

A Report by a Panel of the
NATIONAL ACADEMY OF PUBLIC ADMINISTRATION
For the Center for Internet Security and Deloitte & Touche LLP



Increasing the Effectiveness of the Federal Role in Cybersecurity Education



October 2015

ABOUT THE ACADEMY

The National Academy of Public Administration is an independent, non-profit, and non-partisan organization established in 1967 and chartered by Congress in 1984. It provides expert advice to government leaders in building more effective, efficient, accountable, and transparent organizations. To carry out this mission, the Academy draws on the knowledge and experience of its over 800 Fellows—including former cabinet officers, Members of Congress, governors, mayors, and state legislators, as well as prominent scholars, business executives, and public administrators. The Academy helps public institutions address their most critical governance and management challenges through in-depth studies and analyses, advisory services and technical assistance, Congressional testimony, forums and conferences, and online stakeholder engagement. Learn more about the Academy and its work at www.NAPAwash.org.

COVER IMAGES CREDITS

Top row, left to right:

https://www.iti.illinois.edu/sites/default/files/Cybersecurity_image.jpg

<http://robertsiciliano.com/wp-content/uploads/2013/12/3D.jpg>

<http://www.capitalfm.co.ke/lifestyle/files/2014/10/Hackers-2.jpg>

Bottom row, left to right:

<https://ceng.calpoly.edu/features/cal-poly-announces-major-new-initiative-in-cybersecurity-education/>

<http://cdn.nextgov.com/media/img/upload/2013/09/18/cyber02/nextgov-medium.jpg>

<https://www.quanterion.com/projects/critical-infrastructure/>

A Report by a Panel of the

**NATIONAL ACADEMY OF
PUBLIC ADMINISTRATION**

For the Center for Internet Security¹ and Deloitte & Touche LLP

August 2015

**Increasing the Effectiveness of the Federal
Role in
Cybersecurity Education**

PANEL

David Wennergren* *Chair*

Ramon Barquin *

Shelley Metzenbaum*

Alan Shark*

** Academy Fellow*



¹ Department of Homeland Security, HSARPA, Cyber Security Division, September 2015. This material is based on research sponsored by Air Force Research Laboratory under agreement number FA8750-12-2-0120. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

Officers of the Academy

Robert J. Shea, *Chair of the Board*
Nancy R. Kingsbury, *Vice Chair*
Dan G. Blair, *President and Chief Executive Officer*
B. J. Reed, *Secretary*
Sallyanne Harper, *Treasurer*

Study Team

Joseph P. Mitchell, III, *Director of Project Development*
Joseph Tasker, Jr., *Project Director*
Karen S. Evans, *Senior Advisor*
Franklin S. Reeder, *Senior Advisor*
Harrison Redoglia, *Research Associate*

The views expressed in this report are those of the Panel. They do not necessarily reflect the views of the Academy or Deloitte and Touche LLP.

National Academy of Public Administration
1600 K Street, N.W.
Suite 400
Washington, DC 20006
www.napawash.org

As used in this document, “Deloitte Advisory” means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

September 2015
Printed in the United States of America
Academy Project Number: 2244

Foreword

The Internet's vulnerabilities were first exposed nearly three decades ago, in 1988, when a Cornell University graduate student distributed one of the first computer worms. The Morris Worm, named for its creator Robert Morris, rendered 6,000 computers unusable and generated up to \$1 million in damages. While Morris was eventually tried and convicted of violating the Computer Fraud and Abuse Act, his actions brought to light a new type of vulnerability from which federal agencies are now expected to protect themselves and the nation.

In 2015, our critical infrastructure and day-to-day operations are more than ever tied to the Internet. And with connectivity come increasing threats from malicious hackers and criminals who attack banks, power grids, schools, health records, credit cards, and defense capabilities. In 2013, hackers successfully stole 40 million credit card records from Target shoppers, and as recently as June, it was revealed that the files of millions of federal employees stored at OPM had been breached. Each year, the federal government spends billions of dollars to combat the ever-growing threat, but, as evidenced by the recent cyberattacks reportedly linked to nation states, each year the threat becomes more serious.

Such events have brought cybersecurity to the forefront of the government agenda. Implementing plans to strengthen our law enforcement, intelligence, and defense capabilities as they relate to cybersecurity will require that the nation remedy its current shortage of qualified cybersecurity professionals in both the government and private sector workforce. To address this issue, the Academy conducted an assessment of the National Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE) and the CyberCorps®: Scholarship for Service (SFS) program to recommend ways to enhance the federal role in cybersecurity education, as well as strengthen the ability of students and employers, both public and private, to make informed decisions about cybersecurity education and professional development. The Academy Panel made recommendations to support the federal government in furthering its development of a cadre of competent cybersecurity professionals.

I am pleased that the Academy has had the opportunity to conduct this review. I thank our funders, Deloitte & Touche LLP and the Center for Internet Security; those in the CAE and cybersecurity community who provided us with information pertinent to our study; the members of the Academy Panel, who provided invaluable expertise and thoughtful analysis throughout to this undertaking, and the professional study team who provided critical support throughout this project.

Dan G. Blair, President and CEO
National Academy of Public Administration

Contents

Foreword	i
Executive Summary	1
Section 1: Cyber Threats and Cyber Education—An Introduction to the Study	4
A. The Federal Effort to Promote Cybersecurity Education.....	5
B. The Study	7
Section 2: Background on the Cybersecurity Workforce.....	10
Section 3: Background on the National Centers of Academic Excellence	12
A. The CAE Designation Process.....	12
B. Revision of the Program: The Current Value of a CAE Designation.....	14
Section 4: Background on the CyberCorps®: Scholarship for Service Program	17
A. Scholarship Track.....	17
B. Capacity Track	19
C. Program Evaluation for Both Tracks.....	20
Section 5: Findings and Recommendations.....	22
A. Observations to Help Distinguish Between the CAE and SFS Programs	22
B. The Panel Recommendations	23
Summary of Panel Recommendations	34
Appendix A – Participating Individuals and Organizations	35
Appendix B – Panel and Staff	37
Appendix C – Illustrative Core Knowledge Units	39
Appendix D – The NICE Workforce Framework	41
Appendix E – Letter from Sen. Carper (D-DE) Endorsing this Study	42

Executive Summary

The nation's critical infrastructure is increasingly reliant on information technology, while cyberattacks continue to get worse. A well-trained cybersecurity workforce is essential to both government and private industry. With cyber threats growing, however, the United States faces a severe shortage of properly trained and equipped cybersecurity professionals.

Two programs that seek to enhance cybersecurity education at the nation's colleges and universities are at the center of the federal effort to alleviate the shortage: The National Centers of Academic Excellence in Information Assurance/Cyber Defense (CAEs), a program managed by the National Security Agency (NSA) and the Department of Homeland Security (DHS), and the CyberCorps®: Scholarship for Service (SFS) program managed by the National Science Foundation (NSF). The CAE designation was created to promote higher education in information assurance, with the expectation that it would ultimately result in a greater number of highly skilled cybersecurity professionals. The NSF program was introduced in 2001 to alleviate the shortage in the federal cybersecurity workforce by offering scholarships to students in return for commitments to work in the federal sector after graduation. The NSF program also offers capacity building grants to participating schools for additional faculty, facilities and research projects.

After reviewing the features and operation of both programs, conducting an extensive literature review and a large number of interviews with program administrators, participants, academic specialists and cybersecurity experts in both the private and public sectors, the Panel formulated four major recommendations for improving the CAE and SFS programs:

1. Strengthen the hands-on education component in both the CAE and SFS programs.
2. Identify, track, and use performance indicators for both the CAE and SFS programs.
 - a) Collect information on graduates of CAE programs to enhance evaluation, improvement, and selection of graduates and schools
 - b) Develop and test to the "outcomes" features of Knowledge Units (KUs) and make results available (anonymously) to inform choice and encourage continuous improvement; consider competitions and challenges as hands-on testing environments; and
 - c) Test to scenarios or incident responses in addition to KU outcomes
3. Expand the SFS program to address the entire public sector (federal, state, local, tribal and territorial governments) by default as opposed to special permission and include qualified two-year programs regardless of their association with a four-year institution.
4. Emphasize to the Department of Defense (DOD) senior leadership, including the Secretary of Defense, the importance of the CAE program for growing the federal cybersecurity workforce.
 - a) Develop Knowledge Units (KUs) that recognize the multidisciplinary, multifaceted approach needed in the cybersecurity workforce;
 - b) Map the KUs to the *National Initiative for Cybersecurity Education (NICE) Workforce Framework* and use the framework as an alternative basis for CAE designation

- c) Make future new and renewed CAE designation contingent on a commitment to participate in testing and evaluation of student performance and sharing the data to support school improvement efforts beyond the individual school and employer and student choices;
- d) Require each CAE to align itself with at least one *NICE Workforce Framework* Specialty Area in order to support more valid comparisons to inform employer and student choices and school improvement effort; and
- e) Reinststate the Information Assurance Scholarship Program (IASP) funding for scholarships and capacity building grants for the DOD workforce.

This page is intentionally left blank

Section 1: Cyber Threats and Cyber Education—An Introduction to the Study

There can be no doubt that cyberattacks against United States interests are substantial, severe and continuing to get worse.² The revelations in early July of 2015 that cyber-thieves had stolen security clearance information (wide-ranging highly personal data) on 21.5 million federal employees, contractors, applicants and family members, are bleak confirmation of this.³ This revelation was on top of the 4.2 million pilfered files OPM announced June 4, 2014 involving another breach of federal personnel records.

The threats and attacks affect all aspects of society, business, and government, and they continue to grow as the nation becomes ever more dependent on information technology in every sector of the economy. It is estimated that cyberattacks cost the economy \$400 billion every year.⁴ The threat to national security may be harder to quantify but is potentially more severe.⁵ Nevertheless, there continues to be a shortage of cyber experts working to repel these threats, both inside and outside of government.

The shortage is compounded both by the continuing increase in the total number of cyberattacks and the constantly evolving nature of the threat landscape. The proliferation of cyber threats—such as spear-phishing; the exploitation of zero-day vulnerabilities; the growing base of mobile devices that need to be secured; and the recognition that the emerging Internet of Things increases potential avenues of cyberattack—poses a great challenge for those tasked with defending the networks. Each new threat may require the development of a new set of skills and a new set of responses. As cybersecurity professionals develop, master, and teach the skills necessary to combat one type of cyberattack, those who attack our systems, whether they are our nation’s enemies or simply criminals seeking to profit by exploiting our vulnerabilities, are hard at work putting together new methods for infiltrating our computer systems. While part of the strategy is the development of more robust, resilient technology, developing a workforce that can protect and defend our cyber infrastructure must continue to be a priority.

² According to one recent study, “research found that the number of detected information security incidents has risen 66% year over year since 2009. In the 2014 survey, the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48% from 2013 – an average of 117,339 per day.”

<http://www.cgma.org/magazine/news/pages/201411089.aspx> citing the *Global State of Information Security Survey 2015*, Price Waterhouse Coopers, <http://www.pwc.com/gsis2015>

Similarly, the head of DARPA’s software innovation division said in a televised interview this February that cyberattacks against the U.S. military are increasing in frequency and sophistication. Saying that cyberattacks are “occurring every day”, he noted that the “number of attacks is dramatically increasing” and the “sophistication of the attacks” is increasing as well. *DARPA: Cyberattacks against US military ‘dramatically increasing’ (February 28, 2015)*; <http://thehill.com/policy/cybersecurity/232122-darpa-official-cyberattacks-against-us-military-dramatically-increasing>

See also e.g., Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency* (December 2008)

http://csis.org/files/media/isis/pubs/081208_securingcyberspace_44.pdf

³ See, e.g., [http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/new-opm-data-breach-numbers-leave-federal-employees-anguished-outraged/\(July 9, 2015\)](http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/new-opm-data-breach-numbers-leave-federal-employees-anguished-outraged/(July%209,%202015))

⁴ *Net Losses: Estimating the Global Cost of Cybercrime*. Joint report by McAfee and the Center for Strategic and International Studies, June 2014. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>. See also “Lloyd’s CEO: Cyber attacks cost companies \$400 billion every year”, <http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>. In this article, the CEO of Lloyds of London, the insurance giant, offered the same estimate to the World Economic Forum.

