CLOSING THE TALENT GAP IN FEDERAL IT

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 22, 2016

Serial No. 114–160

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

26–069 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK, MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
SEAN BREBBIA, *Senior Counsel*
WILLIAM MARX, *Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALKER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona

ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

CONTENTS

CLOSING THE TALENT GAP IN FEDERAL IT

Thursday, September 22, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 3:27 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Kelly, and Connolly.

Mr. HURD. The Subcommittee on Information Technology will come to order. And without objection, the chair is authorized to declare a recess at any time.

We are going to be a little pressed for time today. We are going to have a hard stop before votes come out. And so with that, I am going to submit my opening statement for the record so that we can get to the reason why we are here, and that is to talk to our great panel that we have today.

Mr. HURD. And I am going to hold the record open for five legislative days for any members who would like to submit a written statement.

I want to recognize our panel of witnesses. I am pleased to welcome Dr. Joan Ferrini-Mundy, the assistant director of Education and Human Resources at the National Science Foundation; Mr. Scott Montgomery, vice president and chief technical strategist at Intel Security; Mr. Gene Bowman executive director of Alamo Academies and from my hometown of San Antonio; and Emile Cambry, the founder of BLUE1647.

And welcome to you all. And pursuant to committee rules, all witnesses will be sworn in before they testify. So please rise and raise your right hands.

[Witnesses sworn.]

Mr. HURD. Thank you. Please be seated.

Let the record reflect the witnesses answered in the affirmative.

And in order to allow time for discussion, please limit your testimony to five minutes, and your entire written statement will be part of the record.

And again, thank you for being here on such an important issue of closing the talent gap in Federal IT. In my 21 months, this is the one thing I have heard consistently as a problem not only in the government but in the private sector, and it is great to have such a distinguished panel here to talk about this and also advocate some ways that we can help work together and solve this problem.

And with that, I would like to recognize Dr. Ferrini-Mundy for your opening remarks.

WINTNESS STATEMENTS

STATEMENT OF JOAN FERRINI–MUNDY

Ms. FERRINI-MUNDY. Good afternoon, Chairman Hurd, Ranking Member Kelly, and other distinguished members of the Subcommittee on Information Technology. My name is Joan Ferrini-Mundy, and I'm the National Science Foundation's assistant director for Education and Human Resources. Thank you so much for the opportunity to testify before you today on this critical topic for our nation, the preparation of a workforce to provide our nation's cybersecurity.

The directorate that I lead has a unique and crucial mission at a science agency within the Federal Government; that is, supporting the preparation of a diverse, globally competent science, technology, engineering, and mathematics—or STEM—workforce and a STEM-literate citizenry. We do this by providing grants to research and education organizations and institutions across the country to support innovation in STEM education to build capacity in STEM education for diverse students and to do research and evaluation of those efforts.

Our funding supports both formal education and education outside the formal system, for example, work in museums, public television programming, and other public engagement. And in addition, we fund very important programs for scholarships and fellowships.

Our education investments are closely related to the National Science Foundation's research investments, particularly in the area of secure and trustworthy computing where we fund leading researchers in cybersecurity areas from cryptanalysis to cyber physical systems to social networking and more.

Today, I'll focus on just a few of the NSF programs that help to build the Nation's workforce for information technology and cybersecurity. Specifically, NSF's CyberCorps Scholarship for Service, or SFS program, was launched in 2001. We coordinate closely with the Office of Personnel Management and with the Department of Homeland Security to continue to recruit and educate the next generation of cybersecurity professionals broadly defined.

SFS makes awards to institutions of higher education to provide scholarships to undergraduate and graduate students in strong academic programs in cybersecurity and to develop and enhance those cybersecurity programs so that they can remain at the cutting edge and of the highest quality.

Students may be supported for up to three years, and in return, they agree to take cybersecurity positions in local, State, tribal, or Federal Government for the same duration as their scholarships.

To date, the overall placement in cybersecurity-related positions for SFS graduates in government is 94 percent. As of last month, there were 62 active SFS institutions, nearly 3,000 scholarship recipients over the 16 years of the program, over 2,000 graduates, and over 600 current scholarship-holders.

NSF's Advanced Technological Education, or ATE, program also has a very strong presence in information technology and cybersecurity education. That program makes competitive awards to community colleges that partner with other academic institutions and with local industry to education science and engineering students for technician positions. These are students at the undergraduate and secondary school levels. ATE funds comprehensive centers which may have either a national or regional focus, and currently, they are supporting six large cybersecurity-focused centers that serve the entire nation.

NSF also supports the development of a high technology workforce for the Nation at the undergraduate and graduate levels through several other programs, including the Research Experiences for Undergraduates program, which offers intensive summer research experiences in all areas of STEM, including cybersecurity.

Taking a longer view, NSF aims to fund projects that inspire K-through-12 students to consider high technology and cybersecurity careers. The SFS program has partnered with the National Security Agency to offer summer camps for K-through-12 students and teachers to build the pipeline.

And to help provide better access to computer science at the K-through-12 level, NSF has taken on a leading role in the Computer Science for All initiative with a commitment of $120 million over the next five years. Introduction to computational thinking and to elements of computer science at the K-through-12 level can help lay groundwork for the wider range of career choices later on.

Finally, NSF partners with other Federal agencies in cybersecurity education through the activities of the National Science and Technology Council Committee on STEM Education, the National Initiative for Cybersecurity Education, and the Cybersecurity National Action Plan.

Thank you so much for the opportunity to testify today on a topic that we at the NSF see as critical for our nation's future. I will be pleased to answer any questions that you and the other members of the committee may have.

[Prepared statement of Ms. Ferrini-Mundy follows:]

Testimony of

Joan Ferrini-Mundy, Ph.D.
Assistant Director for Education and Human Resources
National Science Foundation

Before the
Subcommittee on Information Technology

for the
Committee on Oversight and Government Reform
U.S. House of Representatives

September 22, 2016

"Closing the Talent Gap in Federal Information Technology"

Good afternoon, Chairman Hurd, Ranking Member Kelly, and other distinguished members of the Subcommittee. My name is Joan Ferrini-Mundy and I am the National Science Foundation's Assistant Director overseeing Education and Human Resources (EHR). I appreciate the opportunity to testify before you today.

The mission of NSF is "to promote the progress of science; to advance the national health, prosperity and welfare; [and] to secure the national defense..." NSF has a longstanding commitment to supporting research that drives scientific discovery, maintains America's global competitiveness, and builds the modern workforce that is critical for addressing the complex challenges that face the Nation. Within NSF, the mission of the EHR directorate is to provide the research foundation to develop a science, technology, engineering, and mathematics (STEM)-literate public and a diverse STEM workforce ready to lead science, engineering, and innovation for the future. Several NSF-supported programs have a key role in closing the talent gap in Federal information technology, and in the information technology (IT) workforce more generally. Here I highlight the NSF's CyberCorps®: Scholarship for Service (SFS) and Advanced Technological Education (ATE) programs in detail, and mention several other areas of investment that are critical to the development of the high-tech STEM workforce. I also will address NSF's contribution toward engaging, encouraging, and supporting a longer-term solution to the need for a larger and well-prepared Federal and national IT workforce of the future. Finally, I will briefly describe NSF's broader collaborations across the Federal government in the area of cybersecurity education.

The Cybersecurity Challenge and Preparation of Tomorrow's STEM Workforce

Advances in information technology (IT) have transformed all of our lives, enhancing our communications, expanding our capabilities, improving quality and personalization in a variety of sectors, and creating new economic and social opportunities. Every aspect of society has been transformed by the IT revolution, which is critical to national priorities in commerce, education, financial services, healthcare, manufacturing, and defense. Yet those same advances come with vulnerabilities: we hear all too often about cybersecurity breaches in government as well as major consumer companies, often impacting our own personal data. These incidents have increased a demand for cybersecurity professionals that far exceeds the supply. According to a report by the RAND Corporation in 2014[1], reports from numerous sources agree that there is a shortage of cybersecurity professionals and it is more pronounced for the federal government.

More broadly, as more recent innovations in IT such as machine learning, big data, artificial intelligence, sensor and instrumental technologies, the Internet of Things (IoT), and robotics shape daily life, education, and the workplace, NSF programs for the preparation of the computer science and STEM workforce play a key role in preparing the cybersecurity workforce of tomorrow, and also more generally a diverse STEM workforce that will be ready for leadership and innovation in data-rich and technology-enabled science, technology and engineering fields.

I will highlight briefly key programs at NSF for preparation of the cybersecurity workforce.

The CyberCorps®: Scholarship for Service Program

The CyberCorps®: Scholarship for Service (SFS)[2] program aims to develop a well-educated cybersecurity workforce for the government through engagement with educators (colleges and universities) and the target employers (government agencies). This program, originally named the Federal Cyber Service: SFS Program, was created as a result of a May 1998 Presidential Decision Directive (PDD-63)[3] which described a strategy for cooperative efforts by the government and the private sector to protect physical and cyber-based systems. In January 2000, a Presidential Executive Order defined the National Plan for Information Systems Protection[4], which included the Federal Cyber Services training and education initiative and the creation of a SFS program. More recently, *The Cybersecurity Enhancement Act of 2014* (Public Law No. 113-274) directed NSF, in coordination with the U.S. Office of Personnel Management (OPM) and the U.S. Department of Homeland Security (DHS), to continue the SFS program to recruit and educate the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, state, local, and tribal governments.

The SFS program funds institutions of higher education, on the basis of their proposals to the NSF competitive merit review system, to develop and enhance cybersecurity education programs and curricula and to provide scholarships to undergraduate and graduate students in strong academic programs in cybersecurity. The institutions must present a clear proposal for why their program is of high quality for the preparation of cybersecurity professionals, at the level of the National Security Agency (NSA) and DHS National Centers of Academic Excellence criteria. The students receiving scholarships must be U.S. citizens or lawful permanent residents of the US and must be able to meet the

[1] http://www.rand.org/pubs/research_reports/RR430.html
[2] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991
[3] http://fas.org/irp/offdocs/pdd/pdd-63.htm
[4] https://fas.org/irp/offdocs/pdd/CIP-plan.pdf

eligibility and selection criteria for government employment. Students can be supported on scholarships for up to three years, and in return, they agree to take government cybersecurity positions for the same duration as their scholarships. The government agencies eligible for job placement include Federal, state, local, or tribal governments. To assist both agencies and students in forging good matches, the NSF program requires a summer internship at a Federal agency. NSF also partners with OPM to host an annual job fair for SFS students and prospective Federal employers.

The SFS program aims for a 100 percent placement rate in government cybersecurity-related positions. The placement rates for the 2013 and 2014 graduating classes were 97 percent and 95 percent, respectively. The placements for the 2015 graduating class are not yet complete but at present 92 percent have been placed. The overall placement rate of SFS graduates in government is 94 percent. As of August 2016, there were 62 active SFS institutions, 2909 scholarship recipients, 2213 graduates and 612 current students. SFS scholarship recipients have been placed in internships and full-time positions in more than 140 Federal departments, agencies, and branches, including the NSA, DHS, Central Intelligence Agency (CIA), and U.S. Department of Justice (DOJ), along with state, local, and tribal governments.

The programmatic aspects of SFS represent forward-looking thinking in terms of what are the most effective means of preparation for cybersecurity professionals. As part of a broad education including computer science, SFS-funded programs incorporate emphases on data science, computer systems architecture, analytics and algorithms, statistics, engineering, social and behavioral sciences, and business and information science.

I would like to highlight the fact that the University of Texas at San Antonio (UTSA) successfully competed for an NSF SFS award, and over the course of six years, UTSA has provided scholarships to support 22 cybersecurity students. Of the students who have graduated from UTSA, all are reported to continue to be employed by the Federal government with the exception of two who deferred their government service commitment in order to obtain graduate degrees. UTSA is a Hispanic-Serving Institution (HSI) with more than 58 percent of its students coming from groups underrepresented in higher education. UTSA is just one example of how the SFS program is helping to increase the pool of well-prepared cybersecurity professionals for the Nation by recruiting students, including those from underrepresented groups, into cybersecurity and information technology careers.

Other established SFS projects are in place throughout the nation. For example, the SFS project at the New Mexico Institute of Mining and Technology provides practical, hands-on applications of cybersecurity coordinated among several academic departments. Research projects are integrated into advanced courses to enhance problem-solving skills. An underlying curriculum principle is to integrate cybersecurity context into all core computer science and engineering and IT courses.

At Carnegie Mellon University, which offers master's level work in cybersecurity, the SFS project features cutting-edge project-based coursework and requires a course in ethics and a project in cybersecurity. The SFS project at the University of Arizona recruits students from throughout the state, with a particular emphasis on recruiting and retaining underrepresented minorities. The project is cross-disciplinary and supports cybersecurity in its broadest definition, including information assurance, network security, information security risk management, and security management practices. The project contributes to meaningful curriculum development that can serve as a model for other programs.

At California State University, San Bernardino, most SFS students are first-generation minority students, transferring from community colleges, often from low-income and disadvantaged backgrounds. This project places great emphasis on ensuring that this diverse student cohort (50 percent Hispanic and 43 percent female) learns the skills required for them to successfully obtain and retain professional employment. Representatives of the program have mentored leaders of other institutions regarding the best practices in recruiting for diversity, placement strategies, leveraging university resources, and project management.

An additional thrust for SFS was put forward earlier this year. The President's Cybersecurity National Action Plan[5] proposes a CyberCorps Reserve program so that SFS alumni may be available over the course of their careers to help the Federal government respond to cybersecurity challenges. The NSF role, as proposed in the President's Fiscal Year (FY) 2017 Budget Request, would be to invest in "the expansion of the SFS program to lay the groundwork for SFS program alumni to be available over the course of their careers to serve the federal government's response to cybersecurity challenges." NSF is participating in a multi-agency effort led by the Office of Management and Budget (OMB) and OPM, along with DHS, the U.S. Department of Defense (DOD), and the U.S. Department of Energy (DOE), to develop models for rapid deployment of cybersecurity teams in crisis situations.

A second emphasis of the SFS program is expansion of the capacity of the U.S. higher education enterprise to prepare cybersecurity professionals who are highly qualified for a changing future. These efforts include research on the teaching and learning of cybersecurity, done in connection with the development of curricula, the integration of cybersecurity topics into relevant degree programs, and the design of virtual learning laboratories. In addition NSF supports strengthening partnerships between government and relevant employment sectors to effectively integrate applied research experiences into cybersecurity degree programs, and to integrate data science and other emerging topics into cybersecurity curricula.

Because the SFS program is a part of the larger cybersecurity ecosystem, SFS collaborates to stimulate the development of the cybersecurity workforce of the future. SFS supports "Inspiring the Next Generation of Cyber Stars" ("GenCyber") summer camps, to seed the interest of young people in this exciting and exploding new field, to help them learn about cybersecurity, and to learn how skills in this area could pay off for them in the future. These overnight and day camps are available to students and teachers at the K-12 level at no expense to them; funding is provided by NSF and NSA. A pilot project for cybersecurity summer camps in 2014 stimulated such great interest that the GenCyber program expanded in 2015, supporting 43 camps held on 29 university campuses in 19 states with more than 1,400 participants. In the summer of 2016, 120 camps at 68 institutions spanning 33 states, plus the District of Columbia and Puerto Rico) engaged about 4,000 students and about 800 K-12 teachers, with support from NSF and NSA.

The SFS program actively seeks to promote greater diversity in the cybersecurity workforce. As one strategy, the program has supported partnerships between majority institutions with strong cybersecurity programs and minority-serving institutions. For example, the University of North Carolina at Charlotte collaborates with two Historically Black Colleges and Universities (HBCUs), North Carolina A&T State University and Johnson C. Smith University, to support students earning bachelor's, master's, and doctoral degrees in cybersecurity. In 2013, NSF funded the launch of the annual Women in Cybersecurity Conference in 2013, an activity now supported by Facebook, Fidelity Investments, IBM,

[5] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

and many other industry, government, and academic partners. Since 2014, the Women in Cybersecurity Conference has maintained a continuing effort to recruit, retain, and advance women in cybersecurity. It brings together women (students, faculty, researchers, and professionals) in cybersecurity from academia and industry to share knowledge, experience, networking, and mentoring on an annual basis. Beyond the annual conference, Women in Cybersecurity has become a community of engagement, encouragement and support for women in the cybersecurity field.

Advanced Technological Education

NSF's Advanced Technological Education (ATE)[6] program addresses the need for IT and cybersecurity personnel at a different educational level and in a different way than SFS. With an emphasis on two-year colleges, ATE focuses on the education of technicians for the high-technology fields that drive our Nation's economy, including information technology and cybersecurity. The program involves partnerships between academic institutions and industry to promote improvement in the education of science and engineering technicians at the undergraduate and secondary school levels.

ATE supports curriculum development; professional development of college faculty and secondary school teachers; career pathways to two-year colleges from secondary schools and from two-year colleges to four-year institutions; research on the improvement of the preparation of the technology workforce, and other related activities.

The ATE program funds large, comprehensive Centers of Excellence, as well as smaller-scale, more focused projects. These efforts may have either a national or a regional focus. The following are the program's major awards supporting cybersecurity education:

Advanced Cyberforensics Education (ACE) Consortium (www.cyberace.org) (Florida) involves over a dozen institutions across Florida, Georgia, South Carolina, and North Carolina. The primary goals are to develop and disseminate cyberforensics curricula, provide professional development for faculty members, and create interest in cybersecurity among high school students.

Cyber Security Education Consortium (CSEC; www.cseconline.net/2014/) (Oklahoma) is a regional center that involves over 40 two-year academic institutions in eight states (Oklahoma, Arkansas, Colorado, Kansas, Louisiana, Missouri, Tennessee, and Texas). Over 100 faculty members offer courses based on CSEC's core information assurance and forensics curriculum, which encompasses information assurance principles, secure electronic commerce, network security, enterprise security management, and digital forensics. Particular emphases are automation and control systems security and mobile-device security.

Center for Systems Security and Information Assurance (CSSIA; www.cssia.org) (Illinois) focuses on providing faculty development and a cutting-edge virtual teaching and learning environment for cybersecurity. CSSIA's Faculty Development Academy has offered courses and workshops (both face-to-face and online) for thousands of educators. CSSIA's virtual teaching and learning environment has been adopted by several hundred educational institutions and is also used extensively for cybersecurity student competitions. CSSIA also leads several initiatives that encourage minorities, women, and veterans to pursue careers in cybersecurity.

[6] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5464

CyberWatch West (CWW; www.cyberwatchwest.org) (Washington) is a regional ATE center that focuses on cybersecurity education and workforce development in 14 Western states. Activities include providing model curricula, offering workshops for faculty, facilitating student participation in intercollegiate cyber defense competitions, and mentoring community colleges that aim to achieve designation as a National Center of Academic Excellence in Cyber Defense – 2-Year Education (CAE-2Y).

National CyberWatch Center (NCC; www.nationalcyberwatch.org) (Maryland) cultivates collaborations among educational institutions, businesses, government agencies, and professional organizations to grow and strengthen cybersecurity education programs and the cybersecurity workforce. NCC's network includes over 200 two-year and four-year institutions in almost all 50 states. Key initiatives include developing and updating cybersecurity degree and certificate programs in cyber defense, network forensics, network security administration, secure software development, and systems security administration; mapping curricula to federal and industry knowledge-and-skill standards, job roles, and professional certifications; and creating model transfer pathways that allow students to move between two-year and four-year degree programs.

