Written Testimony of
Dr. Barbara Endicott-Popovsky
Executive Director, Center for Information Assurance and Cybersecurity
University of Washington

Full Committee Hearing to:
Examine Cybersecurity in our Nation's Critical Energy Infrastructure

before the United States
Senate Committee on Energy and Natural Resources

March 1, 2018

Good morning, Chairman Murkowski and Ranking Member Cantwell, and distinguished Members of the Committee. Thank you for the opportunity to speak with you today about examining cybersecurity in our Nation's critical energy infrastructure, specifically about the public and private interplay in protecting the grid. My name is Dr. Barbara Endicott-Popovsky, and I am the Executive Director of the Center for Information Assurance and Cybersecurity (CIAC) at the University of Washington. Founded in 2004, CIAC is an NSA/DHS designated Center of Academic Excellence in Cybersecurity Defense Education and Research and an NSA CAE Regional Resource Center named to disseminate best practices in cybersecurity education and to mentor other colleges and universities. We convene industry, government and military around shared problems.

CYBERSECURITY CONTEXT

To provide context, four big facts about cybersecurity drive our work and our views on cybersecurity:

1) ***In cyberspace, EVERYONE is our neighbor.***
   This requires new deeper relationships between the military, government, industry, and citizens.

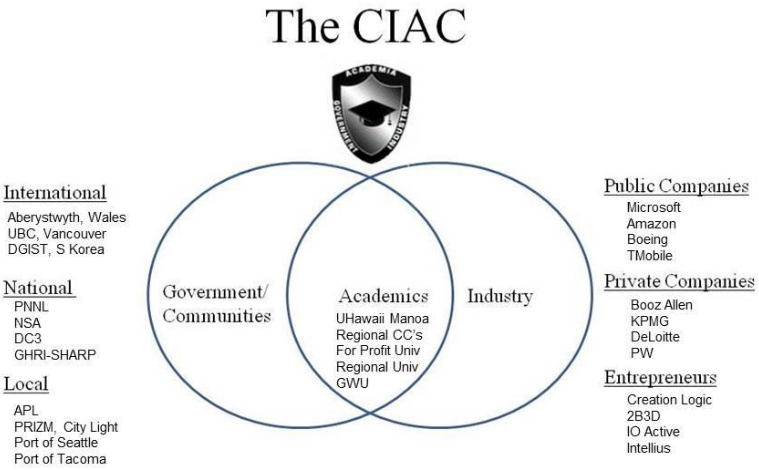


Figure 1: CIAC Cross sector collaborations

2) ***Cybersecurity involves rules & tools***

Although rooted in technology, it also depends on policy and processes at all levels,
communication, & problem-solving.

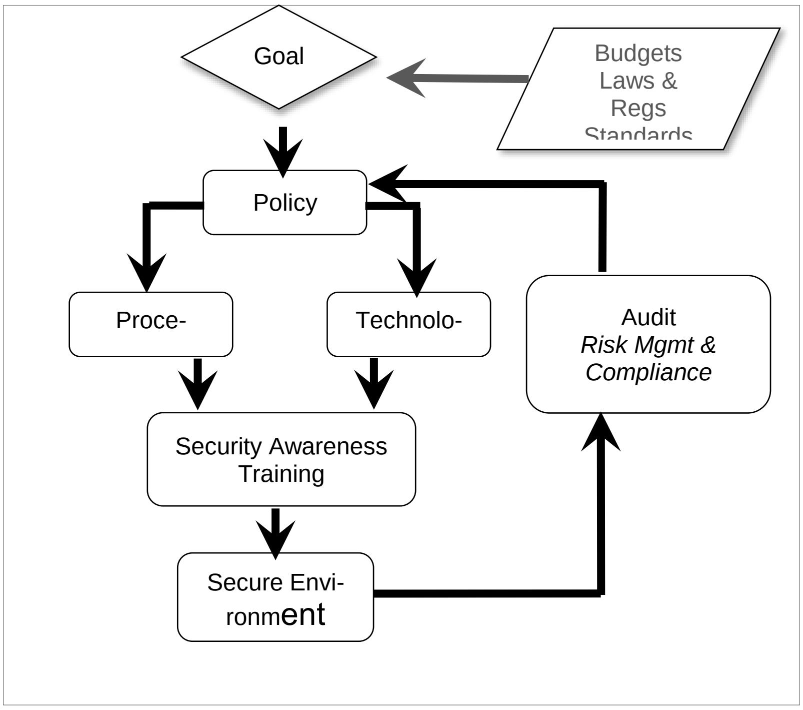
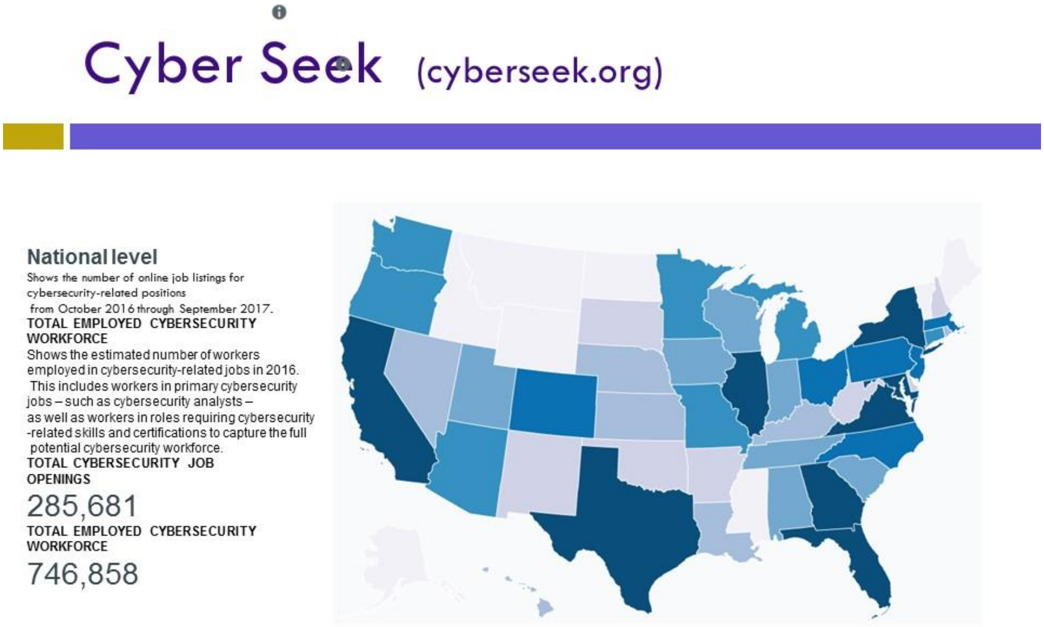


Figure 2: Operational environment for managing cybersecurity

3) ***Not enough talent***

There is a systemic shortage of well-trained talent (and of qualified teachers)



Cyber Seek (cyberseek.org)

National level

Shows the number of online job listings for cybersecurity-related positions from October 2016 through September 2017.