⁵ “Attacks against us are increasing in frequency, scale, sophistication and severity of impact. Although we must be prepared for a catastrophic, large-scale strike . . . the reality is that we’ve been living with a constant and expanding barrage of cyber attacks for some time.” Remarks of James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment Hearing, Senate Armed Services Committee (February 26, 2015);

<http://www.dni.gov/files/documents/2015%20WWTA%20As%20Delivered%20DNI%20Oral%20Statement.pdf>

The ever-shifting threat landscape poses a daunting task for the institutions responsible for preparing students for successful and effective careers in cybersecurity. It is difficult to settle on a core set of knowledge, skills, and abilities to address a threat that continues to change at such a rapid pace. What is needed is an educational system that is agile—able to continuously adapt and improve to understand, meet, and overcome the latest threats.

A. The Federal Effort to Promote Cybersecurity Education

In order to respond to this need, a large number of the nation’s colleges (both two-year community colleges and four-year schools) and universities now offer courses and programs in cybersecurity. Some offer just a few courses, while others offer an entire concentration or even one or more majors. The academic departments where these courses are offered vary. Computer science and electrical engineering degrees often feature concentrations in cybersecurity. Business school degrees in Business and Management IT (at the bachelor’s degree level) and MBAs with concentrations in information security administration are also becoming more common. Other schools offer interdisciplinary degrees such as “MS in Information System Security” or sector-specific programs such as degrees with a focus on cybersecurity in the health care sector.

The federal effort to support and enhance cybersecurity education takes several forms, two of which are the focus of this study: NSA/DHS designation of the National Centers of Academic Excellence in Information Assurance/Cyber Defense at participating colleges and universities; and operation of a scholarship and grants program called the CyberCorps®: Scholarship for Service (SFS) program, administered by the National Science Foundation (NSF).⁶

1. National Centers of Academic Excellence in Information Assurance/Cyber Defense

As part of the response to the need for improved cybersecurity education and training, NSA established a program in 1998 under which a number of America’s colleges and universities have been granted a designation known as a Center of Academic Excellence in Information Assurance/Cyber Defense (CAE).⁷ As discussed in greater detail in the sections that follow, the CAEs have grown from seven when the program was launched in 1999⁸ to 199 in 2015. The CAE designation is granted to schools that apply and meet certain specific criteria established

⁶ These are two of the primary federal programs involved in cybersecurity education efforts, but they are not the only ones. Another is an additional scholarship/grant program known as the Information Assurance Scholarship Program (IASP), established by the National Defense Authorization Act of 2001 and administered by the Department of Defense. This program will also be discussed in the course of this report.

NSF also has grant programs focused on “Secure and Trustworthy Cyberspace” (research grants combining cybersecurity and research on student learning) and “Advanced Technological Education”, focused community college education of technicians in high tech fields. See Hovis, *NSF Funding Opportunities for Cybersecurity Education and Workforce Development*, presentation by NSF Program Director, Advanced Technological Education, http://cybersummit.memphis.edu/presentations/Corby_Hovis.pdf DHS also operates an unpaid internship program for undergraduate students in cybersecurity studies at various locations around the country. See Secretary Honors Program Cyber Student Volunteer Initiative. <http://www.dhs.gov/homeland-security-careers/students>

⁷ When the program was announced in 1999, CAEs were known as National Centers of Academic Excellence in Information Assurance Education (CAE/IAE). The name was officially changed in 2013 to CAE-IA/CD as part of the program’s renovation described in section 3 of this report.

⁸ “NSA Designates First National Centers Of Academic Excellence in Information Assurance Education” (NSA press release), https://www.nsa.gov/public_info/press_room/1999/nsa_academic_exc.shtml

by NSA and DHS.⁹ In addition to attempting to increase the student population studying cybersecurity, the program is intended to increase the number of schools where cybersecurity education can become the focus of coursework and degree programs. It is also intended to expand the faculty with teaching experience and bring more graduating students into the workforce in both in the private and public sectors (and eventually more PhDs with a cyber-concentration into the faculties of the schools). As NSA and DHS put it: “The purpose of the National CAE designation program is to promote higher education in IA and CD and prepare a growing number of IA/CD professionals to meet the need to reduce vulnerabilities in the Nation’s networks.”¹⁰

The CAE designated schools currently receive no federal funds for scholarships or capacity-building grants directly from the program. The NSA and DHS program offices are operated with appropriated funds in those agencies’ budgets, but the program offers no direct federal financial support for CAE designated institutions of higher learning. A scholarship and grants program was authorized in 2001 and is specifically for the CAE program—The Information Assurance Scholarship Program, or IASP.¹¹ It was intended to provide capacity-building grants to CAE-designated schools as well as scholarships to qualified students attending those schools who can pay off their scholarship with equivalent service working in a job at the Department of Defense, but the IASP is not currently being funded by DOD.¹²

2. The CyberCorps®: Scholarship for Service (SFS) Program

The CyberCorps®: SFS program is an interagency program for scholarships and grants to colleges and universities, administered by the NSF with cooperation from DHS, NSA and the Office of Personnel Management (OPM); it has been operating since 2001.¹³ According to the NSF, the SFS program is designed to increase and strengthen the cadre of federal information assurance professionals that protect the government’s critical information infrastructure. It supplies grants to schools for student scholarships. Grants are administered by the receiving school and the school takes responsibility for awarding scholarships to students. The students are required to find employment (including an internship) in the public sector upon graduation, to keep the scholarship from turning into a loan that has to be repaid to the government. As of FY 2010 (latest available data), the government placement rate was above 93%, according to NSF.¹⁴ The SFS program provides additional grants to the participating

⁹ The CAE designation process is described in detail later in this report.

¹⁰ https://www.nsa.gov/ia/academic_outreach/nat_cae/

¹¹ Described in some detail later in this report. See text at footnotes 85 - 88

¹² Interviewees reported that, as of June 2014, the DOD IASP funding provided by DOD CIO was to be phased out at a rate that would ensure current scholarship students would complete their studies and graduate. The DOD Components (e.g., NSA, Army, Navy) were expected to fund any future IASP scholarships. As discussed later in this report, the Panel supports reinstating full funding at the earliest opportunity. It would be highly regrettable for this program to remain unfunded, in light of the ongoing needs for more cybersecurity professionals at the Department and elsewhere.

¹³ See generally <https://www.sfs.opm.gov/>; and https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991

¹⁴ <http://cisse.info/resources/archives/category/26-keynote-presentations?download=257:national-science-foundation-programs-supporting-cybersecurity-education-and-workforce-development> ; see also C. Hovis, “National Science Foundation Funding Opportunities for Cybersecurity Education and Workforce Development”, http://cyberexpo.memphis.edu/2014/presentations/Corby_Hovis.pdf

colleges and universities to improve their cybersecurity education programs, including capacity-building in academic departments (facilities, professors, and so on). These capacity-building grants in recent years have ranged from \$300,000 to \$900,000, ranging from one to three years in length¹⁵ The grants are renewable if NSF approves an acceptable renewal grant application which includes a review of the past use of funds. The program was recently reaffirmed by Congress in the Cybersecurity Enhancement Act of 2014.¹⁶ The Director of NSF is charged with determining the “eligible degree programs” and the “qualifications” a college or university must meet to participate in the program.¹⁷

B. The Study

The gap between workforce needs and available graduating students persists. Demand for cybersecurity professionals at all levels is increasing more rapidly than supply as cyber threats continue to grow at an alarming pace and cyber employment demand extends to more and more sectors of the economy, especially in some of the most critical job groups.¹⁸ Even as the CAE and SFS programs grow and produce more graduates, the question becomes whether the education system in general—and the federal CAE and SFS programs, in particular—are producing graduates with the requisite skills and expertise and have an appropriate focus.

This is a critical time in the development of the CAEs, and their future role in cybersecurity education is not altogether clear. The basis for CAE designation has changed in the last few years and is continuing to evolve to meet workforce needs. New features are being added to differentiate the Centers.

At the same time, there is little systematic information about the differences in focus and performance of the schools participating in the CAE program to guide the hiring decisions of employers, the educational decisions of students, the investment decisions of government agencies, and the curriculum decisions of educational institutions.

And, there is confusion over the distinct but to some extent overlapping features of the CAE program and the SFS program. Until 2008, status as a CAE was an eligibility prerequisite for the SFS program for schools to receive grants for capacity building and scholarships. The requirement that schools participating in the SFS program be designated as CAEs has recently been dropped. Still, schools need to qualify by providing “clearly documented evidence of a strong existing academic program in cybersecurity.”¹⁹ That evidence may include a CAE designation, but NSF points out that “equivalent evidence” documenting a strong program in

¹⁵ C. Hovis, “National Science Foundation Funding Opportunities for Cybersecurity Education and Workforce Development” presentation by NSF Program Director, Advanced Technological Education, http://cybersummit.memphis.edu/presentations/Corby_Hovis.pdf

¹⁶ See Section 302 of Public Law 113-274, enacted December 18, 2014, <http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf>

¹⁷ Id., Section 302(f)(4). The qualifications and eligibility criteria are discussed at some length in Section 3 of this report.

¹⁸ Please see Figure 1 on page 11 of this report, which shows the different job groupings involved in the cybersecurity workforce, and underscores the fact that this is a multifaceted workforce involving many different skill sets.

¹⁹ https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991&org=EHR&from=home

cybersecurity is also acceptable.²⁰ Nevertheless, it appears that every school participating in the SFS program in 2015 is in fact a CAE.

The Center for Internet Security (CIS)²¹ and Deloitte & Touche LLP determined that an independent study by the National Academy of Public Administration (the Academy) should be undertaken to:

1. Assess the role and effectiveness of the CAE program;
2. Identify ways to ensure continuous improvement in the CAE program;
3. Assess the role of the SFS program and attempt to reduce the confusion between that program and the CAE program; and
4. Help to inform student and employer choice.

To that end, the study was to consider useful performance indicators designed to improve CAEs and inform student selection of CAEs and government selection of CAE graduates. These considerations would apply to CAE designated schools whether or not they participate in the SFS program. Also, the study would compare the roles played by the CAE and SFS programs and make recommendations about how they should be focused for maximum impact.

Under the leadership of an Academy Panel, the study team conducted an extensive literature review of the subject and interviewed a number of the participants in the CAE and SFS programs, including government agency administrators, CAE participants, and other members of the academic community, as well as cybersecurity leaders in private industry.

Section two of this report provides a brief background on the multifaceted nature of the cybersecurity workforce.

Section three provides additional background on the evolution of the CAE program and the context for the recommendations that follow.

Section four provides additional background on the development and operation of the SFS program and the context for the recommendations that follow.

Section five describes the Panel's key findings and recommendations regarding the CAE and SFS programs.

Appendix A identifies the individuals and organizations interviewed for the study.

Appendix B provides brief biographies of the Academy Panel of Experts and the study team.

Appendix C provides two illustrative "Knowledge Units" for the CAE program to facilitate the discussion of its emerging structure and recommended continuing improvements.

²⁰ Id.

²¹ The study was initially sponsored by the Council on Cybersecurity, which, as of January 1, 2015, merged with the Center for Internet Security. The merged entity continues in operation as the Center for Internet Security.

Appendix D is a graphic representation of the *National Initiative for Cybersecurity Education Workforce Framework*, referred to as the *NICE Workforce Framework*²² which is referenced at several points in the report.

Appendix E is a copy of a letter from Sen. Tom Carper (D-DE) requesting that agencies cooperate with us regarding this study.