Other Programs for the Preparation of Cybersecurity and IT Professionals

In addition to SFS and ATE, NSF hosts other programs that are intended to, in part, support the development of the IT and STEM workforce. One of these is the Research Experiences for Undergraduates (REU)[7] program, which offers intensive summer research experiences to nearly 5,000 college and university students every year in all of the fields of STEM supported by NSF—including computer science broadly and cybersecurity specifically. In cybersecurity alone, over a dozen NSF-funded REU Sites currently prepare students with research skills that will enable them to pursue graduate school or employment in areas spanning the security of critical infrastructure; security of mobile devices, wireless networks, cyber-physical systems, cloud computing, e-commerce, and software; privacy; and digital forensics.

Two other programs important to workforce development are funded with H-1B Visa Receipts. The Scholarships for STEM (S-STEM) program[8] supports undergraduates with high financial need to pursue STEM careers, and the Innovative Technology Experiences for Students and Teachers (ITEST)[9] provides support to engage K-12 students and teachers in experiences to prepare students to consider STEM and IT career options. Within both programs are examples of outstanding projects focused on preparation of cybersecurity professionals. For example, the ITEST program supports an award to excite girls about IT through after-school and summer programs, and a project to study the effectiveness of a career academy on information technology education. S-STEM supports a project at Capitol Technology University (Laurel, Maryland) for place-bound community college graduates so that they can complete a bachelor's degree at a distance, making it possible for them to join the cybersecurity workforce. Recruitment of new students focuses on minorities and first-generation college students who might not otherwise complete a bachelor's degree.

[7] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5517&from=fund
[8] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5257
[9] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5467

Developing a Computer-Literate Workforce and Society for the Future

Providing access to computer science (CS) education is a critical step to ensure our Nation remains competitive in the global economy and strengthens its overall cybersecurity. Educators and business leaders across the country are increasingly recognizing that CS is a "new basic" skill, necessary for economic opportunity and social mobility. CS is also an active and applied field of STEM learning that allows students to engage in hands-on, real-world interaction with key mathematics, science, and engineering principles. It gives students opportunities to be producers in the digital economy, not just consumers, and to be active participants and active citizens in our technology-driven world. The related computational thinking skills, relevant to many disciplines and careers, are increasingly included in education programs. Those include breaking a large problem into smaller ones, recognizing how new problems relate to ones that have already been solved, setting aside details of a problem that are less important, and identifying and refining the steps needed to reach a solution.

However, wide access to CS education is limited, and there are disparities even for those who do have access to these courses. For example, of the fewer than 10 percent of all high schools that offered any Advanced Placement® CS courses in 2015, only 22 percent of those who took the corresponding AP exam were girls, and only 13 percent were African-American or Latino.

Since 2008, NSF has led the "CS 10K" effort, funding researchers to develop rigorous and engaging curricula with the goal of preparing 10,000 teachers to teach computer science in 10,000 schools across the Nation. NSF is dedicated to broadening the participation of individuals in all fields of STEM, including CS. NSF has supported the research needed to establish best practices for engaging and retaining diverse student populations so that all students have the opportunity to see computer science as engaging, personally relevant and empowering. Through these efforts, NSF-funded projects are building an evidence-based foundation for K-12 CS education and an ecosystem of curricula, course materials, assessments, scalable models of professional development and online support networks and resources for teachers. In addition, The College Board, with funding from NSF, has launched a new Advanced Placement® (AP) computer science course called Computer Science Principles (CS Principles)[10] that is intended to explore the creative aspects of computing and increase the number and diversity of students entering the field. The first exam is scheduled to be administered in spring 2017, and hundreds of schools and colleges across the U.S. are already piloting the course. NSF is now sponsoring the development of an AP CS Principles course with an emphasis on cybersecurity.

NSF's investments in CS 10K since 2008 laid the groundwork for the Computer Science for All Initiative[11] announced in January 2016. As the lead Federal agency for building the research knowledge base for CS education, NSF has committed $120 million over the next five years to CS for All, in order to accelerate ongoing efforts to enable rigorous and engaging CS education in schools across the Nation. Those funds will support continued research and evaluation related to prototyping of instructional materials, scalable and sustainable professional development models, approaches to pre-service preparation for CS teachers, and teacher resources at the K-12 grade levels. NSF also will collaborate with the private sector to support high school CS teachers: as part of its million investments, NSF will pilot and expand professional development approaches in CS to additional schools across the U.S., with additional funding from industry that will enable teachers to attend these pilot programs. Infosys Foundation USA will be a founding member of this public-private collaboration with a $1 million philanthropic donation, and, as an initial participant, Tata Consultancy Services is providing additional support in the form of grants to

[10] https://advancesinap.collegeboard.org/stem/computer-science-principles
[11] https://www.whitehouse.gov/blog/2016/01/30/computer-science-all

teachers in 27 U.S cities. This collaboration will ultimately provide opportunities for as many as 2,000 middle and high school teachers to deepen their understanding of CS.

NSF invests heavily in the preparation of the STEM workforce for tomorrow. Since its founding, NSF has invested in advancing science and the people who would both conduct that science, and be part of the society that will use and appreciate science. Today we have a range of programs that are directly focused on the preparation of the broader STEM workforce, from the Graduate Research Fellowship Program (43 Nobel Laureates were recipients of this fellowship), to the Noyce Teacher Scholarship program, to the EHR Core Research strand on the STEM professional workforce.

Federal Agency Coordination for Cybersecurity Education and STEM Workforce Preparation

NSF continues to work closely with the National Initiative for Cybersecurity Education (NICE)[12] to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. The National Institute of Standards and Technology (NIST) is leading the overall NICE initiative in collaboration with other federal departments and agencies, including NSF, as well as state government, academia, and private industry to build on successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure. One of the primary ways in which NSF is actively engaged with this initiative is through the NICE Interagency Coordinating Council (ICC). The NICE ICC convenes NICE federal government partners for consultation, communication, and coordination of policy initiatives and strategic directions for cybersecurity education. NSF further participates in NICE Education Groups which particularly focus on strategies and recommendations for filling the cybersecurity pipeline through primary, secondary, and post-secondary education.

NSF Director Dr. France Córdova co-chairs the National Science and Technology Council's (NSTC) Committee on STEM Education (CoSTEM), with Dr. Jo Handelsman of the Office of Science and Technology Policy (OSTP). The Federal Coordination in STEM Education Task Force (FC-STEM), which I co-chair with Donald James from NASA, is a subgroup of CoSTEM focused on implementation of CoSTEM's *STEM Education 5-Year Strategic Plan*[13]. Recently, an interagency working group was established on Computer Science for All under the purview of FC-STEM and in connection with the 5-Year Strategic Plan, to develop a strategic framework for government investment in computer science education. NSF co-leads that working group, in partnership with the U.S. Department of Education and OSTP.

Conclusions

Continued investment in fundamental research and development is necessary to improve the preparation of a diverse STEM workforce, ready for innovation and leadership in tomorrow's science and engineering. A critical component of that investment is in the area of preparation of cybersecurity professionals, in order to ensure that our Nation's cyber systems are secure and trustworthy, and that the next-generation science and engineering workforce is increasingly cyber-aware, prepared with the knowledge to keep our systems secure. And, the more general education of tomorrow's scientists and engineers, as well as the preparation of all to be STEM-literate, can include attention to fundamental topics in computer science to help raise general levels of awareness and practice for cyber-awareness. With ongoing support and leadership for cybersecurity research, research and new models in cybersecurity education, and development of the STEM workforce, in both the Executive and Legislative

[12] http://csrc.nist.gov/nice/index.htm

[13] https://www.whitehouse.gov/sites/default/files/microsites/ostp/stem_stratplan_2013.pdf

Branches, NSF and its partners contribute to the protection of our national security and the enhancement of our economic prosperity. This concludes my remarks. I would be happy to answer any questions at this time.

For additional information please see the program solicitations of the CyberCorps®: Scholarship for Service program as well as the Advanced Technological Education program. Portions of this testimony were drawn from the written testimony of Jeremy Epstein, former lead program director for NSF's Secure and Trustworthy Cyberspace (SaTC) program, before the Senate Committee on Commerce, Science, and Transportation on September 3, 2015.

Mr. HURD. Well, Dr. Ferrini-Mundy, I have got to say, we have only been doing this for five minutes, you have already gotten me excited about a couple of things that you mentioned in your opening remarks.

And also, I want to add I was a beneficiary of an NSF program when I was in high school. I got to do an internship at the Southwest Research Institute in San Antonio in robotics, and that got me excited about computer science, and that is why I studied computer science at Texas A&M University. So I am a big fan of what you all do. And this is something that I want to make sure more kids like me have access to this. So thank you for being here.

Mr. Montgomery, you are now recognized for five minutes.

STATEMENT OF SCOTT MONTGOMERY

Mr. MONTGOMERY. Good afternoon, Chairman Hurd and members of the committee. Thank you for the opportunity to testify today. My name is Scott Montgomery. I'm the vice president and chief technical strategist of the Intel Security Group, and my testimony will focus on cybersecurity skills gap and what the government, in collaboration with the private sector, can do to close it.

I've been—I've spent 20 years building, designing, testifying—or, excuse me, testing and certifying information security and privacy solutions for a variety of public and private sector organizations.

Intel is a global leader in computing innovation, designing and building the essential foundational technologies that support the world's computing devices. When you combine this experience with Intel Security's market-leading cybersecurity solutions, we bring a unique understanding of the challenges threatening our nation's digital infrastructure and global e-commerce.

Despite facing an ever-changing threat landscape, further complicated by the sharp rise in Internet-enabled devices in our personal lives, the job for security practitioners hasn't changed: Protect vital services and data from theft, manipulation, and loss due to external and internal adversaries. We do, however, need to change the way we do our job by focusing on ways to reduce security fragmentation, automate tasks, and force multiply capabilities.

Organizations both in the public as well as private sector are now more vulnerable in more places. Adversaries are increasingly capable of commandeering strategic assets and including the critical infrastructure, yet most organizations still lack the resources necessary to adequately monitor their networks and defend against these sophisticated attacks.

Earlier this year, the Center for Strategic and International Studies, in partnership with Intel Security, released "Hacking the Skills Shortage," a global report outlining the global talent crisis. The results of the research were both stunning and informative.

A majority of respondents—82 percent—admitted to having a shortage of cybersecurity skills, with 71 percent citing this shortage as having a direct and measurable impact upon their organization and making them more valuable hacking targets.

In 2015 alone, 209,000 cybersecurity jobs went unfilled in the United States, in just the United States. Despite 1 in 4 respondents confirming their organizations have lost proprietary data as a result of this specific skills gap, there are no signs that this work-

force shortage will abate in the near term. Respondents estimated an average of 15 percent of their company's available cybersecurity positions could go fully unfilled by 2020.

If the demand for these professionals continues to outpace the supply of qualified workers, the United States will face a deficit of around one million workers in the next five to ten years. With expanding attack surfaces and an increasing advanced targeted attacks around the world, the need for a technically stronger and numerically increased cyber workforce is critical.

So one of the immediate steps we can take to address this issue, in addition to many other sound policy recommendations, the President's Cybersecurity National Action Plan, CNAP, calls for a $62 million increase in spending to expand training and educational programs. Specifically, the plan would build out the existing CyberCorps Scholarship for Service program, which provides cyber education scholarships in exchange for service in the Federal civilian government. This investment is a great step forward, but we need to be prepared to do a lot more.

In particular, we recommend an even larger financial investment in existing Federal workforce and education programs, a diversity of career paths for interested students, and stronger coordination on these initiatives with the private sector and industry.

As Intel Security vice president and general manager Chris Young and Chairman Hurd have both urged in the past, the government should consider the creation of a Cyber National Guard program. The CyberCorps Scholarship for Service and reserve programs are ideally situated for students looking to pay back their scholarships up front with two or three years in Federal service.

Also, at the State or Federal level, an expanded SFS or SFS-style grant program could train and educate a new class of cyber practitioners prepared to serve their government on a full-time, part-time, or as-needed basis while gaining critical experience with the latest private sector innovations.

The private sector must also be prepared to level-up its collaboration with the government to ensure a steady supply of worthwhile internships, co-ops, and training opportunities. In the CSIS report, a lack of quality training opportunities was cited as a significant reason why cyber practitioners seek alternative employment. For this reason, it is not only imperative that public sector entities compensate their cyber professionals well but also provide ample opportunities for employees to learn new skills and train on cutting-edge technologies.

Intel supports these efforts through a number of initiatives, including investments in STEM education for women and girls, curriculum development, a robust paid internship program, and partnerships with universities like Purdue, the University of Massachusetts, and the U.S. Air Force Academy.

Finally, investing in more efficient technologies and modernizing outdated IT systems will reduce the burden on scarce human resources. The CNAP prioritizes this by calling for a $3.1 billion IT modernization fund to transform cybersecurity management. This initiative has received some congressional support with the introduction and successful markup of the MOVE IT Act, which would enable retirement, replacement, and modernization of legacy IT

that is difficult to secure and expensive to maintain, and reward government departments and agencies who go through harvesting money back out of their programs.

Building out these education and workforce initiatives, in tandem with investments in more efficient cyber technologies, will make a vital down payment toward closing the cybersecurity skills gap.

I would like to once again thank this distinguished panel for giving me the opportunity to discuss these challenges and strongly believe that public-private collaboration will continue to be our best defense. Thank you.

[Prepared statement of Mr. Montgomery follows:]

WRITTEN STATEMENT FOR THE RECORD OF SCOTT MONTGOMERY, VICE PRESIDENT, INTEL SECURITY GROUP CHIEF TECHNICAL STRATEGIST, before the UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON INFORMATION TECHNOLOGY, "Hearing On Closing the Talent Gap in Federal IT"

SEPTEMBER 22, 2016

Good afternoon Chairman Hurd, Ranking Member Kelly, and members of the committee. Thank you for the opportunity to testify today. I am Scott Montgomery, Vice President and Chief Technical Strategist, Intel Security Group, part of Intel Corporation. I am pleased to address the committee on the challenges facing the federal government and the private sector in hiring and retaining qualified cybersecurity professionals. The shortage of these professionals is an interconnected challenge, one that impacts both public and private sector organizations given the common threats they face and the mobility and increasingly connected nature of today's work force. As a member of one of the world's leading cybersecurity companies, my testimony will focus on the skills gap in the cybersecurity ecosystem of companies and governments, and what the government, in collaboration with the private sector, can do to close it.

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity. I work for the Intel Security Group Chief Technology Officer (CTO) and manage the worldwide team that carries CTO titles. Together we drive the company's technical innovation, evangelize our expertise, thought leadership, and offerings to public and individual audiences, and work to increase the public trust by cooperating with law enforcement on cybercriminal investigations and disruption. With more than 20 years in content and network security, I bring a practitioner's perspective to the art and science of cybersecurity. I have designed, built, tested, and certified information security and privacy solutions for such companies as McAfee, Secure Computing, and a wide variety of public sector organizations.

INTEL'S COMMITMENT TO CYBERSECURITY

Intel is a global leader in computing innovation, designing and building the essential foundational technologies that support the world's computing devices. Combining Intel's decades-long computing design and manufacturing experience

with Intel Security's market-leading cybersecurity solutions, we bring a unique understanding of the cybersecurity challenges threatening our nation's digital infrastructure and global e-commerce. Governments, businesses, and consumers face a cybersecurity threat landscape that is constantly evolving every day with each new technology that is brought to market at a faster pace than ever before. The sharp rise of internet-enabled devices in government, industry, and the home exacerbates this already difficult challenge. It is thus critical that we collaborate and coordinate our efforts across the public and private sectors to ensure the safety and prosperity of our collective digital future while promoting innovation, protecting citizens' privacy and civil liberties, and preserving the promise of the Internet as a driver of global economic development and social interaction.

With the rising volume and complexity of threats, the shrinking time and resources available to handle them, and now the dramatic increase in internet-enabled devices and delivery mechanisms such as cloud computing, security practitioners must evolve their approach. The job hasn't changed: protect vital services and data from theft, manipulation, and loss due to external and internal adversaries. But we need to change the way we do the job by focusing on ways to reduce security fragmentation, automate tasks, and force-multiply capabilities.

Intel Security believes that a platform-driven approach best enables organizations to effectively block threats, identify compromises, and expedite remediation. It's at the center of our commitment to making what we call the "Protect, Detect, and Correct" life cycle easy for organizations to deploy to enable a safe and connected world. Focusing on open, integrated solutions to work within a platform and placing a premium on the development of easy-to-use customer interfaces can expedite the threat defense life cycle and help organizations optimize the use of valuable resources like trained cybersecurity professionals.

THE THREAT LANDSCAPE

Over the past decade, attackers have evolved from recreational "hackers" with limited capabilities to organized crime and state-sponsored adversaries with dedicated resources and highly skilled personnel. At the same time, as organizations become increasingly reliant on digital infrastructure, security breaches can have a more pervasive and cascading impact on data security and operational resiliency. Organizations are more vulnerable in more places.

Adversaries are now capable of commandeering strategic assets and critical infrastructure. Yet most organizations still lack the resources necessary to adequately monitor their networks and defend against increasingly sophisticated attacks.

Add to that the sobering realization that while adversaries' goals remain relatively easy, trying to find the lowest hanging fruit in terms of a weak system or an undertrained or cooperative insider, defenders must be impenetrable 100% of the time. Today we realize as an industry this goal is mathematically unlikely to be achieved, even for properly funded and adequately staffed security vendors or large corporations.

The Global Cybersecurity Skills Gap:

Earlier this year, the Center for Strategic and International Studies (CSIS), in partnership with Intel Security, released "Hacking the Skills Shortage", a global report outlining the talent shortage crisis impacting the cybersecurity ecosystem across companies and nations. The results of the research were both stunning and informative.

A majority of respondents (82 percent) admit to a shortage of cybersecurity skills, with 71 percent of respondents citing this shortage as having a direct and measurable impact on organizations whose lack of cyber talent makes them more attractive hacking targets.[1] In 2015, 209,000 cybersecurity jobs went unfilled in the United States alone.[2] Despite 1 in 4 respondents confirming their organizations have lost proprietary data as a result of their cybersecurity skills gap, there are no signs that this workforce shortage will abate in the near-term.[3] Respondents estimated an average of 15 percent of their company's available cybersecurity positions could go unfilled by 2020.[4]

If the demand for cybersecurity professionals continues to outpace the supply of qualified workers—and all the evidence suggests it will—the United States could

---

[1] Center for Strategic and International Studies, *Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills*, p. 4, (May 2, 2016), http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

[2] Id. at 5.

[3] Id. at 7, 8.

[4] Id. at 7.

face a cybersecurity skills deficit of around 1 million workers in the next 5 to 10 years.[5] With the increase in cloud, mobile computing, and the Internet of Things, as well as advanced targeted cyberattacks and cyberterrorism across the globe, the need for a technically stronger and numerically increased cybersecurity workforce is critical.

Intel's Commitment to Closing the Skills Gap:

Public Private Partnerships

Given the current cybersecurity skills shortage, organizations across the spectrum cannot manage their protective defenses alone. Security is a shared goal carrying a shared responsibility. As a result, the strategic partnerships that have grown between public and private sector entities over the last two decades have never been more important.

At a national level, critical industry sectors supporting the safety, security, and economic growth of the United States were among the first to self-organize in partnership with government agencies to assess and mitigate threats to U.S. critical infrastructure. These public-private partnerships are fueled by a joint commitment to defend critical infrastructures against increasingly sophisticated cyberattacks, and they thrive on sharing threat indicators, best practices, and incident response in a mutual, non-regulatory environment.