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

Shows the estimated number of workers employed in cybersecurity-related jobs in 2016. This includes workers in primary cybersecurity jobs – such as cybersecurity analysts – as well as workers in roles requiring cybersecurity -related skills and certifications to capture the full potential cybersecurity workforce.

TOTAL CYBERSECURITY JOB OPENINGS

285,681

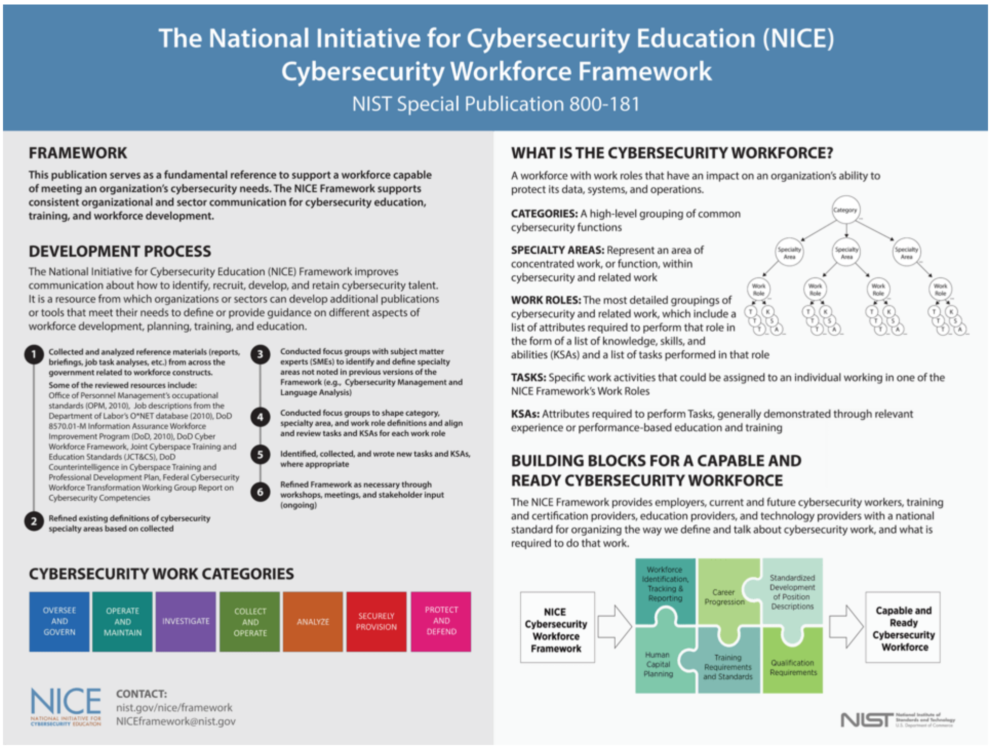
TOTAL EMPLOYED CYBERSECURITY WORKFORCE

746,858

Figure 3: Operational environment for managing cybersecurity

4) ***Cybersecurity is becoming a profession***

It's not one thing--32 separate career paths have already been identified.



**The National Initiative for Cybersecurity Education (NICE)
Cybersecurity Workforce Framework**

NIST Special Publication 800-181

FRAMEWORK

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

DEVELOPMENT PROCESS

The National Initiative for Cybersecurity Education (NICE) Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

1. **Collected and analyzed reference materials (reports, briefings, job task analyses, etc.) from across the government related to workforce constructs.**
   Some of the reviewed resources include: Office of Personnel Management's occupational standards (OPM, 2010), Job descriptions from the Department of Labor's O*NET database (2010), DoD 8570.01-M Information Assurance Workforce Improvement Program (DoD, 2010), DoD Cyber Workforce Framework, Joint Cyberspace Training and Education Standards (JCT&CS), DoD Counterintelligence in Cyberspace Training and Professional Development Plan, Federal Cybersecurity Workforce Transformation Working Group Report on Cybersecurity Competencies
2. **Refined existing definitions of cybersecurity specialty areas based on collected**
3. **Conducted focus groups with subject matter experts (SMEs) to identify and define specialty areas not noted in previous versions of the Framework (e.g., Cybersecurity Management and Language Analysis)**
4. **Conducted focus groups to shape category, specialty area, and work role definitions and align and review tasks and KSAs for each work role**
5. **Identified, collected, and wrote new tasks and KSAs, where appropriate**
6. **Refined Framework as necessary through workshops, meetings, and stakeholder input (ongoing)**

CYBERSECURITY WORK CATEGORIES

OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

CONTACT:
nist.gov/nice/framework
NICEframework@nist.gov

WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

BUILDING BLOCKS FOR A CAPABLE AND READY CYBERSECURITY WORKFORCE

The NICE Framework provides employers, current and future cybersecurity workers, training and certification providers, education providers, and technology providers with a national standard for organizing the way we define and talk about cybersecurity work, and what is required to do that work.

NICE Cybersecurity Workforce Framework
Workforce Identification, Tracking & Reporting
Career Progression
Standardized Development of Position Descriptions
Human Capital Planning
Training Requirements and Standards
Qualification Requirements
Capable and Ready Cybersecurity Workforce
NIST National Institute of Standards and Technology U.S. Department of Commerce

Figure 4: NICE framework standardizing cybersecurity workforce specialties

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

CYBERATTACKS: HOW DID WE GET HERE?

