NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY REQUEST FOR INFORMATION:
STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE: WORKFORCE DEVELOPMENT

A COLLABORATIVE RESPONSE FROM THE NSA/DHS NATIONAL CENTER OF ACADEMIC EXCELLENCE (CAE) NATIONAL RESOURCE CENTERS (CNRCs) AND CAE REGIONAL RESOURCE CENTERS (CRRCs)

CONTRIBUTING AUTHORS:

DR. AGNES CHAN, NORTHEASTERN UNIVERSITY

DR. EMAN EL-SHEIKH, UNIVERSITY OF WEST FLORIDA

DR. FRED KLAPPENBERGER, NATIONAL CYBERWATCH CENTER

DR. MARGARET LEARY, NORTHERN VIRGINIA COMMUNITY COLLEGE

CORRINNE SANDE, WHATCOM COMMUNITY COLLEGE

DR. JOHN SANDS, MORAINE VALLEY COMMUNITY COLLEGE

DR. DEANNE WESLEY, FORSYTH TECHNICAL COMMUNITY COLLEGE

MORGAN ZANTUA, UNIVERSITY OF WASHINGTON

DR. WAYNE LEWIS, UNIVERSITY OF HAWAII

CONTENTS

I. INTRODUCTION 3

II. COLLABORATIVE CNRC/CRRC RESPONSE TO NIST RFI QUESTIONS 10

Question 1 10

Question 2 13

Question 3 14

Question 4 14

Question 5 16

Question 6 19

Question 7 21

Question 8 22

III. CONCLUSIONS 24

IV. REFERENCES 25

I. INTRODUCTION

Cybersecurity Workforce Development Needs and Context

This introduction provides context for the collaborative CNRC/CRRC response to the request for information on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development* put forth by the National Institute of Standards and Technology (NIST).

The cybersecurity workforce gap is growing and projected to reach 1.8 million by 2022, according to a 2017 Global Information Security Workforce Study (GISWS) sponsored by BAH, (ISC)2, and the Center for Cyber Safety and Education. Over 19,000 information security professionals were surveyed for the study. Part of the survey focused on employment perspectives and priorities of Millennials. A key finding was that organizational training, mentoring, and leadership programs are the primary factors determining the career choices of Millennials. To address labor market demand and generational considerations, two recent growth trends need to accelerate:

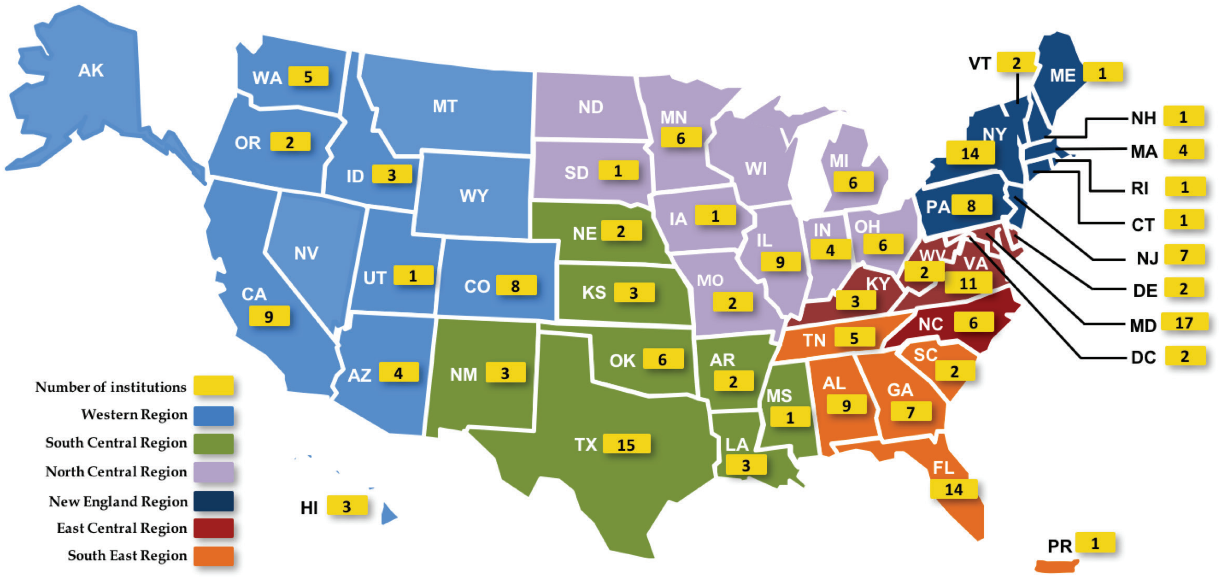
(1) The expansion in the number and variety of postsecondary cybersecurity education degree programs.
(2) The scale and depth of integration of partnerships between colleges/ universities and business/industry.

A rough estimate based on the stated 2022 projections is that our national effort must translate to 400,000 cybersecurity-trained individuals added to the workforce per year over the next five years.

National Security Agency (NSA) / Department of Homeland Security (DHS) National Centers of Academic Excellence (CAE) Program

The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Center of Academic Excellence in Cyber Defense (CAE-CD) [www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/] and Center for Academic Excellence in Cyber Operations (CAE-CO) [www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/] programs.

