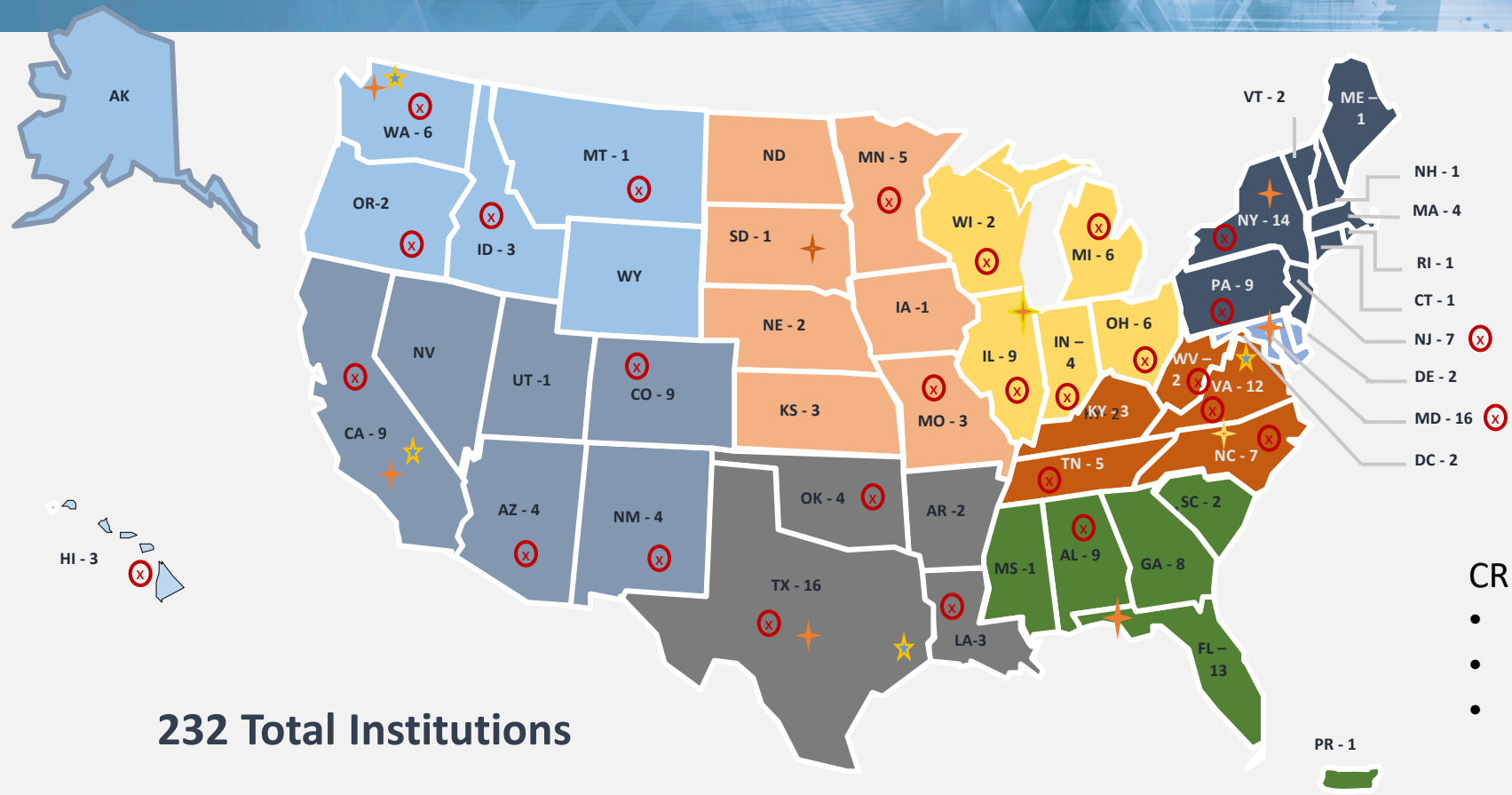
## National Information (Assurance) Education & Training Program



# CAE in Cyber Defense



# New Paradigm 2017



**Legend:**  
 State - # of CAEs as of November 2017  
 States with designated Community Colleges (X)

- CRRCs:**
- Build regional community
  - Provide Faculty Professional Development
  - Assist Candidate Institutions

**232 Total Institutions**

★ 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)