²² See <http://csrc.nist.gov/nice/workforce.html>

Section 2: Background on the Cybersecurity Workforce

The shortage of cybersecurity professionals has been studied before. This study relies on that earlier work for its understanding of the nature of the cybersecurity workforce. One such recent report observed:

The problem is both of quantity and quality especially when it comes to highly skilled...professionals. [The United States] not only [has] a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts.²³

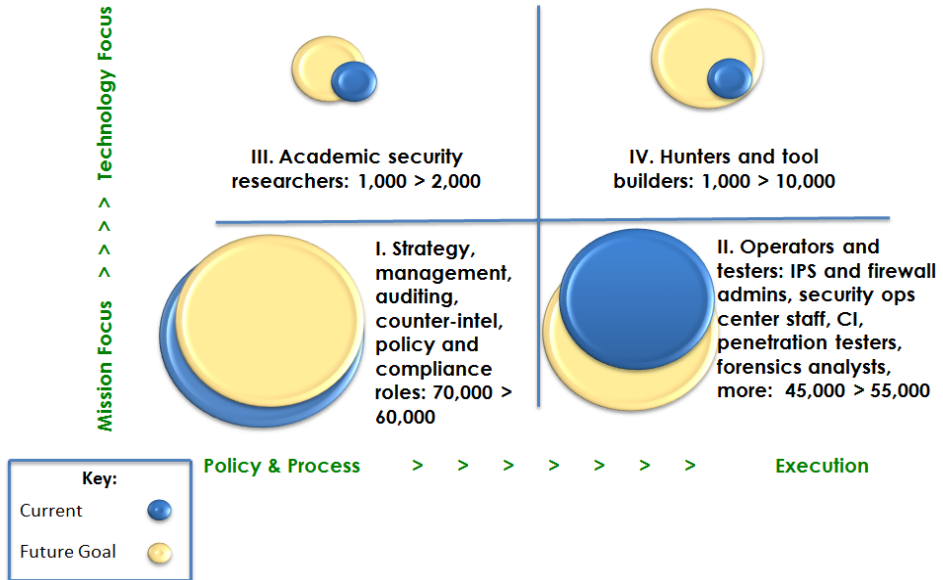
It has become clear in recent years that the cyber security workforce needs are multifaceted and varied. Many types of skills are needed. While some identifiable job groups have long been established and the needs for technical expertise are great, not all needed job categories are wholly or even primarily technical. Moreover, even in the technical fields, every graduate needs to master problem solving and critical thinking. One recent presentation graphs the job groups this way:²⁴

²³ Center for Strategic and International Studies, *A Human Capital Crisis in Cybersecurity* at 2 (Washington, 2010) available at http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkwhteVersion.pdf

²⁴ "US Cyber Challenge", Presentation by Karen S. Evans at the DHS 2014 Cyber Security Division R&D Showcase (2014), data drawn from CSIS, "A Human Capital Crisis in CyberSecurity", supra note 18.

Figure 1: Supply and Demand in Cyber Security Job Groups

Supply & Demand in Cyber Security Job Groups



Section 3: Background on the National Centers of Academic Excellence

A. The CAE Designation Process

The CAE program was created by the NSA in 1998, with the first group of seven educational institutions designated in 1999.²⁵ DHS became a formal partner in the program in 2004. As of July 1, 2015, there were 199 colleges and universities with CAE designations. There are three distinct designations, including Center of Academic Excellence in Cyber Defense, Two-Year (CAE-2Y), Center of Academic Excellence in Information Assurance/Cyber Defense (CAE-IA/CD), or Center of Academic Excellence in Cyber Defense Research (CAE-R). Forty of the 199 institutions carry dual designations as both CAE-IA/CD and CAE-R.

Table 1: CAE Designations in 2015²⁶

CAE Category	Description	Number of schools
CAE-2Y	Two-year community colleges ²⁷	40
CAE-IA/CD	Information Assurance/Cyber Defense	135
CAE-R	Research (graduate studies and research emphasis)	24
CAE-IA/CD & CAE-R	Schools granted designations as both types of CAE	24

There are no defined curricula for CAEs, nor is there a CAE degree as such. The schools designated as CAEs receive no federal funds as a result of the designation; the only appropriated funds spent by NSA and DHS go towards running the program. Designation as a CAE is based on close review of a school's entire curriculum across all subjects to determine that sufficient elements of the curriculum map to a set of CAE criteria historically established by the NSA to justify the designation as a CAE, and now established by NSA in consultation with DHS and participating schools. Additional requirements must also be met, including:

- a) A demonstrably active Information Assurance/Cyber Defense (IA/CD) academic program;
- b) Institutional commitments to:
 - i. view cyber security as a multi-disciplinary field;
 - ii. encourage the practice of IA throughout the institution;
 - iii. encourage student research in the field;
 - iv. accept specifications about faculty size and commitment to IA/CD courses; and

²⁵ The seven schools were James Madison University, George Mason University, Idaho State University, Iowa State University, Purdue University, University of California at Davis, and University of Idaho. NSA press release, supra, note 7.

²⁶ The Panel would note that the category designations in the left hand column appear to convey very little information, unless someone is already an expert in working with CAEs. The Panel encourages the CAE program administrators to consider a more descriptive system for identifying the various CAE designations so that students may better understand the focus of the program they are reviewing.

²⁷ List of schools that are CAE/2Y and CAE-IAE and CAE/R in 2015 after renewals and reviews of new applications: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

- c) A demonstration by the school of its outreach and collaboration program, described as “how IA/CD is extended beyond the normal boundaries of the Institution.”²⁸

The designation is valid for five years, and may be renewed upon application and a new review of curriculum based on then-current CAE criteria. CAE designation is generally featured on college/university departmental websites (although only rarely on an institution’s home page). Schools may, but are not required to, recognize students that graduate from a CAE-designated school. The method of recognition, however, is left up to each school and may vary.

Until 2013, to be designated as a CAE, an institution of higher education had to demonstrate that it could map course content to two of the six national training standards set by the Committee on National Security Systems (CNSS), a committee established by Executive Order and chaired by the Department of Defense.²⁹ The result was then reviewed by the Information Assurance Courseware Evaluation Program (IACE) at NSA. The core knowledge that schools were required to cover was drawn primarily from the CNSS 4011 standard, a national training standard for Information Systems Security (INFOSEC) professionals, which includes information considered to be basic to gaining knowledge about information security.³⁰ Institutions then chose one of the five remaining standards to map their course content. Once this prerequisite was completed, the school had to meet the CAE designation criteria, just as is the case today, as discussed in the preceding paragraphs.

Some criticized the CNSS standards—which were designed for and in fact used as training standards for federal INFOSEC personnel—as too narrowly focused on technical training skills in a post-secondary school education environment. According to one commentator, the 4011 Standard failed to emphasize the “fundamental understanding of principles and concepts,” and how to apply them to specific situations.³¹ Only two of its seven subject categories, for example, require students to do more than list and give examples of the facts about telecommunications and computer networking that they have learned.³² There is often a logical tension between the objectives and mission of an academic institution and a program that is intended to focus on workforce development. Nevertheless, the CNSS standards were seen by the CAE program founders as a way for the program to get started quickly in the face of newly identified needs for more cyber security education in America’s colleges and universities.

²⁸ *National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD) Education Program Criteria for Measurement*, <https://www.iad.gov/nietp/index.cfm> A definition of the “normal boundaries of the institution” could not be found.

²⁹ There may have been some professors involved in promulgating the CNSS standards, but no one argues that they were created with the CAE program in mind or developed in consultation with any colleges and universities.

³⁰ The CNSS 4011 standard, originally known as an NSTISS standard, can be found at <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>. It was developed in 1994 by the National Security Telecommunications and Information Systems Security Committee (NSTISS), a government committee working with a few university professors who were teaching computer security courses at the time. NSTISS is the predecessor of CNSS. The standard was the first of several standards, albeit with a training focus, that educators could use as a guideline for developing information assurance curricula. Altogether, six standards – numbers 4011 through 4016 of the NSTISS series – were involved in creating the CAE designation criteria.

³¹ “A Critical Analysis of the Centers of Academic Excellence Program.” Proceedings of the 13th Colloquium for Information Systems Security Education (2009)

³² The two categories include “build a security plan . . . for an instructor-supplied description of an information and telecommunications system” (item (f)) and “play the role of either a system penetrator or system protector to discover points of exploitation and apply appropriate countermeasures in an instructor-supplied description of an Agency information system.” (item (g)). Agency information systems, as defined in the standard, include both telecommunications and information technology systems.

Some of the CNSS standards have been updated since the 1990s. The 4011 standard has not. In recent years, the standards used for CAE review have become outdated and potentially could impede efforts to update curriculum to address changing cybersecurity needs. For example, while the 4011 Standard requires teaching a broad range of networking information, much of it simply covers background information on networking technology of 20 years ago. More specifically, many types of modern cyber-attacks emerged after the standard was published, like network-borne malware and botnets. The standard also predates widespread use of firewalls and Secure Socket Layer (SSL) encryption to protect network traffic. School curricula generally have kept up to date with modern developments, but one author's report on his successful but extensive efforts (over 5 years) to certify a college textbook on cybersecurity for undergraduates under Standard 4011 gives some indication of the difficulties of using the standard in today's world to teach the subject, much less designate a college curriculum for a CAE.³³

He concludes his report this way:

Although a textbook could be written that focuses exclusively on NSTISSI 4011 topics, such a textbook would be instantly out of date. The textbook described [in this report] incorporates more general and up-to-date topics taken from the IT 2008 curriculum recommendations produced by the ACM and IEEE. This may have increased the textbook's length, but it also makes the textbook relevant to today's students while it complies with the eighteen-year-old training standard.³⁴

B. Revision of the Program: The Current Value of a CAE Designation

Concerns about the CAE program have been raised several times over the years. For example, consider this critique from a report of a workshop in 2010:

The CAE/IAE designation lacks solid prestige. Granting CAE status to so many institutions has diluted the cachet of the label, and private-sector employers don't see CAE as a meaningful credential. Some of the country's most prestigious universities that produce technically accomplished graduates with computer security knowledge are not CAEs. Historically, universities have selectively applied for designation such as "CAE" on the basis of their goals and aspirations, internal competencies, target student audiences, and budgets. Because university departments have not traditionally taught courses geared toward standards such as those that CAEs are required to teach, it is not surprising that many fine universities have not applied to become CAEs. Even among CAEs, there is no independent mechanism for validating outcomes or results, so it is not clear to what extent grant-receiving institutions actually teach to the required standards.³⁵

³³ Smith, R.E., "Certifying a Textbook Under NSTISSI 4011", Proceedings of the 16th Colloquium for Information Systems Security Education at 142-148 (2012)

³⁴ Id at 148.

³⁵ Hoffman, L.J., "Building the Cyber Security Workforce of the 21st Century: report of a Workshop on Cyber Security Education and Workforce Development" (George Washington University 2010), http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/553e7cefe4b0dba62911e197/1430158575885/2010-3a_building_the_cyber_security_workforce_of_the_21st_century.pdf

This kind of critique has given impetus to a substantial revision of the CAE program. Since 2013, the program has been in the process of updating the academic standards to move away from the federal technical training standards on which it was originally based. It has transitioned to designation based on curriculum mapping to a system of Knowledge Units (KUs) intended to represent academic curricula as well as professional workforce needs. The history of the transition to KUs has been complex and is beyond the scope of this study. It is sufficient to say that the initial set of KUs has been established and is available for use in the CAE designation process (renewals or new applications).³⁶ Since CAE designation is for a five year period, participating institutions map to the new KU criteria as their CAE-IA/CD or CAE-2Y designation expires; CAE-R academic standards have not changed. The last of the original designations will expire in 2017.

The KU system is fairly extensive. There are eleven core KUs that every two-year CAE must meet for designation. A four-year school must meet these, and an additional six more core KUs and a minimum of five more “optional KUs” from a list of 49.³⁷ Each KU is specifically named³⁸ and has two elements: (1) a list of the topics covered by the KU³⁹ and (2) identification of the expected “outcomes” of studying the topics listed.⁴⁰ The KUs are not intended to be government-specific like the previous standards. The original KUs were developed in workshops with participation by the government and personnel from the CAE institutions and there are plans for additional workshops in the future to refine the definitions of the KUs and extend the reach of the KUs to new subjects.⁴¹ As the NSA and DHS put it on the program website, “The new CAE IA/CD designation is based on updated academic criteria for Cybersecurity education and affords each CAE institution the opportunity to distinguish its strengths in specific IA/CD focus areas. The updated criteria benefit not only the institution, but also students, employers and hiring managers throughout the Nation.”⁴²

The transition to the system of KUs has received mixed reviews from CAE participating institutions. How well does the new system relate to a more academically-friendly, less “training” oriented curriculum for the CAE program? Answers reflect the range of views about the CAE program generally. Some of those interviewed have reported that the change did little, if anything, to improve the quality and ability of the curriculum to remain up-to-date. Other interviewees, however, looked to the KUs to provide a standard of quality for the curriculum of a program that may be just starting. Still, it is worth pointing out that the KUs are seen by some as

³⁶ NSA/DHS *National Centers of Academic Excellence in Information Assurance/Cyber Defense 2014 List of Knowledge Units and Focus Areas*, <https://www.iad.gov/nietp/index.cfm>

³⁷ Id.

³⁸ E.g., “Cyber Defense”; or “Systems Administration.” See “Knowledge Units”, publication by the CAE team; <http://www.cisse.info/pdf/2014/2014%20CAE%20Knowledge%20Units.pdf> This publication notes that a school’s demonstration of meeting a specific KUs may be based on a course syllabus; prerequisite courses; prerequisite degrees; student assignments; modules in a course/collection of courses or certifications. One course may fulfill the requirements of multiple KUs.

³⁹ Appendix C of this report consists of the text of the “Cyber Defense” and “Systems Administration” Core KUs.

⁴⁰ Some “outcomes” ask for students to “describe” or “list” the information they have learned. In other cases, student outcomes include the ability to “apply” the knowledge or “use” the tool covered in the KU or take some other steps to demonstrate their understanding.

⁴¹ As noted, KU outcomes can consist of either descriptions or demonstrations or a mix of the two. The Panel hopes that in the future there will be a greater emphasis on the demonstration aspect

⁴² https://www.nsa.gov/ia/academic_outreach/nat_cae/

still describing a minimum level of cybersecurity training and education, not as indicators of something that can be recognized as academic excellence.

Thus, even with the recent revisions, there has been some question about the real value of being named a CAE. As noted earlier, the CAE designation brings with it no additional government funding to cover such costs as “administrative overhead, security research or faculty development.”⁴³ The process of obtaining and renewing a CAE designation is often described as painstaking and laborious, characterized by hours of paperwork and mapping of current courses to the NSA-approved KUs. It is perhaps, not surprising to hear—as the study team did in some of its interviews—that beyond the initial marketability of the CAE label to prospective students, and the attractiveness of the designation to some (especially two-year) schools, many interviewees thought the perceived return on investment for schools obtaining the CAE designation was rather small.⁴⁴ That said, there appears to be no diminution in the number of schools applying for or seeking to renew their CAE designation.

For students, the CAE designation is an easy way to identify schools that have a specific focus on cybersecurity education and the faculty and facilities necessary to provide a quality education. Beyond that, however, the value to the students who attend these institutions is more difficult to assess. Employers, while they might recruit specifically from CAE schools with which they have established relationships, tend to rely just as much and possibly more on universities and programs close to their facilities.

Students, if they choose to do so, should also be able to take advantage of the Information Assurance Scholarship Program (IASP), established by the National Defense Authorization Act of 2001 and administered by the Department of Defense.⁴⁵ This is a scholarship and grants program to be administered by the DOD, for the exclusive benefit of students at CAE-designated schools. Scholarships should be available in return for student acceptance of work at a position in DOD upon graduation. There is also a capacity-building grant component to the program. A recent DOD report states that:

Since its inception in 2001, the IASP has been directly tied to CAE-designated institutions. To date, the IASP has employed 593 . . . students, and has enabled CAE’s with 180 capacity-building grants.⁴⁶

The Panel understands, however, that the Department has ceased funding the program at the DOD Chief Information Officer (CIO) level. Interviewees reported that, as of June 2014, the DOD IASP funding provided by DOD CIO was to be phased out at a rate that would ensure current scholarship students would complete their studies and graduate. The DOD Components (e.g., NSA, Army, Navy) are expected to fund any future IASP scholarships. As discussed later in this report, the Panel supports reinstating full funding at the earliest opportunity. It would be highly regrettable for this program to remain unfunded, in light of the ongoing needs for more cybersecurity professionals at the Department and elsewhere.

⁴³ “A Critical Analysis of the Centers of Academic Excellence Program.” Proceedings of the 13th Colloquium for Information Systems Security Education (2009)

⁴⁴ As discussed below, CAEs that participate in the National Science Foundation’s “Cyber Corps®: Scholarship for Service” program would most likely disagree.

⁴⁵ Pub. Law 106-398, 114 Stat. 1654, Section 922 et seq. (2000)

⁴⁶ A DOD Report on the NSA and DHS program for the “National Centers of Academic Excellence in Information Assurance Education Matters, at 6; http://www.cisse.info/pdf/2015/DoD%20942%20Report%20to%20Congress_FINAL.pdf

Section 4: Background on the CyberCorps®: Scholarship for Service Program⁴⁷

The SFS program provides NSF grants to institutions of higher education that address cybersecurity education in two ways. The Scholarship Track provides funding to institutions for awarding scholarships to students in cybersecurity. In return for their scholarships, recipients are required to work after graduation for a public sector or other qualified organization in a position related to cybersecurity for a period equal to the length of the scholarship. The Capacity Track, according to NSF, provides grants to “innovative capacity-building proposals” to increase the ability of the United States higher education enterprise to produce cybersecurity professionals. To participate in the scholarship track, a school must compete for a grant and provide clearly documented evidence of a strong existing academic program in cybersecurity. Such evidence can include: designation by the NSA and DHS as a CAE—IA/CD, CAE—Cyber Operations, or CAE—Research; a specialized designation by a nationally recognized organization (for example, in forensics); or equivalent evidence documenting a strong program in cybersecurity. A CAE designation, as such, is not required.⁴⁸

The program arose out of general educational policies in support of increased attention to cybersecurity in the 1998 Presidential Decision Directive 63, *Critical Infrastructure Protection*⁴⁹ and was first presented as a concrete proposal in the President’s 2001 budget estimate for critical infrastructure protection.⁵⁰

A. Scholarship Track

The SFS program provides grants to colleges and universities for student scholarships in support of education in areas relevant to cybersecurity. Participating schools administer the scholarships. Grantee colleges and universities provide scholarship support to students who (1) compete successfully in a selection process developed by the institution, (2) meet the SFS eligibility criteria, and (3) are confirmed by OPM as qualified for public-sector employment in a cybersecurity related position. The scholarship may apply to undergraduate or graduate programs.⁵¹

In return for their scholarships, recipients must work after graduation for the federal government or, subject to approval of the NSF program office, another qualified government-related employer in a position related to cybersecurity for a period equal to the length of the scholarship. The program’s goal is 100% placement in government cybersecurity positions. While SFS student participants are responsible for their own job searches, the SFS program office, through OPM, provides tools to aid in the job search and organizes an annual job fair. SFS scholarship students are expected to participate actively with OPM to secure both a summer

⁴⁷ The following discussion summarizes information contained in the current NSF grant solicitation for this program. See generally NSF, CyberCorps® Scholarship for Service (SFS) Program Solicitation NSF 15-584 for submissions in 2015 and 2016. <http://www.nsf.gov/pubs/2015/nsf15584/nsf15584.htm>

⁴⁸ A CAE designation by NSA was required for participation before 2008.

⁴⁹ See CRS Report to Congress, *Critical Infrastructures: Background, Policy, and Implementation* (updated 2002), http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30153_02042002.pdf

⁵⁰ Id. at CRS-27.

⁵¹ The scholarship amounts are \$20,000 per year for undergraduate students and \$32,000 per year for graduate students. There are a variety of items included and excluded from the list of covered costs. See <http://www.nsf.gov/pubs/2014/nsf14586/nsf14586.htm>

internship and permanent placement in a federal, state, local or tribal government organization.⁵² A limited number of students may be placed in National Laboratories and certain Federally Funded Research and Development Centers (FFRDCs) or other “qualified” organizations approved and set by the NSF program office each year.⁵³

Students must also participate in other SFS activities such as conferences, workshops, and seminars. According to the NSF, “[t]hese activities are aimed at developing a community of practice that will enhance students’ individual and collective skills in an area increasingly important to the security of the United States.”

In keeping with the grant format of the program, each SFS program school is required to name a Principal Investigator (PI), who has overall responsibility for the administration of the institution’s award, the management of the project, and interactions with NSF and OPM. According to NSF, “[t]he PI and the grantee institution are expected to have or to develop an administrative structure that enables faculty, academic administrators, scholarship recipients, and others involved in the project to interact productively during the award period. The PI is expected to be an integral participant in the educational activities of the SFS project and is required to participate in boot camps, job fairs, symposia and other SFS-sponsored activities.” The SFS program requires much more of its participating schools than simply the award of scholarships with grant funds by the school’s Office of Financial Aid.

NSF reports that OPM partners with it in this program by providing internship and placement assistance to SFS scholarship students, by coordinating students’ transition into government employment, by tracking students’ compliance in the workforce with program requirements, and by assessing whether the program helps meet the personnel needs of the federal government for information infrastructure protection. The student recipients also take on an affirmative obligation to participate in job tracking efforts and the program evaluation surveys.

To be eligible for consideration for an SFS scholarship, a student must be a citizen or lawful permanent resident of the United States. In addition, a student must be one of the following:

- a) a full-time student within three years of graduation with a bachelor’s or master’s degree in a coherent formal program that is focused on cybersecurity at an awardee institution; or
- b) a research-based doctoral student.

Students in their second year of a two-year program at community colleges are eligible for one year of support if there is a formal agreement between a community college and a four-year institution to transfer the student for two years of additional support to complete a bachelor’s degree. Community colleges are eligible only as sub-awardees of the partnering four-year SFS institution’s Scholarship Track award.

Each school must provide NSF with a description of its selection criteria and process, and must submit its list of candidates for SFS scholarships to OPM for final eligibility confirmation.

⁵² Doctoral students may be allowed to replace their summer internship with a research activity following a recommendation from their academic advisor and approval of the NSF program office.

⁵³ See <http://www.firstgov.gov/Agencies.shtml> for a list of Federal, State, Local and Tribal Governments; see <http://science.energy.gov/sbir/about/national-laboratories-profiles-and-contacts/> for a list of National Laboratories; see <http://www.nsf.gov/statistics/ffrdclist/> for a list of FFRDCs. These are the citations given in the NSF grant solicitation. Current statutory authority appears to enable the Director of NSF to identify and determine a “qualified” organization.

Internship placements and final job placements in government organizations typically require high-level security clearances and scholarship recipients are required to undergo the background investigation necessary to obtain such clearances as part of the job and/or internship application process.

Schools participating in the program must have clearly articulated management and administrative plans to support the various program elements. Some of these are common to many scholarship programs with eligibility requirements, such as the ability to verify candidate eligibility, budget for scholarships, and providing stipends of specified amounts of living expenses, tuition, a books allowance, and health insurance. Some are more distinctive to the SFS program, such as the provision for student expenses to travel to and attend the SFS program job fair, and the OPM certification of eligibility. The schools also play a role in coordinating the required summer internship programs with OPM. The schools are required to track student progress during school to see that eligibility is maintained. OPM takes over the tracking of graduates and their employment in qualified public sector organizations.⁵⁴ Participating schools and the student scholarship recipients have to commit to cooperate with the SFS program-level monitoring and evaluation system. Students have to agree to provide the school with annual certification of employment and up-to-date contact information. They must also agree to participate in the surveys conducted by OPM or other program evaluators as part of project-level and program evaluation efforts.⁵⁵

Grant size for the scholarship track to the participating schools ranges from \$1 million to \$5 million.⁵⁶ Grants generally are for a five-year period and are renewable on re-application to demonstrate continuing eligibility. An NSF official recently reported that in 2013 alone, 188 students had graduated from the SFS program.⁵⁷ As noted earlier, the government placement rate exceeds 93%. From the beginning of the program to 2013, 2,071 students had received scholarships and 1,554 had graduated. "SFS graduates have served in more than 140 Federal agencies, as well as in state, local and tribal governments."⁵⁸ As of July 1, 2015, there were 57 schools participating in the program.⁵⁹ All of them have CAE designations.⁶⁰

B. Capacity Track

The SFS Capacity Track provides grants intended to support innovative proposals that are likely to lead to an increase in the ability of the United States higher education enterprise to produce cybersecurity professionals. Grants focusing on capacity building contribute to the expansion of

⁵⁴ Failure to satisfy the academic requirements of the program or to complete the service requirement results in forfeiture of the scholarship award, which will revert to a student loan with repayments pro-rated accordingly to reflect partial service completed. The participating school has to collect loan repayments and submit them to the US Treasury. There is an appeals process for consideration of cases of "extreme hardship."

⁵⁵ This information should be anonymized and made publicly available.

⁵⁶ Hovis, supra note 14.

⁵⁷ Hovis, supra note 14.

⁵⁸ Id.

⁵⁹ See <https://www.sfs.opm.gov/ContactsPl.aspx> This is a list of the participating schools

⁶⁰ Information to consider in future studies on this topic: Time until graduation; number of students who had to repay their scholarship; what percentage of students stayed in the government beyond the required time; pattern of funding students over time

existing educational opportunities and resources in cybersecurity. NSF provided a list of the projects that it would like to see proposed for funding in its current solicitation:⁶¹

- a) Research on the teaching and learning of cybersecurity, including research on materials, methods and small-scale interventions;
- b) Curricula recommendations for new courses, degree programs, and educational pathways with plans for wide adoption nationally;
- c) Evaluation of teaching and learning effectiveness of cybersecurity curricular programs and courses;
- d) Integration of cybersecurity topics into computer science, data science, information technology, engineering and other existing degree programs with plans for pervasive adoption;
- e) Development of virtual laboratories to promote collaboration and resource sharing in cybersecurity education;
- f) Strengthening partnerships between institutions of higher education, government, and relevant employment sectors leading to improved models for the integration of applied research experiences into cybersecurity degree programs;
- g) Evaluating the effectiveness of cybersecurity competitions, games, and other outreach and retention activities; and
- h) Integrating data science into cybersecurity curriculum.

The grant size has ranged from \$300,000 to \$900,000 in recent years.⁶²

C. Program Evaluation for Both Tracks

According to NSF, the agency conducts on-going program monitoring and evaluation to determine how effectively the SFS program is achieving its goals; namely to:

- a) increase the quantity of new entrants to the government cyber workforce;
- b) increase the national capacity for the education of cybersecurity professionals;
- c) increase national research and development capabilities in critical information infrastructure protection; and
- d) strengthen partnerships between institutions of higher education and relevant employment sectors.⁶³

In addition to project-specific evaluations, all projects are expected to cooperate with a third party program evaluation and respond to all inquiries, including requests to participate in surveys, interviews and other approaches for collecting evaluation data. Additional guidelines are provided to institutions that receive Scholarship Track awards. NSF states that “project-specific evaluations should provide indicators of program achievement including, but not limited

⁶¹ See <http://www.nsf.gov/pubs/2015/nsf15584/nsf15584.htm>, supra note 34.

⁶² Hovis, supra note 14.

⁶³ NSF 2015 Solicitation 15-584, supra note 35.

to, the areas of placement, student achievement, faculty development, curriculum and institutional partnerships.”⁶⁴

⁶⁴ Id.

Section 5: Findings and Recommendations

A. Observations to Help Distinguish Between the CAE and SFS Programs

To provide context for the Panel’s recommendations, it is useful to describe how the eligibility, reporting, and evaluation requirement features of the SFS and CAE programs relate to one another, and their similarities and differences. There is quite a lot of similarity, but there are some critical differences, between them:

- a) Before 2008, a CAE designation was *required* by NSF in order for a school to qualify for SFS grants. Since then, schools in theory can demonstrate their high level of commitment to cybersecurity education in other ways. Still, in 2015, every one of the 57 schools in the SFS program has a CAE designation.
- b) The CAE program was expanded to include two-year schools in 2010. The SFS program was not expanded to cover two-year schools until earlier this year (2015), but a two-year school’s eligibility is contingent on a relationship with four-year schools, so that a student has the ability to move onto a four-year program. A two-year school should be eligible for consideration in the SFS program on its own, just as it may qualify on its own for a CAE-2Y designation.
- c) The CAE and SFS programs have complementary goals and objectives, but differ in focus. The SFS scholarship track supports employment across the entire federal workforce and, subject to approval by the NSF program office, across the broader public sector workforce, while the IASP scholarship program available under CAE program auspices, provides assistance only to students headed for jobs at DOD or its components.
- d) The SFS program requires its participating schools to collect a range of program evaluation information from the classes and the students, track the students’ educational progress to maintain eligibility for assistance, and survey the students at various times in their educational careers. NSF says the information is analyzed and used internally for program evaluation, but none of the information or the conclusions or analysis is shared publicly, even on an anonymous basis. The CAE program requires no information gathering by the designated schools about the students—testing or otherwise—but the CAE schools engaged in the SFS program presumably are collecting data for NSF on scholarship students.
- e) The SFS program has a “capacity building” track offering grants to participating schools for innovative curriculum development projects. The IASP for the CAEs is authorized by statute to offer capacity building grants to CAE schools. While the IASP is not currently awarding new scholarships, limited capacity building grants continue to be available.⁶⁵
- f) The SFS program offers grants that provide some funding to participating schools for a variety of projects. In contrast, the CAE program is basically a voluntary designation program for the schools. They receive no funding for improvement projects (such as facilities for the hands-on learning experiences advocated in this report).

Two of many possible ways forward present themselves. One would be a merger of the CAE and SFS programs. In an important sense, however, that would be a step in the wrong direction,

⁶⁵ As noted in the text at footnote 46, the IASP has enabled CAE’s with 180 capacity-building grants since 2001.

maybe even a step backward. The SFS program has recently—in theory at least—moved beyond the CAE model for proof of clearly documented evidence of a strong existing academic program in cybersecurity. The CAE program’s KUs may be a step in the right direction beyond the NSCC standards, but the KUs need to continue to evolve to meet cybersecurity education needs. On the other hand, by officially separating itself from the CAE designation as the only evidence of a commitment to cyber education, the SFS program has the potential of looking beyond the CAE model for ways to develop sound cybersecurity education practices. It should be encouraged to do so, not required to limit itself to the particular features of the CAE education model.

Rather than merging the two programs, the Panel believes the better course is to encourage both programs to continue to grow, along parallel but separate tracks, focusing on different subsets of the workforce and offering the possibility of different platforms for innovation in education.

B. The Panel Recommendations

The Panel has the following four major recommendations:

1. Strengthen the hands-on education component in both the CAE and SFS programs;
2. Identify, track, and use performance indicators for both the CAE and SFS programs;
3. Expand the SFS program to address the entire public sector (federal, state, local, tribal and territorial governments) by default as opposed to special permission and include qualified two-year programs regardless of their association with a four-year institution; and
4. Emphasize to the DOD senior leadership, including the Secretary of Defense, the importance of the CAE program for growing the federal cybersecurity workforce.

The four recommendations are discussed in detail below:

1. Strengthen the Hands-on Education Component in Both the CAE and SFS Programs

Opportunities exist to include the teaching and demonstration of hands-on capabilities, students’ ability to apply the knowledge they have learned to solve real-world problems, in both the KUs of the CAE program and in the grant solicitation for the SFS program. The CAE program can include this requirement as it continues to develop the KUs for all of its different designations. The SFS grant solicitation should emphasize this capacity building at the nation’s colleges and universities and regularly measure to assess the successful implementation and on-going use of the intended capacity.

There is a growing appreciation that cybersecurity education at all post-secondary levels benefits from hands-on learning experiences and laboratory exposure⁶⁶ doing projects with real world tools and moving beyond class room knowledge. The Panel shares this view, which was articulated by virtually all of the employers interviewed, and is noted in a recent opinion survey. According to the survey, one of the factors setting apart the “top schools for cybersecurity” was:

⁶⁶ This is sometimes discussed by referencing processes in other professional school environments such as nursing and medical schools (teaching hospitals).

hands-on learning environment where students and faculty work together on projects that address real life cybersecurity threats.⁶⁷

Developing sound hands-on outcomes and testing to those outcomes will be extremely important to the development of the cybersecurity workforce at all levels. The Panel recommends that DHS and NSA, working with the CAE community, develop appropriately rigorous and objective methods for assessing and continuously improving hands-on learning methods.⁶⁸ The NSF should do the same for its grant solicitation and capacity track award process. In addition, the Panel urges more CAEs and SFS program grantees to look at, apply, and contribute to the emerging scholarship that has identified more effective classroom-based instructional approaches for teaching complex subjects such as physics and engineering that “takes the form of a series of challenging questions and tasks that require the students to practice physicist-like reasoning and problem solving during class time while provided with frequent feedback.”⁶⁹

2. Identify, Track, and Use Performance Indicators for Both the CAE and SFS Programs

Performance indicators can serve a number of roles. They can be used to qualify organizations for CAE designation or SFS grant while excluding others. They can help employers find schools that produce the best students to tackle general cybersecurity needs or the best students with specific cybersecurity skills. They can also be used to inform students’ decisions as to which schools best meet their needs. SFS schools and CAEs, too, can use performance indicators to find ways to improve curricula and find more effective teaching methods. In addition, the indicators can motivate by giving feedback to the schools and creating healthy competition.

The study found no reported performance indicators for the CAEs individually or as a group. Data does not appear to be collected. On the other hand, NSF reports that it collects a relatively large amount of testing and survey data from students and graduates, as well as job placement data, but this program evaluation information is not made available to aid public understanding or analysis, even in aggregated, anonymous form.

A feedback system needs to be developed that promotes continuous improvement at the CAEs, featuring appropriate testing of students, feedback from graduates about their educational experience, and feedback from employers about the strength of those they hire from CAE and other institutions. As for the SFS program, it appears that much of the data collection is in place, but the feedback system, if any, has no components that are available even in aggregate

⁶⁷ Ponemon Institute, “2014 Best Schools for Cybersecurity”, <http://www.ponemon.org/local/upload/file/2014%20Best%20Schools%20Report%20FINAL%202.pdf> at 2.

⁶⁸ The NSA recognized the importance of hands-on”

learning with the establishment of its “CAE Cyber Operations Program” in 2011. According to an NSA release announcing the program:

The CAE Cyber Operations program is intended to be a deeply technical, inter disciplinary, higher education program firmly grounded in the computer science, computer engineering and/or electrical engineering disciplines, with ***extensive opportunities for hands-on applications via labs/exercises.*** (emphasis added)

See https://www.nsa.gov/academia/nat_cae_cyber_ops/ (emphasis added). NSA/ADET also manages a Center of Academic Excellence in Cyber Operations (CAE-CO) program established in 2012 with a total of 14 schools as of 1 Jul 2015. See

⁶⁹ Louis Deslauriers et al, “Improved Learning in a Large Enrollment Physics Class,” *Science*, May 13, 2011, Vol. 332: 862-864. See also Bob Roehr, “Nobel Laureate Carl Wieman: Effective Teaching Should Create Students Who Think Like Scientist,” June 8, 2012 at <http://www.aaas.org/news/nobel-laureate-carl-wieman-effective-teaching-should-create-students-who-think-scientists>

form, to the public. Both CAE and SFS systems need to develop some public metrics to aid student and employer choice.

Regarding the proposed feedback system described above, the Panel recommends that the CAEs:

a. Collect Information on Graduates of CAE Programs to Enhance Evaluation, Improvement and Selection of Graduates and Schools

Students and employers should be able to obtain necessary information about CAEs and SFS schools.

The Panel recommends that five elements of data on CAE graduates be collected and made available in summary form for analysis and that the data collection including tracking graduates in their job pursuits for a period of at least 3 to 5 years.

Two items seem suited to data collection by the CAEs themselves:

1. Time to securing a job
2. Name and characteristics of first employer

Many schools collect such data already for their accreditation process as well as their fundraising. Those CAEs that participate in the SFS program already collect this information on graduates entering the approved public-sector workforce.

In addition, it would be useful to have information about the graduate's developing jobs history. While this information is not necessarily performance information in the strictest sense, it is likely to provide useful insights and trigger constructive questions. It seems best to collect the following data from employers, noting the schools from which a student graduated:

3. Additional training needed on the job
4. Time spent in the initial job
5. Reasons for moving from job to job

In addition, employers could be surveyed to identify the schools they felt produced the strongest students for specific (as well as general) cybersecurity needs.

At first, data collection would be restricted to federal government employers. Most of those interviewed in the course of the study stated that having access to this information would help determine how successful a particular CAE was in delivering results in its educational mission. The recommended measures of educational quality, some collected by schools and some by employers, would not be easy for schools to "game" in an effort to improve their standing.

For performance indicators to be useful—for them to inform schools decisions about how to improve, to support employer hiring and to help students' selection of schools—the indicators need to be collected, analyzed, used, and shared with key decision-makers in government and in the schools, especially front-line teachers and department heads and be made public. Using measurement this way will not happen on its own, however. It

requires intentional management, assignment of responsibilities, and adequate resourcing.

The NSA/DHS program office, with help from OPM, the Chief Human Capital Officer Council⁷⁰ and CIO Council, should collect and collate the information, analyze it, and make it available to help students and employers make choices about CAEs in the future and help CAEs find opportunities for improvement.

In addition, serious consideration should be given to creating and funding structured learning networks that bring educators together to develop, test, and evaluate different instructional approaches in key knowledge areas.⁷¹

b. Develop and Test to the Outcomes Features of KUs and Make Results Available (Anonymously) to Inform Choice and Encourage Continuous Improvement; Consider Competitions and Challenges as Hands-on Testing Environments

Key performance indicators are often used to evaluate the absolute and relative effectiveness of an organization or a particular activity, so it is reasonable to think that such performance indicators would prove useful in evaluating the success of the CAE program in developing the skills and knowledge of the participating students. This does not appear to have been done when the CAE program was tied to the CNSS training standards. With the KUs in place, it is now possible to develop the capacity to assess how well students learned what they were taught and how well they can apply it.

Each KU has one or more student outcomes built into its specifications. Consideration should be given to developing performance indicators around the fulfillment of a few key student outcomes in the KUs. Not all the student outcomes are equally useful. Some KU student outcomes require that students demonstrate how to perform tasks related to the skills learned in the KU, while others simply call for students to be able to list something they have learned or otherwise recite back the contents of a subject area.⁷² Recitation is necessary but it is not sufficient. The KUs need to evolve to focus on demonstration of the ability to apply learned knowledge and skills wisely to real world situations. This means complementing KUs that currently are exclusively conceptual with concrete skillsets, to the greatest possible extent.⁷³

Students should be tested to see if they mastered the concepts being taught. Test results should be made available for analysis without revealing personally identifiable information. Comprehensive development of testing protocols is beyond the scope of this study, but given the importance of the subject matter, it would appear that development of such performance indicators could be of significant value. Testing can take a number of forms, including the use of versions of the innovative cybersecurity competitions and

⁷⁰ See <https://www.chcoc.gov/>

⁷¹ Anthony Bryk et al, *Learning to Improve: How America's Schools Can Get Better at Getting Better*, March 2015

⁷² Compare, for example, the student outcomes for the "Intro to Cryptography" 2Year Core KU 1.7 – four items that all call for the student to "identify" or "describe"; with the student outcomes for the "Networking Concepts" 2Year Core KU 1.9 – five items, two of which that ask the student to "describe", while three call on the student to "track and identify" or "use" various networking tools. CAE Knowledge Units, supra note 14, pages 11 and 13.

⁷³ The Panel recognizes that not all conceptual KU's lend themselves to including a "concrete skillset."

challenges supported and encouraged by Section 301 of the Cybersecurity Enhancement Act of 2014.⁷⁴ Section 301 calls for federal support of competitions to identify, develop and recruit talented individuals to perform cybersecurity duties for both government and the private sector, as well as to stimulate innovation in basic and applied cybersecurity research. The Act includes a substantial list of skills for competitions to cover including (1) ethical hacking; (2) penetration testing; (3) vulnerability assessment; (4) continuity of system operations; (5) security in design; (6) cyber forensics; and (7) offensive and defensive cyber operations, as well as (8) other skill sets determined to be appropriate in the future. Such competitions and challenges—another form of hands-on learning⁷⁵—should be included in testing protocols.⁷⁶ As pointed out earlier, what is needed is a system that encourages continuous improvement; a feedback loop for CAEs, students and employers that would help inform decisions for all parties. This would be one element.

c. Test to Scenarios or Incident Responses in Addition to KU Outcomes

The KUs are useful, but they have two readily identifiable drawbacks as currently structured: First, out of necessity, one real world problem or incident or scenario is broken down into many KUs that, in turn, may have many smaller teachable pieces. Testing to the KUs is a little like testing a law student to civil procedure or a medical student to a particular protocol responding to a particular disease or condition. All of this is necessary but not sufficient for success when the graduate faces a real-world situation that implicates several different skillsets. Second, the KUs continue to tend to focus too much on technical skills, with not enough attention paid to critical thinking, decision-making, and problem solving. The Panel recognizes that this may become less of a problem when the KUs are mapped to the *NICE Workforce Framework*.

The Panel recommends that CAE students be tested in ways that mimic what they will face outside the classroom, just as law students face clinics that combine procedure and substance, research and presentation, and well-prepared opposition; and medical students face challenges in a teaching hospital environment. There can be lots of flexibility in developing vehicles here, but the point is to devise ways to test students on the skills needed to address or solve a problem where they would be using what they have learned from many different KUs perhaps in different courses in different academic departments.⁷⁷

This recommendation also underscores the Panel’s strong belief that a highly functioning cybersecurity workforce includes people with degrees and expertise beyond the realm of computer science and electrical engineering, branching into other disciplines that may be

⁷⁴ Section 301 of Pub. Law 113-274, enacted December 18, 2014, <http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf>. Competition skills are listed in Sections 301(d)(1) through (8).

⁷⁵ This subject is addressed in detail in the section on Recommendation 1, *supra*.

⁷⁶ Full Disclosure: one organization sponsoring challenges and competitions is the U.S. Cyberchallenge, <http://www.uscyberchallenge.org/>, sponsored by CIS, one of the organizations funding this study.

⁷⁷ Examples would include the “teaching hospital” environment at Virginia Tech, so-called because students have opportunities to work with “live data feeds” and real networks at the University; and the Cyber Challenge and similar competitions designed to force students to use their skills and knowledge and collaborate with each other on finding the best solutions to problems, discussed in the text, *supra* at note 75.

useful for prevention, detection, response and recovery to protect and defend the nation's cyber infrastructure.⁷⁸

3. Expand the SFS Program to Address the Entire Public Sector (Federal, State, Local, Tribal and Territorial Governments) by Default as Opposed to Special Permission and Include Qualified Two-Year Programs Regardless of Their Association with a Four-Year Institution

a. Ensure the SFS Program Applies to the Entire Public Sector and Encourages Curriculum Innovation—Beyond the CAE Model of its Current Schools—to Meet the Need for Building out the Cybersecurity Workforce

SFS program obligations to work off the scholarship by employment in a “qualifying” position related to cybersecurity can now be met by employment in the public sector, broadly defined, not just the federal government, with the approval of the NSF program office. Qualifying positions exist at the federal level, but they also exist at the level of state, local and tribal government, at federal laboratories and at a list of federally funded research and development facilities.⁷⁹ This expansion should become the general rule and made a regular part of the program.

It should be underscored that the SFS program is no longer exclusively tied to the CAE program in legislation, despite the fact that all the current SFS schools are CAEs. There is room to recognize outstanding cybersecurity education curricula that go beyond the CAE model. More innovation, with appropriately rigorous evaluation, should be encouraged. One interviewee commented that, historically, it was apparently easier just to get a CAE designation than to put together the information to apply to participate in the SFS program without a CAE designation, regardless of how great a school's curriculum might be. That needs to change. An institution of higher education should be able to show its commitment to cybersecurity education with an innovative curriculum and other features, even if it does not fit the pattern of the CAE designation. Innovation should be encouraged.

The SFS program has resources to support capacity building to enhance cybersecurity education at the nation's colleges and universities.

b. Expand the SFS Program to Include Qualified Two-Year Programs Regardless of Association with a Four-Year Institution

The 2014 Cybersecurity Enhancement Act authorized the SFS program to offer support to community colleges.⁸⁰ The NSF has responded by offering to support scholarship students at qualifying community colleges when they are partnered with a qualified four-year school and go on to that school for a Bachelor's degree. The Panel appreciates this extension of the SFS program to community colleges but believes the program can do

⁷⁸ This subject is also addressed in the Panel's recommendation to develop more KU's that reflect the multifaceted cybersecurity workforce. See text at footnotes 81 - 83,

⁷⁹ See the text and footnotes at notes 39 and 40.

⁸⁰ Community colleges are specifically called out in Section 301(b)(1) of the Cybersecurity Enhancement Act of 2014, Public Law 113-274 (2014)

more. Not everyone in a two-year program is destined to transfer to a four-year school to complete an undergraduate degree. Many students want to stop with an Associate's degree and enter the workforce with that two-year credential. This is especially true for two groups: (1) returning veterans and (2) mid-career executives, both of whom are looking for a career realignment or booster. And employers may find such individuals well qualified to perform a number of cybersecurity roles.

The Panel assumes that the NSF will apply the same rigorous qualification standards to two-year schools that it has applied to four-year schools over the past 14 years. Some two-year schools will not qualify, just as some four-year schools do not qualify. The panel would point out however that more than 20 two-year schools have been designated as CAE-2Y by the NSA and DHS⁸¹, and such schools (and others interested and able to demonstrate their capabilities in cybersecurity education in other ways) should be able to be considered on their own.

4. Emphasize to the DOD Senior Leadership, Including the Secretary of Defense, the Importance of the CAE Program for Growing the Federal Cybersecurity Workforce

As discussed earlier in this report, the CAE program is currently in the process of updating its requirements, an effort the Panel strongly supports. The Panel recommends that the program should develop KUs that recognize the multidisciplinary approach needed in the workforce. Further it should continue its work mapping the KU's to the *NICE Workforce Framework*; start collecting information on its students and the schools along the lines conducted by the SFS program and make data available for analysis on an anonymous basis. Finally, the Department of Defense should reinstate funding the now-dormant IASP program to address its cyber workforce needs.

a. Develop KUs that Recognize the Multidisciplinary, Multifaceted Approach Needed in the Cybersecurity Workforce

Computer science and electrical engineering are critically important skills for cybersecurity, but are not likely to be the sole educational background of a strong cybersecurity workforce. Graduates from other fields as diverse as anthropology, sociology, psychology, and philosophy, may also bring valuable perspectives to a cybersecurity team. The four job groups depicted in Figure 1 include many that emphasize knowledge, skills, and aptitudes other than those listed in the still largely technical KUs.

The Panel understands that the CAE program and its participating schools plan to continue to develop KUs, both in workshops and through online collaboration,⁸² and endorses this process commitment to continuous improvement. The Panel understands that the KUs were originally developed under the assumption that general education areas (i.e. critical thinking and problem solving) would be addressed by the general curriculum of the CAE schools. Nevertheless, the Panel recommends that critical thinking and problem solving be explicitly included in future KUs so that they reflect the multidisciplinary approach needed for a successful cybersecurity workforce. When asked

⁸¹ See table 1, supra.

⁸² <https://www.caecommunity.org/>.

to describe workforce needs, interviewees and the participants in the recent cybersecurity workforce summit⁸³ were as likely to identify communicators who could advance cybersecurity policy needs to a group of users, analysts who could assist in the development of cybersecurity rules for organizations, and cultural interpreters as they were to identify forensic technologists and those with intense knowledge of safe coding. This multidisciplinary approach should be able to be incorporated into the KUs. The Panel also recommends that industry partners be brought into the process as broadly as possible to help continue to make it as realistic as possible and increase its usefulness to employers.⁸⁴

b. Map the KUs to the NICE Workforce Framework and Use the Framework as an Alternative Basis for CAE Designation

Recent efforts have been made to expand the definitions of the cybersecurity workforce and advocate for a workforce possessing a broad set of roles and skills, looking to the future. The *DOD Cyberspace Workforce Strategy*,⁸⁵ with its focus on the government workforce, the more generally stated *NICE National Cybersecurity Workforce Framework*,⁸⁶ and the Department of Labor's Cybersecurity Industry Competency Model⁸⁷ are major accomplishments and together provide a solid foundation for continuing work. The Panel recognizes that these remain works-in-progress and will continue to be developed and refined in the future. Interviewees from both government and the private sector almost unanimously commented on the need for a multidisciplinary workforce reflected in these modern frameworks and models: one that is characterized by good habits of critical thinking and inquisitive perspectives, shaped by hands-on experience in laboratories or other "clinical" settings, and going well beyond a focus on computer science and electrical engineering, however critically important it is to include those disciplines. Any cybersecurity team needs these broad multidisciplinary perspectives.

Section 942 of the National Defense Authorization Act for Fiscal Year 2014⁸⁸ requires that the DOD lead an effort to map the current and emerging KUs to the *NICE Workforce Framework*. The Panel understands that this work has already begun⁸⁹ and fully supports

⁸³ Second Annual Cybersecurity Summit, Arlington, Virginia (March 26, 2015) <http://www.affirm.org/event/affirm-and-uscc-present-2nd-annual-cybersecurity-summit>

⁸⁴ It is often cited that at least 85% of the nation's "critical information infrastructure", however that term is defined (e.g., transportation, telecommunications, public utilities, the financial sector, etc.) is under the control of the private sector not the government of the United States. See, e.g., *Safeguarding the Digital Frontier: The Way Ahead for American Cybersecurity and Civilian Networks*, Hon. Michael McCaul, chairman of the U.S. House Committee on Homeland Security, "**85% of the critical information infrastructure is in the hands of the private sector.**" *Remarks as Delivered at the Center for Strategic & International Studies (CSIS) on March 17, 2015*; <http://homeland.house.gov/document/chairman-mccaul-remarks-csis-cybersecurity>

⁸⁵ http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed%28final%29.pdf

⁸⁶ <http://csrc.nist.gov/nice/workforce.html> "NICE" is the National Initiative for Cybersecurity Education, and is administered by the National Institute of Standards and Technology. See <http://csrc.nist.gov/nice/>The current version of the *NICE Framework* is reproduced in this report as Appendix D.

⁸⁷ <http://www.careeronestop.org/CompetencyModel/competency-models/cybersecurity.aspx>

⁸⁸ Public Law 113-66, Section 942(b)(5)(2013)

⁸⁹ "A Department of Defense Report on the national Security Agency and Department of Homeland Security Program for the 'National Centers of Academic Excellence in Information Assurance Education matters' in response to Section 942 of the National Defense Authorization Act for Fiscal Year 2014 (Public law 113-66)" at page 4, http://www.cisse.info/pdf/2015/DoD%20942%20Report%20to%20Congress_FINAL.pdf

it. Interviewees informed the study team that it appears that the KUs map as a “technical subset” of the *NICE Working Framework*. The recent DOD report states that the “current KUs are designed for a narrower, but critically important focus on the cybersecurity technical workforce.”

This work should be continued. The panel strongly encourages that as this work continues, consideration be given to moving from the KUs to the *NICE Workforce Framework* as a foundation for CAE designation. This is the way forward to a diversified and multifaceted cybersecurity workforce in the government.

c. Make Future New and Renewed CAE Designation Contingent on a Commitment to Participate in Testing and Evaluation of Student Performance and Sharing the Data to Support School Improvement Efforts Beyond the Individual School and Employer and Student Choices

To implement these suggestions, the Panel supports that future CAE designation (new or renewed) should depend on the following. In addition to current requirements, CAEs should be required to:⁹⁰

- a) Survey its students as described above and to make the data available for further study;
- b) Build hands-on learning environments into the school’s CAE program;
- c) Test students regarding the application of the knowledge they are learning, and the outcomes of the KUs. The testing should take place in a campus laboratory or similar environment (similar in concept to a clinic in law school or a teaching hospital in medical school). Test results protecting personal identification would be made available for further analysis and feedback to the schools;
- d) Test to scenarios or incidents beyond the KUs would also become a regular part of the school’s CAE program;
- e) Support program evaluation activities including data collection, as described in the previous section; and
- f) Apply the evidence from emerging scholarship on more effective classroom-based instructional approaches for teaching complex subjects.

The testing along with the feedback from graduates and employers would form the foundation for a program of continuous learning and improvement at the CAEs.

d. Each CAE Should Align Itself with at Least One NICE Workforce Framework Specialty Area to Support More Valid Comparisons to Inform Employer and Student Choices and School Improvement Efforts

⁹⁰ The NSF conditions its grants under the SFS program on agreement to participate in the program along similar lines. The Panel envisions that the CAE program could use the IASP grant program to similar effect.

As a way of exploring more meaningful ways to distinguish the educational objectives of each CAE, the program community should develop a process that would enable alignment of a particular CAE program with one or more *NICE Workforce Framework* Specialty Areas. This would help students and employers do a better job of identifying which CAEs to attend and recruit from, respectively and simplify hiring based on the need for specific skillsets. The additional categories of specialization set forth in the *NICE Workforce Framework's* Specialty Areas offer a lot of useful detail.⁹¹ Developed by DHS and the National Institute of Standards and Technology (NIST), the 25 Specialty Areas (and additional areas specific to military and intelligence work) are shown in Appendix D.

Attaching its name to one or several of these Specialty Areas would allow a CAE to attract students based on their specific interests or skills, as well as allowing employers to sharply narrow their search for future employees, more precisely than is possible using the aforementioned sub-designations.

In addition, these Specialty Areas are ultimately tied to a larger, national framework being adopted by cybersecurity employers in both the public and private sectors. This serves the purpose of helping students and employers identify which CAEs to attend and recruit from, respectively, with an eye towards the larger, national cyber workforce framework. A simultaneous adoption by the CAEs and employers of the *NICE Workforce Framework* would improve the simplicity and consistency of hiring based on the need for specific skillsets.

The Specialty Areas offer identifiable areas of focus that may help the CAEs in marketing efforts as well as provide concrete areas of subject matter expertise.

e. Reinstate IASP Funding for Scholarships and Capacity Building Grants for the DOD Workforce

The 2001 Defense Authorization Act⁹² established the IASP as a grant program as well as a scholarship program. Grants are authorized “to support the establishment, improvement, or administration of programs of education in information assurance. . . . Proceeds . . . may be used for the following purposes: (1) Faculty development; (2) Curriculum development; (3) Laboratory improvements; (4) Faculty research in information security.”⁹³ An institution of higher learning must be a CAE to qualify for a grant.⁹⁴

By law, DOD is allowed to give aid only to students who attend a CAE-designated institution and the program is intended to support the cybersecurity workforce needs of

⁹¹ The Panel is aware that the CAE Community is working on development of “focus areas” as a way to supply additional differentiation. The Panel encourages consideration of moving to the NICE specialty areas instead

⁹² See Section 922 of the National Defense Authorization Act of 2001, Pub. Law 106-398, 114 Stat. 1654 at 1654A-233 (2000).

⁹³ See 10 U.S.C. §2200B, added by Section 922, *supra* note 92.

⁹⁴ 10 U.S.C §2200C.

the Department of Defense. Funding for this program was phased out in 2014. Given the national cybersecurity imperative, it should be funded by DOD.⁹⁵

The grants authority is not currently being exercised by DOD or its components. The Panel encourages invigorating the grants activity for scholarships as well as for grants to help (1) fund the development of a feedback system similar to that of the SFS program and (2) support implementation of the hands-on learning facilities recommendation set out in this report. These are all activities allowed by the language of the legislation establishing the program.

The CAE program is essentially a volunteer program for the participating schools. The schools themselves receive no direct federal funding through the CAE program. Specifically, there is no funding to reimburse expenses of the schools for their efforts to secure or renew the designation, much less engage in the kind of capacity building needed to improve their programs.

This is why a reinvigorated IASP with both scholarship and capacity grant features is so important. Schools in the CAE program clearly need to do more to (1) assess their performance objectively to find areas of strength and areas needing improvement, (2) build facilities appropriate for hands-on learning, and (3) provide information both to students and potential employers that enable them to find the schools and graduates that best meet their needs. The Panel recognizes that, if the CAEs are going to engage in these activities, they need some financial incentives. A reinvigorated IASP with an operating grants facility can provide substantial incentives.

⁹⁵ See footnote 6, *supra*.

Summary of Panel Recommendations

1. Strengthen the hands-on education component in both the CAE and SFS programs;
2. Identify, track, and use performance indicators for both the CAE and SFS programs:
 - a) Collect information on graduates of CAE programs to enhance evaluation, improvement and selection of graduates and schools;
 - b) Develop and test to the outcomes features of KUs and make results available (anonymously) to inform choice and encourage continuous improvement; consider competitions and challenges as hands-on testing environments; and
 - c) Test to scenarios or incident responses in addition to KU outcomes;
3. Expand the SFS program to address the entire public sector (federal, state, local, and tribal governments) by default as opposed to special permission and to include qualified two-year programs regardless of their association with a four-year institution; and
4. Emphasize to the DOD senior leadership, including the Secretary of Defense, the importance of the CAE program for growing the federal cybersecurity workforce:
 - a) Develop KUs that recognize the multidisciplinary, multifaceted approach needed in the cybersecurity workforce;
 - b) Map the KUs to the *NICE Workforce Framework* and use the framework as an alternative basis for CAE designation;
 - c) Make future new and renewed CAE designation contingent on a commitment to participate in testing and evaluation of student performance and sharing the data to support school improvement efforts beyond the individual school and employer and student choices;
 - d) Each CAE should align itself with at least one *NICE Workforce Framework* Specialty Area to support more valid comparisons to inform employer and student choices and school improvement efforts; and
 - e) Reinstate IASP funding for scholarships and capacity building grants for the DOD workforce.

Appendix A – Participating Individuals and Organizations

Carnegie Foundation for the Advancement of Teaching

Bryk, Anthony—President

Cisco

Stewart, John—Senior Vice President and Chief Security Officer

Department of Defense

Davidson, Don—Office of the Chief Information Officer, Office of the Secretary

Keith, Stephanie—Head, Cyberspace Workforce Division

Department of Homeland Security

Scribner, Benjamin—Program Director, National Cybersecurity Professionalization and Workforce Development

Stempfley, Roberta—Deputy Assistant Secretary for Cybersecurity and Communications

General Electric

Puckett, Richard—Chief Security Architect

MITRE Corporation

Stempfley, Roberta—Director of Cybersecurity Implementation

Young, Rocky—Principal Cyber Security Engineer

National CyberWatch Center

Leary, Margaret—Director, Curriculum

National Institute of Standards and Technology

Newhouse, William—Lead, National Initiative for Cybersecurity Education (NICE)

Petersen, Rodney—Program Lead, National Initiative for Cybersecurity Education (NICE)

National Science Foundation

Piotrowski, Victor—Lead Program Officer

National Security Agency

Clark, Lynne—Chief, National Information Assurance Education and Training Program (NIETP)

LaFountain, Steve—Distinguished Academic Chair for Information Assurance and Cyber Associate Director for Education and Training

National Security Council

Caddy, Cheri—Director for Cybersecurity Policy Integration and Outreach

Nuclear Regulatory Commission

Ash, Darren—Deputy Executive Director for Corporate Management/Co-Chair, CIO Council Workforce Committee

Purdue University

Spafford, Gene—Executive Director, Center for Education and Research in Information Assurance and Security (CERIAS)

Stanford University

Wieman, Carl—Professor of Physics and Professor at Graduate School of Education

University of Houston

Conklin, Arthur Wm.—Director, Center for Information Security Research and Education

Virginia Tech

Marchany, Randy—Information Technology Security Officer/Director of IT Security Lab

Appendix B – Panel and Staff

Panel

David M. Wennergren, *Chair*—Senior Vice President of Technology, Professional Services Council. Former Vice President, Enterprise Technologies and Services, CACI International Inc.; Assistant Deputy Chief Management Officer, Department of Defense; Deputy Assistant Secretary (Information Management, Integration and Technology) and Deputy Chief Information Officer, Office of the Secretary of Defense. Former positions at Department of the Navy: Chief Information Officer; Deputy Chief Information Officer for Enterprise Integration and Security. Former positions at Office of the Deputy Chief of Naval Operations (Logistics): Head, Plans and Policy Branch; Head, Program Review and Analysis Section. Former Economic Support Team Leader, Department of the Navy Base Structure Analysis Team; Management Analyst, Naval Industrial Resources Support Activity, and Naval Air Technical Services Facility.

Ramon C. Barquin—President, Barquin International; Board Chair, Atlantic University College; Former President, Washington Consulting Group; Manager, Public Affairs Programs, IBM; Manager, External Programs, World Trade Asia, IBM South East Asia Region; Manager, External Programs & Marketing Research, Americas/Far East Corp., IBM; Various Positions; San Juan, Puerto Rico; IBM Co.

Shelley H. Metzenbaum—Senior Advisor, The Volcker Alliance. Former Founding President, The Volcker Alliance; Former Associate Director for Personnel & Performance, Office of Management and Budget; Director, Environmental Compliance Consortium; Visiting Professor and Senior Fellow, School of Public Affairs, University of Maryland; Executive Director, Performance Measurement Project, John F. Kennedy School of Government, Harvard University; Associate Administrator for Regional Operations and State/Local Relations, U.S. Environmental Protection Agency; Under Secretary, Executive Office of Environmental Affairs, and Director, Office of Capital Planning and Budgeting, Commonwealth of Massachusetts.

Alan R. Shark—Executive Director, Public Technology Institute; Associate Professor of Practice, School of Public Affairs and Administration, Rutgers University, Newark. Former President and Chief Executive Officer, American Mobile Telecommunications Association; Associate Executive Director, Marketing & Communications, Water Environment Federation; Director of Marketing, North American Telecommunications Association; Vice President for Marketing and Communications, American Resort Development Association; Vice President for Marketing, Voice Computer Technologies Corporation; Director of Research and Information Services, National School Boards Association; Director of Programs, Association of Governing Boards of Universities and Colleges; Coordinator, State and Organizational Relations, American Association of State Colleges and Universities; Seabees, U.S. Navy, Vietnam Service.

Academy Study Team

Joseph P. Mitchell, III, *Director of Project Development*—Dr. Mitchell leads and manages the Academy's studies program and serves as a senior advisor to the Academy's President and CEO. He has served as Project Director for past Academy studies for the Government Printing Office, the U.S. Senate Sergeant at Arms, USAID/Management Systems International, the National Park Service's Natural Resource Stewardship and Science Directorate, and the USDA Natural Resources Conservation Service. During his more than 15 years at the Academy, Dr. Mitchell has worked with a wide range of federal cabinet departments and agencies to identify changes to improve public policy and program management, as well as to develop practical tools that strengthen organizational performance and assessment capabilities. He holds a Ph.D. from the

Virginia Polytechnic Institute and State University, a Master of International Public Policy from The Johns Hopkins University School of Advanced International Studies, a Master of Public Administration from the University of North Carolina at Charlotte, and a B.A. in History from the University of North Carolina at Wilmington.

Joseph Tasker, Jr., *Project Director*—Mr. Tasker graduated with a B.A. in Sociology from the University of Oklahoma and earned a law degree from George Washington University. He spent the first 16 years of his career as a practicing lawyer in both the public and private sectors, litigating antitrust cases for the Federal Trade Commission (6 years) and practicing international trade, intellectual property, and government procurement law for 10 years as an associate and partner in a major DC law firm. In 1990, he opened a Washington government affairs office for a major producer of personal computers. After the company merged with Hewlett Packard in 2000, he became the General Counsel and Senior Vice President of Government Affairs for the Information Technology Association of America (ITAA), where he spent seven years as an industry advocate on issues related to cybersecurity administrative and legislative initiatives. Since ITAA merged itself out of existence, he has consulted on a number of projects, most recently providing technical trade advice on the expansion of the WTO Information Technology Agreement.

Karen S. Evans, *Senior Advisor*—Ms. Evans is National Director for the U.S. Cyber Challenge and Partner at KE&T Partners, LLC. She is the former Administrator at the Office of Electronic Government & IT, Office of Management and Budget. Prior to that, Ms. Evans served as the Chief Information Officer at the U.S. Department of Energy. She has held various positions at the U.S. Department of Justice, including: Division Director, Information Systems Management, Office of Justice Programs; Staff Director, Computer Services Staff, Justice Management Division. Ms. Evans was also the Deputy Director of the Farmers Home Administration, Applications Management Division, at the U.S. Department of Agriculture.

Franklin S. Reeder, *Senior Advisor*—Mr. Reeder is Former Director of the Office of Administration at The White House. He has held various positions with the U.S. Office of Management and Budget, including: Deputy Associate Director for Veterans Affairs and Personnel; Assistant Director for General Management and Deputy Assistant Director; Chief, Deputy Chief, Information Policy Branch; Policy Analyst; Chief, Systems Development Branch. In his time on the Hill, Mr. Reeder served as Deputy Director, House Information Systems, Committee Staff, on the Committee on House Administration, U.S. House of Representatives. His prior positions with U.S. Department of the Treasury and U.S. Department of Defense focused on information technology and systems. He is also the Co-founder and founding chair of, the Center for Internet Security and of the Council on Cybersecurity.

Harrison Redoglia, *Research Associate*—As a Research Associate at the Academy, Mr. Redoglia has worked on several prior Academy studies: the Federal Leaders Digital Insight Survey study with ICF International, an Organizational Assessment of the State Department Office of the Inspector General, and a study aimed at developing performance indicators for National Centers of Academic Excellence in Information Assurance. Mr. Redoglia has also worked with Academy Fellows on issues related to the GAO's High Risk List and the 2016 Presidential Transition. Prior to joining the Academy, Harrison worked in the Office of Dan Branch, former Texas State Representative, drafting constituent response letters and collecting voter-related data for campaign purposes. He graduated from Southern Methodist University with a Bachelor of Arts in Political Science with an emphasis on International Relations and minor in Corporate Communication.

Appendix C – Illustrative Core Knowledge Units

Source: National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD) Knowledge Units listing, available at <http://www.cisse.info/pdf/2014/2014%20CAE%20Knowledge%20Units.pdf>

Cyber Defense

Definition:

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

Topics:

- Network mapping (enumeration and identification of network components)
- Network security techniques and components
 - Access controls, flow control, cryptography, firewalls, intrusion detection systems, etc.
- Applications of Cryptography
- Malicious activity detection / forms of attack
- Appropriate Countermeasures
- Trust relationships
- Defense in Depth
 - Layering of security mechanisms to achieve desired security
- Patching
 - OS and Application Updates
- Vulnerability Scanning
- Vulnerability Windows (0-day to patch availability)

Outcomes:

- Students will be able to describe potential system attacks and the actors that might perform them.
- Students will be able to describe cyber defense tools, methods and components
- Students will be able to apply cyber defense methods to prepare a system to repel attacks
- Students will be able to describe appropriate measures to be taken should a system compromise occur.

Systems Administration

Definition:

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration

Topics:

- OS Installation
- User accounts management
- Password policies
- Authentications Methods
- Command Line Interfaces
- Configuration Management
- Updates and patches
- Access Controls
- Logging and Auditing (for performance and security)
- Managing System Services
- Virtualization
- Backup and Restoring Data
- File System Security
- Network Configuration (port security)
- Host (Workstation/Server) Intrusion Detection
- Security Policy Development

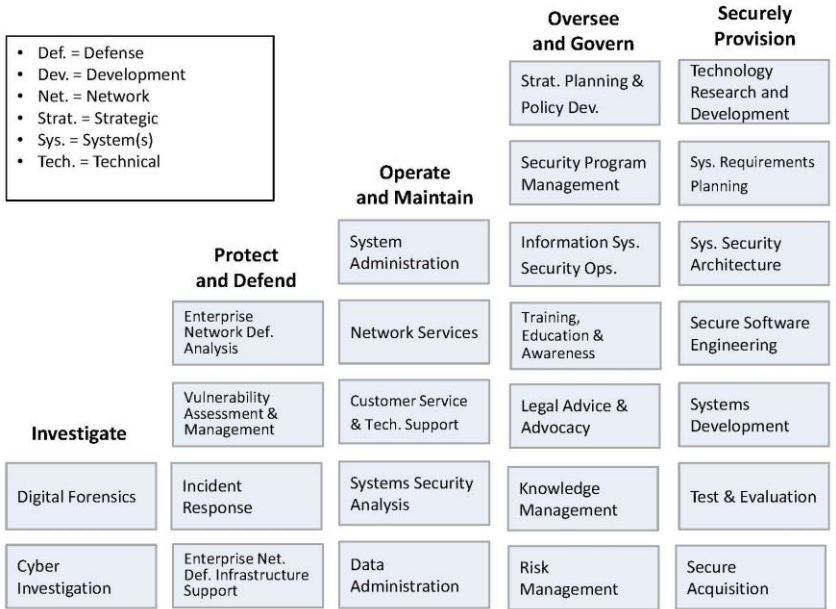
Outcomes:

- Students will be able to apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup.

Appendix D – The NICE Workforce Framework

WORKFORCE FRAMEWORK 2.0

- Def. = Defense
- Dev. = Development
- Net. = Network
- Strat. = Strategic
- Sys. = System(s)
- Tech. = Technical



Appendix E – Letter from Sen. Carper (D-DE) Endorsing this Study

THOMAS R. CARPER, DELAWARE, CHAIRMAN
CARL LEVIN, MICHIGAN
MARK L. PRYOR, ARKANSAS
MARY L. LANDRIEU, LOUISIANA
CLAIRE McCASKILL, MISSOURI
JON TESTER, MONTANA
MARK BEGICH, ALASKA
TAMMY BALDWIN, WISCONSIN
HEIDI HEITKAMP, NORTH DAKOTA

TOM COBURN, OKLAHOMA
JOHN MCCAIN, ARIZONA
RON JOHNSON, WISCONSIN
ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY
MICHAEL B. ENZI, WYOMING
KELLY AYOTTE, NEW HAMPSHIRE

GABRIELLE A. BATKIN, STAFF DIRECTOR
KEITH B. ASHDOWN, MINORITY STAFF DIRECTOR

United States Senate
COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

December 23, 2014

Dr. Willie E. May
Director
National Institute of Standards and Technology
100 Bureau Dr
Gaithersburg, MD 20899

Dear Dr. May:

As you may know, the National Academy of Public Administration (the Academy) is conducting a study on the performance and coordination of cybersecurity education and training programs used by the Federal government. It is my hope that you will support the Academy as it requests pertinent data from your agency and seeks to complete its report.

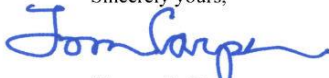
As you are well aware, the federal government and the private sector are facing a severe shortage of properly trained cybersecurity professionals. To meet the growing need for more cyber professionals, the federal government has invested significant funding in training initiatives and many organizations have created cybersecurity education programs. While these efforts are extremely important, there is little systematic information about these educational programs to guide the decisions of students, employers, and government officials.

I believe the Academy's study will provide a needed comprehensive review of the cybersecurity education and training programs used by our Federal agencies. That is why I am encouraging you, as well as officials at the Department of Homeland Security, National Science Foundation, the Office of Personnel Management, the Department of Defense, and the National Security Agency, to support the Academy as it requests information from your agency to complete its study.

Again, I hope that you will support the important study being undertaken by the Academy. Your cooperation will not only help the Academy move forward quickly, it will also help ensure we have the most effective educational programs in place to meet the growing demand for new cybersecurity professionals. Thanks very much!

With best personal regards, I am

Sincerely yours,



Thomas R. Carper
Chairman

cc: Dr. Ernest McDuffie
Mr. William Newhouse

Note—Similar letters were sent to the following agencies: DHS, DOD, OPM, NSA, and NSF.



**National Academy of
Public Administration®**

**1600 K Street, N.W.
Suite 400
Washington, D.C. 20001
Phone: (202) 347-3190
Fax: (202) 223-0823
Website: www.napawash.org**