These programs set the national standards and guidelines for excellence in cybersecurity education, training, and workforce development. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cybersecurity and producing a growing



70 CAE-R, 142 CAE-CDE, and 51 CAE-2Y, 19 CAE-CO at **226 CAE institutions** (many hold multiple designations)
in 45 states + District of Columbia and Commonwealth of Puerto Rico
https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

number of professionals with needed cybersecurity expertise. The impact on Information Communications Technology (ICT) education has been profound, and is reflected by the integral role that cybersecurity now plays in STEM and ICT education. Six incarnations of the CAE program have launched, beginning in 1998 with the inaugural Information Assurance Education (CAE-IAE) program. In the second iteration of the CAE program, DHS joined forces with NSA in 2004 to scale the CAE program. This prudent joining of forces served as a wake-up call, so to speak, to higher education regarding the growing commitment necessary to address the unique dynamic challenges presented by a global information and communication neural network. Analogous to how security professionals model best practices in order to prevent rogue network access, the NSA and DHS continue to present new challenges and opportunities to higher education institutions.

Each CAE designated institution is guaranteed to have at least one exceptional cybersecurity education leader on campus, serving as a liaison to federal agencies and collaborating at a regional or national level with ‘leads’ from other colleges and universities. For these cybersecurity leads, transport through time along the arc of technology is internalized, in a sense, as predictive analytics tuned to chart educational trajectories which optimize opportunities for ICT students. These educators work with an established network of colleagues, carefully avoiding pedagogical black holes as they coordinate the design, development, and implementation of rigorous programs of study aligned to the labor market.

The workflow of a cybersecurity educator is bound to the goals of increasing enrollment in ICT programs, improving graduation rates, and teaching the knowledge and skills necessary for graduates to find jobs and excel as security professionals.

NSA/DHS added CAE in IA Research as an institutional option in 2008 to encourage universities and students to pursue graduate and postdoctoral research in cybersecurity; the timing was good because academia had finally got around to facing the security considerations related to the rapid adoption of Internet-based collaboration tools enabled by converged media. In 2010, the CAE-2Y program was launched to provide two-year institutions, technical schools, and government training centers the opportunity to transform institutional programs and policies to better prepare students for careers in cybersecurity. The CAE-2Y program effected a dramatic increase in cybersecurity education enrollments and degrees earned, marking an inflection point in the national response to the cybersecurity workforce shortage. The emphasis in CAE-2Y on providing a pipeline to four-year degree programs was key to the success of the program.

2016 saw the penultimate incarnation of the CAE program. NSA established a network of CAE-Cyber Defense (CAE-CD) Regional Centers to advance cybersecurity education and workforce development across the nation. The Regional Centers are charged with leading efforts to advance cybersecurity education, creating strong regional cybersecurity communities, providing support to current and candidate CAE institutions, and enhancing the cybersecurity knowledge and skills of the faculty at the newly designated institutions, with the expectation to foster collaboration in order to advance cybersecurity education, training, and research. Since the program was launched, the success rate for institutions applying for CAE designation has increased from 42% to 92%, with a proportional gain amongst higher education institutions offering CAE designated programs which meet national curricular guidelines.

NSA/DHS CAE Regional Resource Centers (CRRCs) and CAE National Resource Centers (CNRCs)

In April 2017, a new hierarchy of CAE-Cyber Defense (CAE-CD) Resource Centers was introduced, coinciding with the announcement of fourteen Resource Centers. [www.caecommunity.org/news/announcing-14-new-cae-cyber-defense-resource-centers] The CAE Resource Centers are a network of participating CAE-CD institutions that provide resource and guidance to applicant institutions. Three categories of resource centers are positioned to assist at a regional and national level – Hub, Consultation, and National.

Hub CAE Regional Resource Centers (CRRCs) act as a hub for institutions within the CAE-CD Candidate Program in a particular geographic region. They support current and candidate CAE institutions, facilitate educational and research collaboratons among CAE institutions and host a variety of program and faculty professional development workshops, seminars, and courses for designated and candidate institutions.

Hub CRRCs:

Central Eastern Region - Forsyth Technical Community College
New England Region - Mohawk Valley Community College
North Central Region - Moraine Valley Community College
South Central Region - San Antonio College
South Eastern Region - University of West Florida
Western Region - Coastline Community College

Consultation CRRCs collaborate with Hub CRRCs to ensure any unique higher education requirements for university degree programs and applicants are addressed.

Consultation CRRCs:

Dakota State University
Northeastern University
University of Houston
University of Washington

CAE National Resource Centers (CNRCs) provide expert assistance and leadership to the CAE-CD Candidate Program and CAE Community in the areas of peer reviewing, program development, and mentoring.

National Resource Centers:

California State University, San Bernardino - CAE Community
Northern Virginia Community College - Peer Review
Prince George's Community College - Program Development
Whatcom Community College - Mentoring