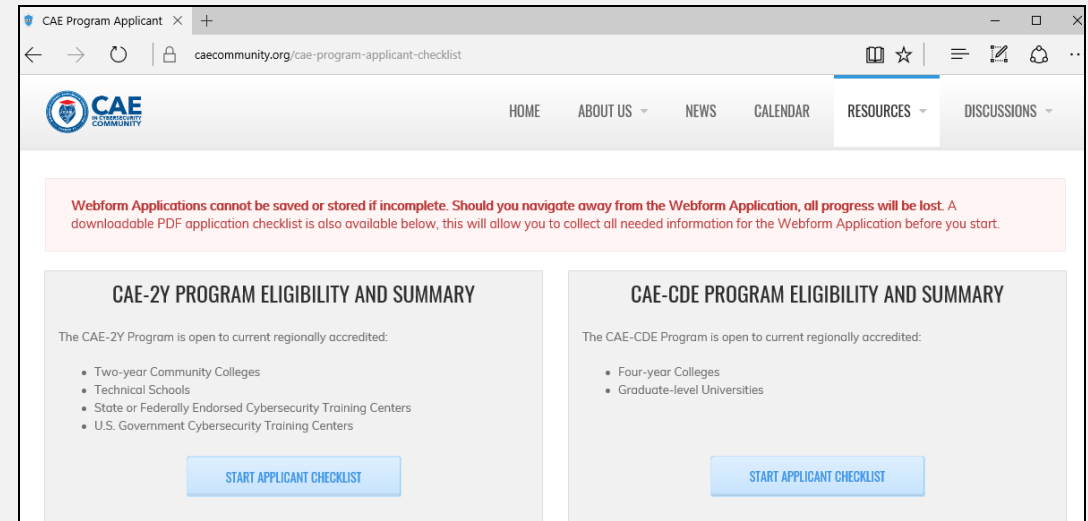
★ CAE Regional Resource Centers (CRRCs)	
North Western Region – University of Washington (WA)	North Eastern Region - Mohawk Valley Community College (NY) and Northeast University (MA)
South Western Region - Coastline Community College (CA)	National Capital Region - Prince Georges Community College (MD)
South Central Region - San Antonio College (TX)	East Central Region - Forsyth Tech Community College (NC)
North Central Region - Dakota State University (SD)	Southeast Region - University of West Florida (FL)
Mid-Western Region - Moraine Valley Community College (IL)	