Intel has been active in many of these partnership initiatives for more than 10 years. Just a few important examples where Intel has a leadership presence include:

- President's National Security Telecommunications Advisory Committee
- Information Technology Sector Coordinating Council
- Information Technology Information Sharing and Analysis Center
- National Cyber Security Alliance
- National Cybersecurity Center of Excellence
- Cybersecurity Framework

Through these partnerships, Intel works to provide hardware, software, and training to advance the rapid adoption of secure technologies around the country. In addition, we remain actively engaged in the development of new cybersecurity

[5] Id. at 5.

guidelines to help public and private sector organizations evaluate their security postures and conduct risk assessments, regardless of size or sophistication.

As these partnerships grow and mature, our company will continue to invest, engage, and contribute. The challenge is never-ending, but we have no doubt that the public-private partnership model will continue to protect and serve our national interests well into the future.

Intel's Investment in Education

Intel believes that young people are the key to solving these global challenges. A solid math and science foundation coupled with such skills as critical thinking, collaboration, and problem solving are crucial for their overall success and the competitiveness of the United States. By making significant investments in STEM programs at high schools and universities, we are addressing one of the most pressing elements of our nation's technology skills deficit and giving students the core skills they need to join the cybersecurity work force. For instance:

- Intel has invested over $1 billion and Intel employees have donated over 5 million hours in the past decade toward improving STEM education in the U.S. and internationally.

- We have invested over $670 million in university programs since 2001 to foster the next generation of technology innovators and leaders. We are collaborating with 700 researchers and 95 universities to enhance teaching resources, develop student courseware, and fund world-class research and technology competitions in information technology fields like security, cloud, and big data.

- Our internship program funds over 100 paid internships each year, providing undergraduate and graduate students with opportunities to work on complex projects that span our product portfolio, including security.

- We have invested more than $100 million annually in programs that promote STEM education, encourage women and girls to seek careers in technology, foster and celebrate innovation and entrepreneurship among the best and brightest young students in the world, and help teachers incorporate best practices in math, science, and classroom technology in their work.

- Our cybersecurity business unit takes pride in empowering families with the tools they need to defend themselves from online threats ranging from cybercriminals to cyberbullies. In 2009, Intel employees began volunteering to teach school-aged children how to use their digital devices responsibly in pilot programs across the United States. Since the original launch of McAfee Online Safety for Kids, the program has vastly grown and maintains a wide global reach. To date, Intel volunteers have educated more than 250,000 children, parents, and teachers worldwide about how to remain safe and secure online.

- Our cybersecurity business unit also donates coursework and professional services through partnerships with a number of flagship state universities, including Purdue and UMass Amherst, to enable students to successfully train in the cybersecurity operations centers that protect their institutions and come away with valuable work experience.

Policy Recommendations to Close the Skills Gap:

In addition to many other sound policy recommendations, the President's Cybersecurity National Action Plan (CNAP) takes steps to reverse the cyber talent shortage in the United States with a $62 million increase in spending to expand cybersecurity training and education programs. In particular, the Plan would build out the existing CyberCorps Scholarship-for-Service (SFS) program, providing cyber education scholarships to Americans seeking to serve their country in the federal civilian government. This investment represents a great step forward, but we must be prepared to do much, much more.

The fierce competition over qualified cybersecurity practitioners that currently exists between the public and private sector will continue unless we can begin producing enough new recruits each year to fill the skills gap. That is why we recommend an even larger financial investment in existing federal cyber workforce and education programs, a diversity of career paths for interested students, and stronger coordination on education and workforce initiatives with the private sector.

As Intel Security Senior Vice President and General Manager Chris Young and Chairman Hurd have urged in the past, the government should consider the creation of a Cyber National Guard program. The CyberCorps Scholarship-for-Service and Reserve programs are ideally situated for students looking to pay back

their scholarships up-front, with two or three years in federal service. But for students interested in serving their government while jumpstarting a career in the private sector, creating an alternative path to scholarship repayment could bring even more talent to bear. At the state or federal level, an expanded SFS or SFS-style grant program could train and educate a new class of cyber practitioners prepared to serve their government on a full-time, part-time, or as-needed basis while gaining critical experience with cutting-edge private sector innovations. The National Guard has had great success producing talented individuals with diverse skill sets, ready to serve their country in times of need, and it would be worth considering how to apply a similar formula to a cybersecurity context.

The private sector must also be prepared to level-up its partnerships with the government and others in industry to ensure a steady supply of worthwhile internships, co-ops, and training opportunities. In the CSIS report, a lack of quality training opportunities was cited as a significant reason why cyber practitioners seek alternative employment.[6] For this reason, it is not only imperative that public sector entities compensate their cyber professionals well, but also provide ample opportunities for employees to learn new skills and train on new technologies. With more robust public-private partnerships in this area, private companies in different industries can reach individuals at every stage in their career and engage them with new opportunities to learn about a wide variety of digital environments and next-generation technologies.

Finally, investing in technologies capable of reducing the burden on existing human resources and modernizing outdated IT systems will benefit organizations of all sizes. The CNAP invests over $19 billion in cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget. This represents more than a 35 percent increase in cybersecurity spending from the FY 2016 budget, a necessary investment to help secure our nation in the future. The Plan also calls for a $3.1 billion Information Technology Modernization Fund to modernize government IT systems and transform cybersecurity management. This initiative would enable the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain. Just last week, the House Committee on Oversight and Government Reform Committee reported the Modernizing

---

[6] *Hacking the Skills Shortage* at 19.

Government Technology Act of 2016 out of committee that authorizes the Administration's Information Technology Modernization Fund. By ensuring that these programs invest in truly cutting-edge information technology solutions that benefit from increased automation, user-friendly interfaces, and strong cybersecurity capabilities, Congress can make a vital contribution to securing critical federal assets.

These education and workforce investments, in tandem with CNAP's other cyber initiatives, will make a vital down payment to help close cybersecurity skills gaps in government and the private sector. Intel is committed to supporting the CNAP's cyber workforce efforts and expanding initiatives like the CyberCorps SFS program, but only the federal government can lead the response. The CNAP is a great step forward, but to remedy our alarming cyber talent deficit we will likely need to recruit more than a million Americans trained in cybersecurity and information assurance.

Conclusion:

I would like to once again thank this distinguished panel for giving me the opportunity to discuss the challenges facing the federal government and the private sector in hiring and retaining qualified cybersecurity professionals. We believe that public-private collaboration will continue to be an effective defense against cyberattacks growing in frequency and sophistication. While much progress has been made, more needs to be done—particularly to close the cyber skills gap nationwide. The government should expand the CyberCorps Scholarship-for-Service and Reserve programs and consider creating a Cyber National Guard program to give students new options to pay back their cybersecurity scholarships with federal service. The government should also increase investments in modern, secure information technologies to help protect federal agencies and enable CIO's to effectively leverage their scarce pool of cybersecurity talent. Paying down these "cyber debts" in people and technology will require both industry and government to step up and make hard choices, and Intel looks forward to continuing our engagement on these matters in the future.

Mr. HURD. Thank you, Mr. Montgomery, and thank you for the reference of the MOVE IT Act, which we had to rename the MGT Act, which passed this morning by the way, and that is a pretty significant thing and it was because of the great leadership of folks like Robin Kelly to make that happen.

And I also want to thank your organization and Ms. Kelly because this idea of a Cyber National Guard really sunk in with me at our field hearing in Chicago. And I am glad we went and did that, and I am glad, through you all's participation, and it really is what—you know, that kind of collaboration outside the Beltway with, you know, participants, you know, outside the government where you really get some of these cutting-edge ideas. So thank you for that.

Mr. Bowman, welcome. Did you bring me any breakfast tacos?

Mr. BOWMAN. I should have. I ate them. Sorry.

Mr. HURD. Well, Mr. Bowman, you are now recognized for your opening remarks for five minutes.

STATEMENT OF GENE BOWMAN

Mr. BOWMAN. Thank you very much. Mr. Chairman and members of the committee, I'm pleased to be here today speaking to you on behalf of the Alamo Academies.

The Academies are an outstanding program providing opportunities and clear pathways for young men and women to achieve their American dream. I would like to briefly describe the model, then spend the remainder of the time sharing a few stories of our successful graduates who are today closing the talent gap in the Federal IT career field, as well in the private sector.

The Alamo Academies is an innovative STEM—you heard it before, science, technology, engineering, mathematics—demand-based model connecting high school juniors and seniors with employers. These students earn 30 college credits at no personal cost, they obtain nationally recognized industry certificates, and they participate in an experiential learning environment between their junior and senior summer, a paid internship, the program's key component kind of like what you did earlier in your career, where they have the opportunity during this internship to apply the knowledge and skills they learned in the college classroom in a real-world environment leading to high-wage jobs or further higher education while addressing critical workforce needs.

And let me tell you about five of our graduates who are cyber warriors today. Two of them are 22, one is 19, and the other two are 18 years old, and all five share the following experiences. They participated in the Academy's Information Technology Security Academy. They completed paid internships with cybersecurity industry partners. They all have earned multiple national industry certificates. They all competed in the Air Force Association's CyberPatriot competition. They were all on the Academy's team that won the local mayor's Cyber Cup competition as the best CyberPatriot team in the San Antonio region. And each of their teams also made it to the top 12 in the Nation and competed in the CyberPatriot National Championship in Washington, D.C.

As a side note and bragging a little bit, the Academy's team has won the mayor's Cyber Cup and advanced the national champions

competition five out of the last six years. Two of these young men, Mario and Robert, were on the National Championship Team in 2012. Both Mario and Robert and the other 14 members accomplished their paid internship with the Department of Defense at the Air Force's 33rd Network Warfare Squadron as entry-level security analysts. Each was awarded a secret clearance at 17 years of age and also offered part-time employment during their senior year helping defend our nation.

At 22, Mario already has six years of intense cybersecurity experience supporting DOD initiatives, and shortly after graduation from the Academies, Mario was offered a position at the Pentagon right down the road here as a computer network defense analyst with an interim top-secret SCI clearance. He recently returned to San Antonio as a lead cybersecurity analyst with a DOD contractor supporting the Air Force's Weapon and Tactics Team known as the Computer Emergency Response Team, which I know you're familiar with.

Mario has also added recruiter to his duties. He recruited two of our recent graduates to be part of our Cyber Warrior talent pipeline. These two graduates, Reed and Kyle, are both 18. They're CyberPatriot national finalists, completed paid internships with cybersecurity industry partners, and are starting their careers as tier II security analysts.

Finally, two other examples, Skylar and Robert, Skylar is 19 years old, CyberPatriot national finalist—seeing a theme here—and is employed as a security analyst with the same cybersecurity consulting agency in San Antonio that he accomplished his paid internship with, a smart move by that company, growing their own workforce.

Robert, 22, has taken his cybersecurity talent into the private sector. He's a security analyst, is a member of the Information Security Operations Center for his IT company in San Antonio. All of these young men have accelerated their careers with great salaries, benefits, and no college debt. They're having a transformational impact on their families and our community. These outstanding graduate stories are part of today's submitted written testimony.

So the moral of this story, a solid model, the Alamo Academies, a community collaborative with college-level instruction, national industry certificates integrated into the curriculum, connected to industry through paid internships where the student receives real-world experiences and mentoring and providing opportunities to participate in competitive programs like CyberPatriot. It's producing outstanding talent immediately out of high school to help close the talent gap in Federal IT and the private sector.

I want to thank you for your time and the opportunity to share the Alamo Academies story.

[Prepared statement of Mr. Bowman follows:]

Testimony of

Colonel Olen "Gene" Bowman, USAF, Ret.

Executive Director
Alamo Academics

San Antonio, Texas

Before the hearing
Subcommittee on Information Technology
of the
U.S. House of Representatives
Committee on Oversight and Government Reform

Regarding
Closing the IT Gap in Federal IT

September 22, 2016

ALAMO COLLEGES

ALAMO ACADEMIES

Table of Contents

ALAMO COLLEGES

ALAMO ACADEMIES

I. Introduction

Mr. Chairman and Members of the Committee, I am pleased to be here today speaking to you on behalf of Alamo Academies. Alamo Academies is an industry-driven, demand-based, workforce and economic development program. Over the past 15 years, this community collaborative program has served as the pathway for young men and women to achieve the American Dream.

II. Alamo Academies -- Advancing the School-to-Career Pathways

Alamo Academies, a non-profit organization, is a national award winning, innovative, Science, Technology, Engineering and Mathematics (STEM) based model partnering with industry, the Alamo Community College District, high schools and municipalities.

San Antonio addressed the "skills-gap" issue by founding Alamo Academies. Our model provides the region high-tech, high-skilled talent by developing a pipeline of college educated technicians to staff new jobs and replace a retiring workforce in targeted industry clusters: Aerospace, Advanced Manufacturing, IT & Security, Nursing and Heavy Equipment.

This model provides high school juniors and seniors with tuition-free career pathways into critical demand STEM occupations. Students attain industry and academic certificates leading to high-wage jobs or further higher education while addressing critical workforce needs. Over 1,200 graduates have received experiential training in industry-driven curricula resulting in 95% of the two-year graduates entering higher education or high-wage careers.

The Framework

Target: High School Juniors and Seniors

1. Industry Demand-driven and Collaborative Program
2. Dual Credit Program of Studies Leading to College Diploma
3. Nationally Recognized Industry Certifications
4. Stackable Credentials
5. Comprehensive Student Support Systems

Figure 1

ALAMO COLLEGES

ALAMO ACADEMIES

Since inception in 2001, we have been recognized as a "Best Practice" model by the Manufacturing Skill Standards Council (MSSC) and Texas Higher Education Coordinating Board (THECB). Alamo Academies received the prestigious Bellwether Award recognizing outstanding and innovative programs that successfully lead community colleges into the future.

National Journal cited Alamo Academies as one of the nation's top workforce innovations. Joe Wilson, Lockheed Martin (retired), stated *"We were trying to develop a strategy to replace a retiring workforce and wanted to make sure we transferred the knowledge and experience employees had before they retired. We partnered with the Alamo Colleges to develop a pipeline of young workers prepared to take jobs in our industry. The rest is history."*

Conceptual Model

Alamo Academies is an educational model driven by industry's projected/quantifiable workforce requirements. It is a collaborative process identifying curriculum pathways, recruitment, matriculation, support systems and target enrollment. Students are bussed to an Alamo Colleges campus daily where they engage in 2 ½ hours of experiential learning. During the two-year program of studies, students earn more than 30 college credits with courses articulating to an Associate of Applied Science (AAS) degree at no personal cost. Upon graduation, students can either attain a high-wage/high-skill career in a demand occupation or continue with their higher education pathway. The Academies model is replicable as evidenced by the additional pathways created. While the first program in 2001 focused on Aerospace, the model has produced four additional pathways: IT & Security (2002); Advanced Manufacturing (2004); Health Professions (2009); and Heavy Equipment (2014).

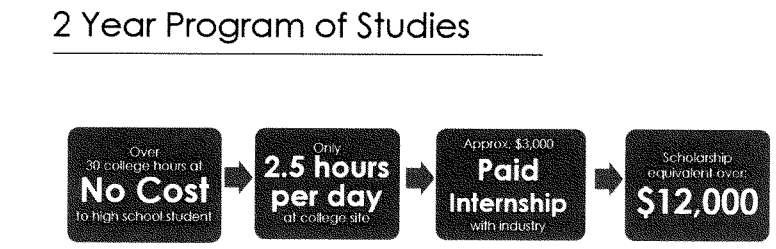


Figure 2

ALAMO COLLEGES

ALAMO ACADEMIES

Paid Internships

As a key component of the program of studies, students participate in a mandatory paid internship – the ultimate real world experience. During the summer between their junior and senior year, students earn approximately $3,000 and college credit from their internship. Klaus Weiswurm, CEO of ITM, states *"we have seen that the paid internship component is such a transformative element in the maturation of the student. It is also beneficial to the industry partner as they have the opportunity to closely observe the work ethic and skills of the potential employee prior to actually hiring them."*

Community Partnerships

Each partner provides a unique contribution. Alamo Colleges provide facilities, equipment and instruction; each Independent School District (ISD) provides textbooks and round trip transportation; employers pay their intern's salaries; and municipalities fund operating costs.

Testament to community support is San Antonio's city ordinance stating *"The Academies represent a cost-effective economic development investment for the City and also reinforces the stated goals of the City's Strategic Plan for Enhanced Economic Development."*

Graduates Data
(2001 - 2016)

1,269 Graduates	
Continue to Higher Education / Industry	95%
Industry Certificates Awarded	2,370
Economically Disadvantaged	86%
Annual Student Enrollment	400

Diversity	
Hispanic	70%
Caucasian	22%
African-American	6%
Asian	2%

Gender	
Male	78%
Female	22%

Figure 3

ALAMO COLLEGES

ALAMO ACADEMIES

III: IT & Security Program Curriculum & Associate of Applied Science (AAS) Degree Pathway

Industry partners' involvement ensures that curriculum aligns with changing industry needs while keeping our students a valuable asset to the workforce. The Alamo Academies curricula allow students to earn stackable credentials encouraging them to continue their professional growth and promote lifelong learning.

For example, the first page of the IT & Security curriculum describes the Academies dual credit program of studies to include industry and college workforce certificates while the second page describes the courses articulating to the AAS degree (shown in red).