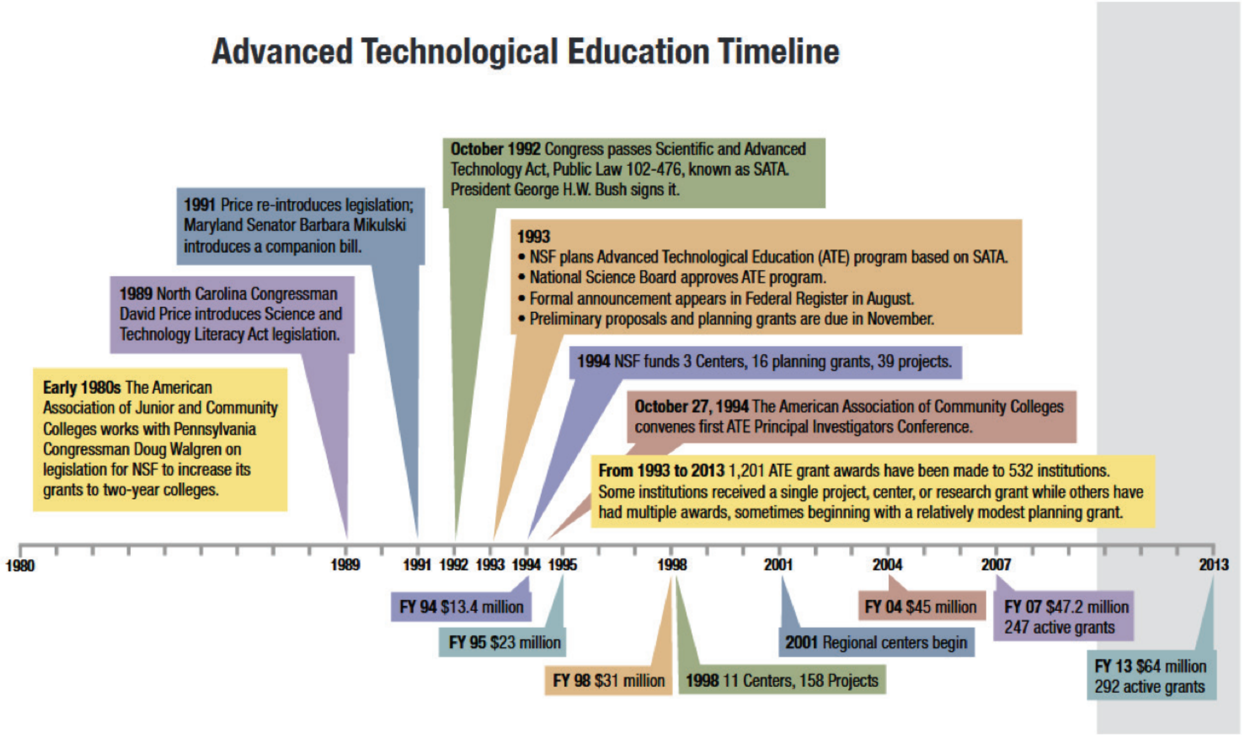
**NOTE: These designations and roles will continue to evolve based on emerging needs and academic institutions willingness to take on responsibilities.*

The 2017 introduction of the CAE Resource Centers, including four National Centers, was the latest iteration of the NSA/DHS program, and surely will not be the last. The size and quality of the national cybersecurity workforce is moving in the right direction as a direct result of the leadership of the NSA and

DHS, raising the bar in postsecondary cybersecurity education by way of the CAE Programs. The influence of the CAE program on cybersecurity education continues to grow and U.S. cybersecurity education is guided by the principles circumscribing CAE designation.

National Science Foundation (NSF) Advanced Technological Education (ATE)

The *National Science Foundation (NSF)* is a federal agency which is key to the success effort to scale the cybersecurity workforce. The NSF *Advanced Technological Education (ATE)* program has been front-and-center in this effort. The first round of ATE grants were awarded in 1994, long before cybersecurity programs existed in community colleges.


Advanced Technological Education Timeline

Early 1980s The American Association of Junior and Community Colleges works with Pennsylvania Congressman Doug Walgren on legislation for NSF to increase its grants to two-year colleges.

1989 North Carolina Congressman David Price introduces Science and Technology Literacy Act legislation.

1991 Price re-introduces legislation; Maryland Senator Barbara Mikulski introduces a companion bill.

October 1992 Congress passes Scientific and Advanced Technology Act, Public Law 102-476, known as SATA. President George H.W. Bush signs it.

1993
- NSF plans Advanced Technological Education (ATE) program based on SATA.
- National Science Board approves ATE program.
- Formal announcement appears in Federal Register in August.
- Preliminary proposals and planning grants are due in November.

1994 NSF funds 3 Centers, 16 planning grants, 39 projects.

October 27, 1994 The American Association of Community Colleges convenes first ATE Principal Investigators Conference.

From 1993 to 2013 1,201 ATE grant awards have been made to 532 institutions. Some institutions received a single project, center, or research grant while others have had multiple awards, sometimes beginning with a relatively modest planning grant.

FY 94 $13.4 million

FY 95 $23 million

FY 98 $31 million

1998 11 Centers, 158 Projects

2001 Regional centers begin

FY 04 $45 million

FY 07 $47.2 million 247 active grants

FY 13 $64 million 292 active grants

NSF manages, in addition to the ATE program, several important grant programs that build capacity in cybersecurity, coding, and STEM education. For example, the Scholarship for Service (SFS) program provides scholarships for students enrolling in cybersecurity and cyber intelligence programs. This introduction focuses on the unique role and success of the ATE program.

NSF established three ATE Centers to lead the development and dissemination effort in cybersecurity education:

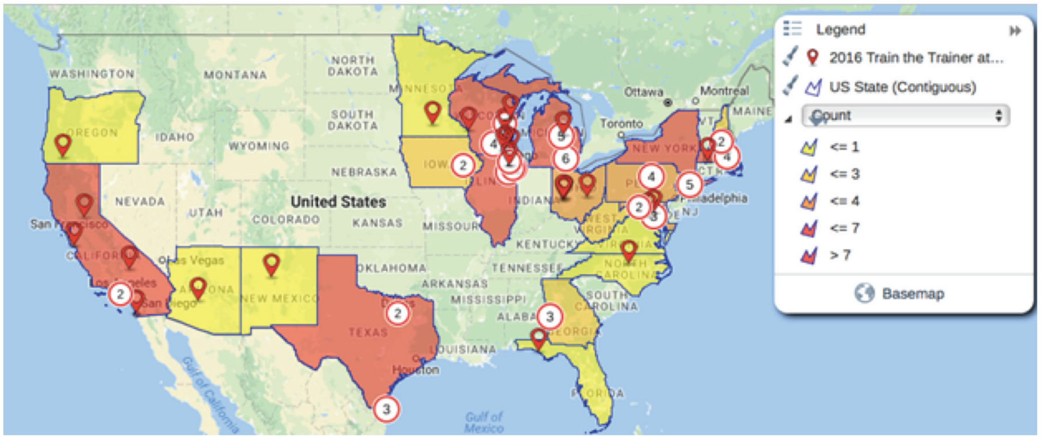
- **CyberWatch Center**
  Prince George's Community College; Largo, MD

- **Center for System Security and Information Assurance (CSSIA)**
  Moraine Valley Community College; Chicago, IL
- **CyberWatch West**
  Whatcom Community College; Bellingham, WA.

The ATE Centers serve as expert resources and provide professional development to ensure that college cybersecurity and information assurance programs meet government and industry standards. The ATE Centers provide similar services; for example, all ATE Centers host online repositories for educators to access up-to-date resources, such as labs and presentation materials. In addition, each ATE Center focuses on a few specialty areas. Colleges across the country depend on ATE Centers for training and resources. The training and resources enable faculty to adequately prepare the nation's technicians with the hands-on skills necessary to work on the front lines of defending the country's computer networks and IT infrastructure. Note that the modality for ICT teacher training has evolved along with technology, from in-person training, to hybrid models, and now to synchronous distance education. ATE Center staff often find themselves setting an example at their respective college or university regarding the professional use of emerging technologies in their effort to effectively deliver services to partner institutions.

NSF ATE grant program solicitations require applicants to work with local K-12 educational institutions in meeting the objectives set out for the project or center. It is therefore common for NSF ATE sites to also model best practices in the geographic vicinity in terms of their active engagement with area high schools. High school academies, career clusters, programs of study, and early college options are almost always carried out in alignment with local colleges. In this way, the NSF ATE program has a definitively positive impact on interagency collaboration, articulation programs, dual credit programs, and K-12 digital literacy in the geographic region.

This narrative is intended as overview of undergraduate cybersecurity technical education, so this is not the place to delve into the specifics of exemplary educational institutions. However, it does succinctly serve the purpose of this effort to illustrate what success looks like with one ATE Center that has been a national leader since 2003 in cybersecurity education: the *Center for System Security and Information Assurance (CSSIA)* based at Moraine Valley Community College in Chicago. CSSIA has earned a reputation for its stellar faculty professional development record, having trained thousands of cybersecurity educators over the years:



In its effort to scale its ICT teacher training system, CSSIA built a Virtualization Data Center (VDC). The VDC provides students and instructors 24/7/365 access to perform labs in ethical hacking, digital forensics, security scripting, A+, Network+, Linux+, Security+, Cisco, Palo Alto Networks, Juniper, VMware, EMC, Red Hat Linux, and Windows 10. The VDC also serves as a platform for regional and national cybersecurity competitions, such as the Collegiate Cyber Defense Competition (CCDC). Because of the complex nature of remote lab environments and the demand for students to participate in cybersecurity competitions, CSSIA has become a national resource for colleges either deploying remote lab environments or requiring access to a remote lab environment. Finally, CSSIA has led the ICT technical curriculum development effort over the years, as a natural augmentation to its remote lab environment services; CSSIA subject matter experts have authored hundreds of original labs used by colleges nationwide for their remote lab systems.

Lastly, it needs to be emphasized that CAE and ATE sites are proactive about partnering with various branches of the U.S. military, especially when it relates to helping to prepare veterans for careers in cybersecurity.

Acknowledgement of contributing authors:

- Dr. Agnes Chan, Northeastern University
- Dr. Eman El-Sheikh, University of West Florida
- Dr. Fred Klappenberger, National CyberWatch Center
- Dr. Margaret Leary, Northern Virginia Community College
- Corrinne Sande, Whatcom Community College
- Dr. John Sands, Moraine Valley Community College
- Dr. Deanne Wesley, Forsyth Technical Community College
- Morgan Zantua, University of Washington
- Dr. Wayne Lewis, University of Hawaii

II. COLLABORATIVE CNRC/CRRC RESPONSE TO NIST RFI QUESTIONS

The following represents the collaborative CNRC/CRRC response to the NIST Request for information on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development.

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, dz organization, and sharing of information about cybersecurity education, training, and workforce development programs?

Two-hundred and twenty-six educational institutions have earned the NSA/DHS CAE designation. There are CAE institutions in 45 states, Washington, D.C., and Puerto Rico. CAEs are academic institutions and programs which have undergone an in-depth assessment and have met the rigorous requirements to be designated a Center of Academic Excellence. Designation is valid for five academic years, after which the school must successfully reapply in order to retain its designation. Students attending CAE designated institutions are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program. Students attending CAE designated institutions are also eligible to apply for the Federal Cyber Service Scholarship for Service Program. Students who complete the approved program of study receive explicit recognition for their portfolio. CAE institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role supporting our Nation's information systems.

There is a pressing need to standardize terms – for instance the Bureau of Labor Statistics does not have any occupations with the term "cyber" in the title. Need to establish an SOC (standard occupational classification) code from the Department of Labor to track employment outlook.

The Bureau of Labor Statistics (BLS) needs to more closely examine the degree requirements associated with different occupations, as they specify requiring a Bachelor's degree to be a Network Administrator. When a close examination is performed of the tasks that they associate with this role, they do not differentiate between what would be entry-level (Junior Administrator) versus more senior-level administrators. This does not allow for job growth and results in many of these positions remaining unfilled as many individuals who graduate with 4-year degrees are no longer interested in filling what are perceived to be more technician-based roles.

Community colleges have a difficult time gathering information on where students are working or transferring (into a senior institution, for example), once they leave. Having access to state tax filings by employers would help to some extent; however, this still would not allow us to track whether or not the student is working in the field. Without this data, we cannot state if our program has successfully met its goals.

- Employment security data is broken down by state and county, but doesn't include the term cyber.
- Need to reclassify state job descriptions and private sector descriptions to align to the NICE Framework.
- Additional job classifications for cybersecurity jobs listed in NIST 800-818 do not have corresponding job titles in BLS https://www.bls.gov/ooh/ and O*NET online https://www.onetonline.org

A variety of organizations publish reports that include data, metrics and recommendations on cybersecurity education, training and workforce development. The Partnership for Public Service and Booz Allen Hamilton published Cyber In-Security: Strengthening the Federal Cybersecurity Workforce (2009) and Cyber In-Security II: Closing the Federal Talent Gap (2015) identified findings and recommendations for attracting and retaining cybersecurity talent in the federal government. (ISC)2 in partnership with Booz Allen Hamilton published bi-annual reports on information security, including the most recent 2017 (ISC)2 Global Information Security Workforce Study, which provide data and recommendations for growing the global information security workforce (2017).

- According to a 2015 analysis from the Bureau of Labor Statistics, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years (2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/).

- A recent ISACA report estimates that the global shortage of qualified cybersecurity professionals will reach 2 million by 2019 and Cybersecurity Ventures predicts 3.5 million cybersecurity job openings by 2021 (2017, https://www.herjavecgroup.com/cybersecurity-jobs-report-2017-edition/).

Partnerships among academia, government and industry, along with dynamic tools are needed to facilitate the collection, organization, and sharing of up-to-date information about cybersecurity education, training, and workforce development. Such partnerships and tools can help educators and employers keep up with the rapidly changing landscape of cybersecurity jobs and workforce needs, and strategically strengthen our nation's workforce.

CyberSeek, a partnership between the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE), Burning Glass and CompTIA, is a powerful tool that provides up-to-date, detailed, actionable data about supply and demand in the cybersecurity job market (2017, http://cyberseek.org). Such a tool can be enhanced in several ways to support and help expand workforce development initiatives. For example, expanding job categories to cover critical infrastructure and other emerging job needs and linking the tool to employment opportunities can take an already powerful tool to the next level.

The designation of CAEs has set the standard for educating and training cybersecurity workforce. To evaluate if these standards are appropriately provided by the educational institutions, we need to examine what the outcomes are, that is,

- where and what the graduates are working on?
- are employers satisfied with the training that these graduates have attained?
- can the graduates continue to learn and develop in the field of cyber security?

Recommendations:

1.1. A comprehensive study of the graduates of these programs should be conducted. Possible coordination through State Employment Security Departments or EMSI (career builder - as an additional method of identifying career pathways).

1.2. To enhance the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs, we recommend systematic expansion of the NSA/DHS National Centers of Academic Excellence (CAE) Program. This will increase the number of institutions offering high quality cybersecurity education and training programs and thus enhance cybersecurity workforce development. The NSA recently established a network of CAE National Resource Centers (CNRCs) and CAE Regional Resource Centers (CRRCs) to advance cybersecurity education and workforce development across the nation. This program will help increase the number of CAE designated institutions across the nation, enhance cybersecurity knowledge and skills of faculty at those institutions, and enhance collaborations

that advance cybersecurity education, training and research.
1.3. Funding should be directed specifically to gather workforce data in order to better understand current and future workforce needs and the impact of exsisting programs.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

As the cyber defense industry matures there's a greater need to specify workforce categories, specialty areas, work roles and knowledge skills and abilities. The NIST/NICE framework provided a solid foundation.

- NIST efforts to advance cybersecurity education, training, and workforce via the NIST Cybersecurity Workforce Framework are commended
- NIST Framework needs to be tied in with job search tools and databases
- Cisco conducted a study along these lines
- Cooperation from and among industries and government sectors is needed: what are the expectations for each role and each category?
- There is no agreement, however, as the Bureau of Labor Statistics (BLS) data does not agree with the Framework roles; also a lack of standardization between BLS and Framework job titles and tasks
- Businesses are also concerned about the growing shortage of cyber-defense professionals. Cisco Systems commissioned the Gardner group to complete a comprehensive study of cyber-security positions related to IoT

Recommendations:

2.1. Standardization of work roles and KSAs by encouraging adoption of the NIST NICE Cybersecurity Workforce Framework.

2.2. Apply standards also to curricular development.

2.3. Involve HR organizations.

2.4. Creation of formal internship and apprentice programs that define specific cyber-defense related positions, qualifications and skills.

2.5. Expand Cyberseek (CyberSeek.org) and other tools to include broader categories, like critical infrastructure and industrial control systems security.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

With the adoption of the NIST/NICE framework and the ISO 27000 series standards, organizations are required to establishing formal policies for hiring and evaluating workforce credentials. These standards require closer collaboration between government agencies, business and academia in order to build a more competent cybersecurity workforce.

- CAE institutions are setting an example by requiring well-defined personnel policies regarding security awareness that are enforced; however this is not the case across all educational institutions.
- Employers should update hiring practices.
- Standards like ISO 27000 specify job credentials. More needs to be done to formalize workforce education and training in relationship to hiring policies.

Recommendations:

3.1. Both the NICE Cybersecurity Workforce Framework and the ISO 27000 standards should be promoted as a means for organizatons to identifiy and establish specific cybersecurity realated hiring policies.

3.2. Academia need to become more familiar with and align to industry required credentials including QSA and CISA.

3.3. Organizations should be encourged to implement cybersecurity and collaborate with government and industry to expand adoption of programs such as NSA Day of Cyber and DHS Cybersecurity Awareness Month.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic?

As a result of the on-going rash of data breaches and high profile ransom related incidents, employers have better recognized the value of hireing and buliding a skilled cybersecurity workforce. Keeping pace with the ever changing cybersecurity workforce skills is like chasing a moving target, technologies, products, attack and defense tools are changing on a daily basis. Foundational skills if well defined in the NIST NICE framework and NSA/DHS KUs, however advanced skills must be able to continuously evolve. Centers of excellence and innovation should be establish to lead academia to implementing advanced studies. These centers can be universities, colleges and community colleges.

- Mixed responses from employers cause confusion in program development
- Qualifications that are not necessary (imposed by HR and others) impact the ability to hire; example is requiring a computer science degree (typically focused on software development) for a network manager position
- Disconnect between supervisors and HR policy.
- HR requirements outdated or following de facto requirements
- Listing experience requirement for an emerging topic is unrealistic
- Failure to consider or value community college graduates

Computer Science versus IT Tech Requirements

- Solicitations from Federal Government agencies mistakenly as for “computer science” degrees for network engineers and administrators.
- 80% of all Computer Science graduates go into software engineering, not networking roles.
- Industry and even academia do not understand the difference between computer science and IT.
- Computer science graduates are often not “trained” on the required technologies, and not interested in performing the tasks that the employer is seeking for these other cybersecurity and networking engineer positions.
- It is important to point out that the Burning Glass studies often used in support of these “millions” of cyber-related jobs are in networking systems and hardening systems, not computer science; they do not need to be filled with individuals holding a Bachelor’s degree, just trained individuals.

University of Washington Center for Information Assurance and Cybersecurity (CIAC) conversation with industry and government:

- There is a ‘gap’ between the classroom and the workplace.
- UW CIAC has a study in place to advance a Collaborative Education Model and close the gap in order to turn out more ‘breach ready’ employees in less time.
- A national panel of experts from academia, corporate America, government, and military organizations is providing guidance and insight as thought leaders in cyber security.

Recommendations:

4.1. Organizations shoud be encouraged to utilize the NIST/NICE framework when drafting and posting cybersecurity related positions.

4.2. In addition to technical skills, employers want problem solving, critical thinking, communications and project management skills. Also, higher level positions in cybersecurity are needed - 50% of executives and high level managers require business management skills and organizational change competencies.

4.3. Increase employer engagement with academic programs and out-of-classroom cybersecurity related events, i.e competitions, job fairs, and awareness campagins.

4.4. Continue to evolve NIST Cybersecurity Workforce Framework to align to changing workforce needs.

4.5. Encourage employers, K-12, and higher education to use framework as common language.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today and what makes them effective?

Several federally funded cybersecurity workforce development programs have had significant impact on the nations ability to grow and sustain a highly qualified pipeline of cybersecurity professionals.

NSA/DHS CAE Program

One of the most impactful programs in creating a sustainable cybersecuirty workforce has been the NSA/DHS CAE programs. This program enables employers to have confidence that the graduates they hire have been exposed to a standardized set of knowledge and skills vetted by academia.

CAE Statistics

- There are currently 226 CAE institutions. (See CAE map in Section I)
- 25 new CAE since beginning of C5 project (October, 2015): 19 new CAE-2Y and 6 new CAE.
- New application process launched with CNRC/CRRC program, resulting in increased CAE candidate applications: 11 CAE applicants for June 2017

submission date.
- 17 CAE Mentors countrywide supporting mentee colleges.
- 34 colleges currently being mentored.
- CAE designation rate increased from 42% to 92% since the CRRC/CNRC Program was launched in 2016, effecting a significant expansion of higher education institutions offering CAE designated programs that meet national curricular guidelines and strengthen the national cybersecurity workforce.

The CAE program provieds a model cybersecurity culture: CAE criteria require 2Y and 4Y institutions to implement a series of institutional policies, procedures, and standards that help to both protect the institution and create a cybersecurity culture. Impact extends beyond the campus to K-12, government, and industry partners. Developing a culture of cybersecurity nationally is essential to the long-term effort.

NSF ATE Centers for Cybersecurity:
CSSIA, CyberWatch West, and National CyberWatch

- Share same goals and objectives
- Charged to increase the national CAE count
- Provide resources, training, and travel funding for faculty to attend conferences and training
- Model proven successful, effective
- Contribute to growth of cybersecurity community
- Connect faculty regionally
- Provide leadership in development of quality curriculum
- Help faculty stay current and learn emerging topics, such as the Internet of Things (IoT)
- Provide training for faculty to take back to their classroom

NIST Regional Alliances and Multistakeholder Partnerships (RAMPS) Program
The NIST RAMPS Program was launched to develop regional and statewide consortia and communities to strengthen cybersecurity workforce development. This program can be expanded to support other regions.

Cybersecurity Competitions:
GenCyber, CyberPatriot, NCL, CCDC

Cybersecurity competitions provides students from middle school to college exposure to cybersecurity as a career and exposure to industry professionals.

NSF Scholarship for Service (CyberCorps):
Student scholorship program, capacity building program

- Funding for students to attend college
- Option to go to work in government to pay off scholarship,
- Helps fill government fill positions otherwise left vacant
- Opportunity for students to attend college.
- Funds for students to attend technology conferences to enhance the students learning of cyber concepts Experiential learning opportunities
- Opens the student to additional career opportunities and education pathways
- Enables recipients to focus on learning and not worry about paying the rent or affording food
- Encourage NSA/NSF collaborative support for cybersecurity education: SFS, ATE, GenCyber

Industry Certifications:
ISC2 CISSP, SANS, CompTIA Security+, Cisco CCNA Routing and Switching, Cisco CCNA Cyber Operations

- Industry certifications establish workforce and academic standards
- Industry certifications identify key knowledge and skills from the employer and vendor perspective
- Provide credentials for new participants in the workforce.
- Provide an independent benchmark for graduates of academic programs to measure theyre kowledge and skills

Recommendations:

5.1 Federally funded programs including NSA/DHS CAE, NSF ATE and SFS, and NIST RAMPS Programs are vital in continuing to grow and sustain the cybersecurity workforce. Funding of these programs provides a vital resource for academic institutions.

5.2. The recognition and support of industry certifications is critical in the continued growth of a highly qualified cybersecurity workforce.

5.3. Leveraging high quality programs, staff snd faculty in the form of centers or hubs, is critical in building a community of high quality academic programs. The creation of hubs and centers also help create a culture of cybersecurity.

5.4. Create a culture of cybersecurity through extension of the CAE Program beyond higher education to K-12, government, and industry partners. Developing a culture of cybersecurity nationally is essential to the long-term effort.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

The preparation of cybersecurity professionals has severral unique challenges, these challenges include difficulty finding and training highly qualified faculty. These programs also requrie complex teaching and learning environments and the challenge of contiunuosly infusing emerging technologies. Perhapos the greatest challenge is increasing awareness of careers in this industry in building sustainable pipelines from our k-12 systems.

- Hiring practices and policies, long delay for federal jobs
- Flexible pathways and timely education models; e.g., competency-based education (CBE) models is one solution: competency-based education approaches teaching and learning more often in context of learning concrete skills than abstract learning; differs from other approaches in that the unit of learning is extremely fine-grained
- Agile and flexible pathways for offering up-to-date education and training programs

Recommendations:

6.1. Workforce certification should be used to address the credentials and skills gap.

- Professionalization of discipline
- Explore licensure of professionals, including required CE for faculty and professionals
- Support continuing education programs
- Better models for training students and faculty: flexible, dynamic
- Streamline security clearance process
- Better internships and apprenticeship programs
- Incorporate security auditing and compliance knowledge
- Best practice models for faculty recruitment, retention, professional development and advancement
- Structured programs and enhanced collaboration between academia, government, and industry to support cybersecurity education, training, and workforce development
- Collaborative programs for internships, apprenticeships, coops, certification, training, and facilitation of security clearances

6.2. Employers and workers need to be able to adapt quickly to changing market and new technologies developments and demands:
One of the main challenges of public policy is to foster institutional arrangements through which government departments, employers, workers and training institutions can respond effectively to changing skill and training needs, and indeed play a strategic and forward-looking role in anticipating future needs.

6.3. *Continuous stakeholder involvement:*

Good-quality training outcomes further depend on maintaining a high quality of training contents, methods, facilities and materials. Apprenticeships, and more generally the combination of classroom-based and work-based training, produce the best results. Skills standards should be set and tested by involving stakeholders in the process."

6.4. *K-12 Issue:*

- Lack of firm STEM foundation in K-12 education the root cause for shortage of cybersecurity professionals among US citizens
- A national culture change is required to address this problem; STEM, cybersecurity, and fundamental education begins with Sesame Street

6.5. Financial and administrative support to build relevant and practical models for training students, veterans, and faculty, including cohorts, boot camp styles programs and training partnerships between employers and academia (European model).

6.6. Government leadership in streamline security clearance process for new employees and advanced level students.

6.7. Better leadership and funding of internships and apprenticeship programs in cybersecurity.

6.8. A national initiative to include cybersecurity pathways of studies in the career pathways publications, framework and programs.

6.9. A shift in the national culture is required to address this problem; STEM, cybersecurity, and fundamental education begins with in k12.

7. How will advances in technology or other factors affect the cybersecurity workforce needed in the future?

As IoT technology advances and our household items, medical devices, and vehicles become interconnected and hackable, liability, privacy, and resiliency issues is emerging. Retail and medical workforce will have ethical, possibly legal imperative, to educate consumers on the benefits, features, and repercussions of owning smart appliances or being the recipient of an automated medical device.