At least weekly we hear about significant data breaches or cyberattacks that threaten the financial health and privacy of millions of online users, or describe attacks by nation states or terrorist groups with a political or propagandistic agenda. To the citizen observer, it must appear that those responsible for managing networks are helpless to do anything about rising online crime and threats. To a certain extent that assumption is true. We will never have 100% secure systems. Technologies alone won’t fix things. Users assume a certain amount of risk online. Many just don’t realize it. The idea shatters our comfortable sense of security we’ve developed over decades of experiencing reliable infrastructure. It’s no wonder the public is disturbed by what they are reading in the news. There is no cyber 911 we can call if things don’t work.

How did we get here? How did our online interconnectedness, that has created so many benefits, resulted in so many challenges? Have we been so enamored of creating the next new digital device or online service that we didn’t take time to consider the unintended consequences that we’ve introduced into our lives?

We’re living through digital transformation that’s challenging how we think and breaching the silos that used to organize our lives and our thinking. We have been clinging to mental models from the physical world and the industrial age that blind us to the changes around us. The embrasure of technology is moving so fast, it’s difficult to keep up with the unintended consequences of what this has done to our daily reality and how society as a whole functions.

In one sense, we are rapidly smashing our Industrial Age mental models where organizations are structured in hierarchies, knowledge is structured by discipline, our work is in discrete silos—departments and sectors: military, government, industry, academia—replacing it with interconnectedness that, as a by-product, also enables online fraud, online voting scams, illegal downloads, and continuing threats to network security. But who saw this coming? Like Mickey Mouse as the Sorceror’s Apprentice in *Fantasia*, we have assumed the wizard’s powers without anticipating the risks! What was meant for good has ushered in unexpected problems. The Internet has brought convenience, savings, and productivity, but it also has created troubling dislocations that we didn't anticipate.

NEW MENTAL MODELS NEEDED

1. Cross Sector Collaboration: Public Private Partnerships

Civilians are used to calling 911 for emergencies of all kinds, but who do you call in the event of a major cyber outage? There are no cyber fire departments. The DoD is prepared to defend their own networks to support their missions, but who will step in on the civilian and private sector sides to restore power, to assist with maintaining our communities? There is no one. This vacuum is a national security threat.

In Washington State we've benefited from a National Guard whose leadership, coming from the tech industries, have created cyber civil support teams that assist government agencies and utilities to assess their vulnerabilities through penetration test exercises.

Working across civilian and military boundaries is not so easy, given the legal authorities issues that arise. Their lessons learned about how to manage crossing authorities in nanoseconds is preparing organizations locally and could be disseminated across the country for maximum preparedness.

Public and private, we have two very different missions: the mission of the military is to protect the Homeland, and the mission of private sector to innovate and maintain profitability for the Board and shareholders. Blending missions is not an easy task, but the time has come where the cost of not integrating resources significantly outweighs the benefits of maintaining independent response plans. This is especially true given the workforce shortage of cyber specialists.

One very important nexus between theses missions – public, private, federal, military – is the primary role of providing life safety. Profitability becomes secondary to protecting critical infrastructure. A unifying component is the legal obligation that critical infrastructure partners have to maintain continuity of operations. Two recent studies on this topic are: the 2017 Rand "Cyber Power Potential of the Army Reserve Component" and the 2017 PNNL report on Public/Private/Civilian/Local/Federal partnerships (draft only). These reports create an excellent case for greater training, but they need a framework to operationalize the teams necessary for comprehensive cyber response. Critical infrastructure private sector partners have an opportunity to leverage the work of the Guard to increase their surge capacity through efforts to expand the existing cyber civil support teams to include the Cyber mission. One of the most impactful contributions that could come from private sector critical infrastructure cyber response and threat intelligence teams would be the coordination of credentialing, training, and funding of area command centers to respond to a cyber disaster.

For this reason, Rep Kilmer from Washington State has joined with colleagues in the House to propose proliferation of cyber civil support teams across the country through all National Guard, modeled after the work being done by the Washington National Guard. Appendix 2 and 2b provide insight.

2) Cyberwar: A New Case of Mutually Assured Destruction

In this country we have had the luxury of two oceans on either side, left and right, with two 'soft' countries above and below us that are basically cooperative and ‘like us.’ This can inure us to what we have done by becoming virtual next door neighbors with all of our friends online. I’m fond of telling my students that my mother named six kids that I was absolutely to avoid like the plague when I was growing up. I still remember the name of the boy at the top of the list. These were perennial troublemakers in the neighborhood; if you hung around them, you were assured of no-good. (I can attest to it, having smashed a church window, by accident, playing softball with a couple of them!) Now we are side-by-side with cultures and countries radically different from our own, with very different world views about IP (Intellectual Property), freedom, ethics, etc. Why do we expect them to behave like us? They don’t and they won’t,

At some point we will need, for cyberspace, 1) the equivalent of the Kennedy/Krushchev era ‘red phone’ to ensure we don’t misread each other’s online actions and 2) the equivalent of nuclear disarmament talks to define the rules and tools of acceptable online activities for civil societies. There is no doubt in my mind that cyberwarfare can be as deadly as nuclear war and result in mutually assured destruction, as Admiral Rogers testified this week.

3) Tragedy of the Commons

This is a case of ‘ tragedy of the commons,’ in which a shared-resource, the Internet, is accessed by users who act independently according to their own self-interest, behaving contrary to the common good, thus spoiling that resource for all. Many users have placed reliance on that resource and will be lost without it.

Again this argues for agreed to behavior standards for all, but there would need to be a means of enforcement. This has not proven easy in the case of individuals and in the case of nation states there seems to be no appetite. We are left, perhaps, with the need for a catastrophic failure before a solution can be developed. I don't see a solution in my lifetime. I do see a need for thoughtful interim behaviors on the part of all users, individually, during this interesting period while we shed the industrial age infrastructures we grew up with for something as yet to be developed.

TALENT DEFICIT

To deal with all of this change and its significance and impacts, we have a huge deficit in talent to handle the cyber problems we face. The lack of talent in the field of cybersecurity is keenly felt across all sectors of the economy—industry, government, military, the academy. While cybersecurity education has been called a national priority by some, there still are hundreds of thousands of cybersecurity jobs going unfilled, and the gap will take a long time to close.[1]. Of further concern, we have gathered anecdotal evidence that employers in both government and industry consider many recent cybersecurity graduates woefully unprepared for the realities of the workplace, taking too long to become effective. For that reason, CIAC has adopted an approach to address both the supply and preparedness problems, with the application of a lightweight cooperative learning model—designed specifically to develop and graduate 'breach-ready' cybersecurity professionals.