ALAMO COLLEGES

ALAMO ACADEMIES

Information Technology and Security Academy

1st Year Program of Studies
5 courses with total of 18 credit hours

Fall Semester		Credit
ITSC 1305	Intro to PC Operating Systems *Introduction to personal computer operating systems including installation, configuration, file management, memory & storage management, control of peripheral devices & use of utilities.*	3
ITSC 1425 *Testout Certification PC Pro	Personal Computer Hardware* *Current personal computer hardware including assembly, upgrading, setup, configuration, and troubleshooting.*	4
	Fall Semester Total	**7**

Spring Semester		Credit
ITNW 1425 *Testout Certification Network Pro	Fundamentals of Networking Technologies* *Introduction to architecture, structure, functions, components & models of the internet. Covers principles and structures of IP addressing, Ethernet, media & operations.*	4
ITSC 2439	Personal Computer Help Desk Support *Diagnosis and solution of user hardware and software related problems with on-the-job and/or simulated projects.*	4
	Spring Semester Total	**8**

Summer Semester		Credit
ITSC 2364	Practicum: Computer & Information Sciences, General *Practical, general workplace training supported by an individualized learning plan.*	3
	Summer Total	**3**
	Year 1 Program Total	**18**

Level I Certificate of Completion
Computer Desktop Support Technician

2nd Year Program of Studies
4 courses with total of 12 credit hours

Fall Semester		Credit
ITSC 1316 *Testout Certification LINUX Pro	LINUX Installation & Configuration* *Introduction to the UNIX operation system including multi-user concepts, terminal emulation, use of system editor, basic UNIX commands, & writing script files. Includes introductory system management concepts.*	3
ITSY 1342 *Testout Certification Security Pro	Information Technology Security* *Instruction in security for network hardware, software, and data including physical security, backup procedures, relevant tools, encryption, and protection from viruses.*	3
	Fall Semester Total	**6**

Spring Semester		Credit
ITSE 1302	Computer Programming *Introduction to computer programming with emphasis on the fundamentals of design, development, testing, implementation, and documentation. Includes language syntax, data and file structures, input/output devices, and files.*	3
ITSE 1311	Beginning Web Programming *Skill development in web page programming including mark-up and scripting languages.*	3
	Spring Semester Total	**6**
	Year 2 Program Total	**12**

Level I Certificate of Completion
Information Technology & Security

Two Year Program of Studies: 9 Courses totaling 30 credit hours

Information Technology and Security Academy

Level I Certificate of Completion
Computer Desktop Support Technician

Level I Certificate of Completion
Information Technology & Security

ASSOCIATE OF APPLIED SCIENCES

Computer Support Specialist

Semester 1		Credit
ITSC 1301	Introduction to Computers *or other**	3
ITSC 1309	Integrated Software Applications	3
ITSC 1305	Introduction to PC Operating Systems *or other**	3
ENGL 1301	Composition I	3
	Select Additional communication (90) Core	3
	1st Semester Total	15

Semester 2		Credit
ITNW 1425	Fundamentals of Networking Technologies *or other**	4
ITSC 1425	Personal Computer Hardware	4
ITNW 1454	Implementing and Supporting Servers	4
ITSC 1316	LINUX Installation and Configuration	3
	2nd Semester Total	15

Semester 3		Credit
	Select Language, Philosophy & Culture (40) *or other**	3
ITSE 1302	Computer Programming *or other**	3
	3rd Semester Total	6

Semester 4		Credit
ITSC 2439	Personal Computer Help Desk Support	4
ITSE 1311	Beginning Web Programming	3
ITSC 2325	Advanced LINUX	3
ITSC 2321	Integrated Software Applications II	3
	4th Semester Total	13

Semester 5		Credit
ITSY 1342	Information Technology Security *or other*	3
	Select Mathematics (20) Core	3
	Select Social & Behavioral Science (80) Core	3
ITSC 2264	Practicum Computer & Information Sciences	2
	5th Semester Total	11
	Program Total	60

DC/ITSA: 29 Total AAS Hours: 60

Hours needed Post DC/ITSA: 31 General Academics: 15
Specific Hours: 45

* See San Antonio College degree description for more information: http://mysaccatalog.alamo.edu/

Vers 9.2016

ALAMO COLLEGES

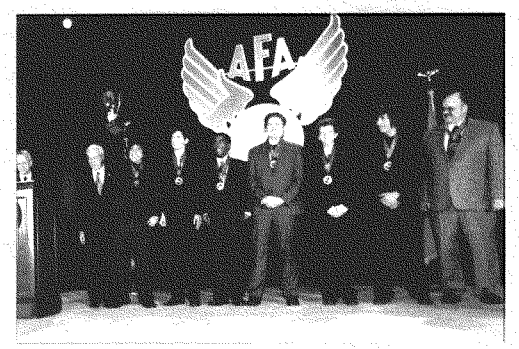
ALAMO ACADEMIES

IV. Air Force Association's CyberPatriot: The National Youth Cyber Education Program

In addition to the paid internship, Alamo Academies' students benefit from an additional opportunity to apply the knowledge and skills learned in the classroom by participating in the Air Force Association's CyberPatriot Competition. Beginning in 2007, the Air Force Association and the University of Texas at San Antonio, Center for Infrastructure Assurance and Security worked together to develop and test a rigorous and demanding high school cyber defense competition known as CyberPatriot. The objective was to inspire high school students toward careers in cyber security or other STEM disciplines, critical to the nation. Today, CyberPatriot is the premier national youth cyber defense competition, in the U.S. and overseas. It includes three preliminary rounds of virtual competition, each six hours in length, executed from a team's home campus. The national championship is a grueling event which lasts for three days, requires each team to compete while defending their own network against some of the best Red Teams in the nation.

The first year of competition was restricted to a very small number of Junior ROTC teams. By 2010 the competition was up and fully running to include non-Junior ROTC teams (Open Division) for the first time. San Antonio business, academic, and government entities helped identify and align subject matter experts as mentors, conducted several clinics to help prepare students and coaches, and organized a recognition luncheon -- the San Antonio Mayor's Cyber Cup.

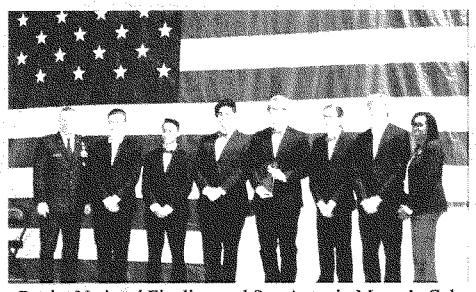
The Alamo Academies' 2011 Information Technology & Security Academy (ITSA) team won the inaugural Mayor's Cyber Cup and finished 3rd in the nation, out of approximately 650 teams. In 2012, the ITSA team returned and won the 2012 CyberPatriot National Championship (Open Division) in Washington, DC. As a magnet school team, the ITSA team had representatives from five different San Antonio area high schools - they came together to win the national championship, beating more than 850 teams for the honor. These young men are now graduating from local colleges and universities and joining the cyber workforce here in San Antonio.



2012 CyberPatriot National Champions and San Antonio Mayor's Cyber Cup Winners

Pictured left to right: Robert Flores, Theodore Belitsos, Kenny Bias, Brian Carvan, Tommy Roberts, Mario Puente, and Coach Mike Matuszek, San Antonio College ITSA professor

In 2016, there were 189 San Antonio area teams competing in the CyberPatriot competition, against more than 3,300 teams from across the nation. The 2016 ITSA team again won the Mayor's Cyber Cup and advanced to compete against the nation's top 12 teams at the CyberPatriot national finals. The ITSA program has won the San Antonio Mayor's Cyber Cup and advanced to the national championship five out of the last six years.



2016 CyberPatriot National Finalists and San Antonio Mayor's Cyber Cup Winners

Pictured left to right: Major General Ed Wilson, Eli Ross, Hector Iruegas, Kyle Volz, Reed Eggleston, Brendan Downs, Carlson Lindley, San Antonio Mayor Ivy Taylor

ALAMO COLLEGES

ALAMO ACADEMIES

V. Closing the IT Gap in Federal IT

Pathways Unbound

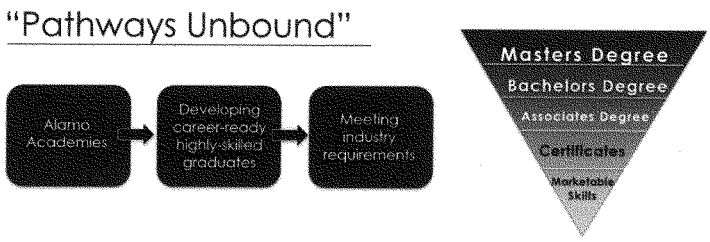


Figure 4

Graduate Testimonials

Career Pathway

Mario Puente – 2012 Graduate

College Pathway

Robert Flores – 2012 Graduate

Hybrid Pathway

Skylar Daugherty – 2015 Graduate

Kyle Volz – 2016 Graduate

Reed Eggleston – 2016 Graduate

ALAMO COLLEGES

ALAMO ACADEMIES

Career Pathway

Mario Puente – 2012 Graduate

I am Mario Puente and I attended Brennan High School and Alamo Academies' Information Technology & Security Academy (ITSA) from 2010-2012. I joined ITSA to get a jump start not only in college credits but to start a career path to lead me to a steady and secure job in the future. My experience at ITSA was truly amazing, a dream come true. I never imagined I'd do or learn the things I did while attending the Alamo Academies. My involvement was life-changing; I wish for more young people to have the opportunity to experience the field of IT as I did.

I earned college credits while in high school toward my Associates Degree which helped boost me ahead of my peers. I also learned the basics of computers and received real world training from college professors and industry professionals. Four years later, I am now a Lead in my position. I know I wouldn't be where I am today if I didn't learn the things I did from ITSA! I am the go to guy at my job because of how much I know.

One of two key elements in the ITSA program was my involvement with the Air Force Association's CyberPatriot program. CyberPatriot is the best thing that ever happened to me. The competition gave me true real world experience in the field of cybersecurity. It opened my eyes to what is possible in this career pathway. The competition was challenging like nothing I'd experienced before. I realized that our team possessed the skill and aptitude to be successful in the competition as long as we put 100% to it. In 2012, our team advanced to the national championship in Washington, DC to earn 1st place.

The second key element of the program is the paid internship I received during the summer following my first year at Alamo Academies. I was provided with an internship at the 33rd Network Warfare Squadron (33rd NWS). This experience jump started my career path. The skill sets and mentorship I received proved invaluable to my future. As an ITSA intern, I was fortunate to earn a Secret Clearance. This distinction made me further realize the important sensitivity of my position. I began to feel more confident through my internship and realized that I could have a successful future in IT. My confidence continued to grow as many companies were looking to hire me after learning of my role within the 33rd NWS.

After graduating from high school and Alamo Academies, I decided to jump right into the working industry right away because on the job training is what industry is looking for! My experience working alongside the 33rd NWS continued to move me forward. Though I did go to college part time (online), I chose to take a small hiatus due to being offered a position at the Pentagon. In my role at the Pentagon, I served as a Computer Network Defense Analyst with interim TS/SCI, (Top Secret Clearance/Sensitive Compartmented Information). This was another life-changing experience. Through working alongside seasoned professionals in this arena, I more clearly understood the need for my current skillset as well as the future need for advanced learning. I knew this was just the beginning of my career.

As of today, I have returned to Texas as a full time DoD Contractor. I am a Lead Cyber Security analyst with 22nd Century Technologies supporting the United States Air Force's Weapon and Tactics Team known as the Air Force Computer Emergency Response Team. I have earned the following certifications: Microsoft Certified Professional, Certified Ethical Hacker, and Security+. My current role has recently expanded to include recruiting skilled members to our workforce of which I am glad to return to Alamo Academies to locate skilled graduates in the San Antonio area.

With the wealth of experience gained in the past four years, I am now completing my education in Information Assurance and Cyber Security as well as a Minor in Digital Forensics. I am confident returning to finish my degree because I understand continued education is a critical component for higher paying jobs when looking to advance in the Cyber Security field.

Alamo Academies helped me obtain incredible opportunities and experience toward the employment I am proud to have today. Without participating in this program, I would not be as successful as I am today. At 22 years of age, I am a Cyber Security professional earning an amazing salary with multiple certifications, nearly six years of on-the-job experience in supporting DoD initiatives, and no college debt. I appreciate this experience and look forward to opportunities to share the message. Recently, I had the privilege to refer 2016 graduates of ITSA to my current employer. It is an honor to be able to give back. Speaking from personal experience, this model is the vehicle for young men and women to gain on-the-job experience and become qualified with the skills necessary for critical jobs needing to be filled in Federal IT.

ALAMO COLLEGES

ALAMO ACADEMIES

College Pathway

Robert Flores – 2012 Graduate

I am Robert Flores Jr., and I attended Judson High School and ITSA. I joined ITSA because I found the information security industry exciting as it is ever-growing, ever-changing and provides a huge technological challenge in adapting to new technologies and cyber-attacks. Data security remains a crucial element to business managers worldwide who must connect their intra-networks to the Internet in order to compete in the global market. I was confident that someday I would play a significant part in maintaining the Internet's revolutionary role by making individuals who use it feel secure. My experience at ITSA was incredible and I owe a huge portion of my success to ITSA since it was an invaluable launching pad to my vision which I am currently enjoying at Rackspace.

Participating in ITSA was an enormous benefit. I earned an Information Technology and Security Certification and 20 months as an intern with the Air Force that put my knowledge to use in a professional workforce environment. But most important is the incredible network of professionals, instructors, and fellow students I developed since my first day at ITSA. They supported me every step of the way! CyberPatriot made me a Rock Star as I met numerous government and state officials. The highlight being when, as Team Captain of the ITSA CyberPatriot Team, I led my team at national level competition in Washington D.C. and we were the CyberPatriot Open Division National Champions for 2012.

My decision to pursue my education first was simple because there is no substitute for knowledge/ education and it is seen as a strong foundation and a key ingredient for being successful. In May 2016, I earned a Bachelor of Business Administration in Cyber Security with a Minor in Digital Forensics from UTSA (University of Texas at San Antonio). I was fortunate to not incur any college debt since I used the Hazelwood program because of my father's military service as a Texas native. Plus, I earned and hold three certificates: CompTIA A+, CompTIA Security+, and CompTIA Network+.

I am a Rackspace employee since graduating from UTSA. In fact, I got a Rackspace employment offer a year prior to graduating. I am a Security Analyst as a member of the Information Security Operations Center (ISOC) Team at Rackspace in San Antonio, Texas. My employer is providing me a great salary, great benefits and tuition assistance.

The ITSA experiences definitely helped in obtaining employment because it was my foundation that included my first internship with the Air Force. I had a total of three paid internships prior to graduating from UTSA and joining Rackspace.

ALAMO COLLEGES

ALAMO ACADEMIES

Hybrid Pathway

Skylar Daugherty – 2015 Graduate

As a Junior in high school, my future path was unclear. I was facing the beginning of my independence and I had no idea where to start. Being such a pivotal time, I had to act quickly. I made the last minute decision to enroll in the Information Technology and Security Academy (ITSA) offered by Alamo Academies. I can say without a doubt that this was the best decision that I have made in my life so far. Little did I know, the decision would solidify the foundation from which I would continue into the career that I currently enjoy.

I cannot state enough how the majority of my success at this stage in my life is due to my involvement with ITSA. A key contribution to my success came from the CyberPatriot program. As much fun as it was to learn about information technology in the classroom, it was more fun to apply that knowledge in a real competitive environment. This allowed me to not only reinforce the knowledge that I had gained from my professors, but it also pushed me to learn on my own and gave me a constant thirst to want to learn more.

Through the help of Alamo Academies, I was able to earn my Associates degree in Information Assurance and Cyber Security from San Antonio College only a year after I graduated from high school without acquiring any college debt. I plan on continuing my education in order to earn my Bachelor's degree in the same field.

Most importantly, the internship program offered by ITSA allowed me to earn a position at Delta Risk LLC; a cyber security consulting agency located in downtown San Antonio. Originally hired as an intern focused on web development, I was later hired as a full time employee with a focus shifted toward cyber security, an area in which I have great confidence due to the teaching I received.

ITSA introduced me to a world of opportunity that I would have never had the access to otherwise and, because of these opportunities, not only am I the first in my family to graduate college, but, at just 19 years old, I have been able to earn a position within the career field that I want a future in. I feel incredibly confident that the help and teaching that I received from the Information Technology and Security Academy has given me a future that I could have only dreamt of having.

ALAMO COLLEGES

ALAMO ACADEMIES

Hybrid Pathway

Kyle Volz – 2016 Graduate

My name is Kyle Volz, I attended Alamo Heights High School, and Alamo Academies' Information Technology & Security Academy (ITSA) from 2014-2016. I joined Alamo Academies because I have always had an interest in technology and thought that it would be a good opportunity for me to further my knowledge in the field of IT.

I quickly learned that joining ITSA was the right decision for me. The teachers were very helpful and knowledgeable and assisted us through the difficult coursework. I learned various subjects in the field from Hardware to Security Protocols to Programming. Without a doubt, this knowledge inspired me to learn more and ultimately qualified me to get the job that I now have.

I also participated in the CyberPatriot competition both years while at ITSA. In my senior year, our team won the San Antonio Mayor's Cyber Cup and advanced to the National Finals in Baltimore, MD. This experience helped me to apply the knowledge in a structured and competitive environment. The winning recognition also helped immensely by providing proof to show potential employers the skills that I have acquired through my time at Alamo Academies.

Currently, I hold the following certifications: CompTia Security+ and Certified Ethical Hacker (CEH) and am earning credits toward two Associate degrees at San Antonio College. I am proud to say that I have been referred and earned employment with DoD contractor, 22nd Century Technologies. At eighteen years old, I am being awarded a security clearance, earning a salary commensurable with other IT security professionals with full benefits and a 401k plan allowing me to gain my independence so much earlier than I had ever imagined.

What I have learned at Alamo Academies from the teachers and the CyberPatriot mentors is the reasons behind why I am able to get this job. Through ITSA, I was able to network with potential employers and understand the skills required for the workforce. I gained confidence and continued to apply knowledge that makes me a valuable asset to their team. I would not be where I am today without this direction. I look forward to giving back to the program as I continue to progress in my skill sets in my new role. I

highly recommend young men and women interested in the IT field get a head start on their education and experience in the field through Alamo Academies, ITSA.

ALAMO COLLEGES

ALAMO ACADEMIES

Hybrid Pathway

Reed Eggleston – 2016 Graduate

My name is Reed Eggleston and I attended John Marshall High School and Alamo Academies' Information Technology & Security Academy (ITSA) from 2014-2016. I was attracted to the program because I wanted to do something different that would challenge me. I enjoyed computers and thought that I was fairly knowledgeable before joining ITSA. Within the first semester, I realized that I had much to learn. ITSA provided a wealth of knowledge at my disposal through college professors and industry professionals who specialize in the field.

I can truly say my experience at ITSA was spectacular. It gave me direction in life and the critical technical knowledge that allowed me to pursue high paying and in-demand jobs right out of high school. A few standout benefits include industry certifications, connections with industry professionals, and an understanding of unfilled IT jobs in the community. After my first year in the program, I had an internship with cyber security firm, Delta-Risk. The internship provided me with experience and connections that I still keep in contact with today. The leadership was impressed with my performance sharing, "If you ever need a job, come back and we'll hire you." To hear this comment was confirmation that I was moving in the right direction.

I share with new members of the ITSA branch of the Alamo Academies, "You don't really feel the true power of the Academy unless you join CyberPatriot," and I still believe this. The CyberPatriot competition brought out the best in myself as a student and as a leader; allowing a framework to which I could practice cybersecurity in my daily life. I had to hone my ability to self-learn and apply security concepts inside and outside of the classroom. It also promoted my competitive drive to increase my skill sets among some of the best young professionals in the nation.

Serving as the captain of the ITSA 2016 CyberPatriot team was a remarkable experience in both cyber security and also in leadership. Together our team studied at least 3 hours a day, nearly every single day, for over a year so that we could make it to national finals in the competition and I don't regret it in the slightest. Advancing as one of the top 12 teams in nation to the Open Division National Championship gave us the confidence to push ourselves to new heights. That experience continues to prove valuable in my life, today.

Today I hold both CompTia Security + Certification as well as Certified Ethical Hacker (CEH) from EC-Council. Thanks to an ITSA alumnus, I was referred and hired as a Tier II Analyst for DoD defense contractor, 22nd Century Technologies Inc. in San Antonio, TX.

Alamo Academies' ITSA program taught me how to do many things, from being professional in an office environment to hands on skills that I need in the workforce. Another highlight is the networking that stemmed from ITSA and CyberPatriot; I was able to build relationships with professionals in the field who are eager to share their experiences to help me along my journey. I enjoy giving back to ITSA and frequently mentor current students. I am grateful to the program for allowing me to build the foundation from which I am still expanding upon.