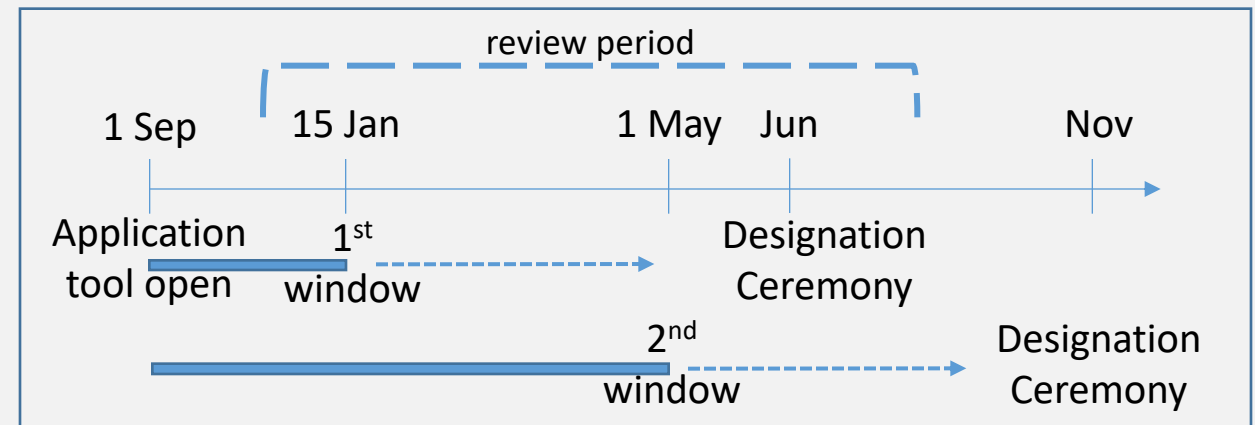
# CAE-CD Candidates Program

<https://www.caecommunity.org/cae-program-applicant-checklist>

- 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



# CAE Designation Requirements

## Curriculum

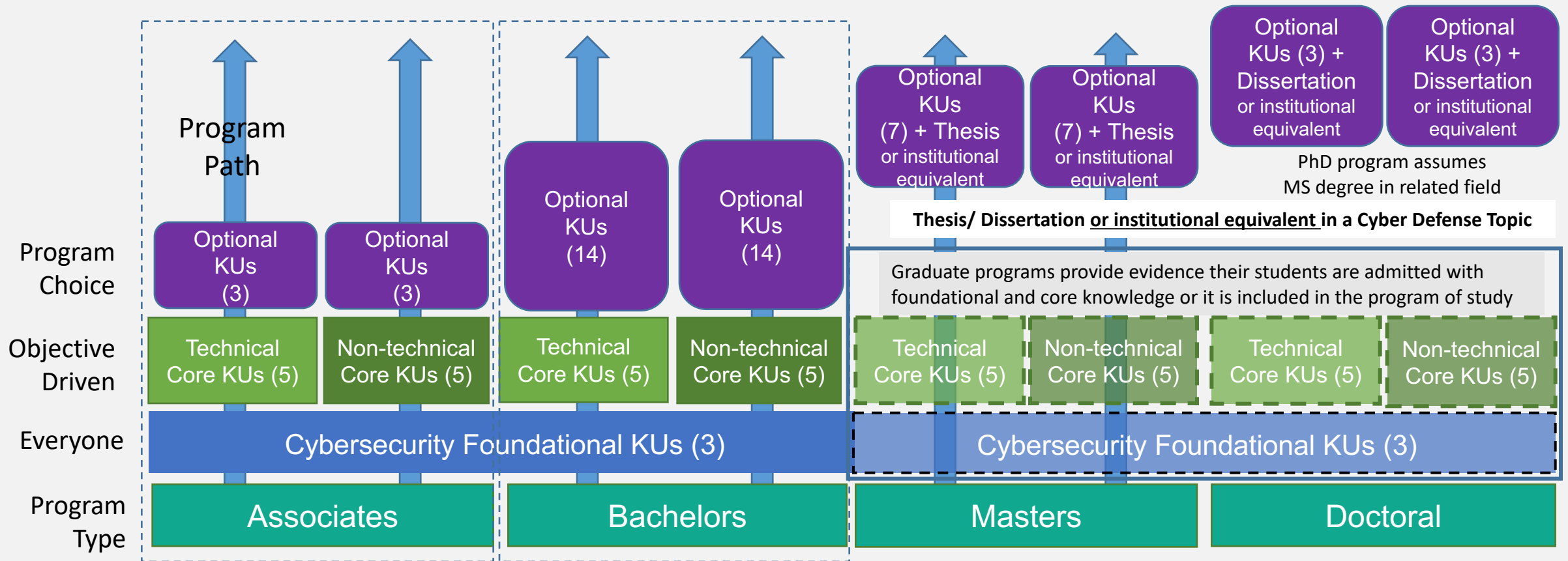
Mapped to Knowledge Units  
Student Path and Recognition  
Faculty Qualifications  
Program Maturity  
Interdisciplinary  
Focus Areas

## 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)

# CAE-CDE Designation Requirements

Effective 2019 Application Cycle (1 Oct 2018 – 1 May 2019)