[1] [cyberseek.org] and this is just the US view. There is a deficit worldwide that at least doubles their numbers.

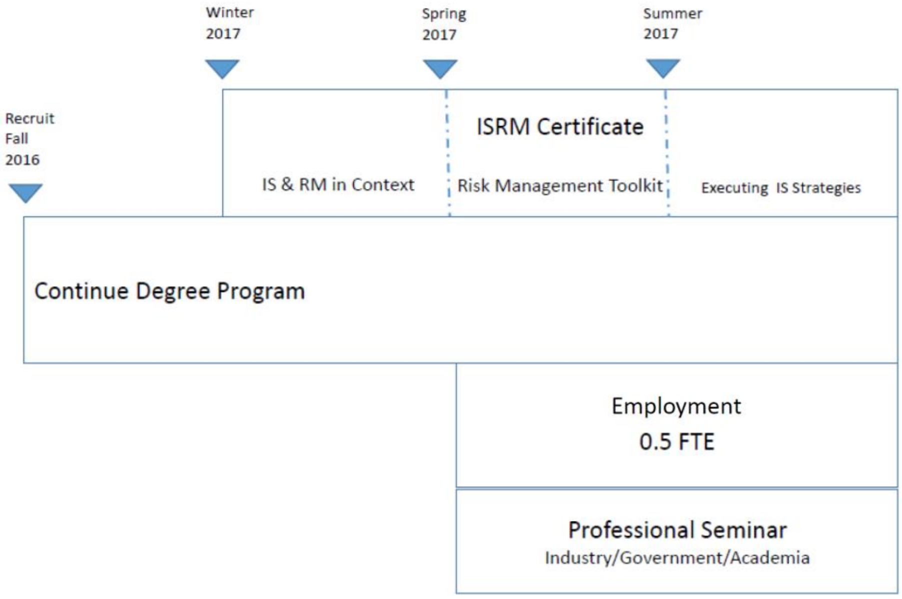


Figure 5: Cybersecurity Cooperative Learning Model

Because imposing a cooperative learning structure (such as European countries have, or a few universities in the United States and Canada, where a year of work interleaves a year of school) would be costly and disruptive to most academic institutions, CIAC devised a cybersecurity cooperative learning pilot where students maintain their current academic load in the last year of their degree programs and, in addition, opt into an integrated program of professional instruction and half-time industry employment. The additional professional education includes: 1) an information security and risk management certificate that covers all the necessary knowledge units required to meet NSA/DHS/NIST standards and 2) a professional seminar conducted in partnership with industry to help students triage their work experience with what they've learned formally in the classroom.. The addition of the professional seminar and certificate elements in the pilot accelerate student readiness for work when they formally graduate, based on employer and student data collected.

T-Mobile served as our initial industry partner and collaborator in developing this cooperative learning program. In addition to their support, government is also a partner. The National Information Assurance Education and Training Program (NIETP) is interested in the dissemination of the cooperative learning model and the lessons learned during the pilot period. This is conceived as a two-year pilot. This first year 10 students, constituting one cohort, were engaged with one employer. Students were selected based on technical foundation, interpersonal skills, team participation, and collaborative problem-solving abilities. Certificate scholarships were provided. A second year of the pilot is currently being conducted with more industry partners for the purposes of incorporating lessons learned from the first year and refining and generalizing the model.

In the second year, data collected will provide insight into several questions: 1) /how this program will be scaled, 2) how and to what degree this kind of a program accelerates cybersecurity job readiness, 3) what are best practices for conducting such a program.

PROFESSIONALIZATION OF CYBERSECURITY: STANDARDS

Cybersecurity is and must professionalize. The Manning and Snowden incidents argue for professional standards of behavior and selection, like we see in other professions (medicine, dentistry, law, etc.) We also see education standards taking hold with more NSA CAE's adopting the curricular standards laid out by NIST/NSA/DHS and the emergence of ACM guidelines and ABET accreditation on the technical side.

We've also seen one of the infrastructure sectors, telecommunications, become the first to step up to exploring whether or not new or additional educational standards need to be created for cybersecurity specific to that sector. Telecommunications supports virtually all of our critical infrastructure. For this reason, CIAC joined the Communications Security, Reliability and Interoperability Council (CSRIC), led by T-Mobile, to address this and other workforce issues specific to telecommunications cybersecurity professionals.

We learned that much of the existing work by NIST, NSA, DHS on workforce development, work roles, education standards, etc., could be leveraged by the telecommunications sector and we posit by other critical infrastructures, as well, saving time and resources. For this reason, CSRIC findings are located in an appendix to this testimony for the committee's reference in the hopes that these findings could be informative.

Please note that we will need specific incentives for students to work in critical infrastructure cybersecurity. Critical Infrastructure is competing with industry for the same scarce talent pool and they can be salaries that are much higher. For that reason, CSRIC recommended a scholarship for service program for critical infrastructure.

ANOTHER MOON SHOT PROJECT

With commitment to truly solve the cybersecurity talent problem systemically, and provide the stable, steady funding that that would imply, it will require the kind of effort that turned the education system around during the project to put a man on the moon. It took 10 years, but we did it.

ACKNOWLEDGEMENTS

I wish to acknowledge the following organizations and individuals—representing military, industry and government respectively—for their contributions to the appendices that follow: The Washington National Guard led by Col. Gent Welsh, the Communications Security, Reliability and Interoperability Council (CSRIC) led by Bill Boii, Senior VP, T-Mobile, and the National Initiative for Education and Training Program (NIETP) at NSA led by Chief Lynne Clark.

These are offered for your further research efforts. More material is available upon request.

APPENDIX 1 (pp 14-17)

EXAMPLE INDUSTRY COLLABORATION

Communications Security, Reliability and Interoperability Council (CSRIC) final report recommendations (Executive Summary below) apply equally to other critical infrastructure like the energy sector and could be leveraged to accelerate workforce development initiatives therein. University of Washington CIAC collaborated with the T-Mobile on this project. The full report is available on request.