ALAMO COLLEGES

ALAMO ACADEMIES

ADDENDUMS

Program Curricula & Associate of Applied Science (AAS) Degree Pathways

A. Information Technology & Security Academy (ITSA) Curriculum & Associate of Applied Science (AAS) Degree Pathway: Computer Support Specialist

B. Aerospace Academy (AA) Curriculum & Associate of Applied Science (AAS) Degree Pathways: Aircraft Technician Airframe or Aircraft Technician Powerplant

C. Advanced Technology and Manufacturing Academy (ATMA) Curriculum & Associate of Applied Science (AAS) Degree Pathways: CNC Manufacturing Technician or Manufacturing Operations Technician

D. Health Professions Academy (HPA) Curriculum & Associate of Applied Science (AAS) Degree Pathway: Nursing

E. Heavy Equipment Academy (HEA) Curriculum & Associate of Applied Science (AAS) Degree Pathway: Diesel/Construction Equipment Technology

ALAMO COLLEGES

ALAMO ACADEMIES

Addendum A

Information Technology and Security Academy

1st Year Program of Studies
5 courses with total of 18 credit hours

Fall Semester		Credit
ITSC 1305	Intro to PC Operating Systems *Introduction to personal computer operating systems including installation, configuration, file management, memory & storage management, control of peripheral devices & use of utilities.*	3
ITSC 1425 *Testout Certification PC Pro	Personal Computer Hardware* *Current personal computer hardware including assembly, upgrading, setup, configuration, and troubleshooting.*	4
	Fall Semester Total	**7**
Spring Semester		**Credit**
ITNW 1425 *Testout Certification Network Pro	Fundamentals of Networking Technologies* *Introduction to architecture, structure, functions, components & models of the internet. Covers principles and structures of IP addressing, Ethernet, media & operations.*	4
ITSC 2439	Personal Computer Help Desk Support *Diagnosis and solution of user hardware and software related problems with on-the-job and/or simulated projects.*	4
	Spring Semester Total	**8**
Summer Semester		**Credit**
ITSC 2364	Practicum: Computer & Information Sciences, General *Practical, general workplace training supported by an individualized learning plan.*	3
	Summer Total	**3**
	Year 1 Program Total	**18**

Level I Certificate of Completion
Computer Desktop Support Technician

2nd Year Program of Studies
4 courses with total of 12 credit hours

Fall Semester		Credit
ITSC 1316 *Testout Certification LINUX Pro	LINUX Installation & Configuration* *Introduction to the UNIX operation system including multi-user concepts, terminal emulation, use of system editor, basic UNIX commands, & writing script files. Includes introductory system management concepts.*	3
ITSY 1342 *Testout Certification Security Pro	Information Technology Security* *Instruction in security for network hardware, software, and data including physical security, backup procedures, relevant tools, encryption, and protection from viruses.*	3
	Fall Semester Total	**6**
Spring Semester		**Credit**
ITSE 1302	Computer Programming *Introduction to computer programming with emphasis on the fundamentals of design, development, testing, implementation, and documentation. Includes language syntax, data and file structures, input/output devices, and files.*	3
ITSE 1311	Beginning Web Programming *Skill development in web page programming including mark-up and scripting languages.*	3
	Spring Semester Total	**6**
	Year 2 Program Total	**12**

Level I Certificate of Completion
Information Technology & Security

Two Year Program of Studies: 9 Courses totaling 30 credit hours

Information Technology and Security Academy

Level I Certificate of Completion
Computer Desktop Support Technician

Level I Certificate of Completion
Information Technology & Security

ASSOCIATE OF APPLIED SCIENCES

Computer Support Specialist

Semester 1		Credit
ITSC 1301	Introduction to Computers *or other**	3
ITSC 1309	Integrated Software Applications	3
ITSC 1305	Introduction to PC Operating Systems *or other**	3
ENGL 1301	Composition I	3
	Select Additional communication (90) Core	3
	1st Semester Total	15

Semester 2		Credit
ITNW 1425	Fundamentals of Networking Technologies *or other**	4
ITSC 1425	Personal Computer Hardware	4
ITNW 1454	Implementing and Supporting Servers	4
ITSC 1316	LINUX Installation and Configuration	3
	2nd Semester Total	15

Semester 3		Credit
	Select Language, Philosophy & Culture (40) *or other**	3
ITSE 1302	Computer Programming *or other**	3
	3rd Semester Total	6

Semester 4		Credit
ITSC 2439	Personal Computer Help Desk Support	4
ITSE 1311	Beginning Web Programming	3
ITSC 2325	Advanced LINUX	3
ITSC 2321	Integrated Software Applications II	3
	4th Semester Total	13

Semester 5		Credit
ITSY 1342	Information Technology Security *or other*	3
	Select Mathematics (20) Core	3
	Select Social & Behavioral Science (80) Core	3
ITSC 2264	Practicum Computer & Information Sciences	2
	5th Semester Total	11
	Program Total	60

DC/ITSA: 29 Total AAS Hours: 60

Hours needed Post DC/ITSA: 31 General Academics: 15
Specific Hours: 45

* See San Antonio College degree description for more information: http://mysaccatalog.alamo.edu/

Vers 9.2016

ALAMO COLLEGES

Addendum B

ALAMO ACADEMIES

Aerospace Academy

1st Year Program of Studies
8 courses with total of 21 credit hours

Fall Semester		Credit
AERM 1201 *10-hr OSHA	Introduction to Aviation* *An overview of aviation maintenance.*	2
AERM 1315	Aviation Science *Fundamentals of mathematics, physics & drawing as they apply to aircraft principles & operations.*	3
AERM 1303	Shop Practice *Introduction to the correct use of hand tools and equipment & precision measurement; identification of aircraft hardware; & fabrication of fluid lines and tubing.*	3
	Fall Semester Total	**8**

Spring Semester		Credit
AERM 1208	Federal Aviation Regulations *A course in the use & understanding of the FAA & aircraft manufacturer's publications, forms & records.*	2
AERM 1205	Weight & Balance *An introduction to FAA required subjects relating to weighing of aircraft, performance of weight & balance calculations, & appropriate maintenance of record entries.*	2
AERM 1310	Ground Operations *An introduction course in fuels, servicing methods and procedures, aircraft movement, securing and operations of aircraft, external power equipment, aircraft cleaning, and corrosion control.*	3
POFT 1220	Job Search Skills *A course to provide students with necessary skills to seek & obtain employment in business & industry.*	2
	Spring Semester Total	**9**

Summer Semester		Credit
AERM 2486	Internship: Aircraft Mechanics & Aircraft Maintenance Technology/Technician *Practical, general workplace training supported by an individualized learning plan.*	4
	Summer Total	**4**
	Year 1 Program Total	**21**

Occupational Skills Award
Aircraft Technology (OSA)
(5 courses, 13 hours)

2nd Year Program of Studies
4 courses with total of 11 or 12 credit hours

Fall Semester		Credit
AERM 1414	Basic Electricity *A study of aircraft electrical systems and their requirements.*	4
AERM 1254	Aircraft Composite *A study of the inspection & repair of composite, Fiberglass, honeycomb, and laminated structural materials.*	2
	Fall Semester Total	**6**

Spring Semester		Credit
	Aircraft Structures Mechanic	
AERM 1241	Wood, Fabric & Finishes *A course in the use & care of various covering materials, finishes, & wood structures including approved methods and procedures.*	2
AERM 1352	Aircraft Sheet Metal *A course in inspection & repair of sheet metal structures.*	3
	Spring Semester Total	**5**
	Year 2 Program Total	**11**
	Or	
	Aircraft Turbine Mechanic	
AERM 1351	Aircraft Turbine Engine Theory *Theory, history & servicing of turbine engines.*	3
AERM 2351	Aircraft Turbine Engine Overhaul *Topics address inspection, disassembly, re-assembly & replacement of gas turbine engines, sections, & components as well as operational troubleshooting & analysis.*	3
	Spring Semester Total	**6**
	Year 2 Program Total	**12**

Level I Certificate of Completion

Aircraft Structures Mechanic or **Aircraft Turbine Mechanic**

Two Year Program of Studies: 12 Courses totaling 32 (Structures) or 33 (Turbine) credit hours

Aerospace Academy

Level I Certificate of Completion
Aircraft Structures Mechanic

ASSOCIATE OF APPLIED SCIENCES

Aircraft Technician Airframe

Semester 1		Credit
ENGL 1301	Composition I *or other**	3
MATH 1333	Contemporary Mathematics II *or other**	3
PHYS 1305	Introductory to Physics I Lecture *or other**	3
ECON 1301	Introduction to Economics *or other**	3
ARTS 2326	Sculpture I *or other**	3
	1st Semester Total	15

Semester 2		Credit
AERM 1205	Weight & Balance	2
AERM 1208	Federal Aviation Regulations	2
AERM 1310	Ground Operations	3
AERM 1303	Shop Practices	3
AERM 1315	Aviation Science	3
AERM 1414	Basic Electricity	4
AERM 1241	Wood, Fabric & Finishes	2
	2nd Semester Total	19

Semester 3		Credit
AERM 1243	Instruments & Navigation/Communication	2
AERM 2231	Airframe Inspection	2
AERM 1345	Aircraft Electrical Systems	3
	3rd Semester Total	7

Semester 4		Credit
AERM 1449	Hydraulic, Pneumatic, & Fuel Systems	4
AERM 1350	Landing Gear Systems	3
AERM 1254	Aircraft Composites	2
AERM 1253	Aircraft Welding	2
AERM 1352	Aircraft Sheet Metal	3
AERM 1347	Aircraft Auxiliary Systems	3
AERM 2233	Assembly & Rigging	2
	4th Semester Total	19
	Program Total	60

DC/AA: 24 Total AAS Hours: 60

Hours needed Post DC/AA: 36 General Academics: 15
Specific Hours: 21

Level I Certificate of Completion
Aircraft Turbine Mechanic

ASSOCIATE OF APPLIED SCIENCES

Aircraft Technician Powerplant

Semester 1		Credit
ENGL 1301	Composition I *or other**	3
MATH 1333	Contemporary Mathematics II *or other**	3
PHYS 1305	Introductory to Physics I Lecture *or other**	3
ECON 1301	Introduction to Economics *or other**	3
ARTS 2326	Sculpture I *or other**	3
	1st Semester Total	15

Semester 2		Credit
AERM 1205	Weight & Balance	2
AERM 1208	Federal Aviation Regulations	2
AERM 1310	Ground Operations	3
AERM 1303	Shop Practices	3
AERM 1315	Aviation Science	3
AERM 1414	Basic Electricity	4
AERM 1444	Aircraft Reciprocating Engines	4
	2nd Semester Total	21

Semester 3		Credit
AERM 2352	Aircraft Powerplant Inspection	3
	3rd Semester Total	3

Semester 4		Credit
AERM 2547	Aircraft Reciprocating Overhaul	5
AERM 1340	Aircraft Propellers	3
AERM 1351	Aircraft Turbine Engine Theory	3
AERM 2351	Aircraft Turbine Engine Overhaul	3
AERM 1456	Powerplant Electrical	4
AERM 1357	Fuel Metering & Induction Systems	3
	4th Semester Total	21
	Program Total	60

DC/AA: 23 Total AAS Hours: 60

Hours needed Post DC/AA: 37 General Academics: 15
Specific Hours: 22

* See St. Philip's College degree description for more information: http://myspccatalog.alamo.edu/

Vers 9.2016

ALAMO COLLEGES

Addendum C

ALAMO ACADEMIES

Advanced Technology and Manufacturing Academy

1st Year Program of Studies
6 courses with total of 19 credit hours

Fall Semester		Credit
TECM 1303	Technical Calculations *Specific mathematical calculations required by business and industry. Includes whole numbers, fractions, mixed numbers, decimals, %, ratios, and proportions. Also, covers converting to different units of measure (standard and/or metric).*	3
MCHN 1320 *10-Hour OSHA	Precision Tools & Measurements* *Introduction to modern science of dimensional metrology.*	3
MCHN 1270 *MSSC Safety Certification	MSSC* *Manufacturing Skill Standards Council Certified production Technician Safety & Quality Modules.*	2
	Fall Semester Total	**8**

Spring Semester		Credit
MCHN 1302	Print Reading for Machine Trade *A review of applied math models and study of different blueprints, with emphasis on machine blueprints and the application of each.*	3
MCHN 1438	Basic Machine Shop I *An introduction course that assists the student in understanding the machinist occupation in industry.*	4
	Spring Semester Total	**7**

Summer Semester		Credit
MCHN 2486	Internship: Machine Tool Technology/Machinist *Practical, general workplace training supported by an individualized learning plan.*	4
	Summer Total	**4**
	Year 1 Program Total	**19**

Level I Certificate of Completion
Manufacturing Skills Trade Helper

2nd Year Program of Studies
5 courses with total of 15 credit hours

Fall Semester		Credit
INMT 2303	Pumps, Compressors & Mechanical Drives *A study of the theory and operations of various types of pumps and compressors.*	3
ELPT 1319	Fundamentals of Electricity I *Basic theory and practice of electrical circuits.*	3
QCTC 1243 *MSSC Quality Certification	Quality Assurance* *Principles & application designed to introduce quality assurance.*	2
	Fall Semester Total	**8**

Spring Semester		Credit
MCHN 1426	Introduction to Computer-Aided Manufacturing (CAM) *A study of Computer Assisted Manufacturing (CAM) Systems. Software is used to develop applications for manufacturing.*	4
RBTC 1305	Robotic Fundamentals *An introduction to flexible automation.*	3
	Spring Semester Total	**7**
	Year 2 Program Total	**15**

Level I Certificate of Completion
Production Tool Operator/Maintenance Assistant

Two Year Program of Studies: 11 Courses totaling 34 credit hours

Advanced Technology and Manufacturing Academy

Level I Certificate of Completion
Manufacturing Skills Trade Helper

↓

Level I Certificate of Completion
Tool Operator/Maintenance Assistant

ASSOCIATE OF APPLIED SCIENCES

Manufacturing Operations Technician

Semester 1		Credit
MCHN 1438	Basic Machine Shop I	4
MCHN 1320	Precision Tools & Measurement	3
MATH 1333	Contemporary Mathematics II *or other**	3
INMT 2303	Pumps, Compression & Mechanical Drives	3
ITSC 2303	Introduction to Computers I *or other**	3
	1st Semester Total	16

Semester 2		Credit
ENGL 1301	Composition I *or other**	3
ELPT 1319	Fundamentals of Electricity I	3
ELMT 1305	Basic Fluid Power	3
PHYS 1305	Introductory Physics I Lecture *or other**	3
RBTC 1305	Robotic Fundamentals	3
	2nd Semester Total	15

Semester 3		Credit
RBTC 2347	Computer Integrated Manufacturing	3
WLDG 1425	Intro to Oxy-Fuel Welding & Cutting	4
RBTC 1347	Electromechanical Devices	3
ECON 1301	Introduction to Economics *or other**	3
	3rd Semester Total	13

Semester 4		Credit
MCHN 1302	Print Reading for Machining Trade	3
ELPT 2419	Programmable Logic Controllers I	4
ELPT 1441	Motor Control	4
MUSI 1306	Music Appreciation *or other**	3
MCHN 2266	Practicum (or field experience) Machine Tool Technology/Machinist	2
	4th Semester Total	16
	Program Total	60

DC/ATMA: 21 Total AAS Hours: 60

Hours needed Post DC/ATMA: 39 General Academics: 18
Specific Hours: 21

ASSOCIATE OF APPLIED SCIENCES

CNC Manufacturing Technician

Semester 1		Credit
MCHN 1302	Print Reading for Machining Trade	3
MCHN 1438	Basic Machine Shop I	4
MATH 1332	Contemporary Math I *or other**	3
MCHN 1320	Precision Tools & Measurement	3
ITSC 1301	Introduction to Computers *or other**	3
	1st Semester Total	16

Semester 2		Credit
ENGL 1301	Composition I *or other**	3
MCHN 2303	Fundamentals of Computer Numerical Controlled (CNC) Machine Controls	3
QCTC 1243	Quality Assurance	2
PHYS 1305	Introductory to Physics I Lecture *or other**	3
MCHN 1426	Intro to Computer-Aided Manufacturing (CAM)	4
	2nd Semester Total	15

Semester 3		Credit
ECON 1301	Introduction to Economics *or other**	3
MCHN 2431	Operation of CNC Turning Centers	4
MCHN 2434	Operation of CNC Machining Centers	4
MCHN 1330	Statistical Process Control for Machinist	3
MUSI 1306	Music Appreciation or other*	3
	3rd Semester Total	17

Semester 4		Credit
MCHN 2435	Advanced CNC Machining	4
MCHN 1352	Intermediate Machining I	3
RBTC 1305	Robotic Fundamentals	3
MCHN 2266	Practicum (or field experience) Machine Tool Technology/Machinist	2
	4th Semester Total	12
	Program Total	60

DC/ATMA: 21 Total AAS Hours: 60

Hours needed Post DC/ATMA: 39 General Academics: 18
Specific Hours: 21

* See St. Philip's College degree description for more information: http://myspccatalog.alamo.edu/

Vers 9.2016

ALAMO COLLEGES

Addendum D

ALAMO ACADEMIES

Health Professions Academy

1st Year Program of Studies 4 courses with total of 14 credit hours		
Fall Semester		**Credit**
BIOL 2401	Human Anatomy & Physiology I *Studying structure & function of cells, tissues, & body systems with emphasis on integumentary, skeletal, muscular, nervous systems including the special senses.*	4
ENGL 1301	Composition I *Focusing on the principles of effective oral and written communication, critical reading & the development of academic writing.*	3
	Fall Semester Total	**7**
Spring Semester		**Credit**
BIOL 2402	Human Anatomy & Physiology II *Studying the structure & function of the endocrine, digestive, respiratory, cardiovascular, lymphatic, genitourinary & reproductive systems.*	4
ENGL 1302	Composition II *Refining skills in academic writing, critical thinking, analysis of literature and research & documentation.*	3
	Spring Semester Total	**7**
	Year 1 Program Total	**14**

2nd Year Program of Studies 5 courses with total of 16 credit hours		
Fall Semester		**Credit**
BIOL 2420	Microbiology for Nursing & Allied Health *Introduction to historical concepts of the nature of microorganisms, microbial diversity, the importance of microorganisms and acellular agents in the biosphere, and their roles in human & animal diseases.*	4
PSYC 2301	General Psychology *Introduction of the study of behavior and the factors that determine & affect behavior and mental processes.*	3
	Fall Semester Total	**7**
Spring Semester		**Credit**
PHIL 2306	Introduction to Ethics *Classical & contemporary theories concerning the good life, human conduct in society, and moral & ethical standards.*	3
PSYC 2314	Lifespan Growth & Development *Study of the relationship of the physical, emotional, social and mental factors of growth & development of the individual throughout the lifespan.*	3
MDCA 1313	Medical Terminology *The study and practical application of a medical vocabulary system. It includes structure, recognition, analysis, definition, spelling, pronunciation, and combination of medical terms from prefixes, suffixes, roots, and combining forms.*	3
	Spring Semester Total	**9**
	Year 2 Program Total	**16**

All classes transferrable into the Nursing Program at San Antonio College

Two Year Program of Studies: 9 Courses totaling 30 credit hours

Health Professions Academy

Prerequisites transferable to Allied Health Career Pathways

ASSOCIATE OF APPLIED SCIENCES

Nursing

Semester 1		Credit
BIOL 2401	Human Anatomy & Physiology I	4
PSYC 2301	General Psychology	3
PHIL 2306	Introduction to Ethics	3
ENGL 1301	Composition I	3
	1st Semester Total	13

Semester 2		Credit
BIOL 2402	Human Anatomy & Physiology II	4
PSYC 2314	Lifespan Growth & Development	3
BIOL 2420	Microbiology for Nursing & Allied Health *or other**	4
	2nd Semester Total	11
	Program Total	24

Semester 3		Credit
RNSG 1128	Introduction to Health Care Concepts	1
RNSG 1125	Professional Nursing Concepts I	1
RNSG 1216	Professional Nursing Competencies	2
RNSG 1430	Health Care Concepts I	4
RSNG 1161	Clinical-RN: Health Care Concepts I	1
	3rd Semester Total	9

Semester 4		Credit
RNSG 1126	Professional Nursing Concepts II	1
RNSG 1533	Health Care Concepts II	5
RNSG 2362	Clinical-RN: Health Care Concepts II	3
	4th Semester Total	9

Semester 5		Credit
RNSG 1137	Professional Nursing Concepts III	1
RNSG 1538	Health Care Concepts III	5
RNSG 2363	Clinical-RN: Health Care Concepts III	3
	5th Semester Total	9