- Recruit and produce more PhDs with practical experience, either through consulting or internships
- Provide resources to faculty members to continue researching and understanding of new technology, in order to bring them to the classrooms.

Internet of Things (IoT) Security Issues

- Security of IoT devices remains very much a concern
- Cybersecurity is the top impediment to IoT deployments
- Hackers use IoT products as easy access point to gain entry to the network, but there's also the prospect they could be hijacked
- IoT deployments can aid intensive workload activities such as security and data analytics.
- IoT-related careers, security and data analytics are needed

Recommendations:

7.1. *Emerging Technologies*

- Expand NIST Cybersecurity Workforce Framework, CAE KUs, and other curricular guidelines to include emerging topics, including IoT security, critical infrastructure and industrial control systems security, AI, machine learning, and other new advances; smart cities and smart homes
- Provide professional development and continuing education on emerging technologies for academic faculty, government, military, and industry partners through the CRRC and CNRC hubs
- IaaS, PaaS, SaaS, Virtualization and Cloud Computing - work closer with emerging technology vendors
- Support agile mechanism for developing curriculum for emerging technologies

7.2. *Business Liaisons and Advisory Boards*

- CNRCs/CRRCs can facilitate learning for advances in technology; project manage curriculum development
- Work with industry and government to research and identify emerging needs and align education, training, and workforce efforts
- Refine Knowledge Units (KUs) as needed, update curricula and certs, provide professional development opportunities
- States will need to be more flexible (agile) with development of new courses and programs

7.3. Investment in building academic programs in community colleges that address Internet-of-Things and security associated with these technologies.

7.4. Investment in building academic programs in community colleges that address IaaS, PaaS and SaaS and the inherit security risk associated with each.

7.5. Investment in academic centers of emerging technologies and innovation.

7.6. Creation of national business/government/academia collaboration networks for research, training and development of workforce supply strategies.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the nation's cybersecurity workforce?

Much progress has been made since the 2002 initial cybersecurity initiatives. However, the field of cyber defense is now involved in just about every facet of the US economy. As a result it is critical that our nation continues to grow and sustain the career pathways that lead student of the future to cybersecurity related fields. The cybersecurity fields are more diverse, complex, and professionals in these fields are now more responsible than ever for the protection of our critical infrastucture and vital information systems.

The following list represents the most impactful programs the nation has invested in to address the shortage of cybersecurity professionals:

- Support and expand CAE Program and CRRC/CNRC Program
- NSF/ATE projects and centers
- Capacity building track of SFS
- Competitions: CyberPatriot, CCDC, NCL, US Cyber Challenge
- Career pathways and clusters; state-level pathways and collaborations
- K-12 Outreach, GenCyber, pathways in K-12 space
- Partnerships with industry

- National consortia and collaborations includes academia, government, and industry
- Enhance collaborations (NIST, NSA, DHS, NSF, DoD)
- Improve international collaborations with cybersecurity leaders/allies
- Provide mechanism for colleges to track graduates
- Involve state leadership in cybersecurity education, K-12/higher education
- Include cybersecurity in publications
- Connect with Association for Career and Technical Education (ACTE)
- Work with CTE state directors

Recommendations:

8.1 Expansion of programs like NSA/DHS CAE programs.

8.2 Continued support of cybersecurity related NSF ATE centers and projects.

8.3 Investment in innovative teaching and learning environments, technologies.

8.4 Creation of a national cybersecurity faculty development network.

III. CONCLUSIONS

Broader recommendations:

- Expand collaborations among government, military, industry, and education
- Develop and disseminate best practice models to address emerging needs
- Support and expand the following, and similar, programs:
- NSA/DHS CAE - Center for Academic Excellence
- NSA/DHS CRRC/CNRC - CAE Regional and National Resource Centers
- RAMPS - NIST Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Workforce Development
- SFS - NSF Scholarship for Service
- GenCyber - NSA cybersecurity program for K-12 students and teachers

The CRRC/CNRC Network of educational institutions welcomes the challenge to support efforts to strengthen the cybersecurity of federal networks and critical infrastructure, as well as enhance workforce development.

IV. REFERENCES

www.nist.gov/nice
csrc.nist.gov/publications/PubsDrafts.html#SP-800-181
nsf.gov/ate
www.nsf.gov/pubs/2017/nsf17556/nsf17556.htm
www.gen-cyber.com
www.iad.gov/NIETP/CAERequirements.cfm
www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/
www.dhs.gov
godefense.cpms.osd.mil/scholarships.aspx
www.us-cert.gov
www.sans.org
www.nationalcyberwatch.org
www.cyberwatchwest.org
www.cssia.org
www.ccis.northeastern.edu/research-area/security
uwf.edu/go/cybersecurity
www.nvcc.edu/cybersecurity
whatcom.edu/about-the-college/cybersecurity-center
www.forsythtech.edu/about-us/davis-itec-cyber-security-center
www.uwb.edu/ciac
www.cbenetwork.org
www.oecd.org/g20/summits/toronto/G20-Skills-Strategy.pdf
www.acteonline.org
www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/
www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/
www.caecommunity.org/news/announcing-14-new-cae-cyber-defense-resource-centers
www.nist.gov/news-events/news/2016/09/nist-grants-take-regional-approach-solve-national-cybersecurity-challenge

A Collaborative Response from the NSA/DHS
National Center of Academic Excellence (CAE)
National Resource Centers (CNRCs) and CAE
Regional Resource Centers (CRRCs)