Courtesy Bill Boni, Sr.VP T-Mobile

March 2017 WORKING GROUP 7 Cybersecurity Workforce

Communications Security, Reliability and Interoperability Council (CSRIC)

Final Report –

Cybersecurity Workforce Development Best Practices Recommendations

Bill Boni (Co-Chair)	T-Mobile
Drew Morin (Co-Chair)	T-Mobile
Bill Newhouse	NICE Program Office at NIST

Executive Summary (excerpted)

The mission of the Communications Security, Reliability and Interoperability Council (CSRIC or Council) is to provide recommendations to the Federal Communications Commission (FCC) to ensure, among other things, optimal security and reliability of communications systems.[4]

Furthermore, the Council's recommendations specifically address the prevention and remediation of detrimental cyber events. Working Group 7 of the CSRIC V is specifically chartered to provide recommendations for the

CSRIC's consideration regarding any actions the FCC should take to promote improvements in cybersecurity workforce development. [5]

The CSRIC V Working Group 7 was tasked to examine and develop recommendations for the CSRIC's consideration regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field.

Specifically, this working group leveraged existing work in this context to enhance the volume and quality of the workforce, including [6]:

(1) **demonstrating the application of the National Cybersecurity Workforce Framework** (NCWF) to the common and specialized work roles with in the communications sector;
(2) **identifying any gaps or improvements in the NCWF** for evolving work roles or skill sets that should be included in sector members' workforce planning; and
(3) **identifying, developing, and recommending best practices and implementation thereof** to mitigate insider threats, including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities within the communications sector and particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. In this respect, the working group should consider means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

In order to manage the scale of the task, Working Group 7 chose to segment the information gathering and analysis process with targeted findings specific to each segment. We then identified best practices based on our analysis for each segment for consideration. This Final Report presents those Best Practices deemed to be most appropriate and impactful for consideration by the CSRIC V as recommendations to the FCC and the Communications Industry as a whole.

The National Cybersecurity Workforce Framework (NCWF)[7] provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Competencies, and KSAs.

1. **Categories** are common major functions regardless of job titles or other occupational terms.
2. **Specialty Areas** are common types of cybersecurity work which are grouped with similar areas under a specific Category.
3. **Competencies** are areas of expertise required for the successful performance of a job function; these are defined in the framework through the association of specific KSAs.
4. **Knowledge, Skills and Abilities (KSAs)** are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training experience, education, or training.

Working Group 7 (WG7) leveraged the prior NCWF analysis and process completed by the Financial Sector as a best practice to accelerate our task of evaluating the NCWF. The summary conclusions are that the NCWF is a viable, flexible framework that can and should be applied to the Communications Sector for Cybersecurity Workforce Development Planning. Building on this finding by the Working Group members, we proceeded to complete the initial evaluation of the "building blocks" – Categories, Specialty Areas, Competencies, and KSAs – for gaps and improvements that should be included in the application of this dataset to the Communications Sector. Our work product is attached to this Final Report as Appendices 1 and 2. It was also delivered to the FCC as a working database in Microsoft Excel format for unrestricted use.
We recognize that cybersecurity workforce development is undergoing rapid change and evolution.

This Final Report provides a lexicon that can be used to articulate the specific Workforce needs of the Communications Sector for roles involving cybersecurity. However, it is a static dataset and needs to evolve as the NCWF matures and Cybersecurity Workforce Development Planning gains maturity in our respective organizations. As part of the Final Report, WG7 provides specific recommendations for consideration by CSRIC on a process for adaptation and improvement of the sector specific dataset.

Recommendations

The CSRIC V Working group 7 was tasked to examine and develop recommendations…to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. Workforce

Development is not about filling job openings, although that is a source of metrics often used to represent the scale of the challenge. Instead, we chose to base our approach on the simple adage – a rising tide raises all boats. This led us to focus on the following broad based recommendations that would expand the available pipeline of skilled candidates for our industry as a whole.

6.1 The FCC Should Support a Process for the Communications Industry to Cooperatively Support Updates to the NICE Cybersecurity Workforce Framework (NCWF)

6.2 Communications Industry can Benefit by Growing Awareness of and Supporting Programs Encouraging K-12 Youth to Study Cybersecurity

6.3 The FCC Should Encourage Communications Industry Development of Cooperative Work-Study Program Partnerships

6.4 The FCC should engage with the Communications Industry to Develop or Expand Scholarship for Service Programs in Industry

6.5 The FCC Should Encourage Communications Industry Cybersecurity Professionals to Help Train the Next Generation

6.6 The FCC Should Encourage the Communications Industry to Participate in the Development of Curriculum Guidelines by the Joint Task Force on Cybersecurity Education

6.7 FCC Should Partner with Communications Industry, Public Safety, and Federal GenCyber to Develop a Cybersecurity Distance Learning Program for Public Safety and Rural Communities

6.8 The Communications Industry Should Support Innovative Cybersecurity Workforce Development Initiatives such as the CyberBlue Program Support to Engage Populations with Disabilities

6.9 Communications Industry Cybersecurity Experts Should Join the National Initiative for Cybersecurity Education (NICE) Working Group or One of its Subgroups

3 In November, NIST released for comment an update in partnership between NICE and DHS that changes the nomenclature back to the NICE Cybersecurity Workforce Framework

4 Charter of the FCC's Communications Security, Reliability and Interoperability Council

5 CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016

6 The FCC CSRIC Working Group Description references the NICE CWF; Working Group
7 has opted to refer to this framework using the April 2014 NICCS designation of the National Cybersecurity Workforce Framework (NCWF) for external consistency

APPENDIX 2A (pp 18-20)

EXAMPLE MILITARY COLLABORATION

Major General Tim Lowenberg National Guard Cyber Defenders Act proposed by Rep. Kilmer to create National Guard Cyber Civil Support Teams.
There are no cyber 'fire departments' for civilians to call in the event of a major cyberattack. University of Washington CIAC collaborates with the Guard in cyber preparedness projects.