Semester 6		Credit
RNSG 2138	Professional Nursing Concepts IV	1
RNSG 2539	Health Care Concepts IV	5
RNSG 2360	Clinical-RN: Health Care Concepts IV	3
	6th Semester Total	9
	Program Total	36

DC/HPA: 24 Total AAS Hours: 60

Hours needed Post DC/HPA: 36 General Academics: 24

Specific Hours: 36

Vers 9.2016

ALAMO COLLEGES

ALAMO ACADEMIES

Addendum E

Heavy Equipment Academy

1st Year Program of Studies
5 courses with total of 18 credit hours

Fall Semester		Credit
DEMR 1406	Diesel Engine I*	4
*HOLT CAT ProTech Engine D&A DE101	*An introduction to the basic principles of diesel engines & systems.*	
DEMR 1416	Basic Hydraulics*	4
*HOLT CAT ProTech Hydraulics TM28	*Fundamentals of hydraulics including components and related systems.*	
	Fall Semester Total	**8**

Spring Semester		Credit
DEMR 1405	Basic Electrical Systems*	4
*10-Hour OSHA *HOLT CAT ProTech Electricity TG01	*A review of applied math models and study of different blueprints, with emphasis on machine blueprints and the application of each.*	
DEMR 1329	Preventative Maintenance	3
	An introduction course that assists the student in understanding the machinist occupation in industry.	
	Spring Semester Total	**7**

Summer Semester		Credit
DEMR 2366	Internship: Diesel Mechanics Technology/Technician	3
	Practical, general workplace training supported by an individualized learning plan.	
	Summer Total	**3**
	Year 1 Program Total	**18**

Occupational Skills Award
Diesel/Light to Heavy Truck Technology Mechanic Helper I (OSA)

2nd Year Program of Studies
4 courses with total of 16 credit hours

Fall Semester		Credit
DEMR 1423	Heating, Ventilation, & Air Conditioning*	4
*HOLTCAT ProTech HVAC TG12 & ASE Refrigerant Recovery & Recycling	*Introduction to heating, ventilation, & air conditioning theory, testing, & repair. Emphasis on refrigerant reclamation, safety procedures, specialized tools & repairs.*	
DEMR 2439	Advanced Electrical Systems	4
	A continuation of basic electrical systems to include lighting, computer controls, and accessories.	
	Fall Semester Total	**8**

Spring Semester		Credit
DEMR 2434	Advanced Diesel Tune-Up and Troubleshooting*	4
*HOLTCAT ProTech Electronic Troubleshooting DE205	*Advanced concepts & skills required for tune-up & troubleshooting procedures of diesel engines. Emphasis on the science of diagnostics with a common sense approach.*	
DEMR 2435	Advanced Hydraulics	4
	Advanced study of hydraulic systems & components including diagnostics & testing of hydraulic systems.	
	Spring Semester Total	**8**

Level I Certificate of Completion
Diesel Heavy Equipment

Two Year Program of Studies: 9 Courses totaling 34 credit hours

Heavy Equipment Academy

Level I Certificate of Completion
Diesel Heavy Equipment

ASSOCIATE OF APPLIED SCIENCES

Diesel Construction Equipment Technician

Semester 1		Credit
DEMR 1405	Basic Electrical Systems	4
DEMR 1416	Basic Hydraulics	4
DEMR 1329	Preventative Maintenance	3
MATH 1333	Contemporary Mathematics II *or other*	3
	1st Semester Total	14

Semester 2		Credit
DEMR 1417	Basic Brake Systems	4
DEMR 1406	Diesel Engine	4
ITSC 1301	Introduction to Computers	3
PHYS 1305	Introductory to Physics I Lecture	3
	2nd Semester Total	14

Semester 3		Credit
DEMR 2432	Electronic Controls	4
DEMR 1423	Heating, Ventilation, & Air Conditioning	4
DEMR 2435	Advanced Hydraulics	4
ENGL 1301	Composition I	3
	Select Social & Behavioral Sciences (80) Core	3
	3rd Semester Total	18

Semester 4		Credit
DEMR 2434	Advanced Diesel Tune-Up & Troubleshooting	4
HEMR 1401	Tracks & Undercarriages	4
DEMR 2366	Practicum: Diesel Mechanics Technology Technician	3
	Select Language, Philosophy & Culture (40) Core *or other**	3
	4th Semester Total	14
	Program Total	60

DC/HEA: 30 Total AAS Hours: 60

Hours needed Post DC/HEA: 30 General Academics: 15
Specific Hours: 15

* See St. Philip's College degree description for more information: http://myspccatalog.alamo.edu/

Vers 9.2016

Mr. HURD. Mr. Bowman, thank you for that. And it gives me hope that we are producing the kind of talent we need in order to defend our digital infrastructure.

Mr. BOWMAN. Thank you.

Mr. HURD. Mr. Cambry, you are now recognized for your opening remarks for five minutes.

STATEMENT OF EMILE CAMBRY

Mr. CAMBRY. Thank you, Chairman Hurd, Ranking Member Kelly, and all the esteemed members of the Committee on Oversight and Government Reform for the opportunity to testify for you today.

My name is Emile Cambry. I'm the oldest child of an immigrant from Haiti and an African-American woman on the west side of Chicago. In their youth, my parents endured the frustration of economic hardship and the pain and indignity of racism and anti-immigrant sentiment firsthand.

But they overcame the frustration, they overcame the pain, and they overcame the indignity to become a doctor and a nurse. They had the work ethic and the access to opportunity necessary to do what statistics said they never would do—succeed.

And they made sure they did everything possible to give my younger brother and sister the opportunities to overcome the obstacles necessary for us to attend top institutions. Thanks to their sacrifice, I was able to study economics at the University of Chicago and business at Northwestern University's graduate school.

I've since had the opportunity to work at JP Morgan Chase in their investment banking unit and teach graduate-level business and economic courses at three graduate institutions.

My parents and all of my life's experience up until three years ago helped me realize one thing. Entire communities and generations of hardworking, incredibly talented men, women, and youth are not being given access to the very opportunities that helped my family overcome the hardships in their life.

That's why I founded an organization that addresses that, BLUE1647, to bring opportunity to opportunity deserts across the country. BLUE1647 transforms lives and communities by going into these opportunity deserts and providing residents with access to 21st century tech skills so they can too access the opportunities necessary for them to overcome the hardships in their life.

The formula was simple: Go where the need is greatest; teach those interested in the most marketable skills; and see people overcome poverty, racism, and other hardships in a way that you've never seen before.

And today, I'd like to take the time to talk about how the various programs and public sector partnerships I've had the chance to build are turning communities with few prospects into hubs for tech rock stars that can and will yield an ecosystem of diverse talent to fill the 1.2 million new tech jobs that will need to be filled by 2020 in this country, and that includes Federal IT.

And already we're starting to see that vision come to fruition. While we were founded in Chicago just three years ago, thanks to the support of people like Congresswoman Kelly, we've since grown to have our tech centers present in eight cities and serve over

16,000 youth and adults. Our classes have included everything from app and software development, traditional IT, cybersecurity, and the Internet of Things.

Physical location of our innovation centers are important, which is why we target in lower socioeconomic areas, and 95 percent of our students are black or Latino.

But we don't water down our curriculum because of space, place, age, or income. Our software development curriculum is Department of Labor-certified for our technology apprenticeship program.

I'd like to take a moment to highlight some of the programs and success stories. Our 1919 Program is our Women in Tech and Entrepreneurship program. Since its inception a year ago, over 200 women have participated in our cohort-based program, which is 12 weeks in length. We have various tracks and have created a community approach for skill development in IT. We will soon be adding tracks in project management and cybersecurity.

We have over a 97 percent net promoter score, and an additional 75 women have begun our program this week. All of these women are black or Latino.

Our 21st Century Youth Project is for students as young as 4 and as old as 17 where we have had some great successes in cohort-based training. We have had students intern at Google, Answers.com, Accenture, and Microsoft, including starting their own ventures. Over 70 students have gone on to matriculate into computer science and engineering programs.

We have hosted the Chief Officers for the United States Digital Services Team, United States Chief Data Officer D.J. Patil, and have held general recruiting events around Federal IT opportunities and careers. Over 200 were in attendance for one event, and the major takeaway was that you can serve your country using the technology skills, which was a new concept to many of our attendees.

We have executed some tremendous public and private partnerships to plant seeds in areas you would not expect. In St. Louis, we are a partner in the Jobs-Plus program, a Federal HUD program over four years to increase employment prospects in housing developments. The housing development we focused on is the Clinton Peabody development, where we became—where before the program started had a 68 percent unemployment rate, 93 percent were led by a single mother. At the development, we are partnered with the St. Louis Housing Authority, the workforce development arm of the—St. Louis, SLATE, and the NAACP of St. Louis.

BLUE1647 installed community Wi-Fi, so residents can participate in having Internet access, and we focus on bridging the digital divide.

We conduct technology classes for adults during the day and provide afterschool technology immersion for youth after school.

In addition to working with one housing development in St. Louis, we started working in six housing developments in Los Angeles this week. We do—the more we can replicate our model and support other programs like ours, we ultimately create a pipeline of tech talent who will be naturally interested in technology careers

Thank you for your time, I'll gladly take any questions that members of the committee might have.

[Prepared statement of Mr. Cambry follows:]

Thank you Chairman Chaffetz, Ranking Member Cummings, Congresswoman Kelly, and all the esteemed members of the Committee on Oversight and Government Reform for the opportunity to testify before you today.

My name is Emile Cambry. I'm the oldest child of an immigrant from Haiti and an African-American woman on the west side of Chicago. In their youth, my parents endured the frustration of economic hardship and the pain and indignity of racism and anti-immigrant sentiment firsthand. But, they overcame the frustration. They overcame the pain. And they overcame the indignity to become a Doctor and a Nurse. They had the work ethic ***and*** the access to opportunity necessary to do what statistics said they never would be able to do.

Succeed.

And, they made sure they did everything possible to give my younger brother and sister the opportunities to overcome the obstacles necessary for us to attend top institutions.

Thanks to their sacrifice, I was able to study Economics at the University of Chicago and Business at Northwestern University's Business school. My brother, Jonathan, despite dealing with a debilitating illness, is a renown concert pianist. My sister, despite dealing with challenges, is a successful graphic designer.

I've since had the opportunity to work at JP Morgan Chase in their investment banking unit and teach graduate level business and economics courses at 3 graduate institutions.

My parents, and all of my life's experience up until 3 years ago helped me realize one thing.

Entire communities and generations of hard-working, incredibly talented men, women and youth are not being given access to the very opportunities that helped my family overcome the hardships in their life.

That's why I founded an organization that addresses that: BLUE1647. To bring opportunity to opportunity-deserts across the country.

BLUE1647 transforms lives and communities by going into these opportunity-deserts and providing residents with access to the 21st century tech skills so that they too can access the opportunities necessary for them to overcome the hardships in their life.

The formula was simple. Go where the need is greatest. Teach those interested in the most marketable skills. And see people overcome poverty, racism and other hardships in way that you've never seen it before.

And today, I'd like to take the time today to talk about how the various programs and public sector partnerships I've had the chance to build are turning communities with few prospects into

hubs for tech rockstars that can and will yield an ecosystem of diverse talent to fill the 1.2 new tech jobs that will need to be filled by 2020 in this country and more.

And, already, we're starting to see that vision come to fruition.

While we were founded in Chicago just three years ago, thanks to the support of people like Congresswoman Kelly, we've since grown to have our tech-centers present in 8 cities and serve over 16,000 youth and adults.

Our classes have included everything from app and software development, traditional IT, cybersecurity, and the Internet of Things. Physical location of our innovation centers are important, which is why we target communities in lower socio-economic areas and 95% of our students are black or latino. But we do not water down our curriculum because of space, place, age, or income. Our Software Development curriculum is Department of Labor certified for our technology apprenticeship program.

I'd like to take a moment to highlight some of our programs and success stories. Our 1919 Program is our Women in Tech and Entrepreneurship program. Since it's inception a year ago, over 200 women have participated in our cohort-based program, which is 12 weeks in length. We have various tracks, and have created a community approach for skill development in IT. We will soon be adding tracks in project management and cybersecurity. We have over a 97% net promoter score, and an additional 75 women have begun our program this week. All of these women are black or Latino.

Our 21st Century Youth Project is for students as young as 4 and as old as 17 where we have had some great successes in cohort based training. We have had students intern at Google, Answers.com, Accenture, and Microsoft, including starting their own ventures. Over 70 students have gone on to matriculate into computer science and engineering programs.

We have hosted the Chief Officers for the United States Digital Services Team, United States Chief Data Officer, D.J. Patil, and have held general recruiting events about federal IT opportunities and careers. Over 200 were in attendance for one event and the major takeaway was that you can serve your country using your technology skills, which was a new concept to many of the attendees.

We have executed some tremendous public and private partnerships to plant seed sin placed most would not likely expect. In St. Louis, we are a partner in the JOBS PLUS program, a federal HUD program over four years to increase employment prospects in housing developments. The housing development we focused on is the Clinton Peabody development, where before the program started, had 68% unemployment rate, and 93% were led by a single mother. At the development, we are partnered with the St. Louis Housing Authority, the workforce development arm of the city of St. Louis, SLATE, and the NAACP of St. Louis. BLUE1647 installed community wifi, so residents can participate in having internet access, while

we focus on bridging the digital divide. We conduct technology classes for adults during the day and provide afterschool technology immersion for youth after school. Our partners focus on placement and case management, and we were able to freeze rent for the community for four years to break the cycle of poverty, because rent has served as a disincentive for residents to pursue further employment prospects. As a partnership, we have exceeded our benchmarks for success. Average income for the community has increased 40%, and enrollments in the job development programs are almost a year ahead of our projected pace.

In addition to working with one housing development in St. Louis, we started working in six housing developments in Los Angeles this week, and we partnered with an adult school in Compton, CA where our first adult cohort has concluded and they are taking their certification exams this week and next for internationally recognized IT certifications. The more we can replicate our model and support other like ourse, we ultimately create a pipeline of tech talent who will be naturally interested in technology careers, impacting Federal IT opportunities as employers and service providers.

That's what one organization with a shoestring budget has been able to do. Imagine what we could do with assistance from the federal government? Help us do more of what we do best, and that's close the talent gap in Federal IT and beyond.

Thank you for your time, I'll gladly take any questions that members of the committee might have.

Mr. HURD. Mr. Cambry, I am usually at these hearings—I usually get outraged when I hear opening remarks, but this time I am inspired by what is going on, so thank you for being here for that.

And I believe the ranking member is going to submit her opening remarks for the record, is that correct? Without objection, so moved.

Mr. HURD. I am going to recognize myself for five minutes and go back and forth with Ms. Kelly until we get the going to go to the Floor for votes. And, Ms. Ferrini-Mundy, my first question for you is these SFS CyberCorps, you said there is about a little over 2,000 graduates from that program starting in 2001. You said about 600 active. What is the head room? Have we hit the cap?

Ms. FERRINI-MUNDY. Well, we're always looking for institutions that can come into the fold. We're funding about 62 different institutions right now, and so a big piece of our activity is to build capacity in more places so that we can broaden out the access for students more widely.

Mr. HURD. So the scholarships, it is basically a scholarship. There is a dollar amount ——

Ms. FERRINI-MUNDY. Right.

Mr. HURD.—it is a range, right, depending on ——

Ms. FERRINI-MUNDY. Right.

Mr. HURD.—the institution. How many more of these could we be doing? Let's assume we have, you know, miraculously you can—I'll let you borrow my magic wand. We have these institutions. Do we have an idea of, you know, is it 600 more students, is it 100 more students, is it 10 more students?

Ms. FERRINI-MUNDY. I mean, we could get back to you with a closer analysis of that. It varies by institution type.

Mr. HURD. Right.

Ms. FERRINI-MUNDY. We're trying to build up our involvement with community colleges so that we again ——

Mr. HURD. Yes.

Ms. FERRINI-MUNDY.—see more of a pipeline.

Mr. HURD. Could we make—I am sure Mr. Bowman would love to be the first, you know, to help be one of the ones that help make that—I don't want to speak for you, Mr. Bowman, but I am assuming you are not part of the 62 institutions that receive some of these CyberCorps scholarships, is that correct?

Mr. BOWMAN. Mr. Hurd, we're not today, but we surely can be tomorrow.

Mr. HURD. Making things happen, huh, Robin Kelly, right here?

And one other thing, and, you know, I am interested in the CyberCorps primarily to figure this idea of a Cyber National Guard, right? These are going to be folks that don't go necessarily in the DOD or the NSA but Social Security Administration, Department of Homeland Security, Department of Interior. We need people there. And to be able to get them out of university when they know that they are going to spend X number of years there and that they probably have a job already waiting, a good-paying job with a company that is willing to loan them back to the Federal Government is important. So I have a lot of questions around that.

But the Computer Science for All program, is that something that BLUE1647 is able to tap into? And I would love your thoughts

on whether that is, and, Mr. Cambry, you know, whether that is something that you are even interested in.

Ms. FERRINI-MUNDY. I mean, absolutely. We have a number of different places where that program is being funded, most—primarily in our Innovative Technology Experiences for Students and Teachers, and we accept applications from all eligible places. We'd love to have great connections that go beyond the set of institutions that we typically see.

So inclusion is a very strong emphasis for us. The other place where we are seeing phenomenal engagement from communities, from community-based organizations, from a variety of industry sectors is under our new INCLUDES program, which has 7 of its 37 First Awards are collaboratives among community organizations focused on high-tech engagement with minority students.

Mr. HURD. Mr. Cambry, are you willing to participate and learn more about it?

Mr. CAMBRY. Absolutely. And for centers like our housing developments, we really look at that as truly a model that we can truly expand and scale, and having programs that—with the curriculum that's already tried and tested only makes our jobs easier, which is trying to create a culture of technology development to get people excited and engaged and pursue paths and careers in technology.

Mr. HURD. Great. Thank you. And back to the CyberCorps for a second, the CNAP talks about investing more money into that program. So, again, when you get back to me on the details, where do we think that headroom is, right, because, look, in Texas alone in 2015 we had 42,000 computing jobs that went unfilled, right? And we are not producing enough to fill that, and that is just in private sector, I believe. And the need in the Federal Government is even more.

And so I am going to stop there and turn it over to my ranking member and come back and ask some more questions about kind of structurally how we can do this in the private sector.

My good friend and the distinguished gentlelady from the great State of Illinois is now recognized for five minutes.

Ms. KELLY. Thank you so much. First, I just want to congratulate you on all your hard work with the bill that was passed today. It showed bipartisanship, which people don't think we can do, but we have done that on this committee. And welcome all of you. I just, though, have to give a special shout-out to Mr. Cambry. Emails on my STEM Council that I started when I came in the Congress—I have a STEM Council and the STEM Academy, and he has helped us greatly, so thank you so much. And thanks for all of your testimony.

I too am very, very concerned about the jobs that go unfulfilled but also the lack of Latinos and African-Americans that are prepared to fill those jobs. And it is extremely important. And when I think about a district like mine where our unemployment rate is—even though everything has gone down but it is still higher than the national average. And then when I visit companies and I hear that they can't find—they don't even need to be college graduates but they still can't find people to fill those positions. So I am very interested in how we can diversify and fill those positions. And they are positions that are not minimum-paying jobs but good-

paying jobs that you can have middle-class income and do the things that you need to do.

I had a set of questions, but listening to you guys, what more do you think that Congress needs to do to help reach these goals of filling these jobs, more diversification? Do you see—besides things we are doing today, how can we be more helpful, I guess? And that is anybody. Don't be shy.

Mr. MONTGOMERY. I think one of the things that is already in motion, if you look at this administration, this has been a very forward-thinking, forward-leaning administration with respect to cyber, the number of policies, the number of directives, the risk management framework itself.

One of the things I would urge is that regardless of what happens shortly that that energy continue because this is a topic that we can't take a four-year break on ——

Ms. KELLY. Right.

Mr. MONTGOMERY.—we can't take a four-hour break on, we can't take a four-minute break on.

One of the things that I think would actually help in addition to that, Intel in 2015 we've committed $300 million to the similar topics as my fellow panelists with respect to women and underrepresented minorities to make the workforce more diverse specifically in technology.

But there has to be—there has to be some protection for the U.S. Government for its own employees. And what I would suggest is that Congress look at modifying the way that talented Federal cyber employees are compensated, retained, and trained because the lure to the private sector is intense because, as you mentioned, Ms. Kelly, the number of spots that are open is so demanding that people are looking down the street when the only change is money because of that intense demand. And we need to make sure that our Federal workforce in particular—and this is what Congress can help with—remains highly paid, highly trained, highly effective, and highly motivated to stay.

Mr. BOWMAN. If I may, Ms. Kelly, thank you for the question about what Congress can do.

For the Alamo Academies, a community collaborative program, homegrown, one of the things that drive that model with our industry partners is a pull system—not a push—a pull system to industry demands and requirements to meet their needs.

And, as Chairman Hurd indicated, he had an internship with Southwest Research Institute that kind of got him excited about his career and got him on a pathway. That's exactly what the Academies are doing today with this model.

We had over 45 internships last year alone just from the IT Academy and about 120 internships in all five academies. That model is limited because our capacity depends on how many internships we can get with companies. So any incentive—and many of our industry partners on the Academies board would love to come and help you work on that issue. Any incentive that can encourage and motivate companies to take on these internship responsibilities even at high school level would show that high school young men and women can accomplish these duties and they can do it successfully if they're in the right model and they're mentored properly.

And we're showing that this is working and it's been working for the last 16 years.

In regards to minorities, though, San Antonio is a majority-minority community, and over 70 percent of our graduates are Hispanics today and 6 percent are African-American. So I think we're achieving that in our local community and modeled like the Academy can do that in whatever community that they're in like Mr. Cambry here, you know. You've got a couple of great models here.

But incentivizing our industry partners to want to take on these internships, there is some cost to them to do that, but the benefit to homegrown product pays off hugely when they come, and that loyalty and that culture they get by getting exposed to it early in life. And they don't have any bad habits. They're coming in very young, and it's easy to get a secret clearance because they haven't done anything bad yet.

[Laughter.]

Ms. KELLY. Did you have any thoughts about ——

Mr. CAMBRY. Yes, and I will just add into that. One of the reasons why we pursued this apprenticeship model for software development was because it gave us stamp of approval that we can take to employers to say they've been trained, this curriculum has been certified, and on top of that we're trying to include folks that otherwise might have been excluded.

So I think that, you know, in addition to what Mr. Bowman has mentioned, any incentives that we can get more employers on board that can give us some opportunities to folks that otherwise wouldn't have gotten them because, once again, as he mentioned, when you don't have college debt and you're still able to pursue some revenue for your family, and especially to be able to jump into the middle class, it has a tremendous effect not just for that family but for that community to say that this is a possible pathway and this is a pathway we can be successful in in a relatively short amount of time with some very intensive training.

Ms. KELLY. How do you get the word out about your programs because that is always my concern, too, that sometimes entities like yours don't know what is out there for you as far as grants because maybe we don't do a good enough job getting the word out, but also how do the young people know that you exist? What do you do to get the word out? Any order.

Mr. MONTGOMERY. May I just—so it's funny that you're asking that because I was thinking the exact same thing. I—with respect to Mr. Bowman's comments, I think there would be a line of employers with paid internships and programs where a matriculating student would enter the internship's organization. I think people would line up around the block because they don't have an alternative today. And I think the challenge is one of awareness.

One of the things that we're doing—and we've sort of relegated our efforts to higher education—is with respect to that exact kind of awareness between local centers such as the University of Massachusetts. We reach out to local employers who are having trouble employing and doing internship programs for kids who are currently in hands-on programs at the university.

I think industry can help by joining forces with the kinds of organizations that NSF and other government organizations have des-

ignated to say, look, here's a workforce that wants to work. They actually want to work, and they want to come help you with your problems. We constantly get asked for those resources. We don't have them either. So I think it is absolutely a challenge of awareness, but I think industry can help with these kinds of outreach as well.

Mr. BOWMAN. If I may, opportunities like this to be able to come to Washington, D.C., and talk about programs that are being successful in the communities that are working together, there's been historical bias that you had to be a four-year graduate to be in the IT career field. And fortunately, the last six or seven years, programs like the Academies connecting with opportunities like the Air Force Association CyberPatriot program where they're getting these young men and women exposed to these opportunities so much earlier in life that you're creating that skill set that they can do the job.

And now, we have enough—well, we don't have enough but we're getting graduates out there in the community with Department of Defense, Defense contractors, and then showing them that they can do this work. So we don't have the companies lined up yet, but I believe in just a few short years with more marketing and exposure and seeing how there's multiple career pathways.

You go to college—Robert, one of our examples, went straight to college and came out and got offered a job a year before he graduated. One of them went right into the workforce. Mario went up to Defense with the Pentagon, so he used a career path. And the other three are using a hybrid. They're going to community college, getting associate degrees, minimal debt, getting scholarships while they're working, continuing their higher education because they see the benefit of it, but they also have that experience.

So here is young men and women getting exposed to that culture and excited about it, and industry is starting to get excited about it as well. So the more we can do to encourage, let our industry partners know that these young men and women can do this work, then we're going to have them lined up at the door. And we can meet that need. Thank you.

Ms. FERRINI-MUNDY. Could I just add one other dimension to think about in this context? And that has to do with the rapidly changing landscape of the cybersecurity world. And so at a place like the National Science Foundation, it's very important for our research investments in such areas as access control and cyber physical systems and privacy and data analytics and so forth. All of that research is teaching us about this rapidly changing landscape.

And it's important, I believe, in thinking about the curricula, the experiences that students get in their preparation for us to keep in mind that this is a dynamic field where we need to continually be updated, be offering internship and authentic experiences so students are working at the cutting edge as early on as they can in this domain, which is part of what makes it both exciting and challenging. It has to stay very current.

Ms. KELLY. With the academy we have, the council actually—we have someone from the elementary level and the two-year and then four-year because that was—and then the industry people because the concern was getting the young people interested anyway, to

whet their appetite, but then making sure the high school and the community colleges are teaching what needed to be taught.

Did you have any ——

Mr. CAMBRY. I'll just add in one last thing. Any time you have a little bit of success and one gets a job or an opportunity, it creates a ripple effect. Yesterday, I got word that one of our students, we—we partnered with an adult school in Compton, California. One of the students got their industry certification in cybersecurity, and they recently got a job at—offered a full-time job at Hewlett-Packard, and all of a sudden I get 50 emails today about folks who say, hey, what is it that your program does? And so I think those kind of small successes have a ripple effect, but you're starting to see people to say I can be successful in this space.

Mr. MONTGOMERY. One of the ——

Mr. HURD. Go ahead.

Mr. MONTGOMERY. Thank you. One of the things that I think Homeland and the Continuous Diagnostics and Mitigation program did well was it put together a framework for organizations to understand their cybersecurity posture, where their gaps were, and how to improve. One of the things that we could do similarly is to create this clearinghouse of these kinds of organizations and academies that have interns available, what their level of training is, what their level of certification is, where their location is in order to incent employers, both government and nongovernment, to have a place to go to fill this need even if it's with interns in temporary assignments because any work that they're doing is going to help the organization, as well as the candidate get some real-time hands-on experience.

But that clearinghouse of these organizations like Mr. Cambry's, like Mr. Bowman's, I'm not aware of it. That would be ideal because then people can shop by their location, shop by their need, and help benefit the local community as well.

Mr. HURD. I am going to recognize myself for another five minutes.

So I think, you know, here there is consensus that there is a need in the IT workforce for professionals who have received their skills through training, certificates, or a degree that is not a traditional four-year model. Is that consensus there? And, Dr. Ferrini-Mundy, the CyberCorps program can be used for those types of things, is that correct?

Ms. FERRINI-MUNDY. Certainly. We—particularly in the capacity-building area, we can be funding the design of innovative curricular approaches, different durations of training, and particularly the connection to the two-year colleges.

Mr. HURD. Yes. But scholarships as well?

Ms. FERRINI-MUNDY. Yes, scholarships also go to two-year college students.

Mr. HURD. Got you.

Ms. FERRINI-MUNDY. Yes.

Mr. HURD. So what do we need to do to grow the program? And what do we need to do to grow the program? And just so I am clear, if I am a senior in high school, do I apply to OPM for this scholarship and then take it to a school or do I have to apply it to one of the 62 institutions for that specific program?

Ms. FERRINI-MUNDY. Right. So you have to apply to one of the 62 institutions, and OPM does a very good job in publicizing these institutions and the program, so that's one thing.

But your other question about what would it take to grow this program in our fiscal year 2017 request, we have indicated that we'd like to lay the groundwork with an increase for SFS alumni to be available over the course of their careers to help the Federal Government respond to cybersecurity challenges. So this is related to the reserve idea, to the cyber surge corps idea.

But at the same time for us at the National Science Foundation, I believe we're beginning to think about this systemically. So we do have the SFS program with its scholarships, but I mentioned our INCLUDES program, our Advanced Technology Education program, the Computer Science for All initiative. And I think that that leads me to believe a more systemic look by us inside our agency at how we think about the pathways, at how we kind of build a context, connect to the research. That would help us address the challenges that we're trying to address in a more comprehensive way.

Mr. HURD. Good copy. Mr. Montgomery, your point about the draw of the private sector, now, the value in, you know, the CyberCorps or a National Guard is saying you are going to commit to the Federal Government for a length of time. If it is the length of time of what your scholarship is or we say it is four years or something, that is what gets someone into the ground floor at protecting digital infrastructure.

And then if we add on top of that that there is participating entities or companies that are willing to help loan those folks back, you know, as their National Guard experience, how do we structure that in such a way that it is not disruptive to business operations?

Mr. MONTGOMERY. There's actually some great Federal examples of this kind of loaning program. There's a program in particular out of OSD called the Corporate Fellows Program where—and this is a little bit different. This isn't students necessarily, but the model could be very, very similar. An officer grade 6 is loaned out for a year. The government pays for the salary; the private company pays for all of the travel and expenses for the military officer. But they're embedded with the company for a year. And the thought is that they'll return to their rotation with cutting-edge management technique and experience with respect to what private industry is doing.

I can see the same exact thing being—with respect to this National Guard of Cyber Warriors as well because the demands in both industry and the private sector is so intense. Getting someone loaned out for the course of a year, the only difference is the company themselves would pay for the privilege. But it could be that kind of fellows program where it is a rotation in, it's a rotation out. But I would urge you to investigate that program because those paperwork—that paperwork is already developed. We're already doing those kinds of things.

Mr. HURD. Yes, because the framework can be that you have these kids coming from high school and that they are going to school, whether it is, you know, four-year, two-year, or something else, but then the set of companies that want to see these Cyber

National Guardsmen and women are also the ones providing internships during that educational process as well, right, in order to help hone that so when they finally finish whatever educational opportunities they are looking at.

That is kind of, you know, the concept that I envision of this program to make sure that we ultimately are having a cross-pollination of skill sets between the public and the private sector. Is that crazy?

Mr. MONTGOMERY. Not at all. The number of occasions—when people think about cyber today, they think about a breach, but cyber is a 24-hour occupation. And the number of occasions where a private industry organization has a spike in demand for labor is routine. If you think about anyone with respect to the vertical markets like retail or banking, there are—it is cyclical. They have more demand at different times than they do at other times. And the ramp-up for a guard contingent would be an important bolster to their workforce.

Also, with respect to Presidential Directive 41 where they established the guidelines for what happens in a government breach, the same thing can be said for the private sector as well. There is a criminal element that the FBI investigates. There is a hygiene element that Homeland is responsible for. And there is constant need for updates and hygiene and good best practices that this National Guard could take care of an ongoing basis that companies are struggling to find good supply for.

Mr. HURD. Got you. Dr. Ferrini-Mundy, what is the first step that an entity like the Alamo colleges need to do in order to be part of the 62 participating agencies in the CyberCorps?

Ms. FERRINI-MUNDY. Well, I think that Mr. Bowman and I need to exchange business cards and talk about the various possibilities for getting to know the National Science Foundation and its ——

Mr. HURD. I think we can make that happen.

Ms. FERRINI-MUNDY. Okay. It's starting already.

Mr. HURD. And then what about for an organization like BLUE1647 to participate in the Computer Science for All program?

Ms. FERRINI-MUNDY. Same response. And we can point you to the programs that would be, I think, the best-suited to the particular organizations here.

Mr. HURD. Excellent.

Ms. FERRINI-MUNDY. Very exciting. We're looking always to broaden involvement and to reach out more generally.

Mr. HURD. Great. I would now like to recognize for five minutes the gentleman from the Commonwealth of Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman. And welcome to our panel.

Gosh, there are so many facets of this subject. Let's start for a second with internships. I don't know if you know, Dr. Ferrini-Mundy, but when you compare the Federal Government's success with internships to the success in the private sector, you want to guess how well we do?

Ms. FERRINI-MUNDY. No, I'd prefer to have you explain. I don't—I'm not familiar with the ——

Mr. CONNOLLY. Anyone from the private sector want to take a guess at the rough percentage of interns who are eligible and hired

for employment in terms of a successful internship? It is very high. It is, you know, well above 60 percent private sector. In some private sector companies it is like—well, I won't name one that hired my daughter—but it is in the 90 percentile.

We are in the single digits, Dr. Ferrini-Mundy in the Federal Government. It is a fiasco. There is no systematic mentoring. There is no systematic exposure to all aspects of an agency's mission or most of them. There is no morale booster. We actually have people who leave when they kind of talk in any kind of exit interview, if there is one, who say I would rather put my head through a pencil sharpener than ever work for the Federal Government again.

We don't see it apparently as a tool for recruiting the next generation or motivating the next generation or tailoring the next generation, which the private sector systematically does. Otherwise, why have an internship program? Why not make it work for both sides? You try us out for size and we are trying you out, but we have done some screening and orientation so the probability of you sticking around with us is high. And our desire for making a permanent job offer is also high. Otherwise, it is very inefficient, and we are actually turning people off to our mission.

I don't mean to suggest by saying this that you in any way, shape, or form have responsibility. I just point out it is a subject I looked into, and I was appalled at the data I found and what a complete opportunity cost our current internship efforts are in the Federal Government.

And it is relevant to the topic at hand because we can't afford that, especially when it comes to the Federal IT issue and cyber in particular because our IT experts in the Federal Government are aging out. And if you looked at the average age of our counterpart in the private sector, it is much younger.

So the private sector does not have a problem recruiting the next generation to handle the mission. We are. And the only choice we have, it seems to me, is to recruit a younger generation. Well, what are the tools at hand for doing that? And I worry about that. The pay gap is growing. The desirability of the workplace can be a challenge. I think it is very hard for a Federal recruiter to go to a university campus and say I see a 30-year Federal career in your future and you are going to love it.

Now, partly, we are to blame. Congress has done a great job in making the Federal workplace a less desirable place in public imagination. We have disparaged the workforce, we have frozen salaries, we have cut benefits. None of that brings any glory on us, and I think frankly was designed in some cases to do just that, make it less desirable as a career choice.

But we can't afford to continue to do that, certainly not in the sphere that the chairman and ranking member here are exploring because IT is just too important. Security is involved, national security is involved, privacy is involved. And so I think this is a critical topic, and I think there are things we can do to make it easier on ourselves to do that recruiting and to make it more attractive, internship programs being one of them. That is not rocket science. And the private sector has lots of models that are profoundly successful that we could emulate or learn from or benchmark against if we would only try.

But longer term, we are going to have to suspend some normal civil service workplace protections if we are going to have fellows who go in and out of the government. That is not so easy. That is really not so easy. I wish it were, so we are going to have to be less rule-driven if we are going to do that while still protecting everybody involved. We are going to have to look at more flexibility, obviously, in pay scales. If we are not willing to do that, we will never attract a talent comparable to that we face in the private sector.

So I think there are lots of issues here for us to continue to explore. I thank you so much for having this hearing because I think this is a critical piece of what we are trying to do in IT modernization and upgrading the Federal Government.

Thank you, Mr. Chairman.

Mr. HURD. Amen, brother.

Last round of questions from me and then we will wrap it up. And, Dr. Ferrini-Mundy, are the folks that are participating in the CyberCorps, are they staying around in the Federal Government? You gave some stats at the very beginning. Can you characterize that for me?

Ms. FERRINI-MUNDY. Well, I would like to first just mention briefly how excited they are as they enter the Federal Government, and so although the incentive of a scholarship is powerful and the payback requirement is definitely there, this jobs fair that we do in conjunction with OPM every January attracts 100 Federal agencies, and students are hired on the spot and do their security clearances while they're ——

Mr. HURD. And this is a jobs fair for ——

Ms. FERRINI-MUNDY. For the SFS graduates.

Mr. HURD. Okay.

Ms. FERRINI-MUNDY. So we know that they're welcomed into the Federal Government with—warmly, and the data that we have indicates that about 70 percent stay beyond their service requirement. So we are again tracking to see how long they stay and what they do, but their entry is very quick and smooth and they're quite in demand.

Mr. HURD. And how does—I don't know if it is NSF or OPM. How do they prioritize which agencies are in need of these potential SFS or is it this—it is a free-for-all and you come to this job fair and that is how you do it?

Ms. FERRINI-MUNDY. I think I—it's my understanding that there is no prioritization particularly, but the agencies show up, they make themselves available, they talk with students. And we'd love to invite the members of the subcommittee to join us next year when we go through it. It's quite fascinating.

But, as I understand it, there's no ——

Mr. HURD. Yes.

Ms. FERRINI-MUNDY. It's an open discussion.

Mr. HURD. Please do. And in my remaining three minutes and 18 seconds, I want to go down the line. And, Mr. Cambry, I want to start with you. This notion of a Cyber National Guard, I think you are attracting people in from areas that may not be exposed to this. We can expose them to, you know, the CyberCorps program. We can expose them to institute like the Alamo Academies,

equivalents in your neck of the words. And then we have companies like Intel that are interested in hiring them.

What do you see is kind of the next step in trying to achieve that vision? And that is really—my question down the line—and, Mr. Cambry, you are going to have the last word.

Mr. CAMBRY. For us, it always has been can we change the narrative so people can see themselves being successful in these positions? So that's kind of the standpoint we took since we first started.

Now, our standpoint is to also convince the employers that there is some value to investing in these folks from the community and other nontraditional settings. We've also been able to partner with colleges, community colleges, and a whole host of other people as part of this ecosystem of kind of support.

What that next step for us has always been, partnering with organizations that either do the placement or that have those direct connections to those employers because, once again, the more that we can focus on our students and our constituent base and not as much on trying to find the perfect match with the employers, it makes our job easier because then we can push harder downstream and really start cultivating that level of talent and really focus even more on our curriculum, placement, and being able to do the testing necessary to make sure they're ready.

Mr. HURD. Thank you. And thank you for being here. And everybody, the remaining—you have got 30 seconds to answer that question. Mr. Bowman, you are recognized for 30 seconds.

