RAMPS

and the Colorado Springs Cybersecurity Ecosystem

Final Report of the National Initiative for Cybersecurity Education
Western RAMPS (Regional Alliances and Multi-stakeholder Partnerships to Stimulate) Cybersecurity Education Project

May 2019

This report was prepared by Pikes Peak Community College using Federal funds under award 2016 NIST-NICE-OJ (70NANB16H323) from the National Initiative for Cybersecurity Education at the National Institute of Standards and Technology, US. Department of Commerce. The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the National Institute of Standards and Technology or the US. Department of Commerce.

Table of Contents

Glossary of Abbreviations

AAS	Associate of Applied Science
AFCEA	Armed Forces Communications & Electronics Association
ATD	Association for Talent Development
AY	Academic Year
BEA	Business and Education Alliance
BPSS	Business, Public Service & Social Sciences Division of Pikes Peak Community College
CAE2Y	Center of Academic Excellence for Two-Year Schools
CAE4Y	Center of Academic Excellence for Colleges and Universities
CAP4K	Colorado's Achievement Plan for Kids
CASP CE	CompTIA Advanced Security Practitioner Continuing Education
CCCS	Colorado Community College System
CDE	Colorado Department of Education
CDLE	Colorado Department of Labor and Employment
Chamber/EDC	Colorado Springs Chamber and Economic Development Corporation
CISSP	Certified Information Systems Security Professional
CNG	Computer and Networking Technology
CompTIA	Computing Technology Industry Association
CRIB	Cyber Range in a Box
CTE	Career and Technical Education
CTSO	Career and Technical Student Organization
CWDC	Colorado Workforce Development Council
D2	Harrison School District 2
D3	Widefield School District 3
D11	Colorado Springs District 11
D14	Manitou School District 14
D20	Academy School District 20
D38	Lewis Palmer School District 38
D49	School District 49
D60	Miami-Yoder School District 60 JT
DHS	United States Department of Homeland Security
DoD	United States Department of Defense
HCS	Holistic Cyber Security
IAT III	Information Assurance Technical Level III Certification
ICAP	Individual Career and Academic Plan
ISSA	Information Systems Security Association
IT	Information Technology
JROTC	Junior Reserve Officer Training Corps
LPIC	Linux Professional Institute Certification
MSA	Metropolitan Statistical Area
NCSAM	National Cybersecurity Awareness Month
NICE	National Initiative for Cybersecurity Education

NIST	National Institute of Standards and Technology
NSA	National Security Agency
OEA	Office of Economic Adjustment (US Department of Defense)
PPCC	Pikes Peak Community College
PLTW	Project Lead the Way
PWR	Postsecondary & Workforce Readiness
RAMPS	Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education
SHRM	Society for Human Resource Management
SCI	Sensitive Compartmented Information
STEM	Science, Technology, Engineering and Mathematics
TK	Technology Knowledge
TS	Top Secret
UCCS	University of Colorado Colorado Springs
USAFA	United States Air Force Academy
USDOL	United States Department of Labor

Cyber Prep Steering Committee Members

Higher Education

Gretchen Bliss	Cybersecurity Director, Pikes Peak Community College
Jamie-Lynn Figure	Cyber Prep Program Manager (2017-2018), Pikes Peak Community College
Steve Fulton	Information Assurance Faculty, Regis University
Ernie Greene	Cyber Prep Program Manager (2016-2017) Pikes Peak Community College
Chelsy Harris	Dean of High School Programs & Concurrent Enrollments, Pikes Peak Community College
Joe “Hark” Herold	United States Air Force Academy CyberWORX Program
Terri Johnson	Cybersecurity Lead Faculty, Pikes Peak Community College
Dallas Pierce	Associate Dean of Business & Technology, Pikes Peak Community College
Debbie Sagen	Vice President Workforce Development, Pikes Peak Community College

Industry

Hank Bond	Senior Executive for Global Governments Engagement, root9b
Patty Bonvallet	Technology Development Manager, Boecore, Inc.
Randel Castleberry	Founder & CEO, Aspen Logix
Mary Graft	Director of Cyber Education and Training, National Cybersecurity Center (2017-2018)
Sara Kinney	Founder & CEO, RIM Technologies
James Krainock	Lead Forensic Investigator, root9b
Steve Mayhew	Executive VP/COO, E&M Technologies, Inc.

School Districts

Nikki Carter	Career and Technical Education Director (D-3)
Kevin Duren	Executive Director, Secondary Student Learning & Math Achievement (D-3)
Diane Forsythe	Director for College & Career Services (D-20)
Ernie Greene	Cybersecurity Instructor (D-2) (2017-2018)
Natalie Ihli	College & Career Services School to Work Alliance Program Coordinator (D-20)

Patrick Krumholz	Principal, Fountain-Fort Carson High School (D-8)
Woody Longmire	Coordinator of Student Services (D-2)
Markus Moeder-Chandler	Assistant Principal, Fountain-Fort Carson High School (D-8)
Duane Roberson	Director of Career and Technical Education (D11)
Emily Sherwood	Alternative Cooperative Educator (D11) (2016-2018); Post-Secondary Workforce Readiness Specialist (D8) (2018-present)
Rhonda Spradling	College & Career Services Coordinator (D20)
William Tomeo	Cybersecurity Instructor, Early College High School & Career Pathways (D-11)

Key to School Districts

D2: Harrison School District

D3: Widefield School District

D8: Fountain-Fort Carson School District

D11: Colorado Springs School District

D20: Academy School District

Workforce Development

Dana Barton	Director of Business and Customer Service, Pikes Peak Workforce Center (2016-2018)
Dianne Kingsland	Executive Director, Stemsco
Scott Nelson	Commander, U.S. Army Reserves and Instructor, SecureSet Training Academy (2016-2018)
Michelle Wallace	Program Manager, Stemsco

Internship Site Sponsors

Mustafa Akcogodan	Pikes Peak Community College
Kim Archer	LeaderQuest
Pam Barnett	Barnett Engineering & Signaling Laboratories LLC
Patty Bonvallet	Boecore Corporation
Rebecca Decker	Center for Technology Research and Commercialization
Russ Fellers	SAIC
Tony Gooch	Harris Corporation
Woody Longmire	Harrison School District 2
Sean Kearney	TechWise
Sara Kinney	Rim Technologies

Aikta Marcoulier	Colorado Springs Small Business Development Center
Nicki Mathis	Summit Technical Solutions, LLC
Steve Mayhew	E&M Technologies
Jeff Montoya	Colorado College
Steve Schoenberg	Eclypses
Patrice Siravo	System High Corporation
Lawrence Wagner	Spark Mindset

Introduction

The Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education grant, held by grantee Pikes Peak Community College in Colorado Springs, Colorado, facilitated the organization of the Cyber Prep program. Cyber Prep is a multi-stakeholder partnership of more than 30 employers, community organizations, and educators from area school districts, higher education institutions, and private training providers. Together, these organizations are helping teens to choose cybersecurity careers by providing a variety of opportunities for them to explore, learn, and work in the cybersecurity industry.

Executive Summary

During the past four years, the Colorado Springs region of Colorado has been developing and implementing a cybersecurity economic development plan to diversify from its economic base as a military community. As is the case nation-wide, workforce development is at the heart of this diversification program, because the lack of a skilled workforce is particularly acute in cybersecurity.

As part of this strategy, Pikes Peak Community College (PPCC) applied for and received at National Initiative for Cybersecurity Education (NICE) to serve as one of several regional partnerships around the nation to accelerate workforce development. This NICE initiative, the RAMPS Cybersecurity Education program, was designed to help regions solve their workforce shortages by developing education programs that worked. In the Colorado Springs area, a team of school district, PPCC, and industry representatives applied for and received the RAMPS funding, calling their project Cyber Prep.

Cyber Prep was designed to introduce teens to cybersecurity careers in the following ways:

- build cybersecurity workforce development pathways to address local workforce needs, complement an emerging IT career pathway in Colorado, and align with the NICE Strategic Plan,
- develop and nurture cybersecurity programs in area high schools and in the PPCC Area Vocational Program that articulate to the PPCC cybersecurity degree;
- create and pilot a summer cyber work experience through job shadowing and/or internship programs for area high school students; and
- explore registered apprenticeships as a way to ensure a sustainable cyber workforce for the future.

The project began in October 2016 and concluded in March 2019. A total of 45 individuals representing industry, education, government, and non-profit organizations participated in shaping and implementing Cyber Prep programs and activities. The program served hundreds of young people and accomplished all of its major objectives.

Cyber Prep resulted in the development of five new high school Career and Technical Education (CTE) programs in area school districts, resulting in an enrollment of 246 students, a 396 percent enrollment increase from the 62 students in AY2017. The Cyber Prep team also helped to develop a career and academic pathway in cybersecurity for the State of Colorado, developed and implemented a new Career and Technical Student Organization (CTSO) called **sudoCYBER**, that now boasts 250 members in 19 different clubs statewide, offered a paid

internship program to 31 high school cybersecurity students in local companies during the course of two summers, and worked extensively with local firms to understand the nature of their workforce skills shortages and gaps and then reported those findings publicly for use in new workforce training and academic program development.

Perhaps most importantly, the Cyber Prep team has solidified into a passionate group of workforce developers who know that the successes they have enjoyed together will help young people in a variety of CTE programs, as the workforce pipeline development process is similar across many industries and occupations in the region and in Colorado.

The Cyber Prep program team is now preparing to integrate into the Chamber/EDCs larger Ecosystem Growth Strategy—an economic development strategic plan designed to help retain, grow, and attract cybersecurity firms—in order to continue their work.

Background

Colorado Springs is the most heavily defense-impacted community in Colorado and one of the most heavily impacted in the United States. A 2014 study identified the aerospace and defense industry's direct and indirect impact on the Colorado Springs Metropolitan Statistical Area (MSA) as 44 percent of the economy. The MSA has over 55,800 direct employees associated with the military installations of the Fort Carson army post, Schriever Air Force Base, Peterson Air Force Base, Cheyenne Mountain Air Force Station, and the U.S. Air Force Academy.

The region has a sizable defense contractor base—more than 67,000 direct jobs and an additional 37,000 indirect or induced jobs—are associated with providing services to the military posts and contracting with the various branches of the military. Most of these jobs are in command and control, space and satellite operations, and information technology.

As part of a community-wide defense diversification initiative, the Colorado Springs Chamber and Economic Development Corporation (Chamber/EDC) studied local defense contractors with an eye toward those with potential for commercialization, finding that information technology and aerospace manufacturing were two sectors with promise as both are primary employers supporting high wages with defense-funded products and technologies that may be readily adapted for use in commercial markets.

The Chamber/EDC research found that 47 percent (118) of the 250 defense companies in Colorado Springs provided information technology (IT) services to include network defense and data storage, and that several of these companies had significant talent and service lines in cybersecurity. Thus, the Chamber/EDC decided to aggressively promote cybersecurity as an area of economic diversification for the region. As a result of its advocacy, Governor John Hickenlooper declared Colorado Springs as America's Cyber Capital in December 2015, launching an initiative to focus Colorado's economic development in cybersecurity in the Colorado Springs area.

The Governor also helped to launch the National Cybersecurity Center in Colorado Springs, which he envisioned as helping state and local governments better manage their growing need for cybersecurity products and services. (www.cyber-center.org) Further, the Governor rallied the region's higher education providers to create new academic pathways to cultivate a highly qualified cybersecurity workforce. In response, Pikes Peak Community College (PPCC) leaders agreed to develop a new cybersecurity associate degree program, supplemented by non-credit industry certification programs that would help to quickly develop a qualified workforce.

Chamber/EDC leaders approached PPCC leadership in January 2016 about creating a joint application for funding from the U.S. Department of Defense Office of Economic Adjustment Industry Resilience program to grow the cybersecurity ecosystem in the region. PPCC would serve as the fiscal agent and would organize workforce development efforts in cybersecurity.

The Chamber/EDC would organize a strategic planning effort to identify the region's assets in cybersecurity, identify barriers to developing a thriving ecosystem based on successful initiatives in other parts of the world, and develop an action plan to exploit the assets and break down the barriers. The team submitted an application in March 2016 (the Cybersecurity Ecosystem Growth Plan) that was awarded in April 2017 and started in June 2017.

Next, the Chamber/EDC held a summit in Colorado Springs in May 2016, bringing together more than 250 cybersecurity experts, educators, and defense industry leaders to discuss the region's potential to develop its cybersecurity economy. The biggest barrier to success uncovered at the summit was the dearth of labor, a nationwide challenge magnified locally by the high concentration of defense contractors. If the region were to pursue diversification and expansion in cybersecurity, workforce development needed to top the to-do list.

An informal result of the summit was the strengthening of a network of cyber educators who recognized the need to align their efforts at program development and expansion. This informal coalition included representatives from several local school districts and Pikes Peak Community College, and was encouraged by a handful of industry leaders who were already supporting local educational programs.

In June 2016, this group formalized its network into an application to the National Initiative for Cybersecurity Education (NICE) to serve as one of several regional partnerships around the nation to accelerate workforce development. This NICE initiative, called the Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education, was designed to help regions solve their workforce shortages by developing education programs that worked. In the Colorado Springs area, the network agreed to use the Chamber/EDC Ecosystem Growth Plan as the foundational planning tool for organizing stakeholders for the RAMPS project.

More specifically, the team agreed to focus the RAMPS application on ***developing multiple ways to introduce teenagers to careers in cybersecurity***. Called Cyber Prep, the program would allow PPCC and its current workforce development collaborators to establish a formal, sustainable partnership between secondary school districts, employers, and the College to:

1. build cybersecurity workforce development pathways to address local workforce needs, complement an emerging IT career pathway in Colorado, and align with the NICE Strategic Plan,
2. develop and nurture cybersecurity programs in area high schools and in the PPCC Area Vocational Program that articulate to the PPCC cybersecurity degree;
3. create and pilot a summer cyber work experience through job shadowing and/or internship programs for area high school students; and
4. explore registered apprenticeships as a way to ensure a sustainable cyber workforce for the future.

In October 2016, Pikes Peak Community College was awarded a grant by the U.S. Department of Commerce as the Western Regional RAMPS grantee, one of five regional alliances around the nation. The initial team of Cyber Prep members recruited others, and the core team grew to 17 members, while the number of active participants grew to a total of 45.

In order to capture the effects of Cyber Prep on the region's ability to attract youth into careers in cybersecurity, the next section of this report summarizes the state of education programs, workforce needs, and internships prior to the RAMPS award.

Workforce Needs

In 2016, the Chamber/EDC staff identified 96 companies providing cybersecurity services or related training and instruction in the Colorado Springs MSA, most of them in defense-related areas. This company asset map was used to invite companies to the initial summit and to participate in a survey to find out more about their capabilities and concerns. See Appendix A for the asset map, produced as part of the Chamber/EDC's first marketing brochure about cybersecurity.

PPCC staff used the asset map to identify companies hiring locally for cybersecurity positions. Of the 96 companies on the map, 59 were hiring locally, and 36 had available cybersecurity positions. The college team researched 81 positions at these 36 companies, examining the level of security clearance cited and the certification and/or degree requirements. This allowed the team to determine the skills, knowledge, and abilities required for the full range of open positions available in the region. This analysis, the May 2016 Cybersecurity Position Analysis, also helped PPCC faculty and advisory board members to shape its new degree program.

At the same time, the College commissioned a larger labor market study from the region's local economic forum director, Dr. Tatiana Bailey, to include an employer survey of workforce needs that would include an in-depth look at the skills, knowledge, and abilities employers sought in cybersecurity positions. This study did not conclude until well into the RAMPS project as most employers were reluctant to complete it. These results are examined later in the report (Appendix B).

For the 81 open positions studied, the following attributes were found (see Glossary for all acronyms):

- Clearance Requirements
  - 32 required no clearance or a Secret clearance (the lowest level of clearance)
  - 38 required a Top Secret clearance with Sensitive Compartmented Information (SCI) access and an additional eight required a Top Secret clearance
  - Three required the highest level of clearances available
- Degree Requirements
  - Seven positions required an Associate degree and an additional one preferred at least an Associate degree
  - 48 positions required a Bachelor's degree or higher and an additional 16 preferred at least a Bachelor's degree
- Certification Requirements
  - 31 required the CISSP
  - 27 required Security+
  - 17 required CASP CE
  - 14 required the IAT III
  - Many positions required a handful of other certifications, usually as a "preferred" attribute
- Experience
  - Two required at least one year of experience
  - 21 required 2-5 years of experience
  - 27 required 6-9 years of experience

- 15 required 10 or more years of experience
- 16 did not specify experience as a requirement

By June 2018, the Chamber/EDC had completed the Cybersecurity Ecosystem Growth Plan and had updated the cybersecurity asset map. The new map lists 128 cybersecurity-related companies and the Plan concludes:

> *The Colorado Springs cybersecurity industry has a disproportionate impact on the city's economy: approximately 3,000 cybersecurity workers have a $530 million direct economic impact. The cybersecurity industry also supports an additional three thousand jobs in adjacent industries and via the spending of the city's cybersecurity workers for a total employment impact of 6,000 jobs in Colorado Springs. Altogether, the cybersecurity industry has a $915 million economic impact on Colorado Springs. So, despite the fact that the industry's total workforce impact of six thousand jobs makes up only 1.4% of the city's total workforce, it is responsible for 2.7% of the total economic impact of Colorado Springs.*

Secondary and Post-Secondary Education Opportunities

College and University Programs

Formal cybersecurity education programs at the bachelor's, master's, and Ph.D. level have existed in the Pikes Peak region of Colorado for over a decade. In fact, save for the area surrounding Washington, D.C., Colorado had the highest concentration of Center of Academic Excellence (CAE4Y) colleges and universities in the nation in 2015 as indicated in Table 1.

These programs reported enrollment and graduation rates of fewer than 10 students apiece in Academic Year (AY) 2015, so local hiring managers were recruiting talent from one another and competing nationally to attract qualified workers. Since AY2015, these college and university programs have remained flat, though several have launched initiatives in the last Academic Year to boost enrollment.

The University of Colorado Colorado Springs (UCCS) received a $5.4 million appropriation from the Colorado Legislature in May 2018 to develop cybersecurity research and education programs, allowing the university to hire new faculty. Additional funding from the same legislation is assisting Metro State University, Colorado State University, and Western State University as well as PPCC to develop cybersecurity offerings over the next three years.

Pikes Peak Community College Programs

In response to outreach by federal agencies as well as the Colorado Congressional delegation calling on Colorado's community colleges to respond to the urgent and growing need for a qualified cybersecurity workforce, PPCC faculty had developed a Cybersecurity Certificate as part of its Computer Networking Technology (CNG) Degree in Academic Year (AY) 2013 and began offering the program the following fall semester (AY2014). However, the College lost its only certified cybersecurity instructor later that year to a higher paying job in industry, and the program was dormant until AY2016, when the College found faculty credentialed to teach the higher level courses. Seven students graduated with this certificate by AY2017.

The Cybersecurity Certificate program provides students with foundational knowledge of security threats, risks, and mitigation. Beginning with its fall 2015 meeting, industry members of the PPCC Computing Advisory Board began requesting more cybersecurity-focused

coursework based upon the increasing number and complexity of the security threats they faced. The additional data reported in the May 2016 Cybersecurity Position Analysis allowed the College to solidify plans to offer a Cybersecurity Associate of Applied Science (AAS) degree, which was presented to the Computing Advisory Board in August 2016.

Table 1. Centers of Academic Excellence in Colorado 2015

Institution	Designation	Credentials Offered
University of Colorado Colorado Springs	CAE-IAE, CAE-CDE 4Y	Certificate in Information Assurance Certificate in Secure Software Systems
Colorado State University – Pueblo	CAE-CDE 4Y	B.S. (Computer Security)
Colorado Technical University	CAE-CDE 4Y	B.S. (Cybercrime and Security) B.S. (Cybercrime Investigation) M.S. (Cybersecurity Policy) M.S. (Homeland Security)
University of Denver	CAE-CDE 4Y	M.S. (Cybersecurity)
Regis University	CAE-IAE 4Y	Graduate Certificate (Cybersecurity) Graduate Certificate (Information Assurance)
United States Air Force Academy	CAE-CDE 4Y	B.S. Computer Science B.S. Cyber Science
Colorado School of Mines	CAE-CDE 4Y	Certificate (Cyber Defense Education)

Source: *CAE Community,* last updated 2016, https://www.caecommunity.org/.

As a result of the community's focus on cybersecurity, and due to Colorado Springs' designation as the state's hub for economic growth in cybersecurity, PPCC President Dr. Lance Bolton developed and launched a College-wide Cybersecurity Initiative in April 2016 designed to:

1. speed development of the Cybersecurity AAS degree, to include developing the necessary curriculum and labs to ramp up a large program quickly;
2. apply for Cybersecurity Center of Academic Excellence for Two-Year Schools' (CAE2Y) designation from the US Department of Homeland Security and the National Security Agency;
3. recruit, hire, train and retain qualified Cybersecurity faculty; and
4. participate actively in community efforts to develop and implement the Cybersecurity Ecosystem Growth Plan for the region.

PPCC hired Cybersecurity Director Gretchen Bliss in May 2016 to begin work on these initiatives under the PPCC Workforce Development Division. This allowed the college to begin researching the cybersecurity skills gap, understand employer needs, and explore possible degree programs and career pathways that would need to be developed, giving the college a head start in getting organized for the launch of the Chamber/EDC Ecosystem Growth Planning process that would begin the following year.

The PPCC Cybersecurity AAS degree program was launched in January 2018 with 36 enrolled students; by fall 2018, 123 students had enrolled in the program.

A $900,000 commitment from the Colorado Legislature in May 2018 allowed PPCC to offer a differential salary rate to faculty with cybersecurity industry credentials, and the college is hiring two additional faculty to teach in the new AAS degree program. Also in 2018, the PPCC Foundation received a $50,000 cybersecurity scholarship gift from the Rocky Mountain Chapter of the Armed Forces Communications and Electronics Association (AFCEA).

Finally, after a year spent in the application process, PPCC received its CAE2Y designation in June 2018. This allows PPCC to participate fully in all CAE2Y activities and programs, and may give students preferential hiring treatment by DoD related employers.

In addition to these achievements, PPCC staff have assisted to develop the region's cybersecurity ecosystem in several important ways. First, in order to build general community awareness about cybersecurity, PPCC teamed with local training provider SecureSet to create a monthly Capture the Flag session that occurs on a Friday evening at a PPCC campus or other cybersecurity-related venue. Local industry associations, employers, school districts and others publicize the events.

Since first held in Spring 2017, these Capture the Flag sessions have drawn—on average—50 to 75 participants each month who compete for a couple of hours, eat pizza, and learn from one another. This program has been an enormous success, allowing employers to interact with young people, allow college students to mentor and be mentored, and leading to numerous enrollments in PPCC and SecureSet programs.

Second, PPCC faculty and staff participate actively in the region's robust industry and trade associations. PPCC has hosted or participated in local offerings from the Information Systems Security Association (ISSA), Rocky Mountain AFCEA, Pikes Peak (ISC)^2, and Infraguard, whose members now regularly assist with PPCC programs and mentor students.

As a result of these two successes, the Chamber/EDC now hosts a monthly "Cyber First Friday" happy hour event that draws more than 100 cybersecurity industry professionals together to network, learn about the work occurring at a local company, and interact with myriad support organization representatives like members of the PPCC faculty and staff team.

High School Programs

Beginning in 2008 with the adoption of Senate Bill 08-212, Colorado's Achievement Plan for Kids (CAP4K), the state has been implementing new education policies to help all elementary and secondary students prepare for the world of work. Today, Colorado middle and high school students are required to create and manage an individual career and academic plan (ICAP) that may lead to enrolling in higher education or may lead to a Career and Technical Education (CTE) pathway that is more employment focused.

During this decade of change in K-12 education, PPCC faculty and staff have become advisors and partners to local school district officials needing to diversify, improve, and scale up their CTE offerings in order to meet the new 2021 high school graduation requirements called for in CAP4K. The CAP4K legislation placed Colorado's community colleges squarely in the middle of CTE program growth as the Colorado Community College System serves as the state's coordinating agency for federal Perkins funding. All Colorado high school CTE programs must be approved by and aligned to community college CTE academic pathways and programs. Passage of CAP4K placed PPCC at the center of the CTE talent development pipeline in the region.

The overall goal of CTE programs, as stated at www.coloradostateplan.com is as follows:

> *"To provide quality educational programs emphasizing core academic content, Postsecondary & Workforce Readiness (PWR) competencies, technical skills, and seamless transition to further education or employment and better prepare students, including special populations to meet challenges of the workforce, economic development, and emerging occupations."*

High school students who participate in Colorado certified CTE programs can, depending on the particular curriculum and policies of their individual school district, receive both high school credit and post-secondary college credit through concurrent enrollment programs.

In the PPCC service area, which includes Elbert, El Paso, and Teller Counties, there are 22 school districts plus the Charter School Institute serving a combined total of more than 21,500 high school juniors and seniors in Academic Year (AY) 2018. Every district in the region plus 16 charter schools have concurrent enrollment and/or articulation agreements with PPCC. In addition, PPCC manages 16 high school CTE programs of its own, with 455 area high school students enrolled in AY2018.

Between AY2012 and AY2017 the Pikes Peak region hosted the following CTE programs relevant to cybersecurity. These programs qualified as CTE offerings either as concurrent enrollment or under school district articulation agreements with PPCC:

- Computer Programming/Programmer
- Computer Systems Technologies
- Construction Technology
- Construction Trades
- Digital Design
- Digital Media Technology
- Engineering Technology
- Game Programming
- Information Science/Studies

As shown in Table 2 for all area school districts, a total of 13,343 students enrolled in these cybersecurity-related programs between AY2012 and AY2017, with 6,865 students successfully completing, a 51% completion rate. Completion rates do not distinguish between those who self-selected out of programs due to lack of interest, schedule conflict, or other factors and those who were unable to pass their courses and receive credit.

High schools from El Paso County School Districts 2, 3, 11, 20, 38, 49, and 60 hosted these programs, for a total of seven districts participating in 28 CTE programs, with the bulk of students coming from Districts 49 (5,597), 20 (3,847), and 11 (1,031). Completion rates for individual programs varied widely.

In addition, the PPCC High School Programs Division, which offers CTE programs at PPCC to area high school students that do not have a program at their own school, has similar cybersecurity-related programs. As shown in Table 3, 885 students completed these PPCC certificates from AY2012 through AY2017.

Work-Based Learning Opportunities

No formal internship programs existed in the region for high school students in any of the computer technology-related CTE programs prior to Cyber Prep because the CAP4K legislation

Table 2. AY2012-2016 CTE Enrollment & Completion Pikes Peak Region

Program Name	AY2012-2017			AY2017			AY2016			AY2015			AY2014			AY2013			AY2012		
	Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed	
Computer Information Sciences	1362	778	57%	459	403	88%	440	220	50%	401	120	30%	62	35	56%	0	0	0%	0	0	0%
Computer Information Technologies	137	65	47%	18	3	17%	22	22	100%	26	21	81%	19	19	100%	17	0	0%	35	0	0%
Computer Programming	21	10	48%	21	10	48%	0	0	0%	0	0	0%	0	0	0%	0	0	0%	0	0	0%
Computer Systems Technologies	1934	709	37%	402	174	43%	606	281	46%	698	197	28%	228	57	25%	0	0	0%	0	0	0%
Construction Technology	2883	1470	51%	577	212	37%	541	310	57%	741	345	47%	489	302	62%	535	301	56%	0	0	0%
Construction Trades	31	27	87%	19	19	100%	12	8	67%	0	0	0%	0	0	0%	0	0	0%	0	0	0%
Digital Design	976	375	38%	17	1	6%	5	2	40%	293	85	29%	178	74	42%	285	120	42%	198	93	47%
Digital Media Technologies	983	202	21%	159	34	21%	203	54	27%	278	55	20%	173	40	23%	170	19	11%	0	0	0%
Engineering Technology	4673	3091	66%	888	652	73%	730	471	65%	709	562	79%	1006	610	61%	902	398	44%	438	398	91%
Engineering, Project Lead The Way	0	0	0%	0	0	0%	0	0	0%	0	0	0%	0	0	0%	0	0	0%	0	0	0%
Game Programming	343	138	40%	95	28	29%	138	71	51%	110	39	35%	0	0	0%	0	0	0%	0	0	0%
Total	13343	6865	51%	2655	1536	58%	2697	1439	53%	3256	1424	44%	2155	1137	53%	1909	838	44%	671	491	73%

Table 3. AY2012-2017 CTE Enrollment & Completion PPCC

Program Name	AY2012-2017			2017			2016			2015			2014			2013			2012		
	Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed		Enrolled	Completed	
Accounting	769	269	35%	140	66	47%	112	39	35%	118	53	45%	125	34	27%	132	43	33%	142	34	24%
Computer Information Systems	941	191	20%	196	65	33%	141	33	23%	165	27	16%	148	28	19%	162	19	12%	129	19	15%
Cyber Security	0	0	0%	0	0	0%	0	0	0%	0	0	0%	0	0	0%	0	0	0%	0	0	0%
Multimedia Graphic Design Program	1108	192	17%	202	35	17%	171	32	93	175	28	97	168	33	100	193	35	115	199	29	112
Networking Technology	797	172	22%	146	38	26%	143	22	15%	137	33	24%	123	26	21%	122	26	21%	126	27	21%
Robotics And Automation Systems Technology	187	61	33%	37	21	57%	34	14	41%	29	4	14%	37	15	41%	27	5	19%	23	2	9%
Total	3802	885	23%	721	225	31%	601	140	23%	624	145	23%	601	136	23%	636	128	20%	619	111	18%

did not require full development of high school CTE programs—to include work-based learning opportunities—until AY2017, when rising ninth-graders would begin to select their high school courses. While some schools offered school-based projects, field trips, job shadowing programs, and the like, the Cyber Prep high school internship program became the first industry-aligned high school internship program in technology in the Pikes Peak region.

Cyber Prep

The Cyber Prep program was started in October 2016 as the Western Region RAMPS project for the NICE. Cyber Prep started with the following goals:

Goal 1: Build cybersecurity workforce development pathways to address local workforce needs and complement the emerging IT career pathway in Colorado.