Courtesy Col. Gent Welsh, USAF194 WG (US)

H.R. 3712 – Major General Tim Lowenberg National Guard Cyber Defenders Act

Rep. Derek Kilmer (D-WA) & Rep. Steven Palazzo (R-MS)

Cosponsors [*19D*, 14R]: Bishop (UT), *Bordallo (GU)*, *Brady (PA)*, Brooks (IN), *Carson (IN)*, Cole (OK), *DelBene (WA)*, *Esty (CT)*, Fortenberry (NE), *Gallego (AZ)*, Graves (GA), *Heck (WA)*, Herrera Beutler (WA), *Himes (CT)*, *Jayapal (WA)*, Jones (NC), *Kihuen (NV)*, *Kind (WI)*, *Krishnamoorthi (IL)*, *Larsen (WA)*, Love (UT), McMorris Rodgers (WA), Mullin (OK), Newhouse (WA), *O'Halleran (AZ)*, *Pocan (WI)*, Reichert (WA), *Rice (NY)*, *Rosen (NV)*, Scott (GA), Shea-Porter *(NH),* and *Visclosky (IN)*.
Endorsed: The National Guard Association of the U.S. & the Enlisted Association of the National Guard of the U.S.

The Issue: *"America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security."* -2018 National Security Strategy

The Threat: In December 2017, hackers remotely controlled an industrial safety control system, the first-ever reported successful attack on safety devices widely-used across U.S. energy, chemical, and utility industries. This hack is just the latest in a growing number of cyber-attacks exposing the gap between the authority of federal cybersecurity forces and the needs of states, tribes, municipalities, and private industry. The 2018 National Military Strategy identifies the cyber domain as the tool of choice for state and malicious non-state actors to use as a weapon of mass disruption.

The Problem: Most of the Nation's critical infrastructure is non-federal, which means existing federal cyber efforts leave states, tribes, and municipalities, as well as private industry, to fend for themselves.

The Strategy: The 2018 National Security Strategy promises to work with our critical infrastructure partners to assess their informational needs and to reduce the barriers to information sharing, and to expand collaboration with the private sector so that we can better detect and attribute attacks (Page 13).
"We will work with the Congress to address the challenges that continue to hinder timely intelligence and information sharing, planning and operations, and the development of necessary cyber tools" (Page 32).

The Proposal: This bill seeks to improve our nation's cybersecurity posture by establishing National Guard Cyber Civil Support Teams, of up to 10 members, in every state and territory to bridge the gap between federal and non-federal efforts. Cyber CSTs would serve as first-responders to incidents under the direction of governors and the state adjutant general, building a trusted link between states, critical infrastructure providers, and the federal government.

Why are National Guard Cyber Civil Support Teams a key part of addressing the cybersecurity gap?

- The National Guard is the only US military force that can operate across both State and Federal responses. The US Cyber

Command's Cyber Protection Teams are limited by federal Title 10 authority.

- US Cyber Command needs a "point of presence" in every state and territory in order to rapidly effect information sharing up and down the chain during cyber-attacks.
- States need a dedicated cyber response force structure not beholden to DOD or the Cyber Mission Force in order to be successful in response to state, tribal, and local incidents.
- Numerous reports and testimonies have already called for increased National Guard involvement in the U.S. cyber posture to improve DOD support of civil authorities.
- Despite Presidential Policy Directives, GAO recommendations, and Congressional reports, the DOD has yet to define responsibilities for civil support in cyber incidents or for National Guard involvement.
- The best way to build an efficient response protocol *before* an attack happens is to establish local, dedicated teams that train and routinely share information. The Cyber National Guard teams in Washington, Virginia, and Michigan have built successful relationships with their non-federal partners.

Cyber CST's could lead the effort in their states to defend elections against cyberattack.

APPENDIX 2B (pp 21-25)

Washington’s National Guard Cyber Civil Support Team (articles below) performs penetration tests of local government agencies as well as utilities upon request. They have pioneered working across public and private sector domains, capturing lessons learned that could be shared across the country in order to prepare for major cyber events.

Courtesy Lt. Col. Thomas Muehleisen, (ret.)

Guard attacks on demand

Guardsmen waging war in cyberspace with local agencies at their bidding

By J.M. Simpson on May 14, 2015

You may not be interested in cyber warfare and all that it embodies, but it is certainly interested in you. By the end of 2013, this country entered the era of the mega-breach when Russian-speaking hackers stole 40 million credit-card numbers after penetrating Target Corp. computer systems.

Cyber-attacks are commonplace; companies like Adobe Systems, J.P. Morgan Chase & Company, eBay, Anthem Inc. and others have experienced such attacks. While the specific reasons for these attacks can vary, the end result is the same - serious damage to the infrastructure undergirding this nation's economy.

Eye opening does not describe the challenges this state's computer savvy citizen-soldiers confront in protecting critical entities from an attack. And they are employing those skills to purposely attack willing participants before actual bad guys do the same.

"The threat exists," Lt. Col. Tom Muehleisen, a cyber planner, said. Muehleisen often made allusions to the old Star Trek TV series. "There can be a Romulan war bird parked off the coast."
Can this war bird unleash a photon torpedo that can damage if not destroy part of the state's and/or nation's critical infrastructure? "Yes," Muehleisen answered. "Our mission is to assume a defensive position, to protect critical infrastructure from attack."

Where are these attacks coming from? "There is no such thing as a fully secure network," he continued. "In this business, you work under the assumption of a breach." To that end, Muehleisen and his small team of cyber warfare specialists work to defend against cyberattacks.
While there is no such thing as a fully secure network, critical agencies must make themselves more secure from a binary borne assault.

A cyberattack is a deliberate exploitation of computer systems employed by individuals or organizations that target - zero in on, if you will - computer information systems, networks and/or personal computing devices through the use of malicious code to alter operations or data.
This attack generally results in a series of disruptive consequences that can compromise data and lead to theft, alteration, manipulation or the destruction of a specific computer system.
If a group of bad actors were to successfully deploy computer technology to destroy a power company's ability to provide power, we all could be living in the dark.

"I believe all utilities have to be concerned about their cyber security," wrote Benjamin Beberness, Snohomish County Public Utility District 1's chief information officer, in an email.
The district, or SnoPUD, is a public utility that provides power to 325,000 customers in Snohomish County and on Camano Island. The utility is the second largest public utility in the Pacific Northwest, and it is the 12th largest in the country.

To bad actors with intent to do harm to this country's power grid, SnoPUD is a prime target.
"Every day someone is knocking on SnoPUD's door trying to see what is inside," continued Beberness. The knocking on the door can and

sometimes does come in the form of a powerful cyberattack. Think of that Romulan war bird parked off the coast of Washington potentially arming a photon torpedo and you're getting the idea.