Mr. BOWMAN. Chairman Hurd, thanks again for the opportunity. So it's real simple. Companies that are willing to invest in an intern get to indoctrinate this young man and woman to their culture. And what they're finding is the retention is off the charts. Sometimes it's the first paycheck that these young men and women have received, so they're bleeding that company's blood, that color, forever. Their loyalty is off the charts. So if you invest in it, you get a positive return on investment.

Businesses will not be participating in a program like the Alamo Academies going into their 16th year if there was not a positive return on investment. And internships is that secret ingredient to getting these young men and women exposed just like yourself when you had yours at Southwest Research and here you are today. And that's a pathway to success, so I'm very much for it.

Thank you for the opportunity.

Mr. HURD. Thanks for being here. Mr. Montgomery?

Mr. MONTGOMERY. I think demand is so intense that organizations will take a flyer. What I'd love to see is focus on a clearinghouse where the kids are made available to potential employers because they'll come. They'll absolutely come.

Mr. HURD. Absolutely. Dr. Ferrini-Mundy, take us out.

Ms. FERRINI-MUNDY. Thank you so much, Chairman Hurd, Congresswoman Kelly. This has been wonderful and exciting to talk about this topic. Two points that I'd like to leave us with, one is the critical importance of developing and seeking talent broadly across all groups from this country that have been underrepresented in the STEM fields, in the IT fields, and in the

cybersecurity fields. We need the diversity of this nation to be brought to bear on these challenges.

And second point is that through public-private collaboration, the government and the private sector can work together to understand the changing needs in this domain and the kinds of experiences, certifications, assessments, ability to be certain that people are ready to step in as needed over the course of their career in and out of government so that we are taking the very best talent and helping them learn and grow throughout their careers.

Mr. HURD. I would like to thank our witnesses for taking the time to appear before us today. What you guys do is important to educating our kids and the future of our country, so thank you for that.

And if there is no further business, without objection, the subcommittee stands adjourned.

[Whereupon, at 4:31 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Opening Statement
Rep. Robin L. Kelly, Ranking Member

Hearing on "Closing the Talent Gap in Federal IT"
September 22, 2016

Thank you, Mr. Chairman, for holding this hearing to discuss ways to close the federal IT talent gap, and I thank the witnesses for joining us today. We talked about this issue during our field hearing in Chicago in June as part of the broader conversation about federal efforts to improve cybersecurity. I am glad that this hearing will focus on this very important issue, as it deserves its own hearing.

Our demand for and reliance on technology is expanding. We are living in an era where we always have to be connected. Technology is embedded in our daily lives—we have internet—connected mobile phones, tablets, cars, watches, and appliances. We are transitioning to an era marked by the Internet of Things.

At the same time, the sophistication of hackers is growing, cyberattacks are increasing, and the threat is evolving.

Given these conditions, it is not hard to see why the demand for STEM and cybersecurity professionals has multiplied and why there is a shortage.

The National Science and Technology Council estimates that the United States will need 22 million new STEM graduates by 2018, and that we will fall three million short of that goal. If we just look at the cybersecurity field, we have a shortage there as well. The Center for Strategic and International Studies notes that last year there were more than 200,000 cybersecurity jobs in the U.S. that went unfilled.

To close this talent gap, we need to work on enlarging the pool of STEM professionals by investing in education and workforce development.

I have been working on this in my district and hometown of Chicago. I brought together local professionals to form a STEM Council to discuss ideas and suggestions for improving STEM education in my district. Mr. Cambry, a friend and colleague, whom I have asked to testify here today, is a member of that Council. We implemented one of the Council's ideas—an Academy and boot camp to connect young students, including 6th, 7th, and 8th graders, with STEM professionals to mentor, coach, and inspire the kids to pursue STEM disciplines.

I also believe that we need to increase the number of teachers who can teach STEM subjects. A bill I introduced, the DISTANCE Act, would award scholarships to STEM students pursuing teaching certifications and incentivize them to teach in underserved communities.

Under President Obama, the Cybersecurity National Action Plan (CNAP) is investing $62 million in cybersecurity personnel and the Administration has recently issued a Federal Cybersecurity Workforce Strategy that builds upon the CNAP initiatives.

The National Science Foundation (NSF) administers the CyberCorps Scholarships for Service program which provides scholarships to undergraduate and graduate students studying cybersecurity in exchange for a commitment to join federal service. NSF is also investing about $125 million over five years to fund computer science education in elementary, middle, and high schools throughout the country.

The witnesses before us today are also trying to address the talent gap, and I look forward to hearing about their efforts and receiving their advice.

The federal government and the private sector are competing in acquiring talent from the same pool and need to find ways to work together on increasing that pool so that we can all benefit.

Thank you, Mr. Chairman, and I look forward to the testimony of the witnesses.

CompTIA.

The Computing Technology Industry Association
House Oversight and Government Reform Committee
Hearing Testimony:
"Closing the Talent Gap in Federal IT"
September 22, 2016

Introduction to CompTIA

CompTIA would like to thank the House Oversight and Government Reform Committee for holding this hearing to solicit recommendations on closing the talent gap in our national information technology (IT) workforce. We are a non-profit, high-tech trade association with a membership of more than 2,000 that includes computer hardware manufacturers, technology distributors, and IT specialists who help organizations integrate and use technology products and services. CompTIA's members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. Our partners We also have more than 2,000 partners include worldwide training and testing developers, training providers, and academic institutions.

Our association is the leading developer and provider of vendor-neutral IT and cybersecurity workforce certifications. The CompTIA certifications that are most commonly recommended or required by federal agencies (CompTIA A+, CompTIA Network +, CompTIA Security+, and CompTIA Advanced Security Practitioner) are International Standard ANSI/ISO/IEC 17024 certified. In the past year, we have also completed our full integration of TechAmerica into our public advocacy efforts, adding an additional member base of large technology companies and complementing CompTIA's strengths in education, certification, advocacy, and philanthropy with additional competencies in state, federal and international policy work.

Every day, technology is becoming more engrained in our everyday life. With this incredible change comes the challenge of security and having the right workforce in place to manage those security threats. To combat increasingly sophisticated cyberattacks, it is necessary that we move beyond hardware and software solutions (e.g. firewalls and intrusion detection) and into upskilling our workforce. Furthermore, we must ensure that we foster an environment that encourages innovation while enhancing the existing public-private partnership between industry and government.

Current Security Trends Affecting Today's IT Environments

Security continues to be a top IT priority for companies, as the recent history of new technology models and the reliance on data has brought focus to the need for tight security and privacy. Accordingly, the IT security market is growing, with Gartner projecting overall spending on enterprise security to reach $100.3 billion globally by 2019.[1] However, nearly half of all IT security professionals believe there is some degree of skill gap within their organization. Fifty-three percent of companies with gaps want to be more informed about current threats, followed by desired improvement in current security technology and awareness of the regulatory environment.[2]

That said, issues such as malware, denial of service attacks, and privacy concerns continue to present challenges for the industry. 2016 CompTIA research finds that nearly three in four organizations have experienced a security breach. CompTIA's International Trends in Cybersecurity report notes that security will become a higher priority for more than 8 out of 10

[1] CompTIA 2016 IT Pro Security Report.
[2] Ibid.

managers. We need to do more to build upon our workforce so that we can address these growing concerns, and we need to do it quickly.

New Technology Developments

Rapid introduction of new technologies, including the Internet of Things (IoT) and cloud storage, offer tremendous opportunities for how we function in our daily lives and operate businesses. There are more connected devices in operation than there are people on the planet. Despite security breaches causing devastating effects, one could reasonably argue that given the sheer number of devices and applications in use, the volume of security breaches is actually a low percentage of the total. Nevertheless, there is a responsibility for government and industry to work together to examine some governance approaches and additional best practices. The resulting approaches should foster an environment that will encourage innovation and growth without undue burden from unnecessary regulations. As part of this discussion, we must also focus on programs and policies to ensure we have both the quantity and quality of workers that we need.

Ensuring Our Workforce Is Equipped for the Cybersecurity Challenges of Today and Tomorrow

According to research performed by CompTIA, the growing proliferation and sophistication of hackers, combined with greater reliance on interconnected applications, devices, and systems, has created a security environment that is challenging for even the best-prepared organizations. As noted above, the continued adoption of new and emerging technologies has expanded the attack surface and increased opportunity for human error. Against this backdrop, it is not surprising that CompTIA's April 2015 "Trends in Information Security" report found that the biggest weak spots that lead to cybersecurity breaches are human users of IT.

Though human error often ranks low as a serious concern for organizations, CompTIA's research has shown it is the largest factor behind security breaches. Most recently, human error has been proven to be the cause of 52 percent of all cybersecurity breaches in the workplace.[3] This should not be surprising as large organizations, including both federal government agencies and private sector companies, often make use of thousands of computers in order to carry out their daily missions. When a human being is put in front of those computers, they each bring a level of cybersecurity risk. This necessitates the need for a well-trained IT and cybersecurity workforce with the proven capabilities to identify, mitigate, and respond to risk. With regard to human error, training is the clear answer, but many public and private organizations today struggle with understanding how to afford, access, and institutionalize meaningful investments in training and other solutions, such as certifications, that can better prepare staff tasked with cyber hygiene and security functions to operate in today's environment.

Mitigating Advanced Persistent Threats Through Basic Cyber Hygiene Training

In today's world, organizations face Advanced Persistent Threats (APTs) in which the majority of attacks focus on exploiting naïve end users of technology. Today's APTs involve the

[3] CompTIA 2015 Trends in Information Security Study.

introduction of malware by unsuspecting end users to compromise traditional security measures and create malicious "overlay networks." These networks introduce botnets, ransomware, and spying software designed to obtain a company's intellectual property. Many of these networks are designed to store information – such as credit cards and industry secrets – culled from individuals and companies around the world. Most of the time, these persistent threats are introduced over long periods of time, rather than through a single event.

According to the IBM 2015 Cyber Security Intelligence Index, unauthorized access incidents rose from 19 percent in 2013 to 37 percent in 2014. Furthermore, according to the report, "with an ever expanding array of malware from which attackers may choose— including viruses, worms, Trojans, bots, backdoors, spyware and adware—it seems fairly certain that malicious code incidents will continue for the foreseeable future."[4]

Because APTs can be successful through any employee, all employees should be aware that these threats exist. Cybersecurity training for all company employees is vital, and the evolution of that training to keep pace with the evolving attacks will undoubtedly present a challenge. In many government entities, other forms of training are mandated annually for all employees (i.e. sensitivity training) yet cybersecurity training is optional and stagnant. We urge the federal government to lead by example by requiring basic cybersecurity training/hygiene for all employees.

Validating the Skills of Those With IT and Cybersecurity Job Functions

Beyond basic cyber hygiene training, employees specifically tasked with ensuring security should be trained and equipped to identify long-term threats. Whenever training occurs, testing should also be performed to validate that security workers have retained the skills needed to configure systems so that they are able to gather and interpret seemingly innocuous events that occur over time to detect long-term, continuous threats.

As noted above, IT security is increasingly essential to successful government operations. Maintaining and increasing IT organizational performance in key areas such as IT support and IT security are import goals for all Chief Information Officers (CIOs) and IT leaders. Studies have shown that industry recognized certifications in IT raise the effectiveness of an IT team in carrying out its job functions. Moreover, testing in education settings can, among other things, identify gaps in knowledge, develop retrieval aid that enhance retention of knowledge, and improve the transfer of knowledge to new contexts.

CompTIA has also conducted research on managers' perceptions of the importance of testing after training. Our research on this topic has targeted the U.S. Department of Defense (DOD), which we believe has set the "gold standard" for building a robust IT and cybersecurity workforce. CompTIA's Military Career Path Study found that 74 percent of active duty military personnel with staff management responsibilities classified testing after training to confirm knowledge gains as "very important."[5] Further, these managers reported that testing after training also helped to set a baseline of expertise among staff, provide career path guidance, improve the

[4] IBM 2015 Cyber Security Intelligence Index.
[5] CompTIA 2014 Military Career Path Study: Assessing the Role of Training and Certifications.

performance of a team, retain talented staff, and evaluate staff for promotions or career advancement.[6]

According to a study conducted by the International Data Corporation (IDC) and sponsored by CompTIA, candidates and staff with CompTIA A+ and CompTIA Security+ certifications perform better than staff that is not certified. According to the research, certified employees are: (1) more confident; (2) more knowledgeable; (3) reach job proficiency more quickly; (4) more reliable; and (5) perform at a higher level.

When IT professional are confident in their abilities, they are more likely to be forward thinking, proactively anticipate issues, and solve problems before they impact organizational performance. Having the right skills gives IT professionals the confidence to believe they can achieve their assigned responsibilities. Further, certified professionals are 85 percent more likely to believe they have the knowledge and skills needed to successfully fulfill their jobs.[7] As a result, these certified security professionals are better positioned to properly assess risks, design and implement interventions, and correct policy weaknesses. Because most of today's hiring environments prioritize experience above professional credentials, it is also important to note that CompTIA's research has found that after ten years of security experience or support experience, certified staff has between 20 and 25 percent more core domain knowledge than those with the same experience who are not certified. Once on the job, certified IT professionals have also been found to perform up to 53 percent better than those without certification in critical, job-related activities.[8]

Further, certifications help to put program managers at greater ease with the capabilities of their staff. Research conducted by CompTIA has found that an overwhelming majority of IT professionals and their hiring managers agree on the value of certifications. Ninety-three percent of human resources (HR) executives believe certifications are beneficial, as they offer a competitive edge in the job market, heightened career advancement opportunities, and increased value to employers and their organizations.[9]According to employers, the top benefits of IT certification are: (1) the ability to understand new or complex technologies; (2) higher productivity; and (3) more insightful problem, solving.[10] In addition, CompTIA has found that roughly 8 in 10 hiring managers say it is challenging to find the right candidates with the right skill sets to fill vacant IT positions and verifying job candidates' credentials can be a challenge.[11]

Lessons Learned From Public and Private Sector Cooperation

CompTIA would like to ensure the Committee is aware of effective strategies that are currently being used to promote public and private sector cooperation in ensuring a robust and highlight skilled IT workforce.

---

[6] Id.
[7] CompTIA 2014 IT Support and Security Performance Study: The Impact of CompTIA Certifications on Organizational Performance.
[8] Id.
[9] CompTIA 2015 IT Careers Blog: Four Reasons HR Execs Love Certifications.
[10] Id.
[11] Id.

As was previously mentioned, DOD has worked closely with the training and certification community to consistently up-skill workers. Many certification organizations have participated in the 8570 and successor 8140 initiatives. These initiatives, which require DOD personnel and contractors with information assurance titles to have cybersecurity certifications, are vital for the U.S. Government workforce. This requirement ensures individuals are trained and certified in the skill sets required by their job. DOD's cyber workforce management strategy not only enhances our national security and ensures value from taxpayer investments in IT training, but it also assists DOD in meeting its IT/cybersecurity personnel retention goals and helps our veterans transition their skills to civilian employment once their military service has ended.

As a result, CompTIA was thrilled to see that DOD will play a leadership role in executing the 4th goal of the Federal Cybersecurity Workforce Strategy, which is focused on retaining and developing highly skilled talent in the federal workforce. The DOD model has been so successful that CompTIA once again encourages the U.S. Government to lead by example by encouraging other federal civilian agencies to adopt similar programs. Related to this, CompTIA encourages Congress to review and consider updating to the Government Employees Training Act (GETA) to ensure that all federal government agencies have the flexibility needed to use resources allocated for IT training to pay for industry-recognized certifications where appropriate.

The National Initiative for Cybersecurity Education (NICE) is also a critical element to properly training the nation's workforce. CompTIA has worked closely with NICE to provide real-time information concerning the location of qualified IT workers. Like with DOD, CompTIA continues to provide input and support to this initiative to ensure that skills are being appropriately mapped to jobs.

Furthermore, in 2015, CompTIA, in partnership with Burning Glass Technologies, received a three-year grant from the National Institute of Standards and Technology (NIST) to develop an interactive cyber jobs heat map that will show the demand for and availability of critical cybersecurity jobs across the nation. The project, which is being funded through NICE, will provide data to help employers, job seekers, policy makers, training providers, and guidance counselors in order to meet today's increasing demand for cybersecurity workers. The first version of the heat map will be released in October 2016.

Moving forward, CompTIA believes it is critical to ensure our national IT/cybersecurity workforce has the skills they need. This can be achieved through hands-on training that incorporates experiential learning solutions that can be used to evaluate existing worker skill sets and provide consistent, quick feedback concerning necessary skills. Additionally, CompTIA believes in the value of continued assessment to ensure that IT/cybersecurity personnel have the skills needed to protect today's networks, as well as continuing education to provide IT workers with ample opportunities to re-learn existing skills and also learn new skills to keep pace with new technologies.

Creating a Pipeline for IT and Cybersecurity Talent

While CompTIA is best known for validating the skills of the existing and aspiring IT and cybersecurity workforce, we recognize that a steady talent pipeline is needed to ensure the IT and

cybersecurity workforce of the future. Our nation's businesses are struggling to fill roughly 1 million open IT jobs. We believe these are desirable positions, especially as many of these job vacancies have an average starting salary of $50,000 with growth into the six figures.[12] Despite the appeal of these positions, CompTIA has repeatedly found the average American is unaware of the pathway to a successful career in the IT space. In fact, of the more than 1.5 million individuals CompTIA has certified, many shared anecdotally that they unintentionally found themselves pursuing work in the IT sector.

In most cases, the skills needed to enter the cyber workforce can be achieved through training and industry-recognized certifications. That said, we believe that IT/cybersecurity should be given strong consideration as a profession for individuals looking to enter or re-enter the workforce or make a career change. If formal education is needed, very often a two-year community college degree will suffice. To clarify, there is a varying level of cyber worker. The "cyber ninja," who is at the top of the IT/cyber workforce pyramid, may require a lot more training and formal education. However, the majority of cybersecurity and IT jobs do not require a four-year college degree, and the workforce as a whole requires more of these lower level cyber workers than "ninjas."

We are aware of efforts at the federal level aimed at creating tuition reimbursement for cybersecurity degrees. While CompTIA supports the overarching goal of these initiatives, we believe the federal government can continue to demonstrate leadership and work towards swifter achievement of its overarching IT/cyber workforce goals by prioritizing resources for training and certification efforts. CompTIA believes such initiatives could be executed in a cost effective manner and have tremendous impact among members of the federal workforce who are not enrolled in four-year institutions.

We also know the U.S. Government relies heavily on the use of industry-recognized certifications for professional development. This is evidenced by the Department of Homeland Security's (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS) portal, which highlights that certifications play a large role in getting people the skills they need to enter the cyber workforce. Further, the FY16 omnibus appropriations bill included a provision directing the federal government to take stock of the certifications held by the existing cyber workforce in order to determine what skills may be missing. To summarize, certifications are used to help professionalize the cyber workforce and help provide a common lexicon of the skills needed across the public and private sector.

Finally, CompTIA also supports apprenticeships and vocational models for building out our nation's IT/cybersecurity talent pipeline. We believe the real world experiences that can be gained through these types of apprenticeship and vocational positions can only enhance an individual's training for a successful career in IT/cybersecurity.

Conclusion

While technology has made so many facets of our daily lives easier, it has also brought challenges that will continue to be addressed. Industry's commitment to security remains strong

[12] Source: Burning Glass Technologies.

and the future security of devices will rely on a modernized workforce that is well-trained and equipped to address the challenges that inevitably exist when rapid technology innovation and bad actors exist. To that end, enhanced cooperation between government and industry is vital for our overall security posture. This partnership, which has had a great deal of success in past challenges, must remain nimble and easily adaptable as the threat landscape evolves. With a strong public-private partnership and a well-trained workforce, we trust that together we will be able to rise to the challenges that the future brings.

○