Goal 2: Develop, nurture, and evaluate cybersecurity programs in area high schools and in the PPCC Career Start high school program that articulate to the PPCC cybersecurity degree.

Goal 3: Create and pilot a summer cybersecurity work experience through job shadowing and/or internship programs for area high school students with qualified employers.

Goal 4: Explore registered apprenticeships as a way to ensure a sustainable cybersecurity workforce.

These goals were selected as the most impactful ways that the Cyber Prep team could influence teens to choose a career in cybersecurity by helping them to explore careers, be able to select coursework in cybersecurity as early as high school, and continue to pursue it as their academic pathway in college and beyond.

Progress toward achieving each of the goals is summarized below.

Goal 1: Build Cybersecurity Pathways

Statewide Career Pathway Development

A career pathway is a roadmap to specific job types in high demand fields. Career academic pathways provide a solid sequence of secondary and post-secondary courses, certificates, and degrees as well as industry credentials that lead to specific careers, and industry pathways spell out specific jobs or clusters of jobs that employees can progress through in their careers as they learn new skills and earn new degrees and/or credentials.

While information technology is a high demand field in Colorado and has been for more than a decade, no career pathway had been designed in the state until 2016, the year the RAMPS program was initiated. As a result, the Cyber Prep team approached the Colorado Department of Labor and Employment (CDLE), which manages the Colorado Workforce Development Council (CWDC). The CWDC had initiated a career pathways development project in partnership with the Colorado Community College System (CCCS) in 2015 and had selected information technology as a pathway to map in 2016, but that pathway only hinted at cybersecurity as a distinct field in IT.

Therefore, the Cyber Prep team requested that the CWDC consider building a separate cybersecurity pathway given the attention paid to the lack of cybersecurity talent in the state. In

2017, the CWDC agreed, and the Cyber Prep team helped to launch pathway development process in Southern Colorado, helping the CWDC to assemble the largest group of workforce development partners in the state to respond to requests for developing this pathway. Further, the Cyber Prep team encouraged CWDC staff to use the NICE Framework to organize the conversation with subject matter experts around the state.

In early 2018, CWDC and CCCS staff held focus groups in several locations around Colorado, discussing the elements of a proposed Colorado cybersecurity pathway with industry professionals, business owners, and instructors. The full pathway, completed in June 2018, may be accessed here: www.careersincolorado.org. Though it does not mirror the NICE Framework, the final pathway does contain most elements of the Framework, and ties career pathways into available academic programs in each region of the state.

Career Pathway Development in Industry

Cyber Prep team members facilitated the Colorado Community College System (CCCS), the Colorado Department of Education (CDE), and industry efforts to capture specific cybersecurity industry needs to guide the formulation of a statewide career pathway for cybersecurity. Career pathways provide workers with a roadmap to qualify for career opportunities and progress through industry to a particular position. Cyber Prep efforts to develop common understanding of career pathways included the following:

Industry Pathways

Because much of the cybersecurity work done in the region is classified, it has been very difficult to understand the path a student would take to obtain an "entry level" job in cybersecurity, let along the steps one would take within the career field to get promoted. During the life of the RAMPS effort, the Cyber Prep team used three tools available from NICE that helped, including:

The NICE Framework

The NICE Framework is a resource that categorizes and describes cybersecurity work in order to give curriculum developers, career counselors, industry human resource professionals and subject matter experts a common language about the profession. It is described in NIST Special Publication 800-181, available here: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework. The NICE Framework has been invaluable in helping our area educators, labor market researchers, and recruiters to describe the cybersecurity work taking place locally and develop appropriate pathways.

CyberSeek

The CyberSeek website provides an interactive heatmap that represents the concentration of available cybersecurity jobs across the nation, giving a striking visual of the size of the skills gap nationally (www.cyberseek.org). This tool was developed under the leadership of NICE as a collaboration between the Computer Industry Association (CompTIA) and Burning Glass. This map, which became available to the Cyber Prep team in the spring of 2017, gave more accurate information than the analysis completed by the PPCC team in May 2016, but largely validated the size and scope of the skills shortage locally. For example, the current Cyberseek heat map of Colorado shows that the Colorado Springs MSA has 27.6 percent of all available openings statewide, yet the MSA has only 12 percent of the state's population.

Further, the MSA has a location quotient of 4.7, a number that has been consistently high since Cyberseek launched. In fact, only the area around Ft. Huachuca, Arizona (15.2) and the Capital

Metro Area surrounding Washington, D.C. (6.5) have higher location quotients than the Colorado Springs MSA. This number represents the geographic concentration of workers in a specific industry; it is used by economic developers to determine the intensity of an economic cluster of activity in a region. This information has been very useful in helping the Chamber/EDC to brand the region as a cybersecurity hub.

Cyber Prep members report using CyberSeek regularly, as they discuss the skills gap in their companies, as they discuss new academic pathway development in high schools and higher education and training organizations, and in local trade associations like the Information Systems Security Association. Finally, high school counselors and instructors use the CyberSeek website to explain the concentration of jobs locally, the types of credentials students should consider obtaining, and the portability of these jobs to other parts of the country.

Cybersecurity Workforce Toolkit

This toolkit, updated by NICE in November 2016, provides a comprehensive resource for developing a cybersecurity workforce in any organization. One of the Cyber Prep team's goals was to disseminate this guide widely. The Cyber Prep team held annual Industry Day sessions during each year of the project (April 2017, May 2018, and March 2019) and disseminated the Toolkit at each session.

In addition, the team approached the local chapter of the Society for Human Resource Management (SHRM) to do a presentation about the Toolkit and disseminate it widely to SHRM members. Unfortunately, the local chapter did not have cybersecurity on its radar as a human resources issue until a series of breaches publicized locally—including a well-publicized ransomware attack at a manufacturing plant and a breach involving the US Anti-Doping Agency—prompted the group's programming committee to accept the invitation. A team of PPCC cybersecurity faculty and workforce development staff were scheduled to speak at the March 2019 monthly meeting, but the meeting was cancelled due to lack of registrations. Clearly, attracted the attention of area human resource professionals remains an issue.

Data-Driven Pathway Development

Even with these tools and the limited data PPCC had collected from local companies in its first survey, local educators were still puzzled by the lack of information they had about how to advise students to seek entry level jobs in cybersecurity. As a result, the Cyber Prep team decided to hold an employer focus group that would help them to understand what "entry level jobs" in cybersecurity meant to a variety of employers in the region. Dr. Tatiana Bailey conducted this session with 10 employer representatives from pure-play cybersecurity companies to some of the Fortune 500 companies in the region as well as local firms. The results of this focus group were incorporated with the survey results and published in April 2018. See Appendix B for the full report.

Academic Pathways in Higher Education

PPCC faculty and staff, with help and resources from the Cyber Prep initiative, have convened a series of regular statewide sessions of community college cybersecurity and information technology instructional leaders to discuss the similarities and differences in their academic pathways in cybersecurity. Six participating colleges form this collaboration, including Arapahoe, Aurora, Front Range, and Red Rocks Community Colleges from the Denver Metro Area as well as PPCC and Pueblo Community College. Together, they are finding ways to leverage best practices into each college's cybersecurity program. These conversations increased connectivity and understanding of the wide variety of cybersecurity program efforts and has

motivated additional colleges to apply for CAE2Y. Topics addressed in these sessions include: the evolution of cybersecurity job requirements, course offerings, cooperative new course initiatives, and apprenticeship and internship opportunities.

As a result of the Governor's declaration, the University of Colorado system began discussions about a research-focused convening of colleges and universities and launched the Mountain States Cybersecurity Consortium in fall 2017. This annual session brings together community colleges and public and private universities from Colorado, New Mexico, Utah, and Wyoming to discuss ongoing research initiatives. An outgrowth of these sessions has been an informal sharing of academic offerings, opening up new possibilities for development of new programs and articulation of credits from two-year to four-year schools.

At the spring 2019 session, the Consortium agreed to a new work agenda that was heavily influenced by the Cyber Prep initiative. This agenda includes a regional approach to K-12 teacher training that will help organize the colleges to share responsibility for sustaining a GenCyber teacher training initiative. Funding from GenCyber, a National Science Foundation initiative to train teachers and students, rotates among competing colleges and universities, so the Consortium members are planning a collaborative approach to build a sustainable system of teacher training that leverages GenCyber funds among the participating colleges and universities. PPCC received a GenCyber teacher training grant for summer 2019.

PPCC and the US Air Force Academy (USAFA) CyberWORX program—a design thinking center that brings together industry, academic, and other partners to solve complex cybersecurity issues for the US Air Force—co-hosted a design sprint in Summer 2017 to address the issue of how to attract young people to the cybersecurity field and into careers in the US Air Force. Participants included students from PPCC and Red Rocks Community College, Cyber Prep industry and education team members, and USAFA faculty and staff. Participants developed three project ideas, all outlined in Appendix C. Of the three, two projects were pursued as part of the Cyber Prep project.

First, participants suggested creating cyber clubs for elementary school girls that would focus on social interaction and learning technology skills. The Cyber Prep team picked the Cyber Warrior Princess model, www.cyberwarriorprincess.org, and the PPCC faculty have now led summer camps and interactive weekend sessions for more than 50 girls in the region for the last three years. In addition, Manitou School District 14 has created and sustains a middle school Cyber Warrior Princess club.

Second, participants suggested creating a "traveling cyber camp" that could be set up in any K-12 school, offering students unique cybersecurity learning experiences. While this project is not completed, PPCC faculty and area K-12 teachers are pursuing the idea of equipping a trailer that could be shared by school districts to complete specific cybersecurity labs and demonstrations.

Goal 2: Develop, Nurture and Evaluate High School Programs

Because of the implementation of CAP4K, area high schools had been working on their individual plans to implement the dual diploma program for several years, and most districts already had computer science and/or computer information systems-related programs. Since Colorado Springs had an Intel chip manufacturing plant for many years, the region also had a robust Project Lead the Way (PLTW) program with teacher training support and dual academic credit offered by the University of Colorado Colorado Springs.

At the time the Cyber Prep team assembled, only one school district, Colorado Springs School District 11 (District 11), had a CTE program that led to a recognized cybersecurity credential

with 62 students enrolled in its program in Fall 2016. Due to the concentration of defense contractors locally, the region already had several active and successful high school CyberPatriot competition teams, many affiliated with PLTW programming.

By the time the RAMPS grant concluded, the participating Cyber Prep school districts had enrolled 246 students, a 396 percent enrollment increase from the 62 students in AY2017 to 246 students in AY2019.

High School Program Development

Before beginning Cyber Prep, the RAMPS grant team conducted a capability survey to determine what CTE courses and/or programs of study were in place at PPCC and the 22 school districts in the PPCC service territory, which includes Elbert, El Paso, and Teller Counties in Colorado. At the end of the RAMPS grant, the Cyber Prep staff interviewed officials at the five participating school districts and one additional district to understand their efforts in beginning and growing cybersecurity programs.

Of note, 14 of the 22 school districts in the region are rural, with the associated funding, resources, and teaching challenges that brings to any new or existing program. Cybersecurity offerings at area high schools expanded greatly with the creation of Cyber Prep, mainly among the five participating districts, but awareness of and interest in cybersecurity expanded in every district. Each participating district took a unique approach to developing their programs based on industry requirements and involvement. While the PPCC faculty and staff endeavored to make the implementation of these programs more uniform, the districts resisted these efforts.

In fact, this phenomenon was mirrored by the community colleges in Colorado, where each college had developed a unique approach to teaching cybersecurity, often based upon the strengths of the faculty and the input from its advisory board(s). One of the unifying themes for the community college conversations became the NICE Framework and its implementation in the CAE2Y accreditation process.

As more colleges seek CAE2Y accreditation, their programs are being modified to teach the foundational skills found in the PPCC Cybersecurity AAS degree. The PPCC faculty and staff expect a similar standardization to occur as local school districts seek dual credit options or articulation agreements with area higher education institutions, since most colleges and universities have Center of Academic Excellence accreditations.

By March 2019, six school districts, including the five districts participating in Cyber Prep, had developed Cybersecurity/Computer Science/Information Technology programs with funding from the RAMPS grant assisting with teacher professional development and curriculum development/planning time. In addition, the Cyber Prep staff convened district representatives to discuss their challenges along the way. As a result, each district has balanced college preparation, cybersecurity certification achievement, and hands-on experience in its programming.

In addition, all participating districts plus several others had participated in the Cyber Prep summer internship program, which is described in the next section of this report and in Appendix D. Industry participants in the Cyber Prep internship program were astounded at the proficiency and talent that high school students in cybersecurity demonstrated during their 45-hour internships.

Finally, the Cyber Prep team worked with local industry and the Pikes Peak School districts to formulate the **sudoCYBER** Career and Technical Student Organization (CTSO) based on the CyberPatriot competitions, but can include many other competition and mentorship opportunities. CTSO's are a requirement of every CTE program in Colorado high schools, and

many districts had expressed that the lack of a CTSO framework to fit around the existing competitions they were engaged with, like CyberPatriot, as a reason for their lack of a more formal cybersecurity CTE program.

Each participating school district in the RAMPS grant received funding to develop a cybersecurity education program, train its teachers, and develop the supportive services—like the CTSO or a suitable computer lab—for its program. As with its program development, each district spent these funds in a slightly different way. The summary below describes each district's journey to developing its cybersecurity program.

Harrison School District 2 (D2)

Harrison School District 2 (D2), with a K-12 student enrollment of 11,708 this academic year—75 percent of whom are students of color—has had an aggressive CTE development plan for several years, focused on offering as many dual credit courses as possible. More than 77 percent of all D2 students qualify for the federal Free and Reduced Lunch Program, so college credit attainment is of enormous benefit to these low income students. As the PPCC Career Start program began its cybersecurity programming in AY2017, D2 officials reached out to begin developing a concurrent enrollment pathway for its students based upon the PPCC Career Start curriculum.

While not an initial partner in Cyber Prep, D2 soon emerged as a leader in its commitment to offering a cybersecurity pathway to the PPCC program. Thus, with savings in other areas of the RAMPS project, D2 became a funded school in the RAMPS grant. The ultimate goal of the D2 Cybersecurity program is to have a complete program of study that gives students the skills they need to go right to work in the field upon graduation, matriculate to a community college or four-year university, or join the armed services with the intent of serving in the Military Occupation Skills related to Cybersecurity.

By the fall semester of AY2017, D2 had 10 students enrolled in a seven course (21 credit) PPCC concurrent enrollment program. Unfortunately for the Cyber Prep community—but excellent news for D2—the new instructor hired into the program was Dr. Ernest Greene, who had led Cyber Prep the prior year. He left his position with Cyber Prep to teach at D2 and at PPCC. Dr. Greene was a highly qualified PPCC instructor holding a Colorado CTE License with Information Technology Endorsement to teach grades 7-12. Today, an existing D2 Computer Science teacher manages the program.

As of fall 2018, D2 reported 25 students in its program. The D2 program of study includes the following PPCC Career Start courses:

CIS 118	Introduction to PC Applications (9th Grade)
CNG 101	Networking Fundamentals (10th Grade)
CNG 102	Local Area Networks (10th Grade)
CNG 104	Intro to TCP/IP (10th Grade)
CIS 124	Intro to Operating Systems (10th Grade)
CIS 223	Linux (10th Grade)
CNG 132	Network Security Fundamentals (11th Grade)
CNG 257	Network Defense & Counter Measures (11th Grade)

D2 staff report that they had a waiting list of more than 30 additional students, and hope to expand their program next year to include up to 40 students by hiring two instructors. The

second instructor would be credentialed in Computer Science so that those courses could be taught as well.

The biggest challenges to starting the D2 program were:

- applying for and receiving CDE program approval;
- finding experienced K-12 Teachers with PPCC Instructor qualifications in cybersecurity and a current CDE CTE Teaching license;
- getting the instructor Cisco Network Academy Instructor Certification (most Cisco Instructor Classes take three to six months to complete at a cost of $600.00 per class); and
- recruiting students into a brand new program.

The biggest successes in the D2 program to date are:

- completing the CDE program approval process;
- hiring their current instructor from among current D2 staff to complete program development; and
- increasing enrollment in the second year.

Next steps in D2 program development include:

- adding cybersecurity industry professionals to the Program Advisory Committee to provide internships and eventually employment opportunities;
- finding resources to add a second instructor and purchase new hardware and software; and
- starting a CTSO for cybersecurity in the AY2020 school year and recruiting enough students to make it viable.

Widefield School District 3 (D3)

Widefield School District 3 (D3) has a total student enrollment just over 9,590 this academic year. It boasts first- or second-highest graduation rates in Colorado for African-American students and consistently ranks in the upper third in Colorado in graduation rates for Hispanic students. Almost 44 percent of all students are Free and Reduced Lunch Program eligible and 52 percent are students of color. D3 was a founding member of Cyber Prep, having fielded five competitive CyberPatriot teams between its two high schools for several years—including one all-girl team and an ROTC team. The District aims to provide relevant training that culminates in students receiving industry level certifications and internal internship opportunities.

At the time Cyber Prep began, D3 did not offer cybersecurity courses. However, in the summer of 2016 D3 sent six teachers to a training course offered through SecureSet, a private cybersecurity bootcamp headquartered in Denver that was expanding to Colorado Springs. The SecureSet program was developed as a partnership with the UCCS Extended Studies Division and a non-profit STEM organization (Stemsco) focused on teacher and learner development, thus offering these potential teachers training that could help them to develop cybersecurity training for the District.

This training was unsuccessful as the recruited teachers had little prior computer training and the training assumed a great deal of knowledge and skill in computer fundamentals. As a result, teachers were not prepared enough to develop and deliver curriculum for the following academic year.

By summer 2017, the D3 team had revised its approach, hiring a CompTIA certified instructor to develop curriculum and train teachers based upon the CompTIA suite of training. Teachers

attended this RAMPS-funded training and then developed and offered courses in its two high schools in fall 2017, revising the curriculum based upon input from students and their mentor-coach. As of spring 2019, D3 has 64 students taking at least one IT/Cybersecurity course. This approach has been more successful, resulting in greater support among faculty, staff and students. One-semester courses offered now include:

Introduction to Computer Science

Introduction to Information Technology

Network Administration

Systems Administration

Systems and Network Security

In the next two academic years, D3 plans to have both high schools offering the CompTIA entry-level cybersecurity pathway: A+, Net +, and Secure+ and expects a high passage rate for their courses and the examinations.

The biggest challenges to starting the D3 program were:

- finding and training experienced K-12 Teachers; and
- locating and implementing hands-on, engaging cybersecurity in a very restricted environment such as allowing students to have administrative access, see system settings, network, and troubleshoot;

The biggest successes in the D3 program to date are:

- identifying a couple of students at each school who are skilled, advanced, and trustworthy enough to be used as "student techs;" and
- Developing an elective course called Library Tech Assistant where students use their A+ skills to help keep the computer lab maintained and updated.

Next steps in D3 program development include:

- allowing the Library Tech Assistants to apply for D3 internships, which will be developed to help students bridge from the classroom to employment within the District;
- developing a program for students to test for and receive their A+, Net + and eventually Secure+ certifications prior to leaving high school by becoming a CompTIA testing site and including the industry credentials as course requirements;
- acquiring funding and ongoing support to purchase tools and equipment as well as training for teachers on instructional best practices for teaching the CompTIA suite, to include explicit activities, outcomes and strategies; and
- evaluating **sudoCYBER** for adoption as the District's CTSO in cybersecurity, building upon their success with CyberPatriot.

Because PPCC recognizes the CompTIA certifications as part of its prior learning assessment program, the D3 plan would allow students to have their portfolio of high school work assessed for college credit, another dual credit opportunity. D3 staff remain committed to having industry certification serve as the end goal of their cybersecurity CTE program, and will continue to refine that pathway before considering development of a formal articulation agreement with any higher education institution.

Fountain-Fort Carson School District 8 (D8)

Fountain-Fort Carson School District 8 (D8) is located on and around the Fort Carson army post near Colorado Springs, and has a total student enrollment just over 7,860 this academic year.

Close to 49 percent of all students are Free and Reduced Lunch Program eligible and 50 percent are students of color. D8 was a founding member of Cyber Prep, having had a successful computer science program at its high school for several years, built around its Army Junior Reserve Officers Training Corps (JROTC) program and CyberPatriot teams.

In the summer of 2016, the D8 high school program had 10 students enrolled in an Army JROTC Cisco certification course. By fall 2018, D8 expanded to 31 students in five courses leading to the Linux Professional Institute Certification (LPIC) Exams 1 and 2. Two D8 instructors in CyberPatriot and Computer Science offer these courses and their resulting certifications. The District expects to expand to have 40-50 students in six courses with the same two instructors in the next two academic years, and to include Net Academy certifications based on student interest and need.

The biggest challenge identified at D8 was:

- hiring qualified teachers to expand the current information technology programs into cybersecurity.

The biggest successes in D8 were:

- increasing course offerings; and
- recruiting students for every offering.

Next steps in D8 program development include:

- developing a district-wide cybersecurity CTE program that would draw students from the high school, alternative school, and affiliated charter and home school students. This program will be developed in the AY20 school year for full implementation in AY21;
- involving industry participants by having guest speakers, providing job shadowing opportunities and internships;
- identifying teachers with the correct background able to develop curriculum and attain the credentials necessary to articulate courses to area colleges and universities; and
- expanding the CyberPatriot program into a **sudoCYBER** CTSO

Colorado Springs School District 11 (D11)

Colorado Springs School District 11 (D11) is the region's second largest school district with 25,620 students enrolled in the current academic year. Fifty-eight percent of all students are Free and Reduced Lunch Program eligible, and 50 percent of total enrollment are students of color. As part of its CAP4K strategy, D11 closed a central-city high school several years ago, converting it into a single campus for all alternative schools and as a home to expensive CTE programs that could be housed centrally for all district high schools to send interested students.

This campus, the Roy J. Wasson Academic Campus, is home to the D11 cybersecurity program, which is the region's longest-standing high school cybersecurity program. By the summer of 2016, the D11 cybersecurity program had an articulation agreement in place with PPCC. Thus, the D11 faculty and staff led the way for the other four Cyber Prep partner districts to explore career pathways and curriculum models. While each district eventually chose its own path, these early discussions helped each district shape its own curriculum goals and implementation plans.

In fall 2016, the D11 cybersecurity program had 62 students enrolled in one course with one instructor and CyberPatriot coach who had retired from industry. Built on a model of offering industry certifications affiliated with the Cisco Network Academy and other recognized credentials, the D11 program provides a combination of classroom instruction, hands-on labs,

and summer internships working in D11 facilities. As of fall 2018, D11 expanded to 75 students in its year-long program. Courses in the current program include:

IT Essentials 1

IT Essentials 2

Cyber Security 1

Cyber Security 2

Cyber Security 3

Cyber Security 4

The biggest challenges to starting and sustaining the D11 program were:

- having only one instructor, which is a limiting factor for program expansion; and
- figuring out the right mix and sequence of courses to meet local needs and fit student interests and abilities.

The biggest successes D11 has experienced are:

- hiring an instructor from industry who had the knowledge and connections to develop, teach, and resource the program so effectively;
- recruiting students from across the District;
- a donation of $150,000 in equipment from local company Polaris Alpha, a Parsons corporation; and
- articulating a total of 184 academic credits to PPCC in the past academic year.

Next steps in D11 program development include:

- further involving industry by having guest speakers, job shadowing opportunities, and internships and perhaps even teaching in the program; and
- starting a sudoCYBER CTSO for cybersecurity;

Academy School District 20 (D20)

Academy School District 20 is located on and around the U.S. Air Force Academy, north of Colorado Springs. The District has 25,800 students enrolled this year, 12 percent of whom are Free and Reduced Lunch Program eligible and 29 percent of whom are students of color. D20 was added as a partner district in Cyber Prep in the program's second year as it was focused on developing a central CTE location, the Center for Modern Learning, a new facility completed in summer 2018. D20 officials see their role as offering students the right computer fundamentals—those that will help to shape their pathway in technology in a variety of directions, be it software development, network operations, or cybersecurity.

In the summer of 2016, D20 had no cybersecurity program. As of fall 2018, D20 had expanded to 26 students in a two-year sequence of half-day coursework taught every other day at the Center for Modern Learning. A few additional students participate in PPCC Career Start. The district plans to enroll up to 75 students in the half-day program within the next two years, with one additional high school potentially offering the PLTW Cybersecurity course for an additional 25 students. D20 will likely offer the same certifications as PPCC and other districts, but may consider dropping Cisco courses to focus on CompTIA certifications.

The biggest challenge to starting the D20 program was:

- finding good teachers who had the right credentials.

The biggest success at D20 has been

- getting the program off the ground;
- connecting with the cybersecurity industry through events and our consulting team.

Next steps in D20 program development include:

- expanding industry involvement by offering mentorships and opportunities for working professionals to be in the classroom every day;
- starting industry-involved extra-curricular activities like CyberPatriot competition teams and expanding their **sudoCYBER** chapter; and,
- figuring out their options and opportunities for dual credit with area colleges and universities.

PPCC Career Start

The PPCC Career Start program operates as a high school CTE program on the PPCC Centennial campus. Classes run each weekday morning, with students transported from schools around the three-county PPCC service territory. Most students come from small or rural districts that have limited resources to offer CTE programs on their own. The Career Start program has operated a Computer Information Systems CTE program for many years, adding a Cybersecurity program in AY2018. In its first year, the program enrolled 23 students, and enrolled 21 students in AY2019.

The biggest challenge to starting the PPCC program was in convincing the academic faculty that creating a separate cybersecurity program would not decrease enrollment in the existing computer information system program. In fact, this did not occur. The biggest lesson learned was that most enrolled students were seniors, making a second year of the program impossible to launch right away. Instead, the PPCC faculty have focused on perfecting the first year of the program, postponing development of year two until this summer.

Limiting Factors

While collaborating with teachers and CTE facilitators across the PPCC service area, it became evident that schools still face similar challenges, including:

- Inability to locate and hire qualified teachers with cybersecurity knowledge who also have the credentials necessary to qualify as adjunct instructors at area colleges and universities, limiting opportunities for dual credit;
- Inability to identify, fund, and provide necessary lab equipment, instructors, and examination fees;
- Fledgling relationships with industry partners;
- Varying levels of expertise with and exposure to cybersecurity competitions and the requirements of CTSO adoption and management; and
- Differing perspectives about the credentialing local companies require among entry-level workers.

Unaddressed, these items will continue to hold back growth of cybersecurity opportunities in the region.

Career and Technical Student Organization Development

As part of the RAMPS grant, local high school teachers and CTE staff have partnered with the National Cybersecurity Center to propose a cybersecurity-specific CTSO. The purpose of these

organizations is to provide extracurricular venues (with academic staff and industry leader support) for students to build leadership skills, healthy workplace values, and reinforce technical curriculum. While existing CTSOs touch on topics related to IT, computing, and technology there is no such organization focused directly toward high school students interested in cybersecurity.

SudoCYBER was created as a CTSO framework that could revolve around existing cybersecurity competition programs, like CyberPatriot or the National Cyber League, in order to fulfill state and federal requirements for student leadership organizations to be affiliated with every approved secondary CTE program. The **sudoCYBER** organizational framework is designed to fill the needs of emerging professionals for camaraderie, networking, and skillset expansion/practice. Bylaws were developed for the CTSO based on the Colorado CTE CTSO model bylaws, and disseminated through the **sudoCYBER** website (www.sudoCYBER.org). The bylaws are included as Appendix E.

In fall 2018, the Cyber Prep team held a **sudoCYBER** leadership conference in Colorado Springs, inviting student leaders and their teachers and coaches to attend the half-day session. More than 50 students and teachers attended, firming up their plans to start **sudoCYBER** chapters in their schools. As of January 2019, there are 19 **sudoCYBER** chapters across Colorado involving more than 250 students and their coach-faculty members.

Understanding Workforce Demands

As school district programs began maturing, student recruitment became an increasing concern. District staff found themselves unable to clearly describe career pathways, specific jobs in industry, companies hiring locally, and the like. As a result, at its spring meeting in 2018, the Cyber Prep team formally requested that the staff figure out ways to answer their questions so they could sell their programs better to students and their parents as well as other school officials and faculty.

Subsequently, the Cyber Prep staff outlined a study that was conducted by local labor market economist Dr. Tatiana Bailey. In this study, *Cybersecurity Skills, Training & Certifications*, Dr. Bailey examines job postings in cybersecurity during 2017 and most of 2018 to determine which companies were hiring, in what numbers, and at what levels of positions. In addition, the study detailed the most common skillsets required and the specific skills and certifications associated with these postings. Fortunately, the required skillsets did not change dramatically, making the core curriculum of most emerging cybersecurity programs stable and reliable. Dr. Bailey concluded the study with observations about the cybersecurity labor market nationwide and locally that should help school districts convince parents about the bright outlook for jobs in this field.

One startling finding of the study was that most of the 290 job postings examined during the 23 month period came from only eight companies in the region. Thus, while the identified cybersecurity ecosystem contains more than 125 companies, most hiring activity remains among a few very large defense contractors locally. This information can help students and parents to research careers with specific firms.

Goal 3: Create and Pilot a Summer Work Experience

As employers and school districts have begun to work more closely together—with PPCC representatives at the table as well—it has become apparent that work-based learning experiences like internships, job shadowing, field trips and class projects are crucial to the success of these expanding CTE programs. In addition, all the players agree that having every

school district compete for the attention of the region's employers for advice and work experience placements is unacceptable.

Summer Internship Program

During the summer of 2017, Cyber Prep offered summer internships for 10 high school students from five school districts at seven companies. The PPCC Cyber Prep team discussed internships needs and requirements with local businesses, worked with teachers to identify qualified candidates, facilitated a four-hour interview intensive involving all parties, and helped match qualified students with companies in need of their skills to form mutually beneficial internship partnerships. At the end of the program, both students and employers were pleased with the experience and all indicated that they would participate again.

In 2018, Cyber Prep expanded summer internship offers to 21 students from five school districts at 13 companies. The positive responses from both industry and students in 2017 incited interest in involvement from CTE directors from more districts than the RAMPS grant was able to facilitate in 2018. As the RAMPS grant winds down, the Cyber Prep team is handing off this successful internship pilot program to the Pikes Peak Business and Education Alliance (PPBEA), a new organization fostering work-based learning experiences for students from school districts across the region. The PPBEA conveners are planning a 2019 summer internship program and are seeking sustainable funding to underwrite the effort into the future.