About two years ago, Beberness asked the Guard if it would create "SnoPUD #1 Cyber Security Defense Assessment" in order to test SnoPUD's ability to defend itself. In conducting the test, the Guard fielded a small but highly intelligent and experienced team of determined aggressors.
Penetration, testing and understanding the vulnerabilities of SnoPUD's computer infrastructure and key resources underscored the team's actions.

The team took its role seriously; it pulled no punches in testing SnoPUD's ability to protect itself.
Just as important, in conducting the test, the Guard's cyber warriors zeroed in on the utilities' "smart grid lab," a perfect replica of SnoPUD's actual computer driven operations center.
The cyber warriors utilized a penetration test, or pen test, to assess SnoPUD's abilities to protect itself. It is the blunt end of the Guard's assessment driven photon torpedo launched into SnoPUD's smart grid lab.

During the test, the Guard's cyber warriors entered the lab and began moving from one section to another. "The goal is to get in, look around, and leave without a trace. This testing is a good way to get the attention of the technicians at SnoPUD," Muehleisen said. "If we touch you, we own you."

The Guard personnel involved in this operation had little trouble leaving their fingerprints behind as they found and exploited SnoPUD's vulnerabilities to an actual cyberattack. "SnoPUD is very good at what it does," Muehleisen continued. "They are a proactive agency when it comes to defending against cyberattacks; SnoPUD pushes this agenda at the national level in order to convince other public utilities to engage with organizations like the Guard."

If agencies critical to the nation's infrastructure don't engage in discussions like SnoPUD and the Washington National Guard have, the Romulans most certainly will.

Washington National Guard is on cyber patrol

Joint Forces Defense Assessment Team leads state's cyber-emergency planning

By Melissa Renahan on February 18, 2014

Washington was the first state to find a role for the National Guard in its cyber-security efforts.

"The National Guard, through its existing relationships within every state and territory, is in a unique and important position to help solve what I call the ‘cyber response capability gap.' That gap is the space that exists between what we acknowledge as a threat and our actual capability to do something about it," explained Col. Gent Welsh, former Chief Information officer for the Washington National Guard.

Enter the Joint Forces Defense Assessment Team. Thus far, Washington has used this team to conduct cyber-emergency planning and to search for vulnerabilities within state networks under the direction of the governor. Per mission, there are typically between five and eight team members, representing the State Guard, Air National Guard and Army National Guard for Washington.

"Right now, there is no agency within the federal or state government that has the mission to protect our nation's critical cyber infrastructure and in my opinion, nowhere in our nation's history has a problem been so acknowledged (cyber threats) but yet no comprehensive effort put forth to resolve it in a meaningful and collaborative way," stated Welsh, who has been in the Washington Air National Guard for more than two decades.

"For example, national leaders have talked about a ‘cyber 9/11' but yet the nation still lacks a response force to manage the consequences of a devastating series of attacks which could target our critical infrastructure, not just military infrastructure, and the management and response processes are still in their infancy," Welsh continued.

This is part of the reason why Washington was the first state to find a role for the National Guard in its cyber-security efforts. Given that so many of the state's citizen soldiers work in a technology field in their civilian careers, it made sense to take advantage of that knowledge when they were serving in uniform.

"We want to work on proactive efforts, as well as a response to a cyber attack," explained Russ McRee, who works at Microsoft when he is not serving as a staff sergeant (who is poised to graduate from Officer Candidate School soon) with the Washington State Guard. His job at the software giant is remarkably similar to the role he plays at Camp Murray as both involve him assessing and analyzing threats.

"Where are the gaps? Where a threat meets a vulnerability and then becomes a risk? That's what we're seeking out," said Lt. Col. Thomas Muehleisen, the current Chief Information officer. "I feel fairly good about what we're doing nationally but it starts to break down somewhat at the state level and we're ready to improve that."
Recently, during one such assessment for a large state agency, McRee and his team identified approximately $800 million in identified risk. That figure is calculated by adding up what said agency would have to do in order to recover and restore any lost records, which could run upwards of $200 per lost record, per individual.

"We take on the role of the bad guy and try to compromise systems, find ways in and then take that assessment and information and advise the agency with the intent that now they have the weaknesses," McRee explained.

The cyber team has also worked with 25 other government agencies and private sector partners statewide to lead a cyber exercise that resulted in a standardized response if there was a major cyber threat or incident.