## Knowledge Units (KUs)

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

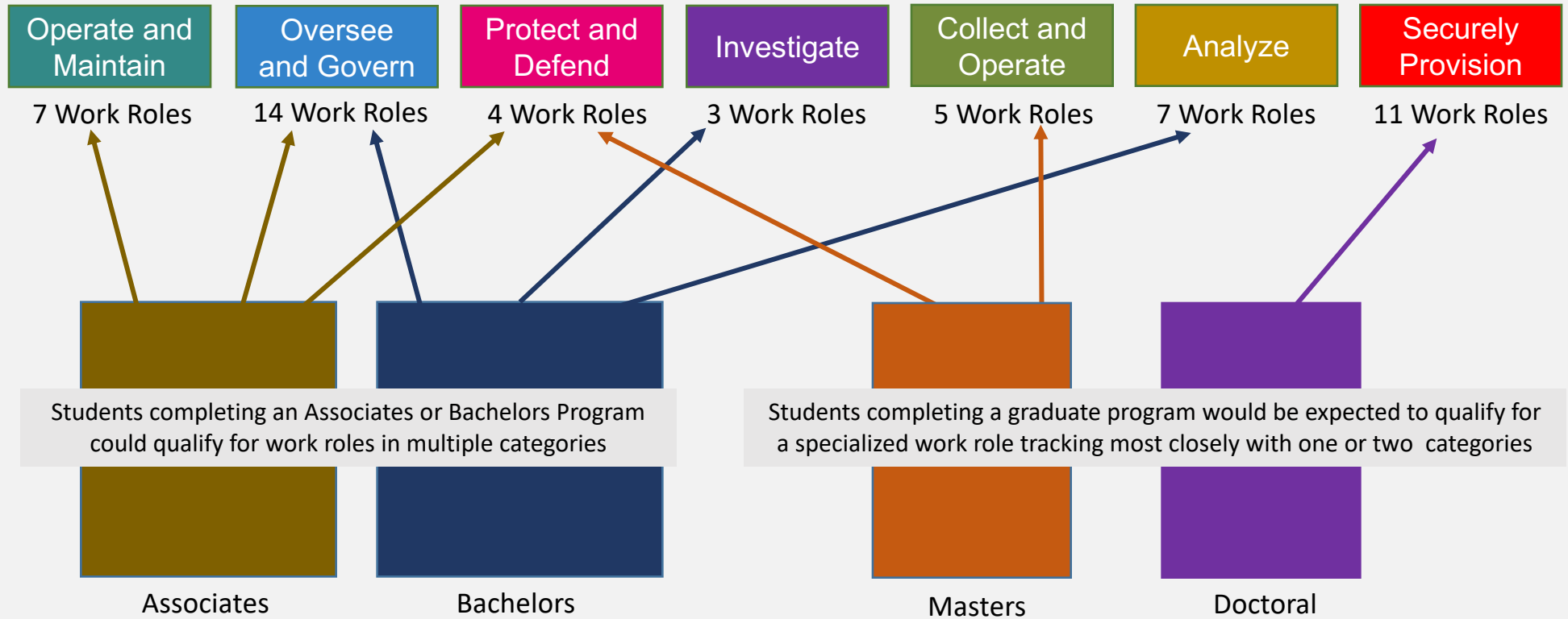
**Technical Core:** Basic Scripting and Programming; Basic Networking; Network Defense; Basic Cryptography; Operating Systems Concepts

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

# CAEs & the NICE Framework

Careers  
Cybersecurity Skills  
Workforce Learning

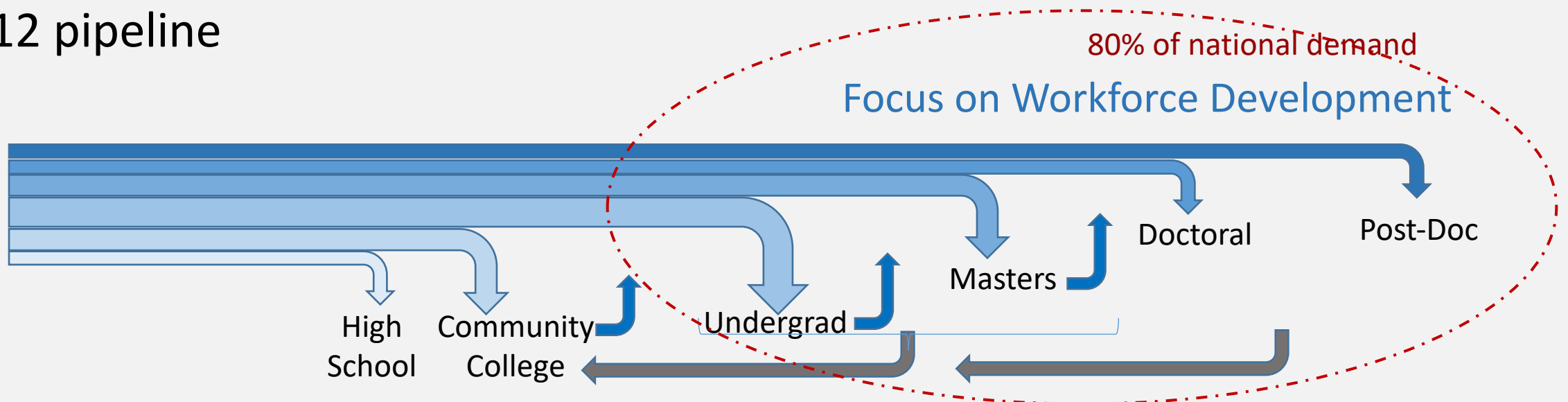
**NICE Framework**  
NIST SP 800-181:  
Categories



- 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



# Contact Information

Lynne Clark, Chief, National CAE-CD Program

410-854-6206

askCAEIAE@nsa.gov

CAE-CD <https://www.iad.gov/NIETP/>

CAE-CD & 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](https://public.govdelivery.com/accounts/USNIST/subscriber/topics?qsp=USNIST_3)

[nist.gov/nice/webinars](https://nist.gov/nice/webinars)