Reports from each of the summer internship programs can be found in Appendix D.

Industry Partner Perspectives

Across the board, employers, while curious to see internship results, were reluctant to even talk about employing high school students at first. However, through the interview process, progress reports, and closing events, every employer was impressed with the quantity and quality of student work in each year of the program.

One of the largest barriers of entry was the lack of security clearances for these students. Due to the length of time background investigations require and clearance processing backlogs, it is impossible to acquire a clearance for an employee in the short time span of a summer internship. This forced employers to analyze the tasks that could be accomplished by an employee without a clearance. While not part of the traditional paradigm of employing a cleared workforce, employers found that there are a wide variety of entry level tasks that can be reassigned to intern level employees.

Examples include:

- Assembling servers
- Organizing server rooms
- Labeling equipment
- Sending emails to coordinate with external partnerships
- Creating (programming or writing) training materials
- Formatting machines
- Entering roster/business hierarchy system data
- Creating/maintaining web presence
- DoD Regulation 8570 PC Compliance
- Configuring Raspberry pi units
- Troubleshooting external or internal customer issues

These tasks also enable employers to experience new employees' skills, ethics, catchability, learning aptitude, and performance without acquiring them for a clearance-based project. For the 2017 intern year, two interns were retained on payroll and submitted for clearances. Two of the summer 2018 interns will be remaining with their companies for the school year. Others were invited back for subsequent summer internships as their academic careers progress. It is too soon to tell if any of these relationships will result in a clearance sponsorship.

Integrating new employees into the cleared workforce is vital for the continued success of cybersecurity. However, it is a resource intensive, time-consuming process that most employers would prefer to bypass in favor of luring another already-cleared individual away from their current assignment and into a new role. In this way, contracted employees are frequently traded among contracting firms. Providing industry partners this perspective on new, entry-level employees mitigates some of the risk of submitting a new employee for clearance as they have already had an introduction to their capabilities, developed a relationship and potentially garnered employee loyalty.

Goal 4: Explore Registered Cybersecurity Apprenticeships

In the first year of Cyber Prep, the team held an Industry Day session that attracted 51 people representing 12 technology companies, each expressing interest in registered apprenticeships. But the press of business prevented any of those companies from pursuing the program further. And, without the implementation of the PPCC Cybersecurity AAS degree program, even college faculty and staff were reluctant to pursue apprenticeships.

At the same time, in spring 2017, the community was approached by CareerWise Colorado (https://www.careerwisecolorado.org/) to consider becoming an expansion site for its successful pre-apprenticeship programs. CareerWise representatives made several presentations to employers, school district personnel, and community college officials in the region over the course of several months. Employers ultimately failed to sign on to the CareerWise Colorado model as they were expected to pay for the program when local school districts were already supporting the addition of work-based learning opportunities in their CTE programs with no cash outlay required of employers.

After two years of pursuing registered apprenticeships as a possible way to develop the workforce pipeline, the Cyber Prep team wrote off this goal as unattainable in April 2018. However, the Cyber Prep staff continued to work with companies and organizations interested in apprenticeships as it remains a goal in the region's Cybersecurity Ecosystem Growth plan.

In October 2018, PPCC was approached by staff from Northrop Grumman's corporate headquarters to consider participating in an apprenticeship program they were about to pilot in Baltimore, Maryland with the University of Maryland Baltimore Training Center; the company has interviewed PPCC students to participate in the program in Colorado Springs beginning this summer.

In addition, the CCCS has organized a statewide apprenticeship working group that is providing support to colleges wanting to develop apprenticeships that would use the CCCS as the sponsoring organization, which would reduce the cost to employers. As a result of this development, the PPCC team drafted a registered apprenticeship built upon the Cybersecurity AAS degree. College officials are gathering input from students, employers, and college officials about the draft model. Cyber Prep employers have expressed great interest in the program, though no formal commitments have been made.

Conclusion and Recommendations

When the Cyber Prep team formed more than three years ago, few pathways existed for high school students to actively engage in learning about cybersecurity. Since that time, many new programs have developed and students have multiple ways to learn about careers and practice their skills. As a coalition of the willing, the Cyber Prep team has become a passionate force for helping young people to find their path in cybersecurity.

At its concluding session, Cyber Prep team members were asked to describe the successes and challenges of Cyber Prep and give advice to other communities considering a similar effort.

Successes

- Because our region has 17 school districts, it was important to not have a "one size fits all" approach to implementing new CTE programs. We liked that the Cyber Prep model allowed each school district to develop programs that would work for their schools and students.
- Overall, the program was well organized and well managed. Team members relied on each other to find information and the sharing of national and teacher resources was very helpful.
- The summer internship program was a good incubator and accelerator for internships across the school districts—not just for cybersecurity but for all of our CTE programs. It was most successful because the companies took charge and really bought in to the process. The "speed dating" interview process for students—rounds of 15 minute interviews with several companies—was amazing for students and companies alike.
- Cyber Prep brought out the best in the students who participated. The diverse group of students we attracted to participate in programming was terrific, and showed employers the talent that is coming up in our local schools.
- The CTSO formation was important and helpful as each district can refine the model to fit its needs.

Challenges

- Engaging employers remains very, very difficult. It is hard to get them to come to the table and stay, especially for the big national companies.
- The industry representatives who made themselves available to help were mostly semi-retired, with outdated skills and examples of what cybersecurity is really all about. While grateful for their assistance, school faculty found it hard to find current, relevant speakers and lab assistants from industry.
- Most of the school districts are operating programs that are still quite fragile. An economic downturn or change in employment locally could shutter these CTE programs relatively quickly.
- The internship program may not survive if sustainable funding is not found to keep it as vibrant as it was during Cyber Prep, because the PPBEA does not have a sustainable funding source yet.
- Finding qualified, passionate instructors remains the biggest barrier to success in the school-based programs. Insuring that programming can withstand changes in instructors is very important; boutique programs built around an instructor's interests are not sustainable.

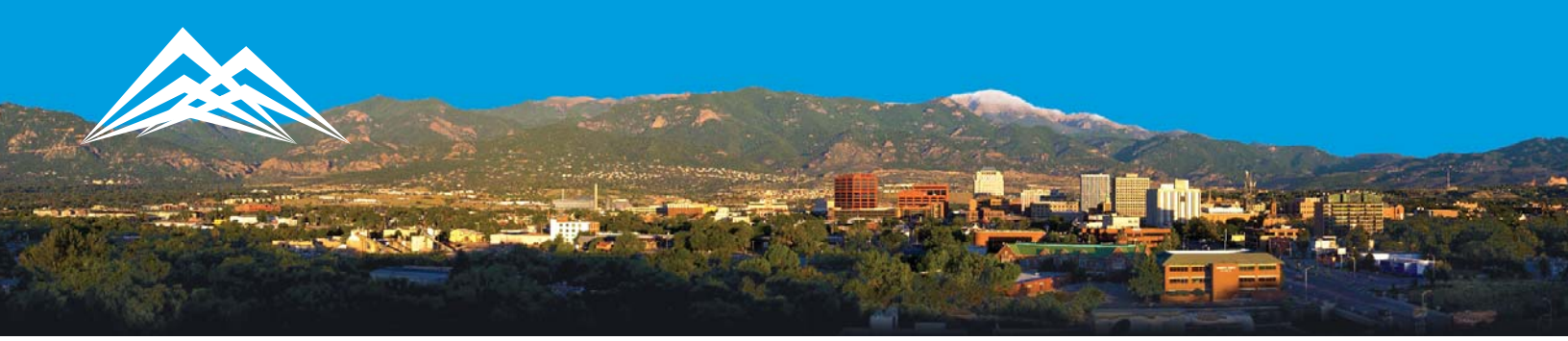
Opportunities

- Because the Cyber Prep effort is becoming part of the larger, Chamber/EDC Ecosystem Growth Strategy, we will be able to keep the core team together to continue programming and planning for the future. We can collaborate on important items like employer engagement, creating a joint advisory board, sustaining the internship program and the like.
- Because the community colleges and universities are now more actively engaged, high school students have many more opportunities for academic pathways, and school districts have more opportunities for concurrent enrollment.
- We need to consider broadening the cybersecurity curriculum into the Computer Science pathway, not just as a discreet CTE offering in area school districts. This opportunity will allow us to engage with higher education in a new way, beyond the boundaries of current CTE programming.
- We have the opportunity to deepen our work from holding competitions and interesting labs into really teaching and reinforcing fundamental computer concepts that will stick with our students for their lifetimes.
- We must plan and implement our ideas for a K-8 curriculum that fits for each school district so that we are modeling excellent cyber hygiene and reinforcing the fact that our region is America's Cyber Capitol.
- We should continue to collaborate in training and supporting our teachers, bringing them together to share ideas and resources. Employers could be very helpful in this respect, perhaps by offering externships or offering support in classrooms.

Advice for Other Communities

- It is important to plan programming for the long haul to make sure it is sustainable. Creating sexy programs will not work over time, you must focus on teaching fundamental skills in an engaging way. Be dynamic in your programming and modify as you go.
- School districts would be wise to partner with post-secondary institutions right away to understand matriculation requirements and support students all the way to college.
- Be sure to link all the way back to middle schools as soon as possible in order to build the most effective pipeline, and consider implementing a K-8 program early, so that you have an easier time explaining cybersecurity as a career field.
- Build a "club system" to attract young people. Create programs that they can join and belong to draw in a broad group of teens and let them explore with each other. When teens are given these opportunities to explore without "making the grade," they will develop a passion for the subject before feeling intimidated about the subject.
- Make your programming fun and allow teens to build skills and habits through experience. Use your club system to link teens with available middle and high school programs and on to college.
- Teach students early on in the internship development process that the value is not just in earning a wage, but is really about access to a network of career professionals eager to help them become successful in this field. This will help them to build a network of their own.

Appendix A: Chamber/EDC List of Companies



CYBER

in Colorado Springs and the Pikes Peak region

With a history of pioneering space, a unique concentration of military bases and commands, and a vision to become the cyber security capital of the United States, Colorado Springs has attracted many of the world's largest cyber companies while being a catalyst for home-grown cyber businesses.

- Cyber security has a long history in Colorado Springs, initiated by the military commands that have historically depended upon information security.
- The cyber infrastructure is in place, supported by an IT and telecommunications infrastructure second to none.
- The strong presence of data and customer support centers rely on safe, secure data storage and transmission. From data centers like FedEx to financial services like T. Rowe Price to insurance carriers like USAA and Progressive, cyber security is paramount and has led to the creation of a robust commercial cyber industry.
- Colorado Springs is the headquarters for the #1 company in the world on the CyberSecurity 500 List: root9B, as well as the home to the Western Cyber Exchange and the Cyber Security Institute for Small and Mid-Sized Businesses.
- Colorado Springs is regularly identified as one of the top five cities for cyber security jobs and is attracting a large cyber security workforce, including individuals separating from the military with extensive security credentials.

Extraordinary Cyber Security Military Presence

- Air Force Space Command: provides resilient space and cyberspace capabilities for the Joint Force and the nation.
- U.S. Northern Command/NORAD Joint Cyber Center: provides cyber consequence, response, and recovery support.

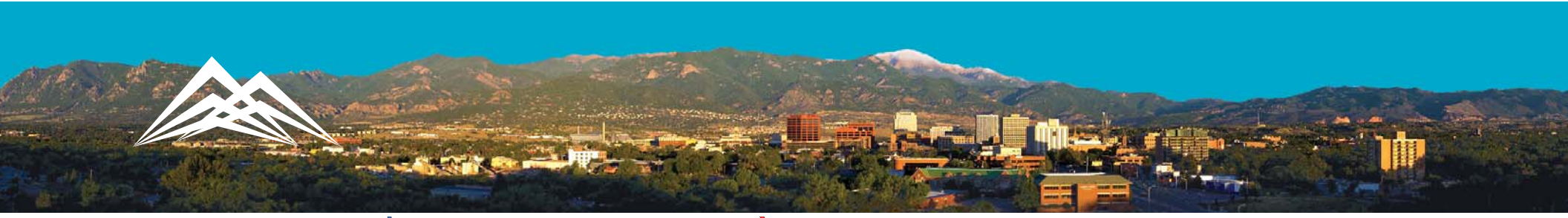
Academic Involvement

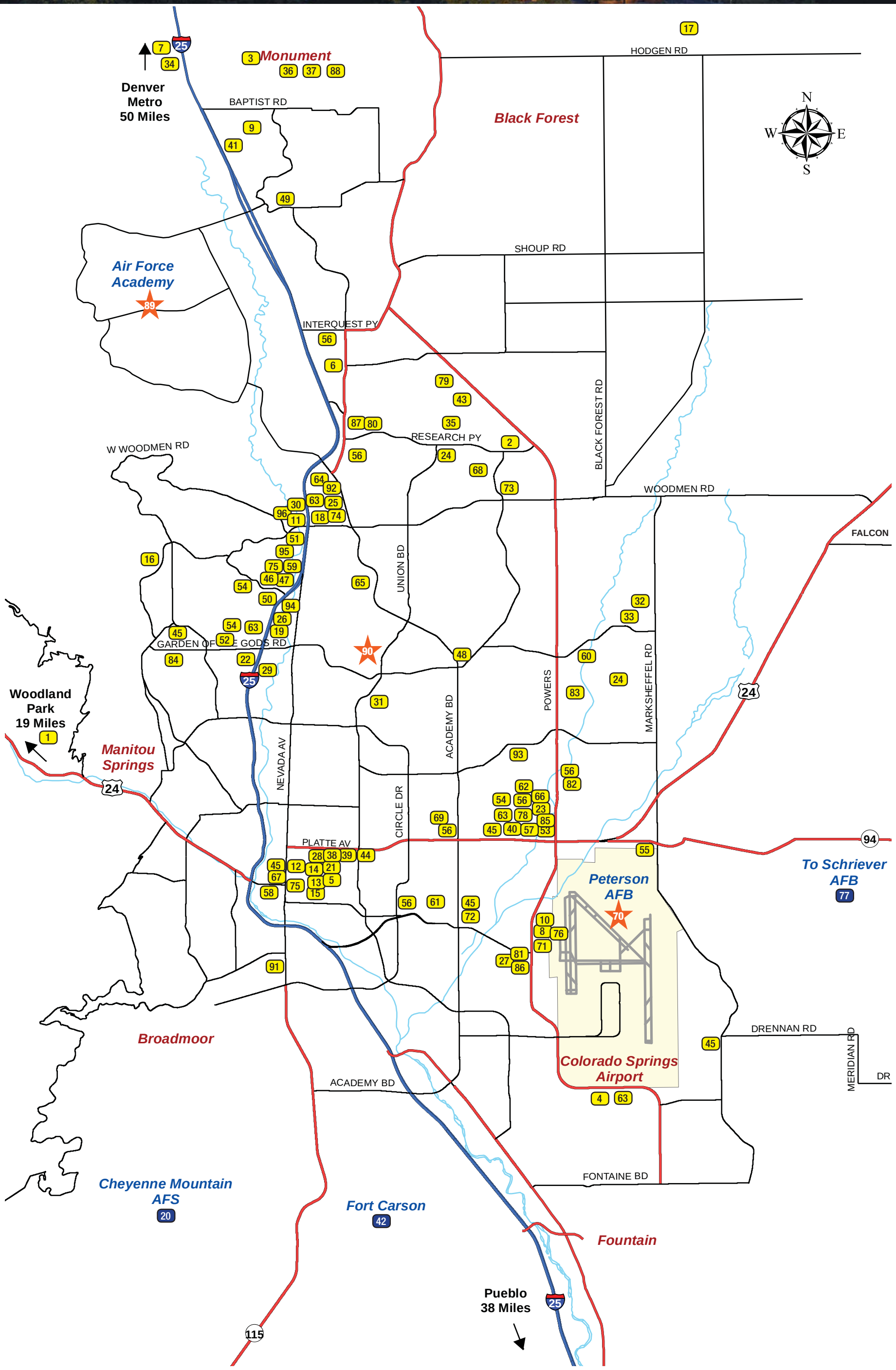
- United States Air Force Academy: Academy Center for Cyberspace Research; Cyber Innovation Center.
- University of Colorado Colorado Springs (UCCS): strong cyber research programs sponsored by the Department of Homeland Security, Department of Defense, IARPA, and NSF that cover a variety of topics including secure cyber infrastructure, resilient cloud, risk analysis for critical infrastructure protection, and cyber degree programs. Cyber P3i Program with U.S. Army Reserve.
- Colorado Technical University (CTU) offers master's degree programs in cyber science with concentrations in computer systems security, database systems, and software engineering.
- Webster University offers a master's degree in cyber security and graduate certificates in cyber security and threat protection.

colorado springs
regional business alliance™

More than 120 years of economic development leadership. A founding member of the U.S. Chamber of Commerce.

For more information on growing your business in Colorado Springs, Colorado, please contact:
Andy Merritt | 719.575.4325 | amerritt@csrba.com





as of March 22, 2016

Colorado Springs and the Pikes Peak Region Cyber Companies

1 Abacus Solutions Group, Inc.
2 ABBA Technologies, Inc.
3 Accinctus LLC
4 The Aerospace Corporation
5 AFCEA
6 Akima, LLC
7 Allied Mountain, LLC
8 Anser Corporation
9 ARX, LLC
10 Barnett Engineering & Signaling Laboratories LLC
11 Blue Light
12 Boecore Inc.
13 Booz Allen Hamilton
14 Braxton Technologies, LLC
15 BrightStar Intelligence Group
16 BurstIQ, LLC
17 C4 Solutions, LLC
18 Center for Space Standards & Innovation
19 CertainSafe
20 *Cheyenne Mountain Air Force Station*
21 CodeBaby Corporation
22 Colorado Technical University
23 COLSA Corporation
24 Combat Training Solutions (Cyalume Technologies)
25 Convergent Performance, LLC
26 CRGT
27 CSRA
28 Cyber Help Inc.
29 Cyber Resilience Institute
30 The Cybersecurity Institute for Small & Mid-sized Businesses (CiSMB)
31 CyberSpace Operations Consulting, Inc.
32 D.R.E.G. Solutions
33 Digital Beachhead, Inc.
34 DocVoyce, LLC
35 Dynamic Aerospace Technologies
36 E&M Technologies, Inc.
37 E-9 Enterprises Inc.
38 esoCyber Alliance
39 esoEdge Legal
40 Femme Comp Inc. (FCI)
41 Five Rivers Services, LLC
42 *Fort Carson*
43 Francis E McIntire Enterprises
44 The Future Company LLC
45 Harris Corporation*
46 i2 Information Security Corporation
47 Imprimis, Inc.
48 Incline Cyber Solutions, LLC
49 Infinity Systems Engineering
50 ISS, Inc. (Intelligent Software Solutions)
51 ISSAC
52 JMark Services Inc.
53 Joint Strategic Solutions
54 L-3 Communications*
55 Leidos
56 Lockheed Martin Corporation*
57 Loop Communications LLC
58 The Macalan Group
59 MainNerve
60 Mannatek Solutions, Inc.
61 Mitre Corporation
62 Modern Technology Solutions, Inc. (MTSI)
63 Northrop Grumman Corp.*
64 Novetta Solutions LLC
65 Olgoonik
66 Parsons
67 Patriot Solutions International, LLC
68 PEGRight
69 PeopleTec, Inc.
70 *Peterson Air Force Base*
(Air Force Space Command;
U.S. Northern Command/NORAD Joint Cyber Center)
71 Quantech Services
72 Quantum Research International
73 Red Mind Solutions, Inc.
74 Riverside Research
75 root9b LLC*
76 S4 Inc.
77 *Schriever Air Force Base*
78 Scitor Corporation
79 Securifense, Inc.
80 Shape Technologies, LLC
81 SRA International
82 StealthCom Solutions, Inc.
83 STEMsCO
84 Storage Networking Industry Association (SNIA)
85 Summit Technical Solutions, LLC
86 TASC / Engility
87 Teledyne Collaborx
88 UAS Colorado
89 *United States Air Force Academy*
(Academy Center for Cyberspace Research; Cyber Innovation Center)
90 University of Colorado Colorado Springs
(Cyber P3i Program with U.S. Army Reserve)
91 Urban Mobile Health
92 USfalcon
93 Vencore
94 Veteran Engineering and Technology LLC
95 Webster University
96 Western Cyber Exchange

Additional Business Alliance Member Investors:

Stellar Solutions Inc. (Denver, CO)

INDUSTRY KEY

Consulting Services (37)
Commercial (4)
Digital Health (7)
Engineering (24)
Information Technology (51)
Manufacturing / Maintenance (4)
Research & Development (23)
Education / Training (23)
Membership / Associations (5)
Military Installations (5)

REGISTERED SMALL BUSINESS KEY

Alaska Native Company (4)
Current SDB Certified (4)
Current 8(a) Certified (5)
Service-Disabled Veteran Owned (20)
Veteran Owned (26)
Woman-Women Owned (9)

Military Installations
Business Alliance Member Investor

Prepared by: colorado springs regional business alliance
102 S. Tejon Street | Suite 430 | Colorado Springs, CO 80903
Phone: 719.471.8183 | www.csrba.com

*Company has multiple locations and/or divisions within the Pikes Peak region

as of March 22, 2016

Appendix B: Cybersecurity Education and Training Assessment

CYBERSECURITY EDUCATION AND TRAINING ASSESSMENT

April 2018

Assessing the Skills Gap in the Colorado Springs MSA

PIKES PEAK COMMUNITY COLLEGE

Contents

Background

During the fall and winter of 2016, Pikes Peak Community College (PPCC) identified 31 cybersecurity companies to survey about the education and training needs of their cybersecurity focused positions and received 15 completed surveys. The focus of this survey was to identify the skills needed in the entry-level cybersecurity workforce so that PPCC faculty could develop a new Associate of Applied Science (AAS) degree in cybersecurity.

In 2017, the College collaborated with the Colorado Springs Chamber and Economic Development Corporation (Chamber and EDC) to develop a grant proposal to the Department of Defense (DoD) Office of Economic Adjustment (OEA). The focus of this plan was to help the region's economic and workforce developers diversify the local defense economy by helping defense-focused cybersecurity companies to enter new markets. Once funding was received in 2017, PPCC took the degree planning training assessment data and contracted with survey experts from Growth Capital Network, a consultancy focused on economic and workforce analyses, to complete this study about the cybersecurity workforce.

The overarching aim of this assessment is to better understand the cybersecurity workforce needs so that existing and future training programs can fulfill local business requirements. Given the high level of specificity in the cybersecurity realm, and the quick pace of change for the requisite employee skills, PPCC recognizes that community feedback from local employers is the most accurate and direct way to understand the required training qualifications.

Methodology

An in-depth survey was created by a cybersecurity expert and a curriculum expert from Pikes Peak Community College. Two experts on survey methodology also assisted in creating the tool (Appendix A). The survey had specific subject areas including:

1) current cybersecurity workforce needs
2) posting protocols for open cyber-related jobs
3) educational and/or training needs for new hires
4) protocols for cybersecurity training for incumbent staff
5) certification and security clearance needs, and
6) satisfaction levels with various types of hired employees

Thirty-one companies representing the breadth and depth of the 95 identified local cybersecurity companies (as of mid-2016) were selected to be contacted for the survey. Representatives from each company received an email and follow-up phone calls to encourage them to complete the survey.

In addition to the survey questions and results, the assessment process also included analysis of real-time data from Talent Neuron, which is an in-depth database of current and historic job openings. Talent Neuron allows queries specific to the Colorado Springs Metropolitan Statistical area (MSA) and the "cybersecurity" occupational group. Various other parameters can also be viewed for these job postings such as desired years of experience, security clearance requirements, and the corresponding number of postings for

various subcategories. The Talent Neuron information was used to augment the survey results, and to help formulate specific questions for a subsequent employer focus group held in the spring of 2018.

Survey Results

Fifteen companies completed the employer survey, representing 16 percent of the 95 identified firms as of mid-2016. Firms that declined to participate gave several reasons, citing the length of the survey (it took more than an hour to complete), the sensitive nature of the firm's work, and the lack of authorization local managers had from their headquarters staff.

Of the companies that did complete the survey, 40 percent (6 firms) consider at least 60 percent of their work to be in the cybersecurity service area, while the remainder of the companies either have a large cybersecurity division within their company (a healthcare firm and an online services company) or the company provides other information technology services and support in addition to cybersecurity. Of the cybersecurity-focused companies, 83 percent provide information technology engineering services, while another 17 percent develop and maintain software and provide related training services.

This small return means that definitive statements cannot be made about the survey results as an "n" of fifteen would not provide statistical significance, particularly because the community now has more than 100 identified cybersecurity-focused companies. However, some patterns could be observed that could then be shared with the focus group attendees (alongside the Talent Neuron information), who represented 10 employers, most of whom did not complete the original survey.

Many patterns in the survey responses were indeed observed. These were discussed during the focus group. The absence of patterns in some of the six subject areas listed above were also telling. The nuances were discussed at length during the employer focus group, and in aggregate, the three sources of information were quite useful in illuminating cyber-related workforce needs. Similarly, the gathered information is now informing modifications to PPCC existing cybersecurity training.

Current Employer Cybersecurity Training

All surveyed companies provided some degree of cybersecurity awareness training. Ten of the fifteen companies (66%) provide a lower level of awareness training while the remaining five (33%) provide a higher level of training.

Locally Sourced Talent

Most of the past, hired cybersecurity personnel of the fifteen companies were locally sourced (74.2%) and a large proportion of their past cybersecurity hires have been former military.

Experience Level

In terms of experience level, about one-third of past hires were considered "entry level." The requisite level of experience for new hires was a point of interest for this study because educators need to know if locally offered education and training programs are a sufficient condition for employment for at least some portion of the open jobs.

In Talent Neuron, a search under "cybersecurity" translates to the "Information Security Analyst" job category.[1] A cross-sectional look at the number of current job postings in this category revealed 352 openings in mid-March 2018. This cross-sectional data point is quite consistent over time. When the search is narrowed to "junior level (0-2) years," the current number of job openings falls significantly to only 41 open positions (12%).

This is not consistent with the survey results, which indicated that about one-third of past hires were entry level. Moreover, the posted, junior positions have skills and certifications at a fairly sophisticated level including:

Table 1. Skills & Certifications for Junior Level (0-2) Years Information Security Analyst

Top Skills	Top Certifications
Cybersecurity (32)	Security Clearance (23)
Information Assurance (22)	Certified Information Systems Security Professional – CISSP (20)
National Institute of Standards and Technology (22)	DoD 8570 Certification (20)
Linux (20)	Top Secret Clearance (14)
Network Security (14)	Cisco Certified Network Associate - CCNA (12)

Source: Talent Neuron, March 2018
Note: Numbers in parentheses show the number of times a skill or certification was mentioned in the 41 open positions for junior level Information Security Analyst.

When employers were asked how much cybersecurity experience is acceptable at entry level, most said two to eight years of experience is acceptable. Almost all respondents stated that the Information Technology Industry Association (CompTIA) Security+ is required and that the International Information System Security Certification Consortium (ISC)[2] Certified Information Systems Security Professional (CISSP) certification is highly desired.

However, the Talent Neuron information shows that CISSP is listed as a requirement for approximately one-third (or 144) of the posted positions (see Table 4 below). The CISSP requires a minimum of four years' cybersecurity experience. Other "highly desirable" certifications for employers include the International Council of E-Commerce Consultants (EC-Council) Certified Ethical Hacker (CEH), Cisco Certified Network Associate Security (CCNA Security), and CompTIA Advanced Security Practitioner (CASP).

During the focus group session with additional local employers, all but one participant noted that there is no such thing as "entry level cybersecurity" work. Instead, they said that individuals needed to be well trained in information technology foundational skills, like software development or networking technology, or, ideally both. After several years doing

[1] Within "Information Security Analyst," the specific job titles include: Cyber information Assurance Analyst; Network Security Engineer; Information Assurance Engineer; Access Control Specialist; and Cyber Security Analyst.

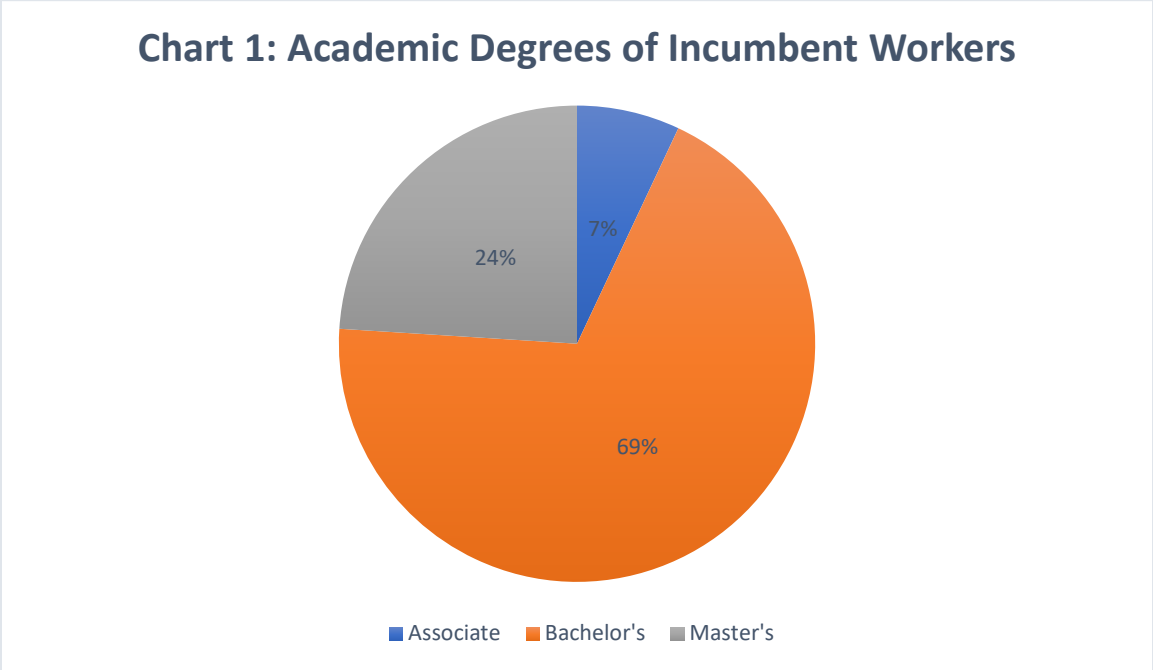
this work, people who are drawn to the security side of the business can then pursue it knowledgeably.

Educational Requirements and Preferences

When employers were asked what their minimum level of education and/or experience was for posted positions, approximately half (eight out of 15 companies) said either high school diploma, associate level degree, low-level certification (e.g. Security +), or equivalent experience. Although this may indeed sound "entry level," the Talent Neuron job postings do not reflect this. As stated above, the junior level position postings have a relatively high level of required skills and certifications (Table 1 above).

It is important to remember in this context that a typical community college associate degree program offers foundational skills that would allow a student to certify at a lower level like A+, Net+, and Security+. For example, the current Cyber Security AAS degree at PPCC offers training that would allow a student to sit for the A+ Net+, CEH, Security+, and CCNA Security exam.

In terms of the level of education for incumbent employees, surveyed responses showed that 24 percent of current cyber employees have a master's degree, 69 percent have a bachelor's degree, 7 percent have an associate degree, 62 percent are former military, and 72 percent have some existing clearance level.



To augment this information on the educational attainment of incumbent workers, employers were also asked how important they felt educational and personal attributes are in terms of their hiring preferences. These results demonstrate that having at least an associate degree is the most important (4.6 out of 5, where 1=not important and 5=very important). Having a bachelor's degree is also highly preferred by employers (3.7 out of 5). Employers state that having an innate talent and desire to learn cybersecurity is moderately important (2.8) as is the possession of a cyber-specific certification (2.6). Interestingly, employers stated that

having cyber experience is not particularly important (1.3) although the discussion above regarding the relatively few junior level postings in Talent Neuron contradicts this.

To better understand what types of associate degrees are most useful, survey participants were given a list of five possible cybersecurity-related Associate of Applied Science (AAS) degrees and they were asked which would be most applicable to their needs. Options included:

1) AAS Cyber Defense - both networking and systems administration fundamentals, with a focus on defensive strategies to securing networks and systems.
2) AAS Network Forensics - hardware, operating systems, Digital Forensics, and network fundamentals with the requisite security concepts required to detect and respond to system and network intrusions.
3) AAS Network Security Administration - networking fundamentals with the requisite network security concepts and best practices required to implement and administer secure network environments.
4) AAS Secure Software Development - Computer Science fundamentals and secure coding concepts. Designed as a transfer degree into baccalaureate programs of study in Computer Science.
5) AAS System Security Administration - systems administration fundamentals with the requisite security concepts and best practices required to implement, administer, and harden operating systems.

Respondents stated that the AAS Cyber Defense was the most desirable, followed by AAS Network Security. Both of these degrees (AAS Cyber Security and AAS Networking Technology with an additional Cybersecurity certification) are offered at Pikes Peak Community College.

Similarly, the survey data around applicants with a two-year cybersecurity degree is inconsistent with the Talent Neuron information. All fifteen employers surveyed said they would accept a two-year degree in cybersecurity; however, when "associate level education" is specified in the current (March 2018) job postings, only one job opening comes up. Of course, it is possible that employers are not specifically stating in a posting that a two-year degree is acceptable. However, given the tight labor market, one take away is that if employers are indeed willing to consider applicants with two-year cybersecurity degrees, they should state it in their job postings. Individuals looking for work who have two-year cybersecurity degrees may assume they are not qualified unless a posting specifies that two-year degrees are acceptable.

The importance of education versus experience is further elucidated by the survey responses that asked employers to rank the easiest attributes to forego when they are hiring. The results in Table 2 further validate the importance of experience to cybersecurity employers; this finding was firmly validated by most focus group participants as well.

Table 2. Applicant Attributes Easiest to Forego (1 = easy to forego, 5 = hard to forego)

Two or four-year degree	1.7
Certification	1.7
Experience	2.6

Demand for Cybersecurity Employees

All fifteen of the surveyed companies state that they are hiring staff in cybersecurity within the next twelve months. The demand from the fifteen companies amounted to 175 prospective jobs for 2017. An important caveat to this is that many of the open positions are contractual because they involve DoD contracting work, and thus are susceptible to sequestration requirements or other contracting delays or changes.

There is likely some double counting in these 175 open positions. There are times when employers have bid on a military contract and they post positions before definitively knowing whether they have won the contract. In addition, other contracts are awarded on a "first to fill" basis, so many firms are recruiting to fill one open requisition. It is difficult to know the extent of this duplication without further analysis, which would be helpful to area workforce developers trying to size programs to meet the demand for local talent.

The contractual or contingency nature of at least some portion of these cybersecurity jobs may dissuade potential employees or students from entering this field. It is also possible that prospective employees or cybersecurity students are more aware in Colorado Springs of the conditional nature of cybersecurity jobs because of the heavy military presence within the community. In fact, these local job seekers and students may be more resilient in the face of this natural churn in the defense contracting world.

Talent Neuron provides a hiring scale that indicates the level of demand for a given occupational group. In the case of "Informational Security Analyst," the hiring scale is 93 out of 100. This high level of demand is also observed across the U.S.

Length of Time of Fill an Open Cybersecurity Position

Employers stated that the average time to hire a cybersecurity employee was thirty to eighty-one days. This does indeed validate the perception that cybersecurity positions are hard to fill. As a point of reference, the average posting duration for all jobs in Colorado Springs is 31 days.

Most Difficult Cybersecurity Jobs to Fill

Employers had a wide range of required cyber jobs that are difficult to fill. They ranged the full gamut: cybersecurity engineer, systems administrators, and policy and governance personnel to name a few. This information is consistent with Talent Neuron data (see Table 3). Indeed, four of the top ten postings in February, and consistently over the past several years, have been in the IT sector. In the month of February, these IT jobs totaled 2,917 open jobs. We know a subset of these persistently open positions are cybersecurity related.

Table 3. Colorado Springs MSA Top Ten Job Openings, February 2018	
1) Registered Nurse (1,368)	6) Administrative Assistant (672)
2) Software Engineer (858)	7) Medical Assistant (671)
3) Systems Engineer (789)	8) Teller (665)
4) Customer Service Representative (784)	9) Certified Nursing Assistant (578)
5) Systems Administrator (698)	*10) Network Engineer (572)*

Source: Talent Neuron

Employers were also asked about higher skill job openings. Three out of the fifteen employers (20%) stated that finding senior people with higher skill sets is difficult. The same proportion also stated that the lack of security clearances is a barrier for hiring especially for young candidates.

Required Cybersecurity Clearances

A look at the required certifications for the open cyber positions in Talent Neuron reveals two important points. One, there are many types of required security clearance certifications. Two, each kind of clearance has a high number of jobs listed with that certification. This means that many of the posted positions require numerous clearances (see Table 4).

Table 4. Required Security Clearances for Open Cyber Positions
Secret Clearance (224)
DoD 8570 Certification (167)
Top Secret Clearance (114)
Top Secret Sensitive Compartmented Information - TS SCI (101)

Source: Talent Neuron

In aggregate, 79 percent of the survey respondent's open jobs require a security clearance with 29 percent requiring secret clearance, 13 percent requiring top secret clearance and 35 percent saying they require higher than top secret clearance. Twelve out of the fifteen companies (80%) do offer clearances; however, 11 of those 12 companies only offer at the secret level. Table 4 shows that a high proportion of posted positions require higher level clearances than the 11 surveyed companies offer. Three of the fifteen (13%) of the surveyed companies do not require clearances.

This validates the disconnect between survey results, which indicate almost of third of positions posted by employers are "entry level," versus the significantly lower proportion shown in Talent Neuron (12%). The list of certifications shown in Table 5 that are associated with all current open positions often require years of experience to attain, likely where previous employers have sponsored clearances. The list provided in Table 5 is not exhaustive; it is simply a list of the top thirteen certifications listed for local positions currently shown in Talent Neuron.

Other Posting Attributes

Survey respondents were asked to rank order the importance of other applicant attributes. The top three most important attributes were:

1) Security design principles
2) Cyber defense
3) Information assurance fundamentals (tied #3)
4) Policy, legal, ethics and compliance (tied #3)

The least important applicant attributes were:

1) Cryptography

2) System administration
3) Basic scripting

Satisfaction Level with Current Cyber Employees

Employers were asked from where they obtained their current employees and what their corresponding satisfaction level is with those employees.

Table 5. Required Certifications for All Open Cyber Positions
Certified Information System Security Professional – CISSP (144)
Certified Ethical Hack – CEH (67)
Associate of Casualty Actuarial Society – ACAS (65)
Information Assurance Technicians – IAT (64)
Cisco Certified Network Associate – CCNA (56)
Information Assurance Management – IAM (55)
GIAC Certified Incident Handler – GCHI (50)
CI Poly – CIP (45)
IAT Level 2 (42)
Systems Security Certified Practitioner – SSCP (41)
GIAC Security Essentials Certification – GSEC (39)
Certified Information Security Manager – CISM (38)
GIAC Certified Intrusion Analyst – GCIA (28)

Source: Talent Neuron

Table 6 below summarizes those results. As a general observation, it is worth noting that employees with a lengthier and more formal education, such as an associate degree, private certification school or bachelor's degree receive the highest satisfaction ratings. Employees who are retired military or from an "other" source (typically poached from another organization) also have high satisfaction levels. The high school graduates and community college certificate recipients had the lowest satisfaction levels.

Table 6. Source and Satisfaction with Current Cyber Employees		
Source	Proportion from Each Source	Satisfaction Level (1=unsatisfied, 5=very satisfied)
Straight from high school	47% (7 of 15 employers)	2.7
Community college certification	20% (3)	2.8
Community college associate degree	40% (6)	3.4
Private certification school	7% (1)	3.2
Bachelor's degree	67% (10)	3.9
Military experience	80% (12)	4.1
"Other" source	73% (11)	4.1

Mediums to Find New Talent

Most employers simultaneously use various methods to obtain new talent. The most frequently cited methods were online (12 employers) and word of mouth (11). Eight employers participate in job fairs, seven poach from other companies, seven utilize social network sites, and six use recruiting agencies. Less frequent hiring mediums include university postings (4), the Pikes Peak Workforce Center (2) and community college postings (1). Given that Pikes Peak Community College has a new cybersecurity associate degree, the low level of postings by employers at PPCC may represent an opportunity to proactively inform local businesses about the availability of graduates from the College's programs.

Training Incumbent Workers

A very high proportion of employers (13) use on-the-job training to keep their employees up on the latest cyber technologies. Ten employers have existing intern programs as well as in-house, on-ground training. Nine utilize online cyber training for their employees. These results indicate that most employers are internalizing their cyber training needs. Nine survey respondents also said they grant training reimbursement to some employees for external training. Virtually all employers stated that they use a mix of all of these methodologies to train existing workers.

Willingness to Address Cyber Workforce Shortages

Employers were asked what they are actively willing to do to help our community build the talent we need around cybersecurity. All respondents (15) stated that they would be willing to guest lecture. Ten said they would host a competition. Fourteen said they would be willing to take in and train interns although the surveyor, Gretchen Bliss, has been trying to solidify internships and has found it to be very challenging.

When employers were asked what they see as the most optimal way to overcome cybersecurity workforce shortages, answers included: better partnerships with higher education institutions, better career pathways, more internships and partnerships, and changes in government requirements and contracting.

Cybersecurity Focus Group Feedback

The above results were shared with participants from ten employers who participated in a cybersecurity focus group. Ten companies participated including: The City of Colorado Springs, Lockheed Martin, Harris, Eclypses/CertainSafe, Mitre, Oracle, Infinity Systems, Digital Beachhead, Macalan Group, and Progressive. The purpose of the focus group was to capture some of the nuances around cyber workforce needs as well as to explore some of the inconsistencies between the one-on-one surveys and the Talent Neuron data.

Cybersecurity Talent Pipeline

The focus group attendees were highly engaged and willing to give their thoughts and suggestions about how the survey results and Talent Neuron data should be interpreted. Some highlights from their input is provided below.

- With respect to **educational requirements for viable candidates**, a high proportion of employers stated that they prefer a candidate with a bachelor's degree (or higher) and at least some experience. They stated that the critical thinking skills

inherent in higher education and the ability to "have seen it all" inherent in extensive work experience enables a cybersecurity individual to more accurately and consistently identify cyber threats.

- Employers state that quick certification programs make applicants think they are in high demand, that they can do any cyber job, and that they should be compensated as such. However, employers do not feel that inexperienced and/or quickly certified individuals are indeed viable candidates for their posted positions.
- One company stood out as an exception stating that they prefer inexperienced cyber employees because they like to mold them to their specific needs (Eclypses). It is important to note that Eclypses provides cybersecurity software and conducts penetration testing as part of its business model, whereas the other companies have cybersecurity talent needs, but are not exclusively in the cybersecurity business.
- Focus group attendees acknowledged that **"entry level" in cybersecurity** is a misnomer. The term "entry level" implies that someone can qualify for a job without a great deal of education or experience. The employers clarified that to them, "entry level" implies a specific baseline of education and experience (see page 2 above for details on employer preferences and expectations).
- Most participants agreed that in order to enter the cybersecurity field, a candidate's pathway must start in general information technology work, in either software development or network maintenance and operations. Without this foundational knowledge, it would be impossible to succeed in cybersecurity work.
- Employers validated that **security clearances** are a barrier to hiring due to the long processing time to obtain a clearance. This exacerbates the conundrum of "entry level" versus experienced cyber applicants since often the more experienced candidates already have security clearances.
- The prevalent need for some level of clearance is much of the reason that so many survey respondents stated that they hire previous military personnel (80%).
- Employers validated the (above-mentioned) notion that **posted cyber positions may be overstated** due to the anticipated hiring needs of military contractors, several of which may be bidding on the same DoD contract.
- Employers were shown the Talent Neuron salary information for cyber positions (local median of $112,950) and agreed that **local salaries** are in line with national levels (U.S. median of $113,100).

Participants and Community Focus around Cybersecurity

Another aim was to discuss the focus of the OEA grant received by PPCC and its partner organization, the Chamber and EDC. Participants were asked about areas of cybersecurity specialization that the region should consider in order to help defense-focused companies to diversify. Specialization topics covered included:

1) Diversification of cyber network security and defense companies from DoD contracting to more general government work or non-governmental (commercial) work.
2) Diversification within the aerospace cybersecurity realm from DoD to commercial applications
3) Focusing company growth opportunities on blockchain technology development

With respect to diversification, focus group participants felt that helping existing DoD network security and defense contractors to diversify would indeed be beneficial. They stated that the smaller, locally headquartered firms, in particular, are ripe for diversification and would be an eager audience. This emerged as a "must do" element for several of the focus group participants.

Companies that work in aerospace were identified as the most relevant for diversification, particularly into the commercial space, because of the local aerospace presence and because the Air Force investment in cyber is significant. Participants cautioned, however, that many of the cyber-relevant components are not in Colorado Springs so the "niche" in cybersecurity would have to be quite specific.

Blockchain technology development had a mixed response. Some companies like Eclypses and Digital Beachhead are already working in this arena with some success. Other companies are not as convinced that blockchain will become a technology staple because it requires too much computing energy and power to be feasible in the long run. Attendees stated that no other community has "claimed" blockchain as the center of its universe, which implies opportunity. However, the inherent controversy and power requirements around cryptocurrency also render it high risk.

There were other possible cyber areas of focus for our community that emerged during the conversation. A key one was SCADA[2] security. Several of the attendees (Mainnerve, Mitre, Eclypses, and Harris) all gave examples of their work in this arena. Attendees also brought up the very salient point that because Colorado Springs Utilities are municipally owned, we have an opportunity to be a test bed for SCADA. The city is also a designated Panasonic "Smart City," making SCADA security solutions especially relevant. Since no other community seems to own this niche, it is possible that it could put Colorado Springs on the cyber map luring more investment and talent to the region.

Another theme expressed by the group was the continued attraction of large commercial companies. Oracle, Progressive, FedEx, SAS, and Walmart have all chosen to place data centers and/or IT satellites in the region not only because we are cost competitive and have some access to talent, but also because of the relative safety from natural disasters. In addition, focus group attendees stated that the low cost of doing business in Colorado versus states like California make it feasible for our region to try to recruit at least the data and security centers of some larger national and multinational firms.

[2] Supervisory control and data acquisition (**SCADA**) networks contain computers and applications that perform. key functions in providing essential services and commodities (e.g., electricity, natural gas, gasoline, water, waste. treatment, transportation) to all Americans.

Concluding Remarks

It was clear from both the one-on-one surveys and the focus group that there is a relatively wide range of cybersecurity workforce needs across the community. Cybersecurity is indeed a vast field and this makes workforce readiness a challenge. However, as the Colorado Springs community hones in on areas of specialization within cybersecurity, required proficiencies for open positions should become somewhat clearer.

Another theme that emerged is that there is a baseline of desired skills in cybersecurity regardless of the niche or niches our community chooses. This implies that higher education institutions can train and educate around those foundational cybersecurity and information technology needs and then perhaps augment with very specific training programs as they emerge (e.g. SCADA security).

Further, because of the national workforce shortage in cybersecurity, it is clear that growing new talent locally is likely the best way to solve the region's cybersecurity talent problem. These study results point to several possible areas of focus where local workforce developers may engage employers, like assisting with development of career pathways for the region's youth to follow, or supporting transitioning service members who are training in computer skills in order to enter cybersecurity careers upon exiting the military.

Interviews conducted by Gretchen.Bliss@ppcc.edu; 719 351-4910

APPENDIX A:
Cybersecurity Survey – Human Resources

All answers are completely confidential. Approximately 30 businesses will be participating in this information gathering and all data will be aggregated for the report back to workforce-related entities. No individual business information will be shared. Your willingness to participate will help inform existing or future workforce initiatives. Thank you for your participation!

Company name: _____ _____

Name/title

_____

_____

*Date of interview:*_____

Business Landscape

1) What products or services do you provide? (NAICS subsector)

NAICS 511210 Applications software, computer, packaged ☐
NAICS 517110 Wired Telecommunications Carriers ☐
NAICS 517919 All Other Telecommunications ☐
NAICS 518210 Data Processing, Hosting, and Related Services ☐
NAICS 541330 Engineering Services ☐
NAICS 541511 Custom Computer Programming Services ☐
NAICS 541512 Computer Systems Design Services(CAD/CAM/LAN Network) ☐
NAICS 541519 Other Computer Related Services (recovery/installation) ☐
NAICS 541611 Admin Management and General Management Consulting Services ☐
NAICS 541618 Other Management Consulting Services (telecomm/utilities) ☐
NAICS 928110 National Security ☐
NAICS Other ☐

2) What year was your company founded and what year did you begin cyber-related work?

3) How much of your overall work load (percentage if available) is cybersecurity related?

4) What percentage of your employees work directly in cybersecurity?

5) What percentage of your employees (only) receive cyber security awareness training?

6) Is this training basic cybersecurity awareness (don't click on a phishing email) or more in depth (technical explanations of threats)?

7) What percentages of your employees are hired from the local community?

Workforce Composition and Needs

8) How many entry-level cybersecurity employees do you have in the following categories (please specify numbers of each)
    a. Full-time
    b. Part-time
    c. Contractual
    d. Temporary
    e. Apprentice/intern

9) How many experienced cybersecurity employees do you have in the following categories (please specify numbers of each)
    a. Full-time
    b. Part-time
    c. Contractual
    d. Temporary
    e. Apprentice/intern

10) Are you planning to hire cybersecurity employees in the next 12 months?
    a. How many?
    b. What are the job categories (entry-level, engineers, programmers, etc.) of these potential new hires?
    c. What is the minimum level of education/experience required to be hired?

11) What specific cybersecurity job categories (from above question) are typically the most difficult for you to fill? Please give the top three and rank order them. (1 being the most difficult to fill)
    a. 1 -
    b. 2 -
    c. 3 -

12) How many weeks does it typically take for you to fill an open cybersecurity position (categorize positions as necessary)?

13) Using the 5-point Likert scale below, how difficult is it for you to fill <u>cybersecurity</u> positions with the requisite cybersecurity knowledge, experience, or certification?

Very Difficult	Somewhat Difficult	Neutral - What I would expect	Easy	Very Easy
1	2	3	4	5

Using the 5-point Likert scale below, how difficult is it for you to fill non-cybersecurity positions?

Very Difficult	Somewhat Difficult	Neutral - What I would expect	Easy	Very Easy
1	2	3	4	5

Position Classification and Requirements

14) What percentages of your positions require the following clearances?
    a. None
    b. Confidential
    c. Secret
    d. TS
    e. TS/SCI
    f. Higher

15) Do you offer clearances for your new hires? What level?

16) What is the education level of your current cybersecurity employees (percentages if possible)?
    a. Masters degrees
    b. Bachelor's degrees
    c. Associate Degree
    d. Former military
    e. Existing clearances

17) From which of the following have your new cybersecurity hires come from in the past five years?
    a. High school ☐
    b. Community College - certificate program ☐
    c. Community College - Associate degree ☐
    d. Private certification school ☐
    e. Four-year university system ☐
    f. Other company ☐
    g. Military ☐

18) Using the 5-point Likert scale below, please rank your satisfaction with the cybersecurity knowledge and/or capabilities of employees obtained from the following sources:

High School:

Not At All Satisfied	Somewhat Satisfied	Neutral - What I would expect	Satisfied	Very Satisfied
1	2	3	4	5

Community College Certificate Program

Not At All Satisfied	Somewhat Satisfied	Neutral - What I would expect	Satisfied	Very Satisfied
1	2	3	4	5

Community College Associate Degree

Not At All Satisfied	Somewhat Satisfied	Neutral - What I would expect	Satisfied	Very Satisfied
1	2	3	4	5

Private Certification School

Not At All Satisfied	Somewhat Satisfied	Neutral - What I would expect	Satisfied	Very Satisfied
1	2	3	4	5

Four-year University System

Not At All Satisfied	Somewhat Satisfied	Neutral - What I would expect	Satisfied	Very Satisfied
1	2	3	4	5

Other Company

Not At All Satisfied	Somewhat Satisfied	Neutral - What I would expect	Satisfied	Very Satisfied
1	2	3	4	5

Military

Not At All Satisfied	Somewhat Satisfied	Neutral - What I would expect	Satisfied	Very Satisfied
1	2	3	4	5

Recruitment/Closing Workforce Gap

19) Which of the following mechanisms do you use most for obtaining new talent (if there are different methods for different job categories, please specify)?

Online postings ☐
Pikes Peak Workforce Center (or other public workforce entities) ☐
Recruit from other companies ☐
Word of mouth ☐
Four-year college/university postings ☐
Job fairs ☐
Community/technical colleges ☐
Social networking ☐
Local newspapers ☐
Recruiting agency/temporary employment service organizations ☐
Other_____

Training

20) If you train incumbent workers, which of the following do you use to train those workers: (to include duration of training)
    a. Online training – if yes, what software or which online program(s)?
    b. On ground training – where do you send employees? Or do you bring a trainer into your business?
    c. Tuition reimbursement for courses, certifications, or four year degrees
    d. On the job training from more senior staff/leadership

Additional areas of interest

21) Are you familiar with digital badging? Do you have plans to use digital badging at your company?

22) Do you have an existing intern program at your company? Is Cybersecurity included in the program already?

23) What do you see as the most optimal way to help your business overcome cyber workforce shortages?

24) Is there anything else you would like to include in your responses to help inform this initiative?

Cybersecurity Survey – Operations

Name/title:

_____

_____

*Date of interview:*_____

Qualifications – Hiring Philosophy

25) When hiring cybersecurity employees please rank in order of importance the following aspects
    a. Two-year degree
    b. Four-year degree
    c. Experience
    d. Certifications
    e. Innate talent/desire

26) How much cybersecurity experience is acceptable? Optimal?

27) Which certifications are required? Highly desired?

28) Would you accept applicants with a 2-year degree in cybersecurity?

29) What specific certifications do you require for your cybersecurity positions? (please list in order of importance)

A+ ☐	Security + ☐	Network + ☐	CISSP ☐	CEH ☐	CCNA ☐
PMP ☐	ITIL Foundations ☐	MSITP ☐	Linux + ☐	SCCM 012 ☐	CNDSP ☐
GSEC ☐	SCNP ☐	SSCP ☐	CISA ☐	GSE ☐	SCNA ☐
CAP ☐	GSLC ☐	CISM ☐	CASP CE ☐	Global Certified Intrusion Analyst (GCIA) ☐	Global Certified Incident Handler (GCIH) ☐
CRISC ☐	MCSE ☐	IAM II ☐	IAT II ☐	IAM III ☐	IAT III ☐
CCNA-Security ☐	CCNP ☐	Other ☐			

Other qualifications/certifications not listed?

30) When experiencing workforce shortages what aspect is easiest to forego when hiring? (please rank order, 1 being the easiest to forego)

a. Degree
b. Certifications
c. Experience

31) Please rank the top three most important areas for your positions (1,2,3) as well as the three least important (10, 11, 12) in order of importance
    a. ☐ Basic Data Analysis - basic abilities to manipulate data into meaningful information.
    b. ☐ Basic Scripting - ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).
    c. ☐ Cyber Defense - basic awareness of the options available to mitigate threats within a system.
    d. ☐ Cyber Threats - basic information about the threats that may be present in the cyber realm.
    e. ☐ Fundamental Security Design Principles - basic security design fundamentals that help create systems that are worthy of being trusted.
    f. ☐ Information Assurance Fundamentals - basic concepts of information assurance fundamentals.
    g. ☐ Introduction to Cryptography - basic ability to understand where and how cryptography is used.
    h. ☐ Information Technology System Components - an understanding of the basic components in an information technology system and their roles in system operation.
    i. ☐ Networking Concepts - basic understanding of network components and how they interact.
    j. ☐ Policy. Legal, Ethics and Compliance - understanding of information assurance in context and the rules and guidelines that control them.
    k. ☐ Systems Administration - skill to perform basic operations involved in system administration.
    l. ☐ Other focus area

32) What degree listed below would be most applicable to your cybersecurity workforce needs? (if multiple, please rank order)
    a. ☐ AS Cyber Defense - both networking and systems administration fundamentals, with a focus on defensive strategies to securing networks and systems.
    b. ☐ AS Network Forensics - hardware, operating systems, Digital Forensics, and network fundamentals with the requisite security concepts required to detect and respond to system and network intrusions.
    c. ☐ AS Network Security Administration - networking fundamentals with the requisite network security concepts and best practices required to implement and administer secure network environments.

d. ☐ AS Secure Software Development - Computer Science fundamentals and secure coding concepts. Designed as a transfer degree into baccalaureate programs of study in Computer Science.
e. ☐ AS System Security Administration - systems administration fundamentals with the requisite security concepts and best practices required to implement, administer, and harden operating systems.

33) What cybersecurity tools/processes are most important for new employees to have? (list top 5 in rank order with 1 as most essential)
    a. 1 –
    b. 2 –
    c. 3 –
    d. 4 –
    e. 5 -

Qualitative/Other Feedback

34) Would you be willing to give a guest lecture or workshop on an area of Cybersecurity for PPCC Cybersecurity students? This gives the students the opportunity to have practical application understanding of course content.

35) Would you sponsor a cybersecurity competition?

36) Would you be willing to provide internships (summer or otherwise) to PPCC students pursuing an AS in cybersecurity? (this would give them some practical experience required by most positions)

37) What do you see as the most optimal way to help your business overcome cybersecurity workforce shortages?

38) Is there anything else you would like to include in your responses to help inform this initiative?

Appendix C: CyberWORX Project Report

AIR FORCE CYBERWORX REPORT 17-003
Air Force Cyber Outreach

MICHAEL V. CHIARAMONTE, Lt Col, USAF
Senior Designer & Facilitator

JEFFREY A. COLLINS, Col, USAF
Director, AF CyberWorx

DESIGN PROJECT CONDUCTED
18 – 20 July 2017 (Sprint)

Produced with input from military units including SAF/CIO A6, 10 CS, 24 AF; valuable regional academic partners Pikes Peak Community College (PPCC), Red Rocks Community College (RRCC), and the University of Colorado-Colorado Springs (UCCS); and our valuable partners in industry.

Air Force CyberWorx™
2354 Fairchild Dr, Ste 4A80
USAF Academy, CO 80840
AFCyberWorx@usafa.edu - @AFCyberWorx - (719) 333–4278

Introduction to AF CyberWorx

CyberWorx is a dynamic organization partnering Airmen, industry, and academia to reimagine how technology might enrich and protect our nation, businesses, and lives. As a human-centric design center, we seek out unique ways to connect Air Force warfighters with current and future technology in meaningful ways. We look to transfer, license, and share promising prototypes, solutions, and knowledge with our partners to create value for both the warfighter and the economy as this is the best way toward operational advantage.

Design Thinking @AFCyberWorx

Design thinking is a common sense, human-centric problem solving method embraced by innovation leaders in industry, but often overlooked in the government sector. The CyberWorx design thinking process is a transdisciplinary method that breaks down silos of standard organizational structures. Organizations naturally form structures based on specializations to facilitate deep expertise, but these structures often impede creativity, collaboration, and knowledge sharing vital to innovation. CyberWorx deliberately reaches across specialties to bring diverse perspectives to a problem in a non-threatening environment. This evokes ideas that would otherwise be missed or stifled. The transdisciplinary design approach teases out meaningful solutions that are intuitive and desirable to Airmen.

Air Force CyberWorx offers facilitated design thinking sessions that bring stakeholders, industry and academic experts together to develop solutions to hard problems. These sessions are tailored to best meet AF needs with differing lengths based on time sensitivity and CyberWorx capacity. One method, which maximizes solution agility and the educational benefit to warfighters and industry partners, is to offer a design sprint where the week-long design project answers a challenge being worked for AF stakeholders. The goal of such a design sprint is to develop low fidelity prototypes that clearly convey the desired Airman experience and the technical and policy developments needed to bring that experience to fruition. These projects help refine the requirement by seeking the right problem to solve and finding meaningful, forward-looking solutions by exploring a wide range of possible answers to the design problem.

> The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers.

For the Air Force Cyber Outreach Design Sprint, CyberWorx brought together 21 participants from Air Force units, academia, non- and for-profit industry, to rethink how the Air Force Academy and Pikes Peak Community College can interest middle and high school students in pursuing cyber-related careers.

Participants

The design sprint was attended by "outsiders" from academia, nonprofit and for-profit industry whose differing perspectives provided unique value distinct from the military members and government civilians attending the sprint. Attendees also had varying levels of experience and expertise in cybersecurity and the middle and high school student populations, providing fresh and diverse opinions on the place cybersecurity has for younger students. The CyberWorx design thinking approach deliberately breaks through the military's hierarchical and mission silos to find hard-hitting answers.

Participants included staff and faculty from regional elementary and high schools, Pikes Peak Community College (PPCC), Red Rocks Community College (RRCC), the University of Colorado-Colorado Springs (UCCS) and the US Air Force Academy (USAFA) in addition to representatives from nonprofits and industries in need of cyber professionals. This collection of unique backgrounds and perspectives opened the aperture of the realm of what's possible as CyberWorx tackled the challenge of interesting students into cyber professions.

Background

The geopolitical climate of today's culture has evolved rapidly in the past decade. With the increased threat of cyber terrorism, fake news and the influence of social media that spans across generations, gender and nationality, the need for cyber professionals is ever-increasing. Whether an individual is a digital native seeking a first-time career path or an experienced worker seeking re-training in the cyber field, it is essential that an educational path be available for them to succeed. There are a variety of options available for a student to enter the cyber field but it is essential that institutions work together to offer the greatest array of opportunities and generate interest as early in academic careers as possible.

The Air Force and Department of Defense in general are falling behind in the cyber race. Recruiting and retaining cyber professionals is a challenge for both military and industry and is essential to success. To help alleviate the problem, CyberWorx and the US Air Force Academy teamed with other institutions on the Front Range to begin the process of building a pipeline of well-educated cyber professionals capable of meeting demand at a variety of levels and abilities.

Design Problem Statement: #AFCyberOutreach

As with most CyberWorx sprints and design projects, the best starting point is to identify a relatively small use case that might lead toward fast solutions with the promise of potential scalability. For this sprint, we chose to **identify how USAFA and PPCC might increase middle and high school student**

participation in classes and clubs aligned with pursuing a cyber career. This may involve strengthening existing STEM outreach programs, modifying existing or creating new programs, partnering differently, etc. (Short name: #AFCyberOutreach)

OBJECTIVES: Push the envelope and come up with creative options for USAFA and PPCC, in partnership with other institutions and companies, to encourage middle and high schoolers to become interested in and stay engaged in academic programs and extracurricular activities which will attract and retain them in cyber career fields/coursework. Deliverable:

> Identify specific approaches and methods whereby post-secondary academic institutions can work with middle and high school students to increase the pipeline of cyber professionals whether they go directly into cyber career fields or into cyber academic programs.

VALUE PROPOSITION: Design will focus on improving the student experience and generating proofs of concept for making cyber programs more accessible and enticing to middle and high schoolers in the Front Range area, thus increasing the portfolio of potential cyber experts for the Air Force and others. If this is successful in the Colorado Springs area, these prototypes can be replicated beyond the local area.

Theme Development

Over the course of the 3-day sprint, participants discussed, assessed, brainstormed, and refined ideas of how to interest students into cyber-related classes and programs. The 21 participants were split into four teams, each encompassing diverse backgrounds.

SOLVING THE PROBLEM: In exploring the problem base, participants were taken through a process of determining –

- What connotes "cyber" to different groups of individuals?
- What barriers exist in developing interest and motivation in cyber?
- What could be done to overcome the barriers in order to *attract, prepare and retain* cyber professionals?

Each of the four teams was then asked to develop themes based on the above and create and act out a story to illustrate the successful evolution of a program to *attract, prepare and retain* cyber professionals.

Design Themes and Personas

Progressing through the design process requires teams to analyze and organize information in a manner that communicates efficiently with stakeholders. This communication is aided by the development of Personas - archetypal descriptions of user behavior patterns into representative profiles, to humanize the design focus and test scenarios. The following stories illustrate the teams' design focus.

TEAM CYBERWORX

Today – Kiana, a young high school teacher in an underserved school has talked with her students and they are interested in starting a coding club but soon found out there are no available computers for such a use. Undaunted, she heads off to find the principal and explain her needs. When she approaches the principal, however, she discovers he has no money available to allocate to the purchases and is just as frustrated as she is that they can't meet student needs.

Meanwhile, Bill, who works for CyberMoney, an organization that provides educational grants, is exasperated that he has money available, but hasn't heard from anyone asking for a grant that matches CyberMoney's criteria. CyberMoney's purpose is to help provide STEM opportunities to K-12 schools and their criteria aren't all that stringent and yet he has available funds and no applicants. On top of that, his boss has been riding him about getting the funds distributed or the amount will be reduced next year since no one seems to need it. Bill knows there are schools that could really use the help, but doesn't know how to reach them.

Future – Kiana's coding club is up and running thanks to a CyberMoney grant. Kiana knows it is because of the joint USAFA-PPCC led CASH (Cyber Acquisition Supplemental Help) program which was established a few years ago as a pilot program in the Front Range region that they were able to find CyberMoney and successfully complete the application form. CASH's database of grant-providing organizations and their grant criterion pointed Kiana in the right direction and the 1-day workshop with follow-on help for actually completing the application enabled her to zip through the process. Bill, at CyberMoney, was able to distribute all the organization's grant money to needy organizations and thanks to CASH he was able to choose from numerous compelling organizations vying for the grant money. In fact, when he showed his supervisors the depth and breadth of the well-articulated needs, they talked about upping his available funds next year as they know the benefits of increased cyber talent for the Front Range as well as he does. Meanwhile, PPCC has seen an uptick in the number of applicants coming out of Kiana's school with in-depth coding skills and is able to build upon those skills as opposed to starting at a more basic level and the feedback from industry on the skill levels of the PPCC cyber graduates has been amazing. For its part, USAFA has led the way in helping match schools and grants and is viewed as a key Front Range partner in "upping the game" of cyber talent in the area. As an added bonus, many of the grant recipients have gained even more exposure to the Air Force Academy and the Air Force mission.

Way forward: An initial inexpensive prototype of a week-long series of workshops to teach educators how to find and obtain grant funding, particularly "micro grants" of $1,000 or less, could be funded and organized by PPCC and USAFA. Grant writers and other volunteers could be utilized to speak at the workshops. Funders are an essential part of the process as well, providing immediate feedback to educators on their proposals and implementation plans.

TEAM CYBERDYNE

Madeline, a young college student at the community college, is making her weekly drive to an elementary school in Colorado Springs and thinking about how excited she is to be a mentor in the new CyberCats program that the US Air Force Academy (USAFA) and Pikes Peak Community College (PPCC) initiated in Colorado Springs a couple years ago. She remembers how lonely she felt in middle and high school as a girl interested in cyber and other tech fields who couldn't find any outlets for her passion. Her first introduction to cyber was thwarted by stigma and gender roles when she idolized a unique character in a game she played in elementary school. The character was an effective hacker with what seemed at the time, to have super powers. Though her father believed she could become like that character and supported her in this dream, she was discouraged from it by classmates and educators who said only males could enter and succeed in such a field. Back then, all the cyber programs were "for the guys" and while she may not have been specifically forbidden to join the groups, it certainly wasn't encouraged or comfortable for her to be there. It was not until college that she realized she really could become a cyber professional.

The USAFA-PPCC CyberCats program was certainly addressing that and Madeline was proud to be in vanguard of making a difference for young girls in the Colorado Springs area. A weekly after-school club for girls K-5, CyberCats was built around a high social interaction foundation that uses game theory. Girls work together to solve problems and move along progressively to a common goal, such as an "escape room," to build cyber skills and confidence. This social experience allows the participants to build confidence at a crucial time in life, when they are trying to figure out who they are and how they fit into the various social groups and hierarchies. The club was even designed to lead into existing programs like Cyber Patriot as an early exposure to the cyber field.

As she pulled into the elementary school parking lot, she noticed her friend and co-mentor, Kesha, pulling up at the same time. Kesha is in her junior year at the Air Force Academy and is the other half of their mentoring "dynamic duo." Due to her Academy schedule, Kesha's availability is a bit more limited than Madeline's, but Madeline knows the girls really benefit from Kesha's perspective. After all, how else would girls in Colorado Springs be able to hear firsthand what it was like to be a girl interested in cyber growing up in Nigeria! The USAFA-PPCC partnership is truly what powers the success of CyberCats!

Way forward: The initial prototype could bring together a focus group of elementary school girls and parents to understand the program better and meet the needs of all the stakeholders. From there, A USAFA-PPCC team would design the program and build metrics for its success. Additionally, local industry would be approached to bring them on as partners working together to make CyberCats a

reality at one or two Colorado Springs elementary schools. Based on experiences gained from the first year of operation, metrics could be refined and the program expanded based on feedback from the schools, PPCC, and USAFA.

TEAM INNOVATIVE INK SLINGERS

Mr. Peterson, a math teacher at Contrails High School in Colorado Springs, sits back in his chair and a smile slowly creeps over his face as he revels in the moment. We did it, he thinks. We really did it. Despite the obstacles, we did it! Contrails had just been announced as the host school for next year's Student Cyber Summit – the annual gathering of Student Cyber Societies (SCS) from around the Springs area and Mr. Peterson was excited (and a bit scared)! Contrails SCS team had pulled together a competitive bid involving a "knock-out" keynote speaker and age-specific breakout sessions guaranteed to wow the elementary, middle and high school students who would be attending. Earning selection as host of next year's summit (the culminating event of the year for the various SCS teams) was a fitting reward for his team's efforts. He knew it would be a lot of work, but with the ever-present support from USAFA and PPCC, he was confident Contrails would not only pull it off but raise the bar even higher for whoever followed them.

Mr. Peterson remembered the "old days" when he'd tried (and failed) to recruit athletes and other students into a cyber club at the high school level but been rebuffed as by then the students had already made their decisions on where to devote their energies (and cyber was not one of those areas). The SCS formed initially at the elementary school level and got the kids interested in and unafraid of cyber before they were deeply engaged in and committed to other activities. By making the society events fun and interesting (and building upon the initial contacts through the Safe and Secure Online program), kids came to view "cyber" as just a part of their life and not something "weird" or "geeky." As the students progressed, they developed and built upon virtual characters which grew, matured, and "learned" alongside the students themselves. The long-term relationships the students formed through the SCS both within and external to their schools became a connection they looked forward to renewing at the annual summit and other events. Mr. Peterson marveled at how far the program had come and the impact it had made on the entire Colorado Springs area. Hearing a commotion in the hall, Mr. Peterson sat up and got ready to greet and congratulate the team that had pulled together the winning presentation – he knew hosting the summit would be a lot of work, but with the ever-present support from USAFA and PPCC for the SCS, he was confident Contrails would not only pull it off but raise the bar even higher for whichever school followed them.

Way forward: Implementation of this program would begin with the most cost effective and least time-consuming piece – purchasing Safe and Secure Online kits for underserved elementary schools across Colorado Springs. These would be provided and metrics kept, testing the program's effectiveness in

increasing awareness and interest in cyber. Based on that interest, a few after school pilot programs of Student Cyber Societies could be launched for elementary school students, concluding with the initial SCS summit, bringing the members together from across participating schools and forming the initial network of SCS members.

TEAM ROGUE ONE

Caroline cautiously peers around the tree, scanning for "enemy" sentries and spies the other team's flag standing upright in the clearing ahead. Success – it appears to be unguarded and within reach. Caroline, normally an introverted 3rd grader at Wahoo Elementary, is in the zone – having adopted her "Virtual and Reality" flag hunter mindset (or her "V&R face" as she prefers to call it). With V&R face on, she takes a few cautious steps forward and thinks about the successes she's already had today while in the Virtual world portion of Camp Cyber Adventure Hero. If she's as successful now in the "R" world as she was in the "V" world earlier, she'd have real bragging rights when she got home at the end of camp. Who knew a camp for elementary school kids could combine cyber and nature and actually be fun!

Though she hadn't really thought of herself as much of a "virtual cyber warrior" prior to coming to Camp Cyber Adventure Hero, her week here had changed all that. From the initial cyber challenges the staff had drawn up to interest her and her fellow campers into venturing into the virtual world to the more interesting and exciting opportunities available as they progressed and became more advanced, Caroline's skill level in the virtual "capture the flag" games had increased steadily – as had her confidence. It helped, of course, that the staffers were really fun and supportive. She was also impressed with their stories and experiences as students at the Air Force Academy and Pikes Peak Community College – it was great to hear there really was life after elementary school!

Caroline hears a twig snap and is pulled back to the "R" world. The camp offered lots of neat opportunities to explore nature and cyber and where they came together – like in the augmented reality glasses they used on a nature hike and she had enjoyed the geo-caching clue search they had done yesterday but her specialty is in capturing flags – both V&R. Looking across the clearing, she sees one of her teammates, Georgia, stomping on sticks and making a racket. "What is she doing? She's going to draw everyone to her!," Caroline's inner voice screams inside her head. Then, she realizes Georgia is doing just that…but on purpose! She's stomping on sticks to distract the other team just like they used a diversion in the "V" world earlier today to enable teammates to virtually secure the flag. As the other team converged on Georgia, Caroline took off at a gallop – legs and arms pumping mightily. She grabs the flag and races back to home base – victory assured in both V & R worlds today!

Way Forward: The initial prototype could be in the form of an after school program since children are comfortable in that environment. USAFA and PPCC would develop (or purchase) an on-line 'capture the

flag" or similar team game for elementary school children where students "capture flags" based on demonstrating knowledge of basic cyber and on-line security. That would then be paired with "capture the flag" or other "real world" games to complement the virtual games. If this pilot proves successful, it could scale up to longer single- or multi-day camps. It would be important to still have to have outdoor atmosphere as well as connectivity of internet for cyber activities. The goal is to teach online security, password security, etc. to young kids to keep them safe before moving to advanced skills. Since it is designed to be interactive and socially engaging, the skills would be better retained and assimilated.

Recommendations – Where to Start Small for Big Impacts

Air Force CyberWorx recommends a phased approach toward implementing the following aspects of these proposals as described below. USAFA and PPCC leadership, along with the solutions owners, will need to decide where to invest and prioritize their efforts based on these recommendations.

Team CyberWorx – Grant-writing to leverage national resources

The biggest impact can be made by shoring up three fronts relative to grants and by initiating a new front.

1) Staff and faculty currently involved in grant research/writing at USAFA and PPCC meet in a ½ day facilitated session in October to work on:
    a. Ways to identify and share information (with each other and local school districts) on available/applicable grants
    b. How to help school districts identify and/or communicate their needs (PPCC lead)
    c. Ways to potentially engage industry or other untapped areas for support (both monetary and non-monetary)
2) USAFA and PPCC host a "1-day grant-writing workshop" between Jan and Mar 2018 for school district POCs (teachers, administrators, etc.) where the focus would be on practical writing pointers, requirements, etc.

Team Cyberdyne – Elementary school Cyber Club focused on girls and social interaction

1) Determine strengths and challenges with existing "Cyber Warrior Princess" program
    a. USAFA cadets and PPCC students go to elementary schools where the program exists and talk with participants and others on pros/cons and potential improvements
    b. USAFA & PPCC faculty/staff talk with Cyber Warrior Princess staff on pros/cons and potential improvements

Team Innovative Ink Slingers – Student Cyber Societies

1) Identify a target district and grade (e.g., District 20, 3rd grade) and put every student in that target district and grade through the ISC2 Safe and Secure Online (SSO) program
    a. USAFA and PPCC fund or identify funding source to procure enough SSO kits to ensure everyone in the target district/ grade receives the training

   b. USAFA and PPCC work with teachers in the target district/grade to ensure they are comfortable with the kits and how to use them (USAFA/PPCC can leverage ISC2 members in the area as an alternative)
2) USAFA and PPCC work with CyberPatriot on ways to energize the existing CyberPatriot programs in the middle schools
   a. Work with local organizations (i.e., AFCEA) with interest in cyber and see if they can identify additional coaches, etc., to lessen load on middle school teachers
   b. Identify opportunities to tie SSO more closely with CyberPatriot

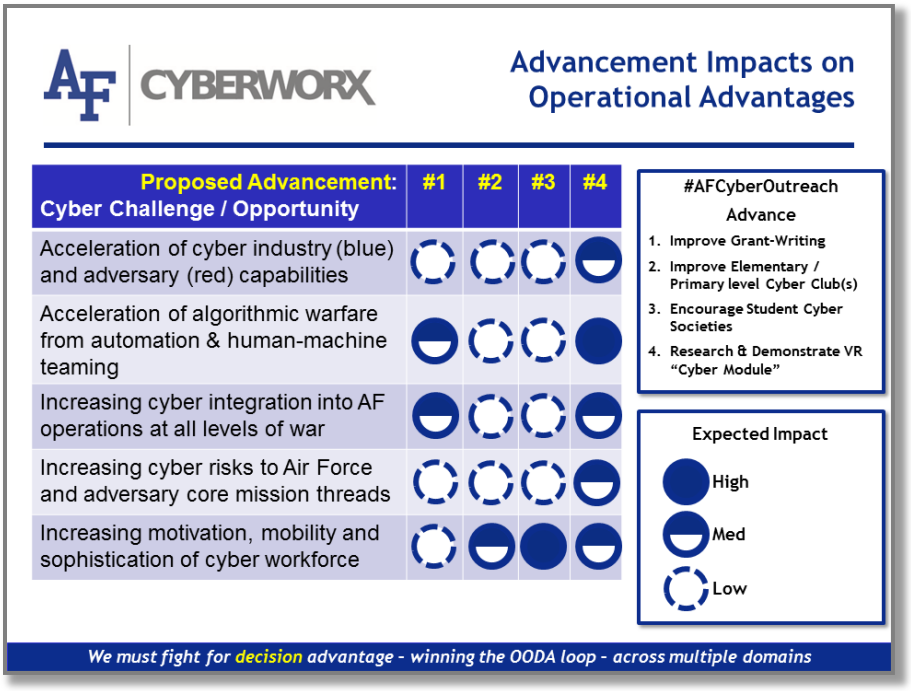
Team Rogue One – V&R Camp

1) USAFA and PPCC create a "cyber module" that can be used by elementary and middle schools during field day activities as part of their rotating schedule
   a. PPCC to identify schools where this could be inserted into existing activities
   b. USAFA and PPCC to develop the module and facilitate its use as part of the field day
2) USAFA and PPCC to engage their cyber clubs for outreach to elementary and middle schools where the cadets/students tie virtual and real world together experientially
3) USAFA host a "cyber day [half day]" for elementary school students with exposure to Cyber City, CyberWorx and a Capture the Flag exercise

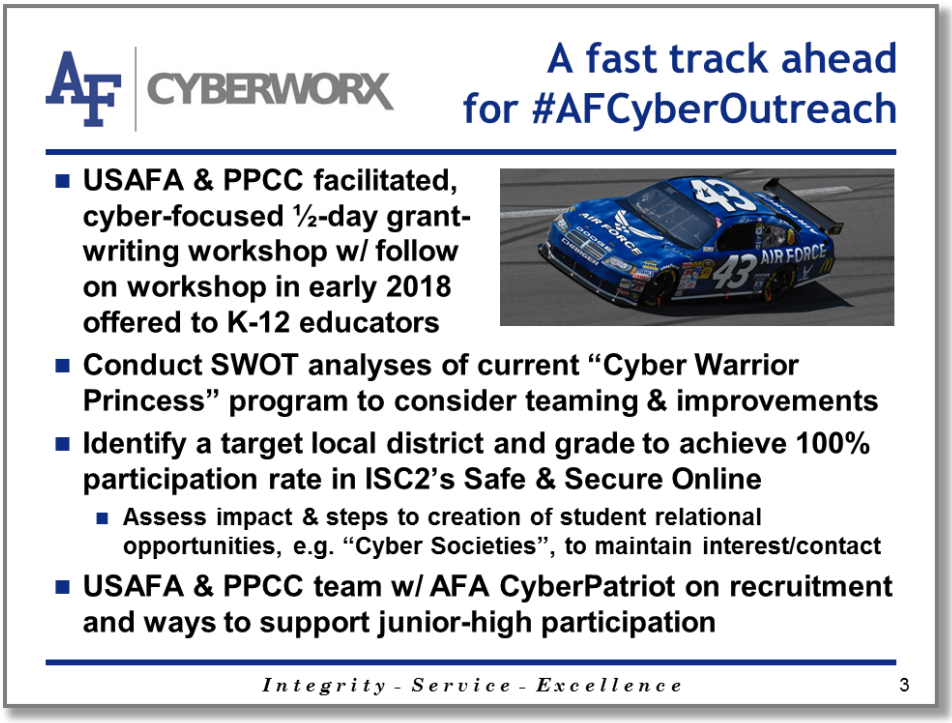
---

3-Slide Summary: Ops Advances + The Fast Track

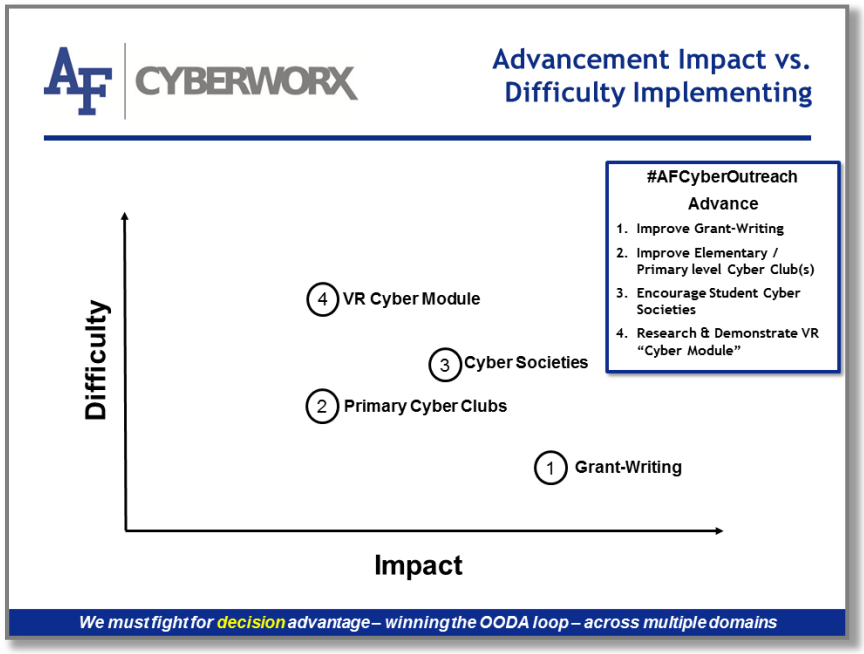
The CyberWorx "three slide summary" section is designed to help you consider the recommendations in this report by weighing the operational improvements proposed against the current cyber challenges and opportunities we face as an Air Force.



In deciding what to do, the decision to do nothing is a decision and brings its own risks. Thus, the "fast track" slide spells out an easy set of actions to take at minimum to start trying to improve and to put the Air Force on a path of discovery in overcoming the challenges that drove this design project.



We recognize we live in a resource-constrained world. Each advance proposed in this report is graphed below: The graph compares the advance's relative impact on the ability of the Air Force to maintain information and decision dominance (x-axis) against the difficulty (e.g., expenditure of time/treasure, cultural evolution, policy change) needed to implement that advance (y-axis). Cultural changes, like some of those proposed in this report, are not easy, but they are possible and needed for success in our digital, cyber-contested world.



CYBERWORX ™

Appendix D: Cyber Prep Internship Reports

Internship Pilot Project Report

January 2018

Table of Contents

Overview

The Cyber Prep program is a multi-stakeholder partnership of more than 30 employers, community organizations, and educators from area school districts, higher education institutions, and private training providers. Together, these organizations are helping teens to choose cybersecurity careers by providing a variety of opportunities for them to explore, learn, and work in the cybersecurity industry. Cyber Prep is facilitated by staff at Pikes Peak Community College (PPCC), under a cooperative agreement from the National Institute for Cybersecurity Education (NICE), a program of the US Department of Commerce National Institute for Standards and Technology (NIST) under award number 70NANB16H323.

During the summer of 2017, Cyber Prep offered summer internships for 10 students from three school districts at seven companies. The PPCC Cyber Prep team discussed internships needs and requirements with local businesses, worked with teachers to identify qualified candidates, facilitated a four-hour interview intensive involving all parties, and helped match qualified students with companies in need of their skills to form mutually beneficial internship partnerships. At the conclusion of the program, both students and employers were pleased with the experience and all indicated that they would participate again.

This report documents the essential ingredients of the program.

Internship Program Development

The internship program was developed by a team of Cyber Prep volunteers including school district internship coordinators, career and technical education staff and cybersecurity instructors along with employer representatives. Together, these team members:

1) Researched labor laws to make certain that the program would be compliant and that they could provide guidance to employers concerned about working with younger people
2) Reviewed internship program documents from the participating school districts to make sure that the program would cover all school district requirements;
3) Addressed liability issues by requiring participating employers to hire the students and pay them a wage or stipend for their work;
4) Developed recruiting materials for employers and students to join the program;
5) Created and implemented a process for interviewing intern candidates and matching them to internship opportunities;
6) Developed and implemented an intern onboarding checklist for use by PPCC, the employer sponsor, and the school district;

7) Tailored the existing PPCC high school internship orientation program to fit cybersecurity internships; and,
8) Outlined the baseline program to be implemented by every employer, including the provision of a $500 stipend to each employer (per intern) for participating in the pilot project, allowing employers to pay the interns a stipend for their work.

Program Recruiting

The Cyber Prep team began recruiting efforts in early spring of 2017. Recruiting focused on finding willing employers and matching them with the best student candidates the school district partners could field.

Employer Recruiting

Employer recruiting began with a series of emails sent to cybersecurity companies by PPCC Cyber Prep team staff and employer representatives. In addition, program flyers were distributed at a variety of area workforce development and cybersecurity industry meetings, including the local chapter of the Information Systems Security Association (see Exhibit A).

The email and flyer invited company representatives to contact the Cyber Prep Program Manager for more information. The Cyber Prep Program Manager met with each interested company team to determine the viability of an internship. This recruiting effort yielded 12 potential employers, seven of which chose to develop and offer an internship. These employers included:

- *Defense contractors*: Barnett Engineering & Signaling Laboratories, Boecore, Rim Technologies, Summit Technical Solutions, and TechWise;
- *Nonprofit organizations*: The Center for Technology, Research and Commercialization (C-TRAC)
- *Training Providers*: LeaderQuest

Employer representatives were given a variety of materials to help them to understand the scope of the internship program and develop their own internship, including the description of Colorado Youth Labor laws (see Exhibit B), an onboarding checklist (see Exhibit C), and sample internship job descriptions (see Exhibit D) as well as the summer internship program schedule.

Student Recruiting

Students were recruited from three school districts participating in some aspect of Cyber Prep, including Air Academy School District 20, Colorado Springs School District 11, and Peyton 23 Jt School District. District Career and Technical Education (CTE) staff as well as the computer faculty at those schools helped to spread the word. The team

Exhibit A: Employer Recruiting Flyer

Cybersecurity Companies Needed to Host Internships

Pikes Peak Community College (PPCC), Cybersecurity Prep Program (CSPP) and local cyber compinies in the Pikes Peak region have partnered to provide summer internships in the field of cybersecurity.

As part of this program all interns will be required to attend a week of immersion activities prior to showing up on your work-site.

These activities will include:

- Bring Your A Game to Work training (attendance, attitude, appearance, etc.)
- Tour of PPCC Teen College Cybersecurity summer camps
- Site visits to multiple and varied cyber companies, the National Cybersecurity Center (NCC) and local universities

Tentative dates are

June 19, 2017 to July 28, 2017

Workforce Development
5675 S Academy room A223
719- 502-2404

Summer Cybersecurity Internships

Cyber companies will:

- Complete internship agreement
- Complete PPCC vendor application and submit invoice by June 30, 2017
- Receive a $500 stipend to pay the intern
- Identify an internship project
- Supervise an intern for 15 hours per week
- Agree to one site visit by PPCC staff member
- Attend final Intern Recognition luncheon

Interns will be:

- High School students in 9th to 12th grade
- Carefully vetted for commitment
- Sincerely interested in the career field
- Paid $500 stipend for 6 week program

10 Internship Sites Needed

If you would like to help these young people further their interest in the field of cybersecurity, please agree to become one of our host sites.

If you are not quite ready to host an intern, please consider allowing us to visit your company for a short tour during our immersion week.

Please Join us in this Project

Contact Info:
Dr. Ernest Greene
Pikes Peak Community College Cybersecurity Prep Program Manager (719) 502 - 2406
ernest.greene@ppcc.edu

PIKES PEAK COMMUNITY COLLEGE

CYBER PREP
Pikes Peak Region of Colorado

Exhibit B: Colorado Youth Labor Laws

Colorado Department of Labor and Employment
Division of Labor Standards and Statistics
633 17th Street, Suite 600 • Denver, CO 80202-2107 • (303) 318-8441 • www.colorado.gov/cdle/labor

Colorado Youth Law

The Colorado Youth Employment Opportunity Act (C.R.S. 8-12-101 *et seq.*) regulates the employment of minors in Colorado. The Fair Labor Standards Act (FLSA) and its regulations do not permit the employment of minors in a variety of circumstances. When both federal and state laws apply, the more stringent standard must be observed. Contact the U.S. DOL for information on FLSA and federal youth laws (www.dol.gov or 1-866-4USWAGE).

DEFINITION OF A MINOR
(8-12-103(5))

A minor is any person under the age of 18, except a person who has received a high school diploma or a passing score on the general educational development (GED) examination.

EXEMPTIONS FROM CYEOA
(8-12-104)

The CYEOA does not generally apply to the following:

1. Schoolwork and supervised educational activities.
2. Home chores.
3. Work done for a parent or guardian, except where the parent or guardian receives any payment therefore.
4. Newsboys and newspaper carriers.
5. Actors, models, and performers are exempt from the age-related restrictions for minors under age fourteen.

WORK PERMITS
(8-12-111)

Work permits are **not** required by Colorado law.

Age Certificates

Any employer desiring proof of the age of any minor employee or prospective employee may require the minor to submit an age certificate. Age certificates are issued by or under the authority of the school superintendent of the district or county in which the applicant resides.

School Release Permits

Any minor fourteen or fifteen years of age who wishes to work on school days during school hours shall first secure a school release permit. Such permit is issued only by the school district superintendent, his agent, or some other person designated by the board of education.

REQUEST AN EXEMPTION
(8-12-104)

- The Director may grant exemptions from some provisions of the CYEOA.
- Any employer, minor, minor's parents or guardian, school official, or youth employment specialist may request an exemption.
- Exemptions are evaluated on a case-by-case basis, and are granted or denied in accordance with the best interests of the minor.
- Exemption determinations involve the scrutiny of such factors as the minor's previous training and safety concerns.

PERMISSIBLE OCCUPATIONS
(8-12-106, 107, 108, 109)

Minors under the age of 9 cannot generally be employed.

Permissible at age 9 or older:

1. Delivery of handbills and advertising.
2. Shoe shining.
3. Gardening and care of lawns involving no power-driven lawn equipment.
4. Cleaning of walks involving no power-driven snow-removal equipment.
5. Casual work usual to the home of the employer and not specifically prohibited.
6. Caddying on golf courses.
7. Occupations similar to the above.

Permissible at age 12 or older:

1. Sale and delivery of periodicals.
2. Door-to-door selling and delivery of merchandise.
3. Baby-sitting.
4. Gardening and care of lawns, and cleaning of walks; contact the Division regarding use of power-driven equipment.
5. Non-hazardous agricultural work.
6. Occupations similar to the above.

Permissible at age 14 or older:

1. Non-hazardous occupations in manufacturing.
2. Public messenger service and errands by foot, bicycle and public transportation.
3. Operation of automatic enclosed freight and passenger elevators.
4. Janitorial and custodial service.
5. Office work and clerical work.
6. Warehousing and storage, including unloading and loading of vehicles.
7. Non-hazardous construction and non-hazardous repair work.
8. Occupations in retail food service.
9. Certain gasoline service occupations.
10. Occupations in retail stores.
11. Occupations in restaurants, hotels, motels, or other public accommodations.
12. Occupations related to parks or recreation.
13. Occupations similar to the above.

Permissible at age 16 or older:

The occupations listed above and the operation of a motor vehicle if the minor is licensed to operate the motor vehicle for such use pursuant to Colorado Revised Statutes Article 2, Title 42.

This complimentary guide is provided by the Colorado Division of Labor Standards and Statistics. Its condensed and simplified content is for general informational purposes only, and does not constitute legal advice. For more information contact the Division, an attorney, or an HR professional.

Guide Revised August 2016

HAZARDOUS / PROHIBITED
(8-12-110)

1. Operation of any high pressure steam boiler or high temperature water boiler.
2. Work which primarily involves the risk of falling from any elevated place located ten feet or more above the ground except that work defined as agricultural involving elevations of twenty feet or less above ground.
3. Manufacturing, transporting, or storing of explosives.
4. Mining, logging, oil drilling, or quarrying.
5. Any occupation involving exposure to radioactive substances or ionizing radiation.
6. Operation of power-driven machinery:
   a) Woodworking machines
   b) Metal-forming machines
   c) Punching or shearing machines
   d) Bakery machines
   e) Paper products machines
   f) Shears
   g) Automatic pin-setting machines
   h) Power food slicers and grinders
7. Any other power-driven machinery deemed hazardous by the Director.
8. Slaughter of livestock and rendering and packaging of meat.
9. Occupations directly involved in the manufacture of brick or other clay construction products, or silica refractory products.
10. Wrecking or demolition, but not including manual auto wrecking.
11. Roofing.
12. Occupations in excavation operations.

WORK HOUR RESTRICTIONS
(8-12-105)

General Restrictions

No employer shall be permitted to work a minor more than forty hours in a week or more than eight hours in any twenty-four-hour period.

School Day Restrictions

On school days, during school hours, no minor under the age of sixteen shall be permitted employment except as provided by a school release permit. After school hours no minor under the age of sixteen shall be permitted to work in excess of six hours unless the next day is not a school day.

Nighttime Restrictions

Except for babysitters, no minor under the age of sixteen shall be permitted to work between the hours of nine-thirty p.m. and five a.m., unless the next day is not a school day. An exception to this rule is a minor employed as an actor, model, or performer.

Exhibit C: Onboarding Checklist

PIKES PEAK COMMUNITY COLLEGE

PPCC's Summer Intern Onboarding Checklist

BEFORE THE INTERN'S START DATE

Expected Outcome(s): Provide the intern with *a welcoming work environment to so that she/he feel "settled in" on their first day.*

Schedule and Job Duties

- ☐ Sponsor calls intern:
  - Confirm start date, time, place, parking, dress code, etc.
  - Identify computer needs and requirements.
  - Provide name of their onboarding buddy.
- ☐ Sponsor and CSPP Intern Coordinator remind intern to complete and submit the PPCC Internship Agreement to the PPCC Workforce Center's Cyber Prep Intern Coordinator

Employer's Socialization Plan

- ☐ Email department/team/functional area of the new intern. Include start date, intern's role, and bio. Copy the intern, if appropriate.
- ☐ Set up meetings with critical people for the intern's first few weeks.
- ☐ Select and meet with the buddy and arrange for lunch with the appropriate person(s) or buddy for the first day and during first week.
- ☐ Arrange for a worksite tour.
- ☐ Prepare intern's calendar for the first two weeks.

Work Environment

- ☐ Put together welcome packet from the department and include: job description, welcome letter, contact names and phone lists, campus map, parking and transportation information, mission and values of the Institute, information on your unit/school, etc.
- ☐ Clean the work area, and set up cube/office space with supplies.
- ☐ Add intern to relevant email lists.

Technology Access and Related

- ☐ Employer provides the appropriate technology equipment (computer, printer, iPad) and software.
- ☐ Arrange for access to common drives, and coordinate SAP roles authorizations.
- ☐ Arrange for phone installation.

Training/Development

- ☐ Ensure that intern attend the PPCC sponsored "Bring You're A Game to Work" orientation.
- ☐ Arrange pertinent trainings required for the job.

PIKES PEAK COMMUNITY COLLEGE

PPCC's Summer Intern Onboarding Checklist

FIRST TWO WEEKS

Outcomes: *The intern feels welcomed and prepared to start working; she or he begins to understand the requirements of the position and your performance expectations.*

Schedule, Job Duties, and Expectations

- ☐ Clarify the first two weeks' schedule, and confirm required PPCC sponsored intern orientation training.
- ☐ Provide an overview of the functional area – its purpose, organizational structure, and goals.
- ☐ Review job description, outline of duties, expectations and describe how intern's job fits in the department.
- ☐ Explain policies and procedures for PPCC's intern stipend, use of sick time, holidays, etc.

Socialization

- ☐ Be available to greet the intern on the first day.
- ☐ Introduce intern to his/her buddy and others in the workplace.

Work Environment

- ☐ Discuss transportation and parking
- ☐ Provide department or building-specific safety and emergency information.

FINAL FOUR WEEKS

Outcomes: *New intern builds knowledge of internal processes and performance expectations; feels settled into the new work environment. Intern is cognizant of his/her performance relative to the position and expectations; continues to develop, learn about the organization, and build relationships.*

Schedule, Job Duties, and Expectations

- ☐ Meet with and debrief the intern after he/she completes the first two weeks.
- ☐ Discuss performance and professional development goals and give intern his/her final four week assignment. (Make it something small and doable.)
- ☐ Continue to provide timely, on-going, meaningful "everyday feedback."
- ☐ Elicit feedback from the intern and be available to answer questions.
- ☐ Give intern an additional assignment.

Socialization

- ☐ Continue introducing intern to key people and bring him/her to relevant events.
- ☐ Arrange for intern to take PPCC's and other relevant job site tours (if not already completed).

Training and Development

- ☐ Ensure intern has attended Human Resources New Intern Orientation.
- ☐ Ensure intern is signed up for necessary training.

Exhibit D: Sample Internship job description and recruiting information

Boecore, Inc. is currently recruiting talented and enthusiastic high school students interested in careers in Cybersecurity to join our Network & IT team in Colorado Springs, CO. Boecore can offer you a wide variety of experience encompassing Department of Defense System Engineering, Network Management, Software Development, Systems Administration and Cybersecurity. You will learn new skills, interact with industry experts, connect with thought leaders and have the opportunity to support Boecore's enterprise network and its users through the implementation of healthy cybersecurity practices using industry tools and strategies.

Cybersecurity intern at a small woman-owned aerospace company that specializes in Enterprise Network IT, Cybersecurity and Systems and Software Engineering. Intern will be located at the corporate office in downtown Colorado Springs and will be introduced to business conduct and protocol in a professional working environment. Intern will be shadowing cybersecurity and engineering professionals to learn varying aspects of those fields to include network security & monitoring, risk assessment, software assurance, vulnerability and penetration testing, basic system administration and IT skills, network upgrades, server installation & configuration, and software coding & testing. Intern will attend corporate staff meetings, will provide written reports on status & progress and will support and provide capability demonstrations to leadership and customers. Intern will also have the opportunity to visit a local AF base and tour enterprise IT facilities including the Network Operations Center (NOC).

Minimum Requirements:

- Currently enrolled as a junior or senior in a local Colorado Springs high school with IT, Networking and/or Cybersecurity course work and extracurricular activity experience.
- GPA of 3.5 or higher.
- Ability to work part time (16-20 hours per week) throughout the summer (approx. June-July 2017) at our downtown Colorado Springs office.
- Basic IT, networking and/or cybersecurity knowledge.
- Applicant must be familiar with Microsoft tools (Word, Excel.)
- Effective interpersonal skills are a must.
- Ability to communicate with diverse levels of people
- Ability to present to diverse audiences regarding projects in which you are engaged.
  (business people & technical staff).
- Works well within a structured environment and still be able to think quickly and easily adapt to changing priorities and events.

developed a recruiting flyer that invited students to contact the Cyber Prep Program Manager for more information (see Exhibit E).

In addition, the region's largest school district, Colorado Springs School District 11, conducted its own recruiting across its five high schools, yielding 60 students in District information technology programs interested in this opportunity. As a result, the recruiting effort yielded approximately 75 students with an interest in the summer internship program, 10 of whom were selected to participate from three different school districts. Of these 10 students, three (30%) were female.

Intern Matching Process

In order to maximize students' exposure to the interviewing process and give employers a sense of the level of qualifications and maturity of local high school students, the Cyber Prep team created a half-day intern matching process. Students interviewed with all seven companies individually in 20-minute sessions.

At the end of the interviews, the students wrote down their top three companies. Company representatives met together after the interviews and talked about each candidate and the opportunities available at each company until they had matched each intern to a company. In the end, every student was matched with a company of his or her first or second choice.

Internship Program Description

The baseline internship program was developed as a six-week experience: June 19 to July 27, 2017. This program included:

- A two-day introduction to the work environment and employer expectations, including a training called *Bring Your A Game to Work*[1];
- Regular field trips to see cybersecurity operations in action, including visits to local company Root9B and the National Cybersecurity Center; and,
- An expectation that students would work at least 15 hours a week for six weeks and would be paid a wage or stipend for their work.

However, several employers chose to make one or more additions to the program:

- Extend the program to cover more than six weeks during the summer of 2017;

[1] *Bring Your A Game to Work* is a program for youth and adults developed and offered through the Center for Work Ethic Development. More information about the program may be found here: https://workethic.org/bring-your-a-game-to-work/

Exhibit E: Student Recruiting Flyer

Summer Cybersecurity Internships for High School Students

Pikes Peak Community College (PPCC), Cybersecurity Prep Program (CSPP) and local cyber compinies in the Pikes Peak region have partnered to provide summer internships in the field of cybersecurity.

Cybersecurity companies across our region have offered to bring in some young, enthusiastic students to learn cybersecurity jobs from inside their company.

Each intern will be individually matched with the cybersecurity company that best fits the student's interest through an application and interviewing process.

All interns will visit multiple cybersecurity job and summer camp sites in the Colorado Springs area to experience first hand the amaizing cybersecurity capabilities that our region has to offer.

Don't miss this opportunity!

Internship spaces are limited!

Workforce Development
5675 S Academy room A223
719- 502-2404

Program Requirements

- High School student (9th to 12th grade)
- Willing to attend "*Bring Your **A** Game to Work*" training prior to the internship
- Willing to work at least 15 hours per week for 6 weeks
- Sincere interest in cybersecurity as a career

Career Prospects

- Security Provision (SP)
  - Software Development
  - System Development
- Operate and Maintain (OM)
  - Technical Support Specialist
  - Network Operations Specialist
  - Systems Security Analyst
- Protect and Defend (PR)
  - Cyber Defense Analyst
  - Cyber Defense Infrastructure Support Specialist
  - Vulnerability Assessment Analyst
- Investigate
  - Cyber Defense Forensics Analyst

10 Internships Available

If you have a sincere interest in pursuing the exciting field of cybersecurity, and would like to participate in a paid internship this summer, act now!

Contact Information:

Dr. Ernest Greene
Cybersecurity Prep Program Manager
(719) 502 - 2406
ernest.greene@ppcc.edu

PIKES PEAK COMMUNITY COLLEGE

CYBER PREP
Pikes Peak Region of Colorado

- Keep the interns on payroll to bring them in for later; seasonal/supplemental/contract projects;
- Submit interns for Top Secret Security Clearances to enable them to more quickly complete the hiring and onboarding process post-graduation (2018); and,
- Offer subsequent internship/employment opportunities for fall 2017 or in summer 2018.

Program Benefits

Participating employers walked away from the experience with a positive impression of the impact students had on their company as well as a positive impression of the impression they had on their student interns. Students walked away with exposure to a professional environment; better awareness of career requirements, skills, tools, and opportunities; and enthusiasm for their career potential.

Employer Benefits

Employers cited the following benefits from their experience with High School interns:

- Employees gained experience mentoring;
- Young interns brought contagious energy and enthusiasm into the workplace;
- Presence of interns and their questions helped refine policies, procedures, and documentation from the ground up;
- Entry level IT tasks were offloaded to interns, freeing experienced employees for other tasks
- Employees were exposed to the various opportunities, training, and information presented to interns, broadening their knowledgebase as well;
- Employees were encouraged to participate in cybersecurity events at the community level, encouraging networking and exposure;
- Companies received positive publicity from webcasts, interviews, panel discussions, news articles, and press releases; and,
- Companies received academic and state funding to offset costs.

Student Intern Benefits

Student interns and their teachers/mentors cited the following benefits for participating students:

- Exposure to a professional, technical environment at a young age;
- Understanding of the skills and tools that are important in industry;
- Hands on experience with industry tools and processes;
- Networking opportunities with companies, professionals, and resources; and,

Employer	Number of Interns	Activities

Boecore	2	• Develop technical skills
		  • Enterprise IT, Cybersecurity, Software Dev & Secure Coding, Design Thinking
		  • Mentoring by cybersecurity SMEs
		  • Implement industry standard cybersecurity practices to support the enterprise network and users
		  • Industry site tours & cybersecurity community events
		  • Whitepaper, briefings and capability demonstrations, Capture The Flag challenge conduct
		• Career Development
		  • Professional office & small business operations
		  • Resume writing & interviewing
		• Out-briefs to Leadership, Colleagues, Students & Industry – Career Panels, Lunch & Learns, Cyber Warrior Princess

TechWise	1	• Support ongoing cybersecurity education efforts, including interactive game/simulation development • Conduct research and usability testing on existing products and services
LeaderQuest	1	• Support cybersecurity instructors in the classroom • Learn about IT industry certifications and the business model for education • Provide general IT support • Provide support for the National Cybersecurity Center summer CyberPatriot camp
Rim Technologies	2	• Provide general IT/Security support • Receive introduction to cybersecurity issues and challenges • Collaborate with industry experts • Develop professional skills
Summit Technical Solutions	1	• Receive introduction to business conduct and protocol • Shadow cybersecurity and IT professionals • Attend corporate staff meetings • Provide written status/progress reports • Provide and/or support demonstrations to leadership/customers

Employer	Number of Interns	Activities
Barnett Engineering	2	• Provide technical support and software development for a new commercial cybersecurity project • Support web development • Prepare for the Security+ Exam
Center for Technology Research and Commercialization (C-TRAC)	1	• Support start-up activities • Assist with policy and program development • Develop web content • Receive introduction to Catalyst Campus companies and programs • Complete leadership training

Table 1: Employer, Intern, and Activity Summary

- Excitement over real world professional opportunities (which provides encouragement to continue to pursue related careers).

Lessons Learned

- It is possible, but time consuming, to coordinate tasks for high school students such that all parties benefit;
- PPCC's involvement facilitating communication between industry and academia saved time and energy on part of employers, allowing them to provide internships that they would not otherwise have had the bandwidth to coordinate;
- Youth, energy, and a blank slate of experience can positively contribute to work environments and provide a driving force for revising policies and procedures, improving employee community involvement as well as their mentoring skills;
- Some students reported that they would have liked to have a unique project, something to show as complete at the end of their 6 weeks;
- The $500 stipend was a crucial component of the program, allowing companies to justify their involvement in a program involving high school students;
- Internship opportunities help foster a strong entry level workforce, as shown by employers' willingness to re-engage with current interns and take on additional interns in 2018

Next Steps

After a successful pilot of 10 interns among seven employers, our next step is to expand the program. For the summer of 2018, we have set the following goals:

- Expand the program to 20 internships
- Begin developing **High School Internship Industry Partner Guidelines**
- Begin developing formal **Intern Qualification Guidelines**
- Begin codifying the intern interviewing and matching process

The summer 2018 Internship Program is intended as a stepping stone between the pilot program and a more extensive, sustainable, long term internship program.

Internship Project Report

October 2018

Table of Contents

Cyber Prep Internship Program

During the summer of 2017, Cyber Prep offered summer internships for 10 high school students from five school districts at seven companies. The PPCC Cyber Prep team discussed internships needs and requirements with local businesses, worked with teachers to identify qualified candidates, facilitated a four-hour interview intensive involving all parties, and helped match qualified students with companies in need of their skills to form mutually beneficial internship partnerships. At the end of the program, both students and employers were pleased with the experience and all indicated that they would participate again.

In 2018, Cyber Prep expanded summer internship offers to 21 students from five school districts at thirteen companies. The positive responses from both industry and students in 2017 incited interest in involvement from CTE directors from more districts than the RAMPS grant was able to facilitate. While the summer 2017 Internship Program was considered highly successful by all parties, many lessons were learned along the way. In response to feedback from employers, several changes were made to both the employer and student side of the internship experience.

Programmatic Changes from 2017

Facilitating Industry Preparedness

The biggest challenges encountered in the pilot year were the unpredicted efficiency of interns and minor difficulties designing projects and hiring minors. In response, Cyber Prep representatives made the following changes to the process:

- Required industry partners to have a well-defined project proposal, and helped prompt project possibilities (See Harris Corporation Student Intern job description in Appendix A).
- Encouraged industry partners to take on interns in pairs so that the students would have a peer with whom to learn and experience the workplace
- Guided industry partners through the process of employing minors
- Gave industry more flexibility with hours and scheduling of interns
- Hosted an interview/hiring event for all applicants and all industries to determine best fit

Facilitating Student Development

The first year revealed that potential interns came to the program with a very broad spectrum of individual skills, it was difficult to predict before making intern/company assignments what skills the companies would be working with. To provide a baseline for all interns, Cyber Prep facilitated a week of half-day orientation sessions prior to the beginning of the program; additional technical training and networking opportunities

were provided weekly during 2-hour lunch and learn sessions for the duration (4 weeks) of the program. Orientation and Lunch-n-Learns provided the following:

- Soft skills training (developed by a third party contractor)
- Weekly soft skills workbook assignments (developed by CyberPrep teachers)
- Technical skills training (planned and taught by active PPCC IT/Cybersecurity college students) including:
  - ✓ Password cracking
  - ✓ Hashing
  - ✓ Standard Industry Tools/Environments
  - ✓ Social Engineering
  - ✓ Cisco and LINUX courses
- Exposure to industry roles, locations, and vocabulary through site visits and guest speakers

In addition to building the skills of the students, these sessions helped build the interns into a cohort. They were able to meet peers across districts and discuss their widely different experiences. This provided the students with a support network as well as conversational exposure to the many aspects of cybersecurity in Colorado Springs. The following table summarizes the industry partners involved, number of interns each company employed, and the activities those interns performed.

Employer	Interns	Activities
Colorado College	1	• Reviewed security logs for problems/issues • Assisted in verifying compliance requirements • Remained updated on policies, requirements, advisories, alerts, and vulnerabilities relevant to the college and its platforms/software
District 2 IT	2	• Installed district software images • Maintained and repaired PCs • Interfaced with technicians to keep inventory up to date • Updated maintenance records • Prepared to act as student assistants in the upcoming school year
Eclypses	2	• Created a white noise random number generator • Created a hacking Raspberry Pi • Trained to locate and log network bugs

Employer	Interns	Activities
Harris	1	• Documented inventory • Created new user accounts • Applied system patches • Supported system backups and restoration from backups • Updated cybersecurity documentation • Assisted with system audits
SAIC	2	• Built cyber range in a box (CRIB) • Designed, supported, managed, tested the CRIB • Created proof of concept, pilots, analysis, and documentation of the CRIB
SBDC	2	• Assisted in the development and implementation of a cybersecurity planning guide for small business needs • Researched cybersecurity components • Communicated with small business members to asses needs
Summit	1	• Shadowed cybersecurity and IT professionals • Presented capability demonstrations to leadership and customers • Wrote status/progress reports
Spark Mindset	2	• Collaborated with product management to define and implement training/education solutions • Assisted in content development • Designed and executed testing strategies • Learned and coded game training scenarios in Unity
System High Corporation	2	• Verified network configurations and operations • Reviewed and updated corporate IT and cybersecurity procedures • Prepared corporate phishing test campaign • Updated corporate cybersecurity training materials • Updated web content • Researched O365 pest practice and used research to make data process management recommendations
PPCC- ITSS	1	• Provided general IT/Security support • Answered help tickets and calls • Closed work order requests • Maintained logs and documentation
RIM Technologies	2	• Receive introduction to business conduct and protocol • Shadowed cybersecurity and IT professionals

Employer	Interns	Activities
		• Attended corporate staff meetings • Provided written status/progress reports • Presented/supported demonstrations to leadership/customers
Barnett Engineering & Signaling Laboratories LLC	2	• Installed/updated software • Performed daily machine maintenance • Provided user assistance resolving technical issues • Maintained company software/hardware needs
Andante	1	• Gathered website requirements • Wrote and presented website design proposal • Designed website prototype • Presented website to Officer Board, incorporate feedback into fully functional website • Deployed Website • Observed community dynamics and report on social engineering opportunities • Identified the scope of personal information of high profile community members that was relevant to events yet safe to disclose publicly • Set up and configured sound system equipment and documented the elements and procedures

Table 1: Summary of Summer Internships 2018

Impact of Internships on Industry Partners

Across the board, employers, while curious to see internship results, were reluctant to even talk about employing high school students at first. However, through the interview process, progress reports, and closing event, every employer was impressed with the quantity and quality of student work. One of the largest barriers of entry was the lack of Security Clearances. Due to the length of time background investigations require and DoD processing backlogs, it is impossible to acquire a clearance for an employee in the short time span of a summer internship. This forced employers to analyze the tasks that could be accomplished by an employee without a clearance. While not part of the traditional paradigm of employing a cleared workforce, employers found that there are a wide variety of entry level tasks that can be reassigned to intern level employees.

Examples include:

- Assembling servers
- Organizing server rooms
- Labeling equipment

- Sending emails to coordinate with external partnerships
- Creating (programming or writing) training materials
- Formatting machines
- Entering roster/Business hierarchy system data
- Creating/maintaining web presence
- DoD Regulation 8570 PC Compliance
- Configuring Raspberry pi units
- Troubleshooting external or internal customer issues

These tasks also enable employers to experience new employees' skills, ethics, catchability, learning aptitude, and performance without acquiring them for a clearance based project. For the 2017 Intern year, two interns were retained on payroll and submitted for clearances. Two of the summer 2018 interns will be remaining with their companies for the school year. Others were invited back for subsequent summer internships as their academic careers progress. It is too soon to tell if any of these relationships will result in a clearance sponsorship.

Integrating new employees into the cleared workforce is vital for the continued success of cybersecurity. However, it is a resource intensive, time consuming process that most employers would prefer to bypass in favor of luring another already-cleared individual away from their current assignment and into a new role. In this way, contracted employees are frequently traded among contracting firms. Providing industry partners this perspective on new, entry-level employees mitigates some of the risk of submitting a new employee for clearance as they have already had an introduction to their capabilities, developed a relationship and potentially garnered employee loyalty.

Next Steps

After two successful pilot years, the CyberPrep internship program will now be turned over to the region's school districts to manage. Ten of the area's 17 school districts have formed a new organization called the Pikes Peak Business and Education Alliance (PPBEA), which has started to engage employers to develop internship programs across these 10 districts, much like we accomplished with CyberPrep. The CyberPrep team will work with the participating employers and the PPBEA to see if a formal handoff can be arranged during this school year.

Appendix A – Sample Internship Job Description

Cyber Security Project

There are so many aspects of cyber security so instead of one project we are giving you three projects to choose from! If you finish one project no worries you can choose another one.

Create a White Noise Random Number Generator

Tired of all those random number generators that just feel the same? Then take a chance at making a difference towards better randomness. The goal of the White Noise Random Number Generator is to be able to create an almost truly random number based on an audio sample taken in the room and converted into numbers. You'll get to work with a Raspberry Pi and the Python programming language to create a program to produce a random number on demand. Laugh, cry, and talk your way to creating something other developers will actually be able to incorporate! Robert R. Coveyou said it best, "The generation of random numbers is too important to be left to chance."

Create a Hacking Raspberry Pi

Ever wondered how it really feels to be Mr. Robot? Here's your chance to find out. Using a Raspberry Pi create a hacking station that can watch traffic on devices, crack wi-fi passwords, spoof accounts, create a fake network and intercept packets. You'll get to work with a Raspberry Pi, Kali Linux and a myriad of tools to experiment with hacking. Do you have what it takes to hack Evil Corp?

Learn How to Be a Bug Bounty Hunter

Ready to be a bug bounty hunter (AKA a hacker who is paid to find vulnerabilities in software and websites)? Than we have the project for you. Learn what it takes to be a bug bounty hunter! No need to change your name to "Dog" unless you want to. Pass on the information you learn to your teammates with weekly briefings.

Appendix E: sudoCYBER Starter Guide

Sudo Cyber

CTSO Starter Guide

Cyber Career & Technical Student Organization Starter Guide 2018-2019

A handbook to assist teachers and districts in establishing a cyber CTSO for the STEM classroom.

Introduction

Dear CTE Educator,

The career and technical student organization (CTSO) is regarded as an integral part of career and technical education (CTE). Extracurricular student organizations play an important part in preparing students to become productive citizens and to assume roles of leadership in their communities. Educators have found that the CTSO is a powerful instructional tool that works best when it is integrated into the career and technical education curriculum.

Cybersecurity CTE courses and programs have been rapidly developed in middle and high schools in response to the critical demand for a skilled workforce in the state, region, and country. Through a grant from the National Initiative for Cybersecurity Education (NICE), a program within the National Institute of Standards and Technology (NIST), the CyberPrep program was formed by Pikes Peak Community College (PPCC). CyberPrep has create a regional ecosystem composed of representatives from PPCC, regional public school districts, regional businesses, and the National Cybersecurity Center which is based in Colorado Springs. Through the CyberPrep program, these organizations have collaborated to develop and launch programs to stimulate student interest in cyber careers, CTE education programs, and internship programs. As existing national CTSOs lack focused programming in cyber, the Sudo Cyber student organization has been created to support the adoption of cybersecurity school curriculum. Educators have recognized the need for a CTSO developed to specifically meet the needs of students interested in cybersecurity.

The Sudo Cyber CTSO and this Starter Guide were created under the CyberPrep program through the collaboration of PPCC Workforce Development, Colorado Springs School District 11 and the National Cybersecurity Center.

The National Cybersecurity Center (NCC) in Colorado Springs, CO, provides cybersecurity leadership, services, and training to a growing ecosystem of citizens that are paying attention to the cyber needs of our nation. The NCC's commitment to workforce development highlights the importance of education initiatives that serve to build and strengthen those with cyber knowledge, skills, and abilities that will help to meet industry and government demand for talent. The NCC has partnered with Colorado's CyberPrep group, including educators from Colorado Springs school districts and Pikes Peak Community College as well as regional industry employers that acknowledge the workforce development needs in cybersecurity.

Sudo Cyber will be an important resource to help students turn their interest in finding and fixing security breaches and protecting our mobile, flexible, and connected ways of life into meaningful career paths. Students that participate in Sudo Cyber will learn about careers that are in high demand, provide high pay, encourage lifelong skill development, are highly dynamic, are transferrable across all industries and organizations, and serve a higher purpose as the digital line of cyber professionals is increasingly recognized and appreciated as an important and meaningful vocation.

This starter guide is meant to be a handbook that provides teachers with an easy starting point for establishing a cyber-focused Career & Technical Student Organization chapter at your school or institution. Good luck with your Sudo Cyber CTSO!

Why is a Cybersecurity CTSO necessary?

Because the skills gap in cybersecurity talent represents a critical regional and national imperative, there is a strong need for opportunities for students to learn about cyber pathways while developing their knowledge, skills, and abilities in a fun, extracurricular environment. Effective Career and Technical Education Student Organizations present students with the chance to learn about diverse career opportunities within the associated field, and a cyber CTSO will keep up with the latest developments in the field of technology.

Cybersecurity is more than the prevue of information technology departments and technologist, it is a *Domain* encompassing every organization, private or public sector, existing at every level and function within an organization. Single individuals, large organizational departments, and huge national divisions are all part of the ecosystem that requires cyber attention. As technology becomes increasingly integrated into our systems, infrastructure, and lifestyle, we have become more dependent on it. This dependency creates a need for a population with the knowledge, skills, and abilities to meet the regional and national imperative for cyber talent. A significant workforce gap exists while education strives to catch up with industry demand for workers with the interest and foundational skillsets to consider a diverse set of career opportunities. Rapid innovations in technology demand that cybersecurity solutions are constantly expanding and evolving, requiring vigilance on the part of consumers of technology as well as those that understand and work with technology on a daily basis. Existing CTSOs do not holistically address the field of cybersecurity. A CTSO focused on cyber will offer students a depth and breadth of opportunities to observe, learn, interact, explore, collaborate, network, and build skills in this vast and critical field. The national CyberPatriot competition is integrated into the CTSO and will expand the scope of cyber events.

What's in a name?

How do you name a new CTSO? You ask the students! The NCC and our partners worked with high school and middle school students in a naming and branding exercise. The result? **Sudo**, the one command to rule them all. Pronounced like "sue dough," it stands for "super user do!" For those that know the open-source operating system Linux, a system administrator (or power user) has sudo as one of the most important commands in their arsenal. Utilizing the sudo command is much better than logging in as root or using the su "switch user" command. Sudo allows users to run programs with the security privileges of another user, by default as the superuser. System administrators can give certain users or groups access to some or all commands without those users having to know the root password. It also logs all commands and arguments so there is a record of who used it for what, and when the action happened. The sudo command also makes it easier to practice the principle of least privilege (PoLP), which is a computer security concept that helps control system access and potential system exploits and compromises.

How will a cyber CTSO benefit a school?

Sudo Cyber offers students the chance to gain exposure to and explore the range of careers available to them in cybersecurity while building skills that complement their classroom learning. They will discover the important roles played by non-IT elements within organizations and begin to understand how workers at all levels of businesses and organizations contribute to the maintenance of safe security postures.

The Sudo Cyber CTSO supports information technology, cybersecurity, and computer science CTE programs and provides an additional platform for the development of problem-solving and critical thinking skills. This CTSO also benefits a school as it will be part of a network of regional cybersecurity academic and business organizations that are committed to cyber education and opportunities for students. Participating students will be able to take advantage of rigorous and challenging learning opportunities outside the classroom, which will in turn strengthen their learning in other high school academic programs. Simple to implement, Sudo Cyber meets the requirements for CTE program approvals.

What does a cyber CTSO look like?

Founded in the 2018-19 school year, Sudo Cyber is a local, school-based student organization with a structure and operation aligned with traditional CTSOs. Cyber CTSOs utilize the Sudo Cyber name, logo, and colors (red, white, and blue). The organization utilizes the school's (or district's) CTE program Advisory Council. Student officers participate in a regional Fall Leadership Conference and all Sudo Cyber members attend the Careers and Skills Conference in the Spring. Students benefit from networking opportunities with other regional teams as well as local industry partners. While there are no national or regional CTSO membership fees at this time, student member dues are at the discretion of the local school Sudo Cyber CTSO.

Steps to Implementation of the Sudo Cyber CTSO

A school, district, or sponsoring teacher (or a pair of teachers, or a group of teachers) identifies and understands the need for a Career and Technical Education Student Organization that focuses on cyber and cybersecurity. Each CTSO has a constitution and/or set of bylaws which outlines rules for the organization, including how membership in the CTSO is determined. To be a viable CTSO, the organization must be available to ALL students participating in the program area. The following steps should be taken:

1. Become familiar with the Sudo Cyber Starter Guide
2. Recruit student members
3. Hold first meeting and elect student officers
4. Adopt the bylaws outlined in the starter guide (or create chapter bylaws); the bylaws should be reviewed every year for relevancy and updated as needed; print the set of bylaws being used by your CTSO and keep them in a file folder or binder tabbed and marked "Bylaws" so that they are available to refer to as needed.
5. Schedule regular meetings
6. Establish a Program of Work for the chapter
7. Join the network of other Sudo Cyber chapters
8. Participate in conferences, competitive events, and collaboration with other chapters
9. Join CyberPatriot
10. Track progress of events / activities for the school year; document organizational activities for review in future years

Resources

COLORADO / CTE RESOURCES	
Colorado CTE Website	http://www.coloradostateplan.com/
Colorado CTSO Websites	http://www.coloradostateplan.com/ctso.htm
CCCS General Procedures	https://www.cccs.edu/sp-3-125c-general-computer-and-information-systems-procedures/
Pikes Peak Community College	https://www.ppcc.edu/cyber-defense-center/resources
CYBER PATRIOT RESOURCES	
CyberPatriot (AFA)	https://www.uscyberpatriot.org/
CyberCamp (AFA)	https://www.uscyberpatriot.org/special-initiatives/afa-cybercamp-program/program-overview
GENERAL / NATIONAL RESOURCES	
NICE Framework	https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
National Cybersecurity Center	https://cyber-center.org/
National Center for Systems Security and Information Assurance	http://www.cssia.org/
National Cybersecurity Framework	https://csrc.nist.gov/publications/detail/nistir/8193/draft
STUDENT / TEACHER RESOURCES	
Stay Safe Online	https://staysafeonline.org/
Hacker High School	http://www.hackerhighschool.org/home.html
Cyber Degrees Resources	https://www.cyberdegrees.org/resources/the-big-list/
Cyber Degrees General Info	https://www.cyberdegrees.org/
ICT Essentials Suite	http://www.ictcertified.com/ict-for-schools/schools-overview.php
National Cyberwatch Center Curriculum	https://www.nationalcyberwatch.org/programs-resources/curriculum/
CAREER RESOURCES / PROFESSIONAL ORGANIZATIONS	
AFCEA	https://www.afcea.org/site/
CompTIA	https://www.comptia.org/
ISSA	https://issa.site-ym.com/default.aspx
IEEE	https://cybersecurity.ieee.org/
ISC2	https://www.isc2.org/
US Dept of Labor Apprenticeships	https://www.dol.gov/apprenticeship/
CareerWise	https://www.careerwisecolorado.org/
Jobs in Cybersecurity	https://www.cyberdegrees.org/jobs/
SudoCyber CONTACT INFORMATION	Info@sudocyber.org

Bylaws

Recommended
Sudo Cyber CTSO Bylaws

ARTICLE I
Name

The official name of this organization shall be "Sudo Cyber Career & Technical Student Organization," also known as the Sudo Cyber CTSO or simply Sudo Cyber.

ARTICLE II
Mission

The Sudo Cyber CTSO will prepare students for careers in the cyber industry through education and leadership opportunities.

ARTICLE III
Purpose

The primary purpose of Sudo Cyber is to serve the needs of its members and strengthen the cyber classroom instruction. This will be done through the following efforts:

1. Foster student interest and enthusiasm for the pursuit of cyber careers.
2. Expose students to the range of career opportunities in cybersecurity and requirement for all business function to participate in maintaining an effective security posture.
3. Expose students to the post-secondary degree and certification programs available to them.
4. Create an ethical cyber culture.
5. Further explore and exercise cybersecurity knowledge and skills in real-world applications.
6. Engage with industry representatives.
7. Develop the critical thinking and problem-solving skills required to defend in a continuously changing cyber domain.
8. Foster the development of leadership and teamwork skills.
9. Foster the development of communication skills.
10. Establish patriotism, citizenship, and sense of community as essential principles.

ARTICLE IV
Organization

Section 1. Sudo Cyber is a local CTSO for cyber, cybersecurity, and related Career and Technical Education programs.

Section 2. A local program advisory committee of industry, educational, management, and labor leaders will serve as an advisory council for the CTSO.

Section 3. The Sudo Cyber Chapter is a group of students involved in the CTSO. The "chapter" could be considered any of the students who are currently enrolled in or who have been enrolled in a CTE cybersecurity or technology program and have signed up to be part of the organization.

ARTICLE V
Membership

Membership composition:

Sudo Cyber is an organization of, by, and for students who are or have been enrolled in a secondary or post-secondary Career and Technical Education cybersecurity or technology program.

ARTICLE VI
Industry Guidance

Industry guidance will be provided by the local advisory council.

ARTICLE VII
Membership Fees

Fees will be determined by the local chapter.

ARTICLE VIII
Student Offices

Section 1. Sudo Cyber student offices will consist of four elected members who will be elected by the general membership of the Sudo Cyber CTSO and be overseen by the advisor.

1. The student offices shall be: President, Vice President, Secretary, and Treasurer.
2. The President runs the meetings.
3. The Vice President assumes parliamentarian duties and the role of the president if the president is absent.
4. The Secretary takes, transcribes, distributes, and stores minutes.
5. The Treasurer establishes and maintains a chapter budget and manages fundraisers.

Section 2. The term of each student office will last for a period of one school year.

Section 3. Each student officer candidate shall be a person who is in good standing within Sudo Cyber and who is currently or has been enrolled as a student in a CTE cybersecurity, technology, or related course or program.

1. For a student officer candidate to run for office, the application process and selection will be determined by a vote of the local chapter membership.
2. The duties of the student officers shall be specified in these Bylaws.

Section 4. Duties of the Sudo Cyber CTSO student officers include:

1. Sudo Cyber student officers shall make themselves available, as necessary, to promote the general welfare of the Sudo Cyber CTSO.
2. Sudo Cyber student officers shall represent the CTSO at the local CTSO Advisory Council meetings.
3. Sudo Cyber student officers should complete the roles of their offices and their chapter's program of work.

a. Program of Work is the chapter's plan for activities for the year.
b. Each Program of Work has the following components:

i. Professional Development
ii. Social Activities
iii. Financial Leadership Activities
iv. Employment-related activities
v. Community Service/Service Learning
vi. Public Relations

c. Chapters should keep records of the Program of Work planned and completed for each school year

ARTICLE IX
Meetings

Local Chapter meetings will be held per the Sudo Cyber CTSO Chapter's Program of Work.

ARTICLE X
Finances

Each chapter of the Sudo Cyber CTSO will follow their district's financial and accounting policies.

ARTICLE XI
Local Governance

The CTSO Advisor and the District CTE Director will provide guidance to the Sudo Cyber CTSO.

ARTICLE XII
Logos, Emblems, and Colors

Section 1. Name and branding for the cybersecurity CTSO is important for growth. The logo, emblems, and colors developed for the Sudo Cyber CTSO is as provided by the founding chapter(s).

Section 2. While using the main Sudo Cyber logo and colors (red, white, and blue) for primary marketing/branding purposes (for instance, on t-shirts, fliers, posters), chapters may develop an additional logo, emblem, or color scheme that may, for instance, match their local school colors. This additional logo or color scheme must retain the name Sudo Cyber and should only be developed by local chapters in accordance with their high school policies. Any additional logos, emblems, or color schemes should represent the cybersecurity industry as they are associated with CTE cyber programs.

ARTICLE XII

Parliamentary Authority

The rules contained in the current edition of **Robert's Rules of Order, Newly Revised,** shall govern the organization in all cases to which they are applicable and in which they are not inconsistent with these Bylaws and any special rules the organization may adopt.

ARTICLE XIV

Amendments

Section 1. These Bylaws may be amended and/or repealed at any local chapter meeting of the Sudo Cyber CTSO by two thirds vote of all the members.

Section 2. Proposal for Amendment: Any proposal from members on amendments must be in writing and filed prior to the chapter meeting where the vote shall take place. Before suggesting an amendment, it must be discussed with the CTSO Advisor and officers of the chapter.

Section 3. A copy of the Amendments will be kept on file with the district CTE Director.

ARTICLE XV

Dissolution

In the event of dissolution of a local Sudo Cyber CTSO chapter, all debts must be paid, and the remaining money shall be donated to the high school's (or postsecondary institution's) scholarship fund or donated to the school as the members see fit.

Chapter Sponsors, Teachers, Administrators:
Please notify us that you have started a Sudo Cyber chapter at your school.

- Gretchen Bliss – Pikes Peak Community College, gretchen.bliss@ppcc.edu
- Mary Graft, Ed.D. – National Cybersecurity Center, mary.graft@cyber-center.org
- Bill Tomeo – Colorado Springs School District 11, william.tomeo@d11.org

Appendix F: Cybersecurity Skills Certification Assessment

CYBERSECURITY SKILLS, CERTIFICATIONS & EMPLOYERS

March 2019

Assessing the Skills Gap in the Colorado Springs MSA

PIKES PEAK COMMUNITY COLLEGE

Contents

Background

Since the spring of 2016, Pikes Peak Community College (PPCC) staff have been developing new programs to train a highly qualified cybersecurity workforce for the region as part of a community-wide effort to grow the cybersecurity ecosystem in the region. In order to determine which programs to offer and why, the staff gathered available data about local jobs. However, because cybersecurity is an emerging field, existing Bureau of Labor Statistics data seriously underestimates the number and types of jobs available in the field. Therefore, PPCC has contracted twice with labor economists from Growth Capital Network, a consultancy focused on economic and workforce analyses, to examine the cybersecurity economy locally and report about the cybersecurity workforce.

The overarching aim of this series of assessments is to better understand the cybersecurity workforce needs so that existing and future training programs can fulfill local business requirements. In the first study, the Growth Capital Network team helped to develop and administer a survey to 31 companies about their workforce, and then conducted a local focus group session to add depth to the analysis and results.

The first study revealed some big knowledge gaps among employers about the specific requirements for the open positions they had available locally since there are thousands of open positions posted at any given time. While many had anecdotal evidence about their hiring preferences and practices, it was clear that there was a need to examine actual job postings to understand the requirements posted for a position versus the preferences of hiring managers and/or talent developers.

The first report drew four important conclusions:

a) entry level positions in cybersecurity are not truly entry level as most “entry level” positions in cybersecurity require at least one or two years’ worth of education plus experience working with hardware, software and computer networks. Hiring managers seem to prefer selecting their best and brightest computer scientists, network administrators, or information systems analysts to groom for cybersecurity careers.

b) cyber-related positions have a very high degree of specificity in their requirements for skills and certifications, yet those qualifications may be unrealistic to find in the available workforce or among those studying to join the profession. This phenomenon seems to describe the crux of the skills gap in cybersecurity locally.

c) the number of posted positions locally is overstated as defense contractors will post requisitions for similar positions, contingent upon the contractor’s ability to land a contract that is currently out to bid. The labor shortage has exacerbated this practice. As a result, the local workforce shortage may not be as big as national data suggests.

d) The need to obtain security clearances places active duty and recently retired (within two years) military at a distinct advantage in hiring, making the development of a home grown talent pipeline of young and/or civilian workers very difficult.

At the same time as this first study was underway, a second cybersecurity project managed by the team at PPCC—Cyber Prep—was working on ways to get teens interested in careers in cybersecurity. In collaboration with area high school educators and administrators, the Cyber Prep team uncovered the need to describe the career pathway in cybersecurity much more specifically in order to answer questions from parents and students. This led the Cyber Prep team to request information about entry level positions available in cybersecurity as a way to make the pathway come alive by describing a student's specific journey to a career in the field.

As a result, PPCC commissioned this second study to examine open positions very closely to help address the four conclusions noted above and give educators accurate descriptions of the career pathway.

This study relied on a technology tool that gathers and analyzes market intelligence called Talent Neuron. Talent Neuron offers "market intelligence technology tools based on large-scale data analytics… (that) provides a clear and normalized view into talent market dynamics across 600 cities, 7,500 companies and 90 roles globally."[1] This study examines on a more granular level the exact skills and certifications listed in local cybersecurity postings during all of 2017 and the first eleven months of 2018 as a way to understand the posted requirements for local cybersecurity positions and examine trends among these positions.

The hope is that this analysis will enable training institutions to tailor their cybersecurity educational programs in an optimal manner that meets the complex employer needs within the Colorado Springs region.

Methodology

Within the Talent Neuron database, it is possible to run queries with a variety of combined search terms and for a specific geographic region. The following criteria were used for the queries analyzed in this report:

1) Colorado Springs MSA
2) "Cyber," "Cybersecurity," and "Cyber" AND "Security" as separate search terms (because different employers use slightly different terminology and there is not one accepted vernacular)
3) All levels of experience
4) All skills
5) All certifications
6) All educational levels
7) All employers
8) All industries

A decision was made to be all inclusive in items 3-8 above so the general landscape of skills and certifications of cyber-related postings could be assessed.

Separate queries were run for all of 2017 and through November of 2018. The relatively lengthy time periods were chosen a) to ascertain trends between the two years, and b) to obtain a sufficient sample size of skills, certifications and employers.

[1] Talent Neuron database accessed 3-5-2019 at www.cbinsights.com/company/talent-neuron

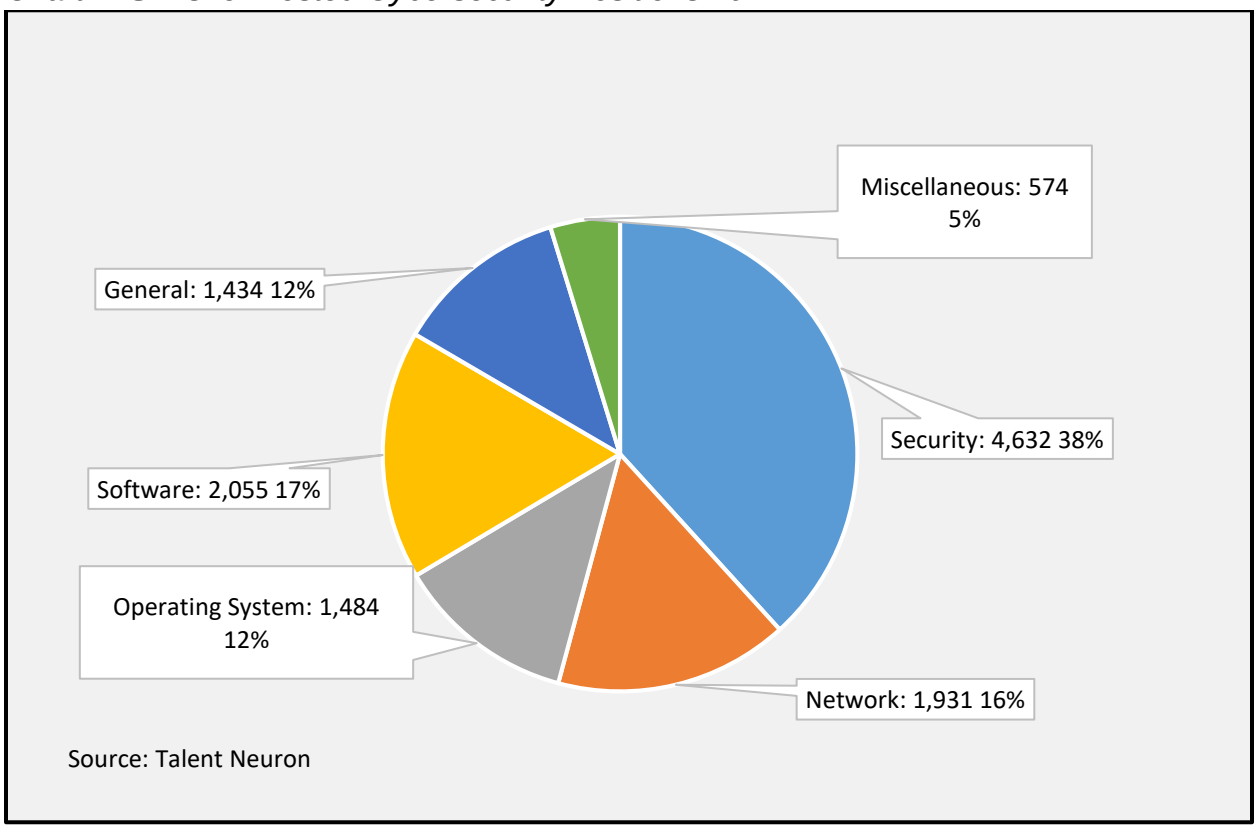
There was enough duplication between the “Cyber” queries and the other two categories, that only the “Cybersecurity” and “Cyber” AND “Security” information was retained and analyzed. In total, this methodology yielded 290 unique job postings in eight companies with a local presence.

Skills

The queries for both years revealed distinct categories, and they are listed below. As the subsequent charts show, there was not much change in the proportion of listed skills for each category from one year to the next.

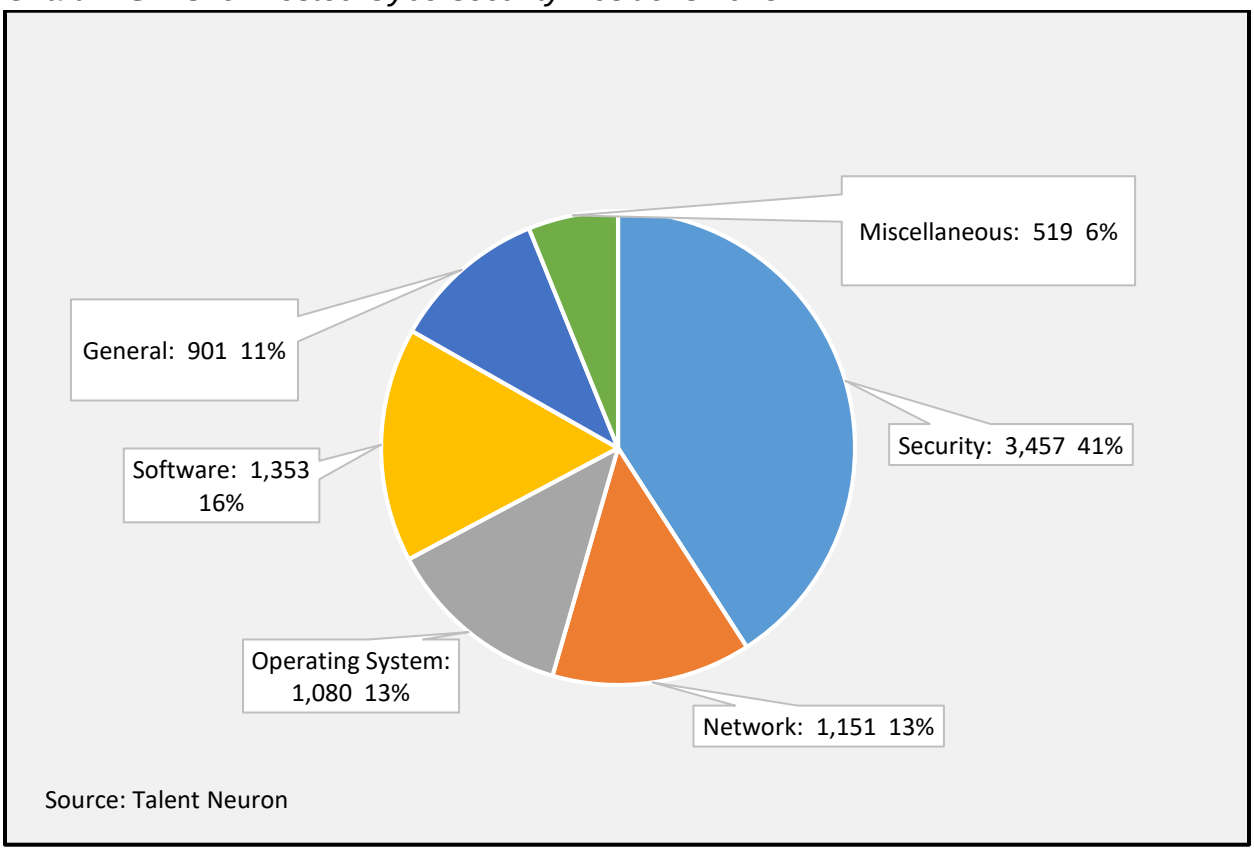
- Security
- Network
- Operating Systems
- Software
- General
- Miscellaneous

Chart 1. Skills for Posted Cybersecurity Positions 2017



The most obvious, general observation is that the vast majority of desired skills revolve around security-related aptitudes. These include cyber-security, information assurance, firewall, information security and a host of other security-type proficiencies. Tables 1 and 2 have the specific breakdown of subcategories in 2017 and 2018 for each of the broader categories represented in the graphs.

Chart 2. Skills for Posted Cybersecurity Positions 2018



Source: Talent Neuron

Table 1. "Cybersecurity" and "Cyber" AND "Security" Skills 2017

Skill Categories and Subcategories	Total	Percent of Total
Security		
Cyber security *(are 46% of all "security" skills listed)*	2,063	
Information assurance *(15%)*	701	
Firewall *(13%)*	593	
Other Security *(28%)*	1,275	
Total Security Skills	**4,632**	**38%**
Network		
Network routers *(20%)*	380	
Network Security *(20%)*	381	
Other Network *(60%)*	1,170	
Total Network Skills	**1,931**	**16%**
Operating Systems		
UNIX *(22%)*	329	
Linux *(42%)*	616	
Other Operating Systems *(36%)*	539	
Total Operating Systems Skills	**1,484**	**12%**
Software		
Microsoft Forefront *(18%)*	363	
Microsoft Office *(20%)*	422	
Other Software *(62%)*	1,270	
Total Software Skills	**2,055**	**17%**
General		
National Institute of Standards and Technology *(24%)*	339	
Other General *(76%)*	1,095	
Total General Skills	**1,434**	**12%**
Miscellaneous	**574**	**5%**
Total Skills	**12,110**	**100%**

Table 2. "Cybersecurity" and "Cyber" AND "Security" Skills 2018

Skill Categories and Subcategories	Total	Percent of Total
Security		
Cyber security *(are 47% of all "security" skills listed)*	1,629	
Information assurance *(15%)*	535	
Firewall *(10%)*	358	
Other Security *(19%)*	645	
Total Security Skills	**3,457**	**41%**
Network		
Network Security *(23%)*	262	
Other Network *(77%)*	889	
Total Network Skills	**1,151**	**14%**
Operating Systems		
Linux *(41%)*	439	
Other Operating Systems *(59%)*	641	
Total Operating Systems Skills	**1,080**	**13%**
Software		
Microsoft Forefront *(18%)*	238	
Microsoft Office *(26%)*	355	
Other Software *(56%)*	760	
Total Software Skills	**1,353**	**16%**
General		
National Institute of Standards and Technology *(37%)*	332	
Other General *(63%)*	569	
Total General Skills	**901**	**11%**
Miscellaneous		
Simulation and Modeling *(41%)*	213	
Other Miscellaneous *(59%)*	306	
Total Miscellaneous	**519**	**6%**
Total Skills	**8,461**	**100%**

Although there was a high degree of consistency in the desired skills between the two years, Table 3 shows the new skills listed in the 2018 job postings that were not listed in 2017. This

potentially shows the evolution of the skills for cyber-related positions and/or the increasing sophistication of employers in terms of how accurately they post the needed skills.

Table 3. New Skills in 2018 Job Postings

Specific Skill	Frequency
Microsoft Power Point	164
Public Key Infrastructure	122
Python	57
Penetration Testing	50
Risk Assessment	45
JavaScript	38
Transmission Control Protocol	37
Windows Servers	36
Security Testing	33
Enterprise Architecture	29

Certifications

Certifications are another key component in understanding employer needs. Knowing the exact certifications in job postings enables higher education institutions and training organizations to properly train and certify students with credentials that will be meaningful to local employers.

This granular examination of desired certifications is perhaps the most telling aspect of this study. First and foremost, the vast majority of desired certifications are for security clearances (see Charts 3 and 4 below). This is likely a region-specific anomaly related to the high presence of US Department of Defense work. Nonetheless, it is key information in terms of understanding the attributes that jobseekers in cybersecurity absolutely need in order to qualify for the preponderance of open (cyber) positions.

Chart 3. Certifications, Non-Certifications & Clearances, 2017

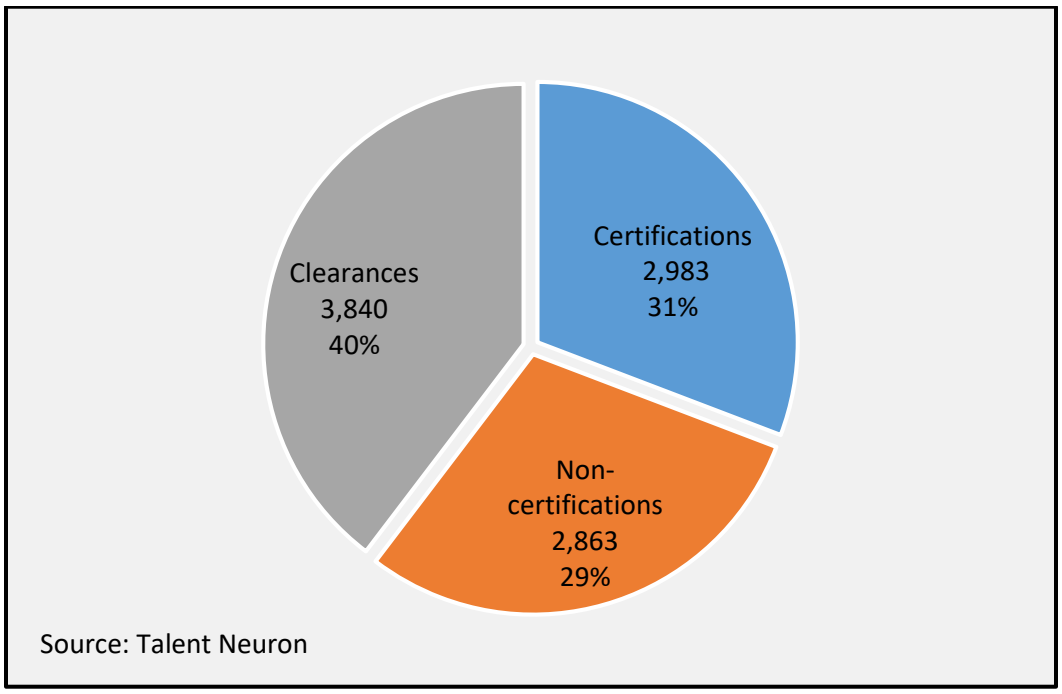
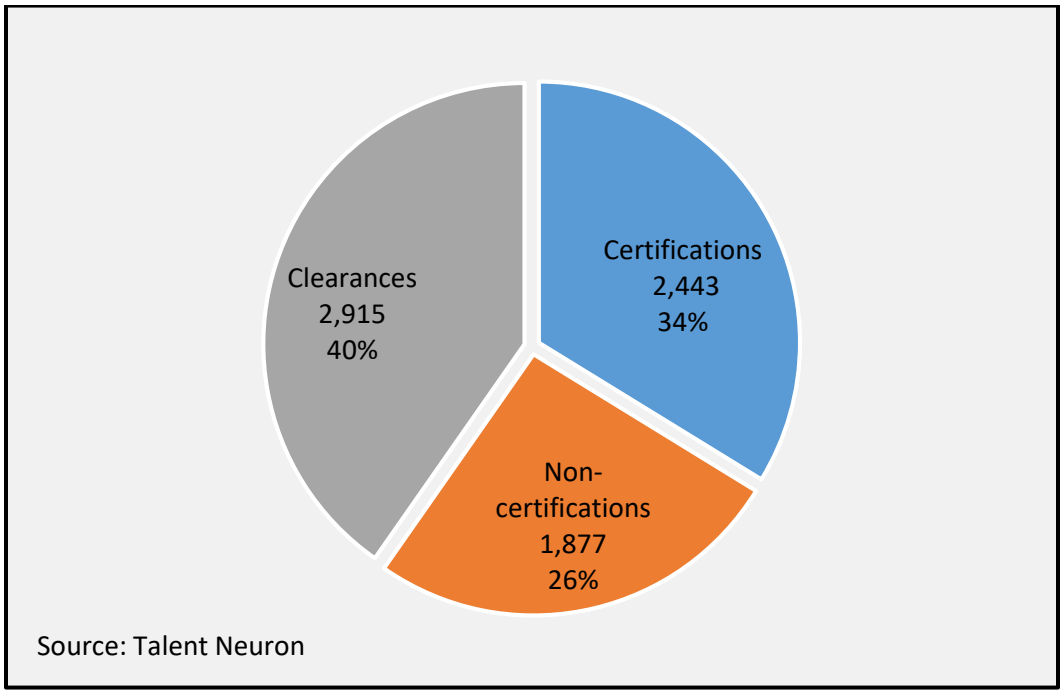


Chart 4. Certifications, Non-Certifications & Clearances, 2018



In addition, there appears to be confusion about what employers are labelling as certifications and what are truly considered certifications by higher education institutions and training organizations. This may be due to either a) a misunderstanding by industry of what certified

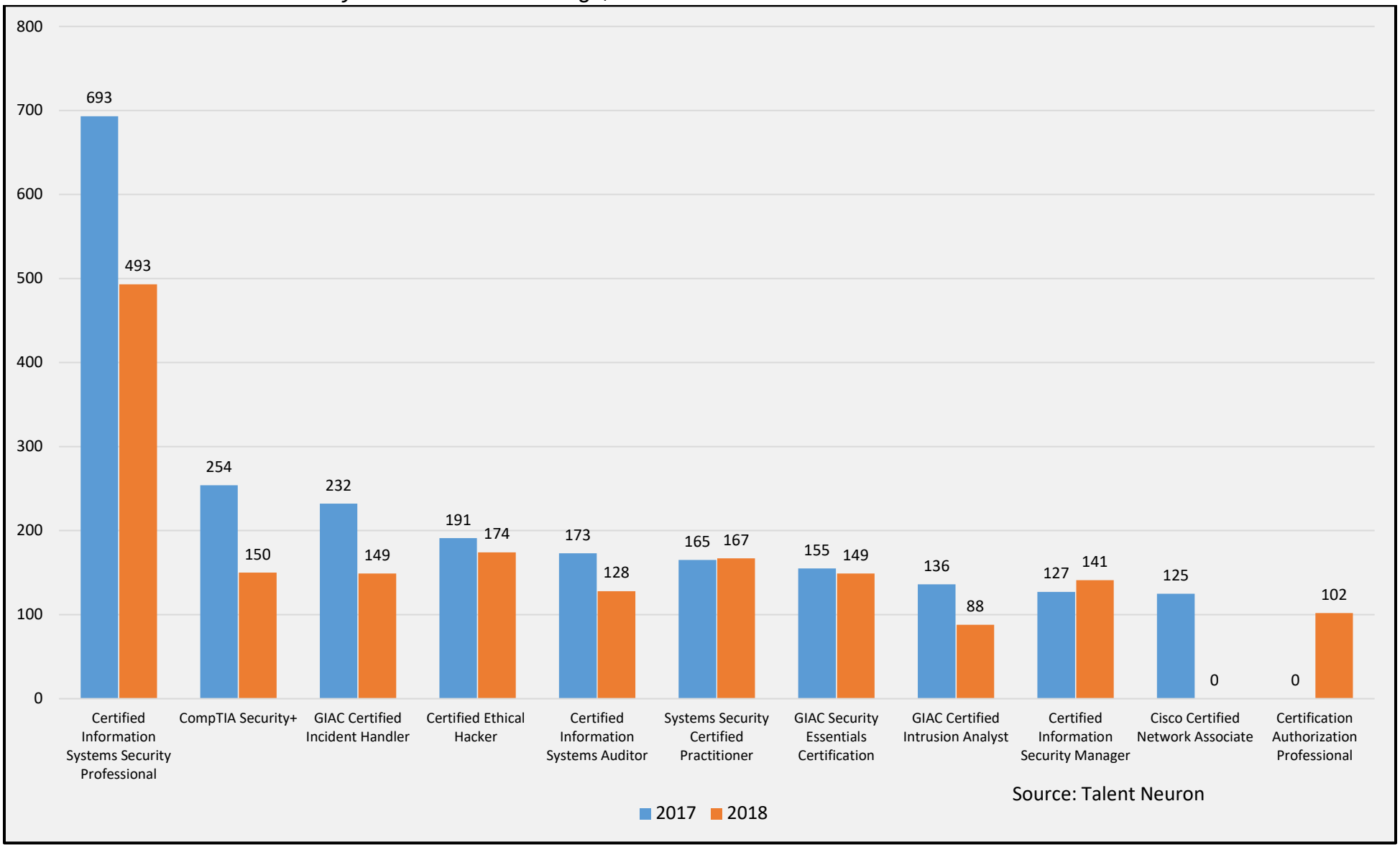
credentials are in existence, or b) a simple mislabeling by employers of desired proficiencies that are not truly certifications. The latter may also indicate that cyber-related job postings should have additional categories to help clarify specific employer needs. As the charts above indicate, academia and jobseekers could benefit from having at least two additional categories in job postings perhaps labelled “Clearances” and “Cyber-related Requirements.”

Since actual certifications are the first point of interest for the purposes of informing future training programs, Table 4 below shows the top ten certifications listed in the job postings for 2017 and 2018. Chart 5 visually represents these data. The numbers above each bar represent the number of times the certification showed up in a listing in the respective years.

Table 4. Actual Certifications for Cybersecurity and “Cyber” AND “Security Job Postings

2017			2018	
Certification	**Frequency**		**Certification**	**Frequency**
Certified Information Systems Security Professional	693		Certified Information Systems Security Professional	493
CompTIA Security+	254		Certified Ethical Hacker	174
GIAC Certified Incident Handler	232		Systems Security Certified Practitioner	167
Certified Ethical Hacker	191		CompTIA Security+	150
Certified Information Systems Auditor	173		GIAC Certified Incident Handler	149
Systems Security Certified Practitioner	165		GIAC Security Essentials Certification	149
GIAC Security Essentials Certification	155		Certified Information Security Manager	141
GIAC Certified Intrusion Analyst	136		Certified Information Systems Auditor	128
Certified Information Security Manager	127		Certification Authorization Professional	102
Cisco Certified Network Associate	125		GIAC Certified Intrusion Analyst	88

Chart 5. Actual Certifications in Cyber-related Job Postings, 2017 & 2018



As was discussed in the skills section, it also can be useful to examine any new certifications that surfaced in 2018. Table 5 below shows the seven new skills that emerged in the 2018 job postings.

Table 5. New Certifications in 2018 Job Postings

Specific Certification	Frequency
GIAC Certified Penetration Tester	34
Comp TIA Advanced Security Practitioner	32
Information Systems Security Management Professional	23
CMMI Level 3 Certification	21
Check Point Certified Security Administrator	16
GIAC Information Security Fundamentals	16
Offensive Security Certified Professional	15

Department of Defense 8570 Requirements

The Department of Defense has numerous requirements for cybersecurity employees that are difficult to label. Some might consider them skills while others might consider them certifications. In reality, however, DoD 8570 requirements are specific to the military and they do not necessarily translate well to civilian-type postings. This doesn't mean, however, that these desired qualifications are not important to employers, especially in Colorado Springs where there is an abundance of military, contractual work. The DoD 8570 requirements serve as a key example of the disconnect that can occur between employer workforce needs, and what the existing labor market realities are.

These 8570 requirements are also important to consider because in 2017, this non-certification was listed in job postings 1,626 times. In 2018, the 8570 requirement showed up 1,050 times. Appendix A has the detailed information for these non-certification requirements.

Occupational Groups

Cybersecurity is an issue for virtually every industry simply because of the ubiquitous presence of computers. Hence, there are cyber-related positions listed in most industry categories. In order to better understand what job titles employers are using for their cyber needs, the queries also produced the names of the occupational groups with their respective frequencies. There was not a tremendous amount of deviation between 2017 and 2018 so for simplicity, Table 6 below shows the combined information for both years.

It is worth noting that after the top 10 job titles, the number of times other occupational job titles are mentioned falls off significantly. Hence, these job titles appear to be the ones preferred by local industry when seeking cyber-related talent.

Table 6. "Cybersecurity" and "Cyber" AND "Security" Combined 2017 and 2018

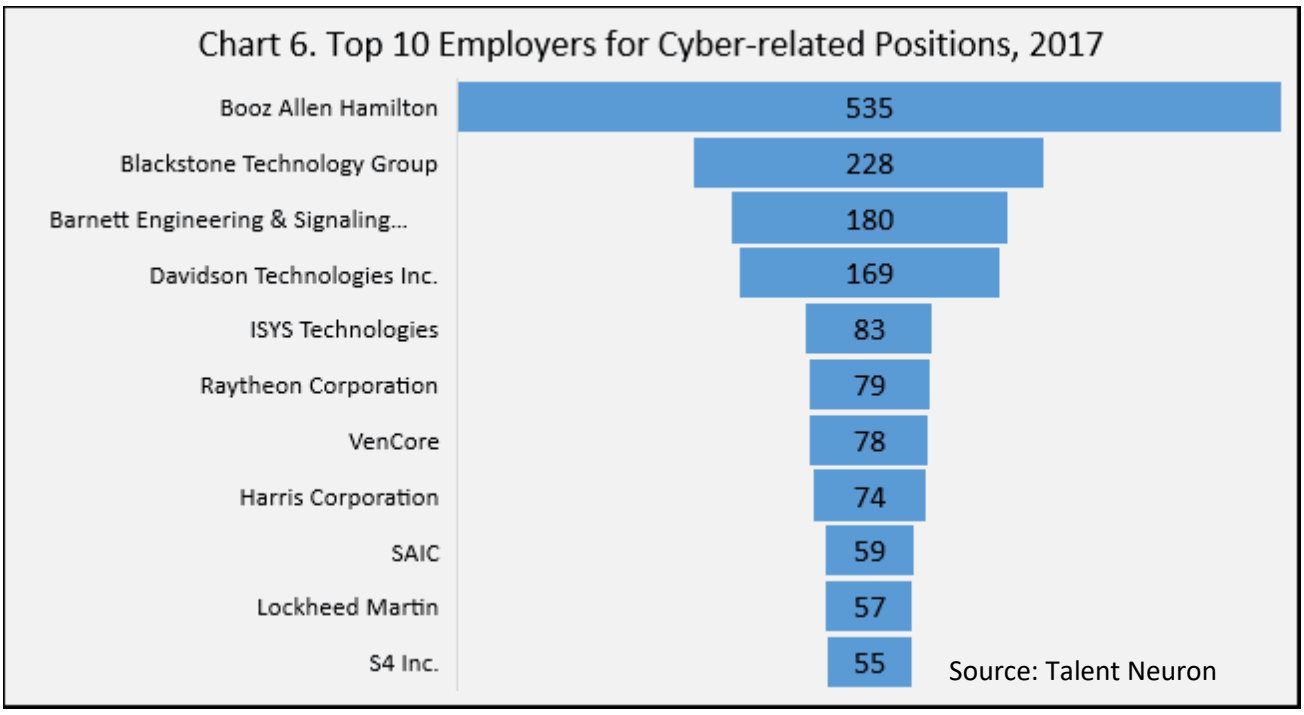
Name	Frequency for Both Years
Information Security Analysts	1,725
Computer Occupations, All Other	541
Network and Computer Systems Administrators	492
Software Developers, Applications	258
Operations Research Analysts	138
Computer User Support Specialists	127
Computer Systems Analysts	124
Software Developers, Systems Software	81
Aerospace Engineers	75
Management Analysts	60

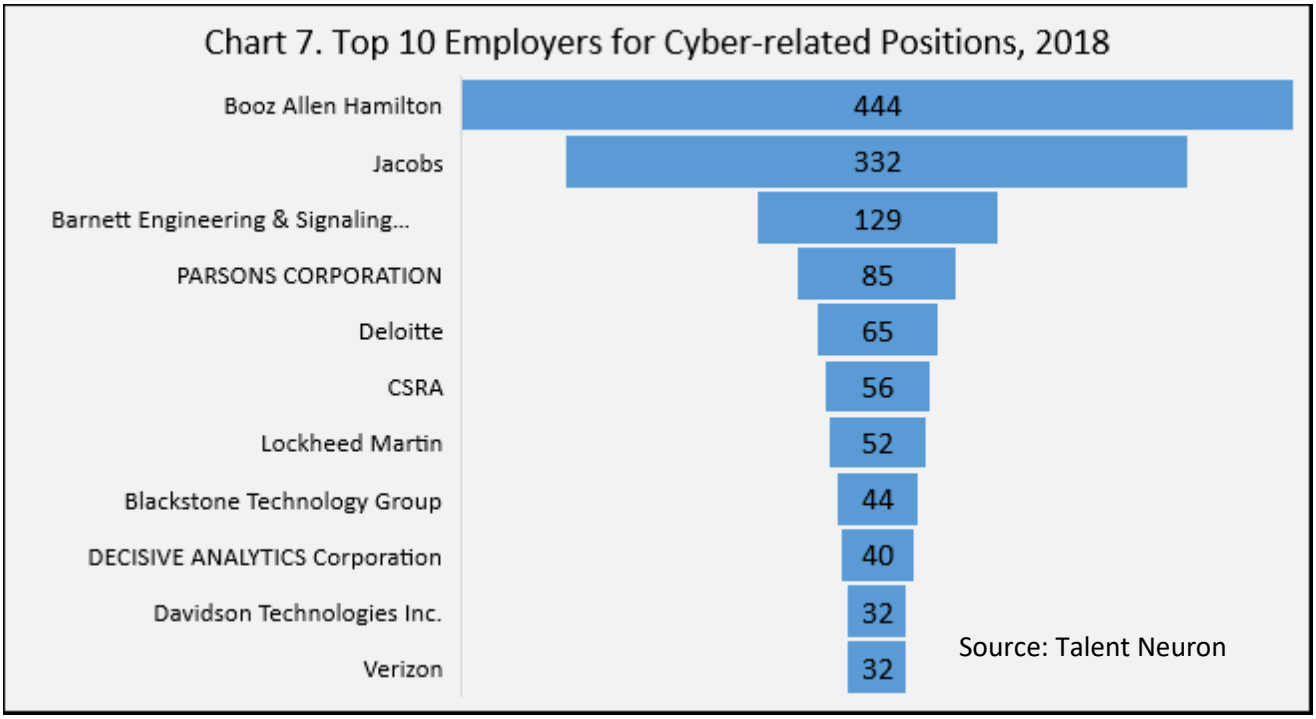
Employers

As was previously mentioned, the high DoD presence in Colorado Springs makes it a somewhat unique community in terms of cybersecurity. The certifications in the job postings showed that many local employers want DoD-specific certifications and/or requirements. Indeed, there are five military installations and the direct military jobs accounted for 17 percent of the total employment in El Paso County in 2017 according to the Colorado Department of Labor and Employment (CDLE). This relatively high percentage may be understated simply because the Bureau of Labor Statistics and CDLE only categorize "military" as those workers who are either directly enlisted in the military and work on base, or who are civilian and work for the military on one of the bases. There is in all likelihood other industry categories that have DoD workers. The civilian "professional and technical" category undoubtedly captures some employment from private consulting firms that do military-related work (hence the understatement within "military" employment).

A look at the local employers with the highest number of job postings in both 2017 and 2018 confirms that much of the demand for cyber-related talent is indeed related to DoD contracts. Charts 6 and 7 show the top ten employers for 2017 and 2018. As in the case of certifications, after the top ten, the frequency of job postings by each employer falls off significantly. Hence, the top ten are good indicators of the largest, local employers in cybersecurity.

As part of the next phase of this work, these employers will be contacted to try and create internship opportunities for local students who are studying within the cyber field and to build a potential apprenticeship program within the PPCC AAS degree in Cybersecurity. Queries were run for each of these top ten employers to capture their specific skills and certifications. This will enable training institutions such as PPCC to tailor their training programs and internship partnerships to the exact skills and certifications demanded by the top cyber employers.





General Comments about the Shortage of Cybersecurity Workers

Information technology now infiltrates every corner of business, large and small meaning that the safety of information is critical to the sustainability of the U.S. as a global economic player. There

are some general trends emerging not only in Colorado Springs, but across the nation that are worth considering as context for this study.

1) Cybersecurity jobs are high paying jobs meaning that closing this skills gap has the significant positive externality of boosting economic development in the regions that have up-to-date training programs for this emerging field.

2) The downside of the high (cyber) salaries means that small businesses cannot typically afford to have dedicated cyber personnel. This logically implies a new and emerging sub-sector of companies that solely address cybersecurity for external, independent companies.

3) These cyber information technology firms can be particularly good resources for higher education institutions in terms of a) providing the latest and greatest information about training needs and b) providing internship opportunities for students who are almost ready to graduate from their (cyber-specific) programs.

4) There is tremendous opportunity to capitalize on the inherent interest in information technology by Millennials and Digital Natives. Local or state efforts in cyber readiness should include mandatory foundations in cyber security as part of middle and high school curricula. These regions will have a comparative advantage in closing this critical skills gap. Such efforts will also provide an opportunity for some youth to have meaningful, high-paying, and high-demand professions.

5) Regions with separated or retired military have an advantage because a high percentage of these newly civilian workers already have some training in cybersecurity and/or have clearances and ethical training that can translate well to the civilian cyber field.

6) Since cybersecurity is a relatively new field with a constantly changing landscape, women may be particularly well suited for training programs. Women often leave the workforce during early adulthood for childbearing and childrearing, but then are great candidates for re-entering the labor force. With the rapid rate of change in cybersecurity, these re-entrants into the labor market could be great candidates for cyber-related training programs. This could present an opportunity to women to pursue high-paying, fulfilling work while also closing the gender gap in terms of STEM professionals and in terms of pay equity. Regions that have cybersecurity training programs can benefit from targeting women.

Conclusion

The complexity of the information technology world is evidenced by the high degree of specific requirements for cyber-related positions. This specificity as well as the changing demands within the cyber field have made the shortage of cyber workers particularly acute. Training institutions must work closer than ever with industry in order to understand the local workforce cyber needs. The level of detail in this report highlights that cyber is complex, and employers need experts who can handle this level of complexity.

For these reasons, communities must closely examine the specific skills, certifications and occupational job titles for the posted cyber positions within their region. This will enable them to have the baseline knowledge of what employer needs are and how employers are articulating

those needs. Next, communities must have strong ties between cyber employers and training institutions whether they are community colleges, IT boot camps, or four-year universities. Training institutions that have a good grasp of skills and certifications have the responsibility to incorporate those skills and certifications into their mainstream IT/cyber educational programs.

Industry has the responsibility to show up when educational institutions request their feedback on current or newly developed curricula. Industry can also contribute by having as many internship opportunities as possible for cyber students. Education experts state that as much as 70 percent of learning occurs through doing making internships in cyber particularly meaningful. Lastly, communities must re-examine skills, certifications and occupational job titles at least once a year in order to stay on top of shifts in the cyber landscape.

Appendix A

DoD 8570 Requirements in 2017 and 2018 Job Postings

Approved Baseline Certifications

IAT Level I (2%)

A+ CE	0
CCNA-Security	47
Network+ CE	0
SSCP	69

IAT Level II (14%)

CCNA Security	47
CySA+	0
GICSP	0
GSEC	149
Security+ CE	150
SSCP	493

IAT Level III (15%)

CASP CE	43
CCNP Security	0
CISA	128
CISSP (or Associate)	493
GCED	32
GCIH	149

IAM Level I (6%)

CAP	102
GSLC	87
Security+ CE	150

IAM Level II (15%)

CAP	102
CASP CE	43
CISM	141
CISSP (or Associate)	493
GSLC	87

IAM Level III (12%)

CISM	141
CISSP (or Associate)	493
GSLC	87

IASAE I (9%)

CASP CE	43
CISSP (or Associate)	493
CSSLP	0

IASAE II (9%)

CASP CE	43
CISSP (or Associate)	493
CSSLP	0

IASAE III (0%)

CISSP-ISSAP	0
CISSP-ISSEP	0

CSSP Analyst (7%)

CEH	174
CFR	0
CCNA Cyber Ops	0
CySA+	0
GCIA	88
GCIH	149
GICSP	0
SCYBER	0

CSP Infrastructure Support (6%)

CEH	174
CySA+	0
GICSP	0
SSCP	167

CSSP Incident Repsonder (6%)

CEH	174
CFR	0
CCNA Cyber Ops	0
CySA+	0
GCFA	0
GCIH	149
SCYBER	0

CSSP Auditor (6%)

CEH	174
CySA+	0
CISA	128
GSNA	38

CSSP Manager (3%)

CISM	141
CISSP-ISSMP	23

So many of the certifications required in the jobs analyzed are based on DoD directive 8570.01 Information Assurance (IA) Workforce Improvement Program. This directive provides *guidance* for the identification and categorization of positions and certification of personnel conducting IA functions within the DoD. These DoD personnel support the DoD Global Information Grid (GIG) per DoD Instruction. The regulation categorizes IA job requirements for each category, specialty, level, and function to enhance protection and availability of DoD information, information systems, and networks. This regulation referred to as “8570” is the “bible” for all government agencies and

contractors when hiring IT professionals. The labeling assigned by the 8570 is often confusing for potential employees because it mixes DoD job classifications with industry certifications.

The 8570 lists certain categories for jobs in a hierarchical manner, bunching industry certifications into DoD categories. As a result, there are numerous certifications for each DoD categorization. For example, to apply to an Information Assurance Management (IAM) Level I position the applicant cannot get an IAM Level I "certification," rather they would be classified as an IAM Level I if they had the CompTIA Advanced Security Practitioner (CASP) OR the SysAdmin, Audit, Network and Security (SANS)/Global Information Assurance Certification (GIAC) Global Security Security Leadership (GSLC) OR the CompTIA Security+ certifications.

Often, job postings will list both the DoD 8570 categories such as IAM Level I and the industry certification such as CompTIA Security+ certifications, which effectively duplicates an application requirement. Potential employees would logically, but erroneously think that the IAM Level I was something different from the CompTIA Security+ certification because they are both listed under certifications in the job posting, when in fact they are the same (duplicative) requirement. These overlaps in certification requirements—using two languages to say the same thing—make determining the true certification requirements for each position challenging. The above chart shows how this confusion plays out. The listings in the chart that are in red are in multiple DoD 8570 categories, so applicants could apply to multiple jobs for which they may not be fully qualified. It also shows how difficult it can be to account for the classification of open positions.

DoD 8570 Requirements			DoD 8570 Requirements		
2017			2018		
Name	**Total**	**% of Total**	**Name**	**Total**	**% of Total**
DoD 8570 Requirement	**759**		**DoD 8570 Requirement**	**668**	
IAT Level 1	**17**		**IAT Level 1**		
CompTIA A+	0		CompTIA A+	0	
CompTIA Network+	0		CompTIA Network+	0	
Systems Security Certified Practitioner	165		Security Certified Network Professional	69	
Cisco Certified Network Associate Security	11		Cisco Certified Network Associate Security	47	
IAT Level 1 Combined Total	**176**	2%	**IAT Level 1 Combined Total**	**116**	2%
IAT Level 2	224		**IAT Level 2**		
CCNA Cyber Ops	0		CCNA Cyber Ops	0	
GIAC Cyber Security Professional	0		GIAC Cyber Security Professional	0	
GIAC Security Essentials Certification	155		GIAC Security Essentials Certification	149	
CompTIA Cybersecurity Analyst+	0		CompTIA Cybersecurity Analyst+	0	
CompTIA Security+	254		CompTIA Security+	150	
Certified Information Systems Security Professional	693		Certified Information Systems Security Professional	493	
Cisco Certified Network Associate Security	11		Cisco Certified Network Associate Security	47	
IAT Level 2 Combined Total	**1,113**	15%	**IAT Level 2 Combined Total**	**839**	14%
IAT Level 3	**214**		**IAT Level 3**		
Certified Information Systems Auditor	173		Certified Information Systems Auditor	128	
GIAC Certified Incident Handler	232		GIAC Certified Incident Handler	149	
GIAC Certified Enterprise Defender	53		GIAC Certified Enterprise Defender	32	
Certified Information Systems Security Professional	693		Certified Information Systems Security Professional	493	
Cisco Certified Network Professional Security	0		Cisco Certified Network Professional Security	0	
CompTIA CASP	44		CompTIA CASP	43	
IAT Level 3 Combined Total	**1,195**	16%	**IAT Level 3 Combined Total**	**845**	15%
IAM LEVEL 1			**IAM LEVEL 1**		
GIAC Security Leadership Certification	76		GIAC Security Leadership Certification	87	
CompTIA Security+	254		CompTIA Security+	150	

Certification Authorization Professional	96		Certification Authorization Professional	102	
IAM Level 1 Combined Total	**426**	6%	**IAM Level 1 Combined Total**	**339**	6%
IAM Level 2			**IAM Level 2**		
GIAC Security Leadership Certification	76		GIAC Security Leadership Certification	87	
Certified Information Systems Security Professional	693		Certified Information Systems Security Professional	493	
Certified Information Security Manager	127		Certified Information Security Manager	141	
Certification Authorization Professional	96		Certification Authorization Professional	102	
CompTIA CASP	44		CompTIA CASP	43	
IAM Level 2 Combined Total	**1,036**	14%	**IAM Level 2 Combined Total**	**866**	15%
IAM Level 3			**IAM Level 3**		
GIAC Security Leadership Certification	76		GIAC Security Leadership Certification	87	
Certified Information Systems Security Professional	693		Certified Information Systems Security Professional	493	
Certified Information Security Manager	127		Certified Information Security Manager	141	
IAM Level 3 Combined Total	**896**	12%	**IAM Level 3 Combined Total**	**721**	12%
IASAE 1 and 2			**IASAE 1 and 2**		
CompTIA CASP	44		CompTIA CASP	43	
Certified Information Systems Security Professional	693		Certified Information Systems Security Professional	493	
Certified Secure Software Lifecycle Professional	0		Certified Secure Software Lifecycle Professional	0	
IASAE 1 and 2 Combined Total	**737**	10%	**IASAE 1 and 2 Combined Total**	**536**	9%
IASAE 3			**IASAE 3**		
Information Systems Security Architecture Professional	12		Information Systems Security Architecture Professional	0	
Information Systems Security Engineering Professional	0		Information Systems Security Engineering Professional	0	
IASAE 3 Combined Total	**12**	0.16%	**IASAE 3 Combined Total**	**0**	0%
CSSP Analyst			**CSSP Analyst**		
Certified Ethical Hacker	191		Certified Ethical Hacker	174	
GIAC Certified Incident Handler	232		GIAC Certified Incident Handler	149	
GIAC Certified Intrusion Analyst	136		GIAC Certified Intrusion Analyst	88	
CyberSec First Responder	0		CyberSec First Responder	0	
CCNA CyberOps	0		CCNA CyberOps	0	
Global Industrial Cyber Security Professional	0		Global Industrial Cyber Security Professional	0	

CompTIA Cybersecurity Analyst+	0		CompTIA Cybersecurity Analyst+	0	
CSSP Analyst Combined Total	**559**	8%	**CSSP Analyst Combined Total**	**411**	7%
CSSP Infrastructure Support			**CSSP Infrastructure Support**		
Systems Security Certified Practitioner	165		Systems Security Certified Practitioner	167	
Global Industrial Cyber Security Professional	0		Global Industrial Cyber Security Professional	0	
CompTIA Cybersecurity Analyst+	0		CompTIA Cybersecurity Analyst+	0	
Certified Ethical Hacker	191		Certified Ethical Hacker	174	
CSSP Infrastructure Support Combined Total	**356**	5%	**CSSP Infrastructure Support Combined Total**	**341**	6%
CSSP Incident Responder			**CSSP Incident Responder**		
GIAC Certified Incident Handler	232		GIAC Certified Incident Handler	149	
Certified Ethical Hacker	191		Certified Ethical Hacker	174	
CyberSec First Responder	0		CyberSec First Responder	0	
CCNA CyberOps	0		CCNA CyberOps	0	
Global Industrial Cyber Security Professional	0		Global Industrial Cyber Security Professional	0	
CompTIA Cybersecurity Analyst+	0		CompTIA Cybersecurity Analyst+	0	
GIAC Certified Forensic Analyst	0		GIAC Certified Forensic Analyst	0	
CSSP Incident Responder Combined Total	**423**	6%	**CSSP Incident Responder Combined Total**	**323**	6%
CSSP Auditor			**CSSP Auditor**		
GIAC Systems and Network Auditor	46		GIAC Systems and Network Auditor	38	
Certified Ethical Hacker	191		Certified Ethical Hacker	174	
CompTIA Cybersecurity Analyst+	0		CompTIA Cybersecurity Analyst+	0	
Certified Information Security Manager	127		Certified Information Security Manager	141	
CSSP Auditor Combined Total	**364**	5%	**CSSP Auditor Combined Total**	**353**	6%
CSSP Manager			**CSSP Manager**		
Certified Information Security Manager	127		Certified Information Security Manager	141	
Information Systems Security Management Professional	0		Information Systems Security Management Professional	23	
CSSP Manager Combined Total	**127**	2%	**CSSP Manager Combined Total**	**164**	3%
TOTAL		**100%**	**TOTAL**		**100%**