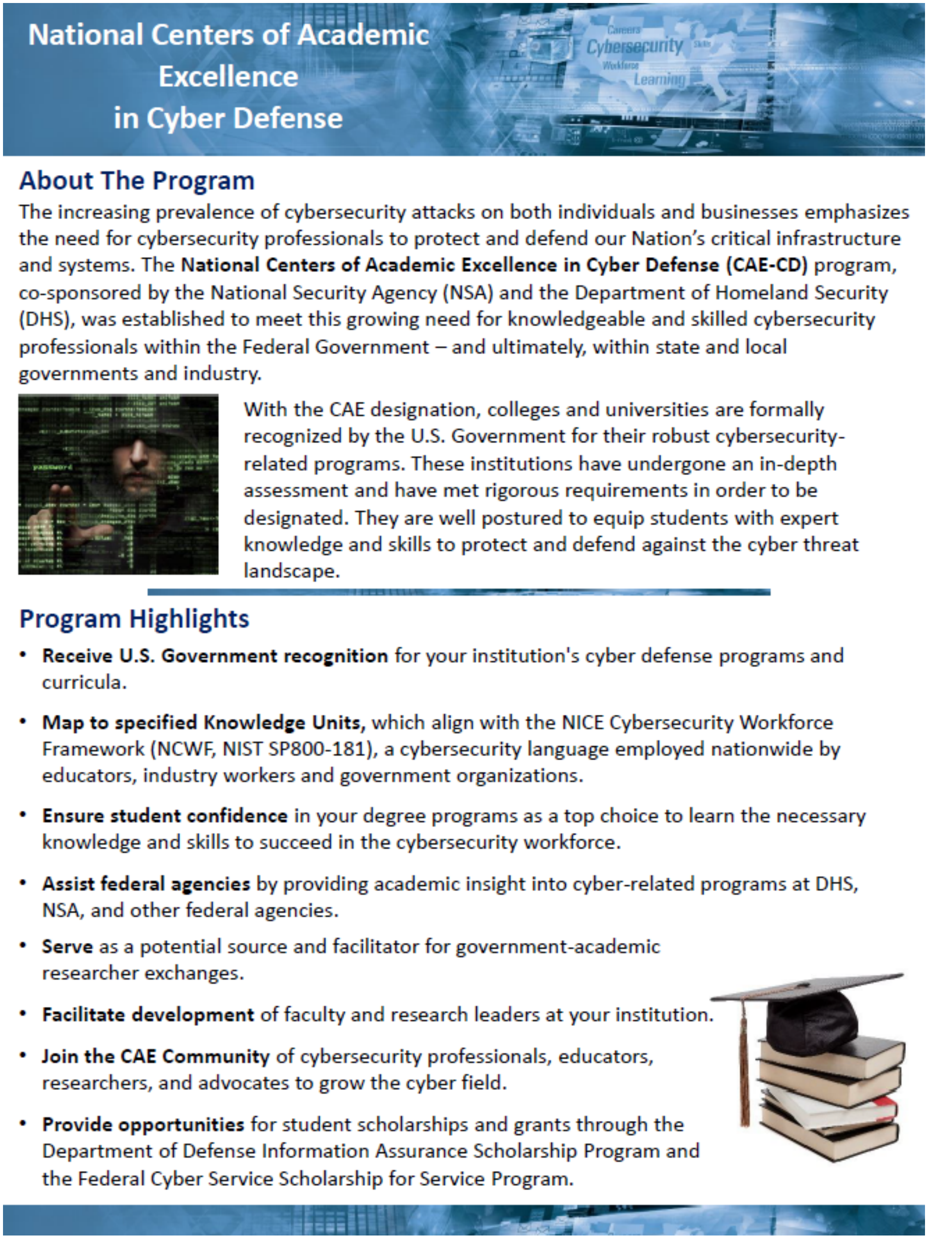
Moving forward, the cyber-security team would ideally like to have staff on duty every day to monitor and compare threat data ... but that is still a work in progress.

"Our duty is to defend the citizenry of our state and that's not just during a flood or combat situation - this is the new frontier. It's active threat and not getting better anytime soon," McRee said.

APPENDIX 3 (pp 26-27)

EXAMPLE GOVERNMENT COLLABORATION

National Centers of Academic Excellence in Cyber Defense



Careers
Cybersecurity
Skills
Workforce
Learning

National Centers of Academic Excellence in Cyber Defense

About The Program

The increasing prevalence of cybersecurity attacks on both individuals and businesses emphasizes the need for cybersecurity professionals to protect and defend our Nation's critical infrastructure and systems. The **National Centers of Academic Excellence in Cyber Defense (CAE-CD)** program, co-sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS), was established to meet this growing need for knowledgeable and skilled cybersecurity professionals within the Federal Government – and ultimately, within state and local governments and industry.

With the CAE designation, colleges and universities are formally recognized by the U.S. Government for their robust cybersecurity-related programs. These institutions have undergone an in-depth assessment and have met rigorous requirements in order to be designated. They are well postured to equip students with expert knowledge and skills to protect and defend against the cyber threat landscape.

Program Highlights

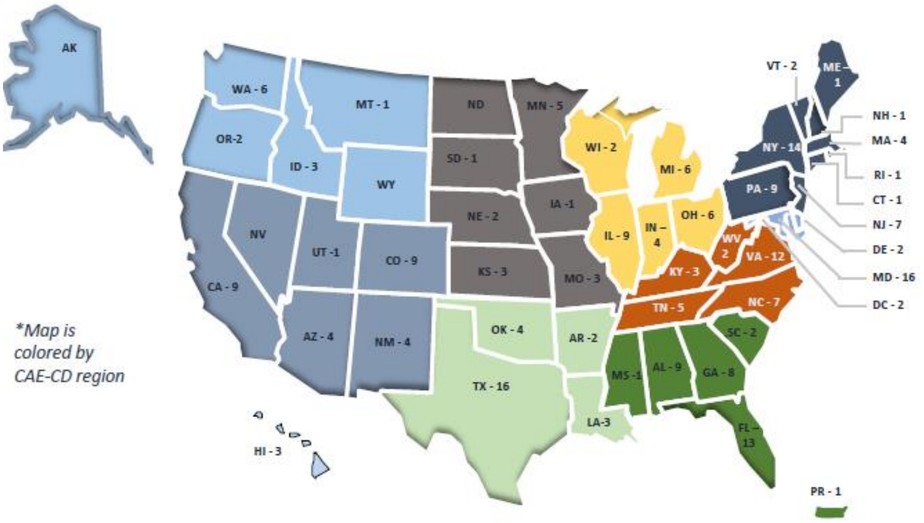
- **Receive U.S. Government recognition** for your institution's cyber defense programs and curricula.
- **Map to specified Knowledge Units,** which align with the NICE Cybersecurity Workforce Framework (NCWF, NIST SP800-181), a cybersecurity language employed nationwide by educators, industry workers and government organizations.
- **Ensure student confidence** in your degree programs as a top choice to learn the necessary knowledge and skills to succeed in the cybersecurity workforce.
- **Assist federal agencies** by providing academic insight into cyber-related programs at DHS, NSA, and other federal agencies.
- **Serve** as a potential source and facilitator for government-academic researcher exchanges.
- **Facilitate development** of faculty and research leaders at your institution.
- **Join the CAE Community** of cybersecurity professionals, educators, researchers, and advocates to grow the cyber field.
- **Provide opportunities** for student scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program.

National Centers of Academic Excellence in Cyber Defense

Eligibility

All regionally accredited two-year, four-year, and graduate-level institutions in the United States can apply for designation as a NSA/DHS CAE-CD. CAE designation is valid for five academic years, after which the school must successfully reapply in order to retain its CAE-CD designation.

CAE-CD Institutions



**Map is colored by CAE-CD region*

232 Total Institutions

In 46 states + District of Columbia & Commonwealth of Puerto Rico

More Information

Visit www.iad.gov/NIETP for more details on how to apply, download the available tools, and submit your institution's application.

Questions? Email AskCAEIAE@nsa.gov

For a full list of schools, visit: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm