California Cybersecurity Workforce Development and Education Strategy (2020-2030): Framework and Recommendations for a California Cybersecurity Career Education Pipeline and Pathway Project (CCCEPPP)

California Cybersecurity Task Force,

Workforce Development and Education Subcommittee

Prepared by Keith E. Clement, Ph.D.

Professor, California State University, Fresno

California Cybersecurity Task Force (CCTF)

Co-Chair, Workforce Development and Education Subcommittee

Prepared for California Cybersecurity Task Force, Co-Chaired by Mark Ghilarducci (Director, California Governor's Office of Emergency Services (Cal OES) and Homeland Security Advisor to the Governor) and Amy Tong (Director, California Department of Technology (CDT) and State Chief Information Security Officer).

September 7, 2020

MESSAGE FROM THE SUBCOMMITEE CHAIR

The California Cybersecurity Education and Workforce Development Strategy Report has been an exciting, innovative, time-intensive, and complicated project/initiative to prepare. The 15 Recommendations contained therein to develop and implement a California Cybersecurity Career Education Pipeline and Pathway Project (CCCEPPP) reflect the input, feedback, and "best practices" of hundreds of participants involved with meetings, webinars, conferences, and in many settings/formats since 2013. The CCCEPPP took years of effort and countless hours to design, develop, and write. This report represents a significant dedication of time and sweat equity to implement coordinated state-level cybersecurity workforce development and education/training "vertical track" pipeline/pathway programs accessible for all Californians in the Golden State.

To achieve cybersecurity education, workforce development, and teaching/research objectives, we develop collaborative partnerships between educational institutions (K-12, colleges, and universities), key public/private sector partners, and Non-Government Organizations (NGOs). We draw industry, educators, and government agencies together to strategize, operationalize, and facilitate statewide cybersecurity education workforce development and education initiatives in California for the equitable upward tech and social mobility of all.

The "orchestration of efforts" and coordination is crucial in designing cybersecurity education and workforce development/training programs that flow seamlessly and transition from one level of education to the next; meets rigorous academic standards and student learning objectives; and furthers the body of cybersecurity theoretical, analytical, and methodological knowledge and skills. But most of all, meets cybersecurity industry and professional communities' (public and private) need for knowledge, skills, and abilities supported by standardized core curriculum and academic standards in fulfilling various position minimum requirements.

Many are interested in the development of a "base-line" template by which quality cybersecurity education and training programs are implemented at the state, local, and regional levels. There are also vigorous movements nationally to develop accreditation bodies in the area of cybersecurity and promulgate academic standards and agreed upon curriculum for these programs and courses. We hope this document assists and supports the accreditation movement in the nascent academic discipline of cybersecurity and serves as a starting point (baseline) to utilize "vertical track" education programs to further important societal strategic objectives, critical mission areas, and enhance cyber preparedness, response, capacity, and digital resiliency.

This Strategy and Recommendation Report achieves several significant organizational and educational objectives and reflects the culmination of many collaborative efforts and contributions from many participants. While wonderful to acknowledge hundreds of participants contributing to this project, I apologize in advance for an inability to acknowledge and thank all personally.

Respectfully, Keith Clement, Ph.D.
Professor- California State University, Fresno
California Cybersecurity Task Force, Workforce Development Education Subcommittee Chair
California Interagency Advisory Committee on Apprenticeships (IACA), IT Subcommittee Chair
California Community College, Public Safety Education Advisory Committee (PSEAC), Chair

EXECUTIVE SUMMARY

Global demand for cybersecurity and information security professionals and personnel has been mounting for decades and reaching a critical point. It is imperative in this modern and information-rich era to have a strong cadre of qualified and prepared cybersecurity specialists and specialized workforce (from technicians through managers) flowing into the labor pool. Based on the reliance of technology in today's digital environment, we need coordinated and linked education, training, and workforce development programs to increase statewide cybersecurity capabilities and enhance cyber-resiliency. To meet current and future critical cybersecurity "high needs areas" and workforce/skills gaps, comprehensive and coordinated strategic academic education and professional workforce training programs are in increasingly heavy demand.

Well-prepared cybersecurity professionals are essential given the dynamic change in scope and breadth of threats and vectors in today's cybersecurity environment. Thus, we seek a framework to design, develop, and implement a California Cybersecurity Career Education Pipeline and Pathway Project (CCCEPPP) to prepare 50,000 statewide entry-level cybersecurity professionals from 2020-2030 and reduce current/future state workforce capability skills/gaps. In order to maximize efficiency and availability of workforce development and education/training programs (and meet diverse key stakeholder needs), we seek innovative ways to balance rigorous academic and professional needs in cybersecurity programs and achieve enhanced student access to quality, cost-efficient, and available cyber-security programs statewide.

- This report provides **15 recommendations** for a blueprint and template to design, develop, and implement the CCCEPPP and additional educational institution toolkits to enhance statewide cybersecurity workforce development and education capabilities. The *California Cybersecurity Workforce Development and Education Strategy* facilitates and coordinates a statewide pipeline/pathway at all levels of education (K-12, Associates, Bachelors, Graduate, and Professional Certification/Training).

- The framework includes the alignment and linkage of cybersecurity model curriculum/academic standards, extra-curricular activities, cyber-competitions, professional and career development, and a host of related issues. The cybersecurity career pathway includes a variety of specialized education programs and workforce development opportunities in "high needs areas" of cybersecurity accessible to all Californians irrespective of geographic location or socioeconomic status/background.

- Additional educational toolkits and resources to support the cybersecurity pipeline and pathway are discussed. One tool to enhance California educational institution incident response and cyber emergency preparedness, information sharing coordination "best practices" is the California Education Institution Threat Assessment Center (CEITAC).

- The *California Cybersecurity Education and Workforce Development Clearinghouse* is where developed all materials and resources will be posted and publicly available.

- *California Essential Workforce Youth Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework* (see Appendix 2).

THE CALIFORNIA CYBERSECURITY CAREER EDUCATION PIPELINE/PATHWAY PROJECT (CCCEPPP) SUMMARY:

This *Strategy Report* describes the design, development, and implementation phases of the California Cybersecurity Career Education Pipeline and Pathway Project (CCCEPPP) to transform statewide cyber education and workforce development. The CCCEPPP is an initiative of the California Cybersecurity Task Force (CCTF) Workforce Development and Education Subcommittee (WDE). The CCTF is Co-Chaired by Director Mark Ghilarducci, California Governor's Office of Emergency Services (Cal OES) and Director Amy Tong of the California Department of Technology (CDT).

The CCCEPPP is an inter-disciplinary statewide initiative to facilitate collaboration and coordination and "roll out" a comprehensive and strategic State of California Cybersecurity workforce development and education plan. There is no current and clearly organized statewide cybersecurity workforce development and education strategy or related pipeline/pathway. Cybersecurity academic infrastructure needs bolstering in capacity and resiliency in this extraordinarily important ecosystem and space. CCCEPPP operates across all levels of education (K-12, community colleges, and universities) and addresses the need for statewide strategic cybersecurity workforce development and education preparation to meet critical "high need" essential workforce needs and emerging areas with significant capability-skill gaps.

The *California Cybersecurity Workforce Development and Education Strategy* discusses the alignment and coordination of cybersecurity K-12 and Higher Education model curriculum, academic standards, extra-curricular activities, cyber competitions, professional/career development, apprenticeships, and related areas to build a solid, linked cybersecurity pipeline/pathway to serve the State of California. **To be successful, public and private sector key partners/major stakeholders must collaborate and work together earnestly to design education and workforce development programs that assure prospective employers program graduates can demonstrate the necessary knowledge, skills, abilities, and competencies to meet minimum job requirements upon pipeline/pathway completion and graduation.**

In addition, *California Essential Workforce Youth Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework* (CEWYA) serves as the first step in the broader cybersecurity workforce development and education strategy process. Thus, CCCEPPP and CEWYA projects represent a facilitative and coordinated effort to reduce current (and growing) statewide critical cyber workforce capability and gaps. The partnership guides the development and implementation of a statewide strategy to create a vertically and horizontally integrated system of Cybersecurity education/workforce development programs, and professional experience opportunities for all students/learners across California.

(CCCEPPP) OBJECTIVE- Design, develop, and implement a coordinated, linked, and seamless state-wide Cybersecurity Career Education Pipeline/Pathway at all levels of education/workforce development (including K-12, Associates, Bachelors, Masters, Doctoral, and Professional Certifications) to prepare 50,000 qualified graduates for professional entry-level cybersecurity positions between (2020-2030) to serve existing and future State of California workforce needs.

EXECUTIVE SUMMARY- CCCEPPP RECCOMENDATIONS

Recommendation #1- (The California Cybersecurity Career Education Pipeline/Pathway Project (CCCEPPP);

Develop and implement a statewide cybersecurity workforce development career education pipeline/pathway to prepare 50,000 cyber-and information security entry-level professionals in a ten-year period (2020 to 2030) to address current/future California critical capability gaps and cybersecurity employment needs.

CCCEPPP SCOPE OF WORK:
Phase I Activity- 2019-2022 Cybersecurity Pipeline: Middle School (7th Grade) through Four-year Undergraduate Degrees (Bachelors of Science/Dual Baccalaureate Cybersecurity Programs); Embedded Stackable Professional Certificate Program components.

Phase II Activity- 2022-2024 Cybersecurity Pipeline: Pre/Transitional K to Middle School (6th Grade), Advanced Graduate/Doctoral Degrees with stackable professional certificate programs.

Recommendation #2- (K-12 Cybersecurity Education);

K-12 Cybersecurity education programs, courses, curriculum, extra-curricular activities, cyber competitions, and professional development opportunities must solidly connect and seamlessly transition into college preparedness and career readiness programs found in Higher Education and workforce development (training) programs statewide.

Recommendation #3- Implement an Associate in Science Cybersecurity Degree (A.D.T. Program) with linked 4 year Bachelors of Science Cybersecurity Degree Program with embedded stacking certificate program specializations;

Development and implementation of a Cybersecurity Model Transfer Curriculum (MTC) program (short-term objective) and Associate Degree Transfer (A.D.T.) program (the long-term objective). In California, the 2- Year/4-Year transferable ADT is the "gold standard" for new and existing degree programs. The true value of an ADT is in the seamless/smooth transition for transferring 2 year to 4-year degree program students.

Recommendation #4- (Graduate Programs, Faculty Research, Teaching, and Service);

Graduate programs (at both the Masters, and Ph.D. levels) advance a variety of critical cybersecurity education, teaching, and research activities. Support advanced/technical cybersecurity advanced degrees; enhanced faculty teaching and student learning; professional development; and research/community service opportunities. Cybersecurity graduate degree programs develop and prepare new instructors, educators, and professors.

Recommendation #5- Align Professional Certifications, Workforce Development Training with Education Programs and CAL HR IT Job Classifications;

Place graduating students (from various exit points in education) into professional cybersecurity entry-level positions. Efficient alignment of cybersecurity education and workforce development processes with employer selection and hiring.

Recommendation #6- Educational Capacity and Instructor Support Component- simultaneous development of a specialized career pathway intended for cybersecurity educators, instructors, and professors (K-12 and Higher Education);

Recommendation #7- Extracurricular Activity Component- (coding camps through cybersecurity competitions); Designation of a State of California Cybersecurity Competition—"the Golden State Cybersecurity Competition";

Project Deliverable: Extracurricular Activity Component- Designation of a State of California Cybersecurity Competition, "Golden State Cybersecurity League," California Governor's Cybercompetition Golden Cup; Cybersecurity Competition Cybersecurity Certificate Programs;

Recommendation #8- Professional Development Component (Mentoring, Career Awareness/Preparation, job shadowing, research presentations, soft skills (like oral and written communication, team player, etc.);

Align model curriculum and academic standards with extra-curricular activities in cybersecurity and professional development component;

Recommendation #9- This recommendation has two distinct, yet related components:

I. Cyber Ethos/Ethical Hacking Education Component- Discuss the value of Public Ethos (Serving the Public, Serving the Field)-

II. Ensuring Employability, The Recruiting, Selection, Hiring Component: Background Investigation for Classified/Public Safety Employment Selection: Character building;

Recommendation #10- Application of Learning Component: Cybersecurity Professional Development Apprenticeships, Internships, and Project Management;

Recommendation #11- Transitioning Military, Veterans, and Disabled Veterans into cybersecurity workforce career pipeline;

Recommendation #12- (Strategies to enhance the participation and retention of Women in Cybersecurity and Technological Fields);

Recommendation #13- (Strategies to enhance the participation and retention of Underrepresented Historical Backgrounds in Cybersecurity and Technological Fields);

Recommendation #14- California Cybersecurity Career Education Pipeline/Pathway Cyber-Hygiene Component: Cyber Hygiene "Best Practices" and Linkage with Education/Academic Programs at All Levels;

Recommendation #15- Formation of California Educational Institution Threat Assessment Center (CEITAC). Enhanced and shared Educational Institution Cybersecurity, Digital Emergency Management, Incident Response and Information Sharing preparedness, response, recovery, and mitigation capabilities.

CONTENTS

SECTION II- CALIFORNIA CYBERSECURITY TASK FORCE, WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE LINKAGES

SECTION III- CALIFORNIA EMPLOYMENT, CYBERSECURITY WORKFORCE, AND EDUCATION SYSTEMS

SECTION XII- CALIFORNIA CYBERSECURITY CAREER EDUCATION PIPELINE/ PATHWAY PROJECT IMPLEMENTATION TASKS/ACTIVITIES AND DELIVERABLES

ACKNOWLEDGEMENTS

The *California Cybersecurity Workforce Development and Education Strategy: Recommendations Report* is a collaborative project and partnership undertaken on behalf of the California Cybersecurity Task Force (CCTF), Workforce Development and Education (WDE) Subcommittee. These recommendations and "best practices" should significantly enhance California cybersecurity educational capability, educator/instructor capacity and result in a reduction of critical statewide cybersecurity workforce skills/competencies gaps.

We acknowledge and thank CCTF for leadership and dedication in securing and protecting state cybersecurity resources and data, as well as; leveraging their expertise in state strategic planning, cybersecurity preparedness, and response. The CCTF serves as an advisory body to State of California Senior Administration and Officials. Thank you very much to Mark Ghilarducci (Director, California Governor's Office of Emergency Services (Cal OES)) and Amy Tong (Director, California Department of Technology (CDT)) for their vision, leadership, experience, and the amazing opportunity to work on California cybersecurity education and workforce development programs and initiatives.

Deepest appreciation for the support and guidance of Tom Osborne (Deputy Director of Homeland Security Cal OES), Jonathan Nunez (Commander, California Cybersecurity Integration Center (Cal-CSIC), and Mario F. Garcia, CISSP, Deputy Commander, California Cybersecurity Integration Center (Cal-CSIC) for their leadership, dedication, diligence, and tremendous work at Cal OES, Cal-CSIC, CCTF, and for supporting the California Cybersecurity Career Education Pipeline/Pathway Project (CCCEPPP). Thanks to all!

We recognize California Department of Technology Colleagues for their support and invaluable assistance on cybersecurity pipeline and pathway development and implementation. Thanks a bunch to Brenda Bridges Cruz, Deputy Director, Office of Professional Development; and Vitaliy Panych, Chief Information Officer (Acting), California Department of Technology.

Our primary task is the development of recommendations for California to enhance statewide Cybersecurity Education and Workforce Development. It is important to acknowledge and note the tremendous contributions from many members and participants who helped in the preparation of this document; attended events/meetings, lent their professional expertise, provided input/feedback, and supported us on the completion of the Subcommittee Recommendations and additional materials found within this report. As the list of recognized individuals and organizations/educational institutions is lengthy (over 15 pages of acknowledgements), it has been included in *Appendix 1*.

We also thank CCTF and Workforce Development and Education Subcommittee partners (past and present) for their support, dedicated contribution of time, and technical assistance as Subject Matter Experts (SME) towards the design and development of statewide model curriculum, academic standards, and recommendations found in the *California Cybersecurity Workforce Development and Education Strategy* and related career education pipeline/pathway. Subcommittee partners are amongst the individuals thanked in the Contributions, Acknowledgements, and Participants in *Appendix 1*.

2020 CALIFORNIA CYBERSECURITY TASK FORCE, WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE MEMBERS

Jared Amalong, Sacramento County Office of Education

Tsegay Arefaine, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Dr. Mohsen Beheshti, California State University, Dominguez Hills

Miki Bellon, Mikology/Silicon Valley Roundtable

Brandon Bjerke, California State Assembly

Darin Bournstein, California Governor's Office of Emergency Services

Brenda Bridges Cruz, California Department of Technology

Helen Bui, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Stephanie Cervantes, Secure Smart Solutions

Dr. Tingting Chen, California State Polytechnic University, Pomona

Dr. Myron Curtis, Sierra College

Dr. Jun Dai, California State University, Sacramento

Christian Douangphouxay, Tachi-Yokut Tribe

John Dunn, California Labor and Workforce Development Agency (LWDA)

Teana Fredeen, SynED/California Cyberhub

Mario Garcia, California Cybersecurity Integration Center (Cal-CSIC)

Dr. Markus Geissler, Cosumnes River College

Davood Ghods, Direct Technology

Paul Giacomotto, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Dr. Richard Grotegut, Western Academy Support and Training Center

Laurie Halcomb, Fairfield Suisun Unified School District

Erle Hall, California Department of Education

Bill Harrison, Tulare County Information & Communications Technology

Dr. Olivia Herriford, Bay Area Community College Consortium

Harsh Jadhav, ACERA

Dr. Tolgay Kizilelma, University of California, Merced

Ken Kojima, California Department of Corrections and Rehabilitation

Keith Koo, Guardian Insight, Host, Silicon Valley Insider Radio and Podcast

Greg Kyritsis, California Commission on Peace Officer Standards and Training (POST)

Greg Lee, California Veteran's Council

Dr. Steve Linthicum, Coastline Community College

Kelly Mackey, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Dr. Assis Malaquias, California State University Maritime Academy

Vicente Medina, State of California

Dr. Eric L. Nelson, University of California, Davis

Harry O'Laughlin, California Department of Insurance

Brian Olson, Envolve Pharmacy Solutions

Vitaliy Panych, California Department of Technology

Robert Patton, California Commission on Peace Officer Standards and Training (POST)

Dave Petree, Security Together

Mike Radford, California Commission on Peace Officer Standards and Training (POST)

Eric Rood, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Eileen Sanchez, California Governor's Office of Policy and Research

Jimmy Sanders, ISSA San Francisco, Netflix DVD

Dr. Mehrdad Sharbaf, Loyola Marymount University

Nadean Shavor, California Franchise Tax Board

RADM (RET) Kenneth Slaght, Cyber Center of Excellence

Allen Stubblefield, Troy High School

Swanson, County of Sacramento

Eric Ureta, Fortinet

Richard Valdez, Disabled American Veterans (DAV)

Paul W., LibertyID

Justin Lloyd Wellner, California Polytechnic State University, San Luis Obispo

Scott F. Wilson, Lawrence Livermore Labs

Rami J. Zreikat, xTerraLink, Inc.

COMMONLY USED ABBREVIATIONS

Academic Year (AY)
Artificial Intelligence (AI)
Associate Degree Transfer Program (ADT)
Bachelor's of Science Degree Program (B.S.)
California Community Colleges (CCC)
California Cybersecurity Integration Center (Cal-CSIC)
California Cybersecurity Task Force (CCTF)
California Department of Education (CDE)
California Department of Industrial Relations (DIR)
California Department of Technology (CDT)
California Division of Apprenticeship Standards (DAS)
California Education Institution Threat Assessment Center (CEITAC)
California Government Operations Agency (GovOps)
California Governor's Office of Business and Economic Development (GO-Biz)
California Governor's Office of Emergency Services (Cal OES)
California Labor and Workforce Development Agency (LWDA)
California Workforce Development Board (LWDA)
California State Threat Assessment Center (STAC)
California State University (CSU)
California State University (CSU) Professional and Continuing Education (PaCE)
California Essential Workforce Pre-and Registered Apprenticeship Pipeline Talent Model (CEWYA)
Career Technical Education (CTE)
Centers of Academic Excellence (CAE)
Chief Information Officer (CIO)
Chief Information Security Officer (CISO)
Chief Privacy Officer (CPO)
Chief Technology Officer (CTO)
Computer Science (CS)
Continuing Education Unit (CEU)
Critical Infrastructure Protection (CIP)
Cybersecurity and Infrastructure Security Agency (CISA)
Department of Defense (DOD)
Department of Homeland Security (DHS)
Emergency Operations Center (EOC)
Federal Education Records Protection Act (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)
Information Communication and Technology (ICT)
Information Technology (IT)
Internet of Things (IOT)
Knowledge, Skills, Abilities (KSA)
Learning Management System (LMS)
Machine Learning (ML)
Massive Open Online Courses (MOOC)
Master of Fine Arts (MFA)

National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology (NIST)
Non-Government Organizations (NGO)
Nonprofit Organizations (NPO)
On the Job Training (OJT)
Professional Science Masters Degrees (PSM)
Public Services (PS)
Regional Occupation Program (ROP)
Registered Apprenticeship Programs (RAP)
Return on Investment (ROI)
Security Operations Center (SOC)
Science, Technology, Engineering, Arts, Mathematics (STEAM)
Science, Technology, Engineering, Mathematics (STEM)
Subject Matter Expert (SME)
U.S. Bureau of Labor Statistics (BLS)
United States Department of Homeland Security (DHS)
United States Department of Labor (USDOL)
United States National Security Agency (NSA)
University of California (UC)
Workforce Development and Education (WDE)

SECTION I- CALIFORNIA CYBERSECURITY WORKFORCE DEVELOPMENT AND EDUCATION

STATEMENT OF THE PROBLEM

Technology is pervasive in modern lives, organizations, and society. Computing, networks, social media connect people, employers, and government with a multitude of linkages across critical industry sectors. Information Technology (IT) continues to transform our world, economy, and personal lives, we need greater numbers of specialized cybersecurity professionals to protect and secure a growing societal reliance on data, mobile devices, Internet of Things (IOT) and everything electronic. Despite known IT risks, threats, and vulnerabilities, however, a dangerous shortage of cybersecurity professionals exist in critical workforce sectors like energy, health care, transportation, civil service, advanced manufacturing, and for small and medium sized business.

Global demand for computer science, cybersecurity, and information security professionals and personnel has mounted for decades. Now it has reached a critical point with over 72,000+ job vacancies alone in California. It is imperative in this modern and information-rich era to have a strong cadre of qualified and prepared cybersecurity specialists and specialized workforce (including technicians, managers, executives, and policy-makers). Based on high technology needs of today's digital environment, a series of aligned and linked education, training, and workforce development is critical to increase cyber-security capabilities and enhance cyber-resiliency. Cybersecurity "high needs areas" with significant workforce/skills gaps, require comprehensive and coordinated strategic workforce development and education programs and solutions.

Current Cybersecurity Workforce Demand-

Cybersecurity is a rapidly evolving "high-need emerging discipline" with tremendous and growing demands for a highly specialized, technical, and prepared workforce. IT employers added 1.5 million new jobs since 2010.[1] Burning Glass reports that 13% of all IT jobs are found in security (2019). The number of cybersecurity job postings has grown 94% since 2013.[2] For each cybersecurity job opening, there is only a pool of 2.3 employed cybersecurity workers for employers to recruit.[3] When comparing cybersecurity "open positions" (i.e. number of total job openings within the total employed cybersecurity workforce), California currently has 72,123 cybersecurity related job openings and 111,644 total employed in the statewide cyber workforce (only 64.5% of available industry positions currently filled).[4] This data indicates significant workforce demand for cybersecurity professionals.

Cybersecurity professionals across industry sectors are in short supply in California and in much the rest of the country. Qualified cybersecurity professionals are "Essential Workforce," found in increasingly scarce supply, and too many current unfilled positions available. It is critical to note a shortage of cybersecurity professionals not only impacts the IT Industry, but also has

[1] CompTIA. Cyberstates 2018. Retrieved from https://www.cyberstates.org/pdf/CompTIA_Cyberstates_2018.pdf.
[2] Burning Glass Technologies. "Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring." Accessed at: https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf electronically on June 2019.
[3] Burning Glass Technologies. "Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring." Accessed at: https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf electronically on June 2019.
[4] Cyberseek Heat Map, Accessed at: https://www.cyberseek.org/heatmap.html electronically on 6/21/2020.

significant implications across industry sectors and critical infrastructure within the state and national economy due to the ubiquitous nexus of technology in a digital society. The problem of cybersecurity workforce gaps are particularly salient and timely today given essential workforce front line COVID-19 pandemic responders, sensitive medical and healthcare research, as well as significantly increased numbers of students and workers studying/working remotely from home.

Future Cybersecurity Workforce Demand-

Future occupational projections/estimates suggest the workforce trend to continue. If current acute cybersecurity professional demands are any indicator, we have every reason to believe future cybersecurity demand will continue to increase as well. U.S. Bureau of Labor Statistics (BLS) estimates an additional 546,200 new tech jobs (about 13% national growth).[5] In terms of future employment projections, 6 of 30 fastest growing occupations found in computer and mathematical occupations today. Increasing numbers of mobile/smart/connected devices drive demand for application software developers (25.6% job growth projection) and increased need for cybersecurity drive demand for information security analysts (31.6% job growth projection). [6] Cybersecurity is estimated for 28% job growth through 2026. [7] The future need for cybersecurity professionals is clear, and discussed in further detail further in the report. As baby-boomers continue to leave the workforce in growing numbers, the record number of highly skilled retirements monthly is not helping fill cybersecurity workforce gaps either.

California must find innovative and comprehensive ways to prepare, develop, and enhance our future cybersecurity talent and workforce pool. The number of available cybersecurity and IT/IS positions continues to climb. Cybersecurity workforce occupational trends indicate an additional and continually steep demand curve for information security specialists to continue into the foreseeable future. We need to graduate and enhance significantly the numbers of qualified candidates each year to meet the constantly growing demand. A cybersecurity workforce and capability gap will persist until we have a comprehensive and state-wide workforce and education strategy. Operational cybersecurity career pipelines and pathways increase the number of qualified entry-level personnel available for public and private sector employment. Unfortunately, there are a variety of challenges and obstacles related to cybersecurity workforce development and education to address first.

[5] Bureau of Labor Statistics. 2018. Occupational Outlook Handbook. Accessed at: https://www.bls.gov/ooh/computer-and-information-technology/home.htm.
[6] U.S. Bureau of Labor Statistics, 2020.
[7] U.S. Bureau of Labor Statistics, 2020.

Cybersecurity Education and Workforce Development Uncertainty and Challenges-

Current and future critical cybersecurity workforce gaps and capabilities are real and pressing issues. The data indicates a significant (and rising) cybersecurity workforce gap that only continues to broaden and deepen in recent years despite tremendous amounts of hiring. The scale of filling current and future California cybersecurity available positions and meeting increased occupational demand is daunting enough, but additional challenges exist. One issue is coordination. Because the speed of tech and pace of innovation is so rapid today, workforce development and educators have a hard time keeping up with the dynamic change.

- How do you develop and prepare workforce in a dynamic environment when job minimum requirements/skills/competencies change routinely?

- How do we factor in for future IT-cyber occupational classifications when some of these positions do not even exist yet? Perhaps tech still in development?

These are key challenges confronting future direction and trajectory of cybersecurity education and workforce development. It is vital to develop and promulgate a coordinated and sustainable, long-term statewide strategy and get Californians working in essential, high need, and newly emerging specialized areas like cybersecurity.

California Cybersecurity Workforce Development and Education Implications-

The demand for cyber professionals far out-paces the current supply of prepared/qualified job candidates. It surpasses our ability to prepare the number of new graduates necessary to keep pace with significant and continual occupational growth in the field. This workforce shortage hampers productivity and reduces our ability to be proactive in securing the capacity to develop, maintain, and operate digital infrastructure in support of many industry sectors. Tech workforce limitations and education obstacles unfortunately bear profound future implications on economics, politics, critical infrastructure protection, organizations, individuals, and our security.

California's large geographical size and diverse population contributes towards our status as the 5th largest world economy.[8] We are home to many high tech/cybersecurity firms/industry driving the tech transformation – there is a critical public interest in quickly closing cybersecurity workforce and skills capability gaps. As such, we need an efficient system to prepare a strong cadre of cybersecurity professionals to fill positions, perform relevant duties, and meet current/ future job responsibilities. Well-prepared cybersecurity professionals are essential given dynamic change in scope and breadth of threats and vectors in today's cybersecurity environment.

Based on high technology needs of the digital environment, a series of coordinated and linked education, training, and workforce development is critical to enhance statewide cyber-security and cyber-resiliency strategies, capabilities, and Critical Infrastructure Protection (CIP). Cybersecurity education workforce development and education programs must meet a variety of

[8] https://en.wikipedia.org/wiki/Economy_of_California#:~:text=The%20economy%20of%20California%20is,of%20India%20and%20behind%20Germany. Accessed electronically on 7.1.2020.

objectives: guide top talent; upskill students from many different backgrounds/economic sectors/industries; and provide preparation to individuals with minimal computing academic and technical experience. We need to educate and prepare large numbers of individuals for IT-Cyber entry-level positions and get them hired and working within this ecosystem.

The Importance/Impact of Technology, Internet, and Cybersecurity on Daily Lives:

We live in a complex technological world today. The digital footprint has grown exponentially in recent years. We see a cascading effect of an ever-expanding digital world with technology touching more and more aspects of life. Newborn babies are given soothing, cooing, comforting, and warm tablet-like devices when placed into incubators when only a few minutes old. For many in our global society today, they will likely have an electronic device in their hands for the rest of their lives as well. Technology, electronics, and the internet have crept into our families, schools, education process, employment, where/how we work, our form of governance, communications, travel, collective action, and many other socially meaningful ways. Computer, technology, internet, e-mail, and social media has wrought tremendous transformative change and "risk" to individuals and organizations globally.

Pervasive technology is a constant reminder of the critical role of cybersecurity in civic and economic life in the 21st century. The internet is where we shop, access government services, file taxes, and conduct countless additional online errands and tasks every day. We do more online and electronically – all the time relying on stored personal data, passwords, medical and credit card information, family photos, etc. Societal reliance on modern technology and innovation; the internet and social media; proliferation of mobile platforms and devices, IOT, smart cities and refrigerators, linked global networks, and all other things electronic are increasingly valued commodities moving into the future. Along with technology, many recognize the extraordinary value of information and privacy today (and our obligation/reason to protect it).

One observation about contemporary information, technology, and communications is in the quick speed of innovation and change: pace of technology and innovation/change accelerates daily. High-end computers and consumer electronics are literally obsolete as we remove them from the box. By the time a new smart device or next generation software/ application reaches the consumer market, it is already hopelessly outdated. Technology is moving forward fast and the path to product obscurity can be quick. New tech is increasingly hard to anticipate. However, the concern grows on how to develop education programs and workforce opportunities to keep up with the amazing pace of tech and related challenge of securing our computers, data, and networks.

Tech has profoundly impacted the economy, revolutionized many industries and operations/ways of doing things. These complexities factor into and increase the difficulty of cybersecurity education and workforce development/training activities. This process is cyclical – as current threats are secured, new generations of threats and vulnerabilities emerge that require additional training and preparations to mitigate.

Going forward, there are many areas of digital Critical Infrastructure Protection (CIP) that require additional workforce development and education support/focus to include public health,

voting/elections, water, energy, agriculture, emergency services, and transportation. Mounting cybersecurity issues pose unique and growing security and defense challenges for public and private sectors, academia, and Non-Government Organizations (NGOs) today.

The Essential Question: How do we prepare a well-informed, specialized, and skilled cybersecurity professional workforce with all the innovative technology, current vulnerabilities/threats, while "cutting-edge" technology, internet, and cybersecurity enterprise continually reinvents itself at an amazing and accelerating pace?

Importance and Impact of Technology, Internet, and Cybersecurity on Public/ Private Sectors and Education/Academia:

The tech, internet, and social media transformation has altered how government provides services/benefits and interacts with the citizenry. The manner in which political values public information is communicated/responded to, social service/benefit delivery, and additional hallmarks of public administration are all deeply impacted. Voting is an essential hallmark of democracy. The need for secure elections and freedom from political interference are cherished fundamental liberties sought, protected, and digitally secured in today's electronic world. What are the impact of social media and social experiments on governance, political campaigns, election meddling, and the role of cybersecurity and the ballot box? These are fundamental aspects of democratic society to be vigorously safeguarded and defended.

The impact of technology, data (information), and cybersecurity cannot be understated. Protecting and securing our state and national cyberspace, critical infrastructure, information systems and networks, government/corporate espionage/personal/financial/ health data is a critical challenge to government (the public sphere) operations and administration. Same for the business/industry corporate world (the private sphere). Cybersecurity touches the lives of all within an increasingly interconnected and networked technological society. Worker productivity in many positions across many industrial sectors throughout the economy rely on technology and thus again cybersecurity is an important factor. Today most (if not all) medium and large sized business have a CIO or CISO (and in most cases both) within the C-level suite. More are adding privacy officers.

As the digital environment has become integral to the operation, administration, and management of government agencies and public institutions, it has similarly transformed the day-to-day way of life for global societies. A substantial premium exists for advanced computing skills, and such employment is competitive. One issue here is that while many may begin their IT and Cybersecurity career in public sector employment, they take this experience with them when recruited by private sector firms offering much more in salary than either public sector or education/higher education employers. This gulf of funding between public and private sector cybersecurity workforce is a problem. We need to find solutions to this problem so both sectors are able to recruit the talent they need. Employers no longer look for the same knowledge, skills, and abilities they did in the not too distant past. While technology, the internet, and cybersecurity changes have all made a large impact on the public and private sectors, its effect on education and

academia has been significant too. The education and academic worlds are dramatically different with technology today.

Cybersecurity has a significant impact on campuses. For example, Louisiana declared a cybersecurity state of emergency orders in July 2019 after several school districts were hit with ransomware attacks. Cities and schools in Texas recently experienced related issues as well. Campus administration must balance student and faculty accessible IT resources with security requirements found in compliance with a variety of federal and state laws and policies (i.e. Federal Education Records Protection Act (FERPA), and student health and psychological services centers complying with Health Insurance Portability and Accountability Act (HIPAA) privacy protections). There are many campus cybersecurity issues and potential threats and vulnerabilities.

Additionally, faculty teaching/student learning technology models and practices have changed in the classroom, further emphasizing the role of cyber in securing them. It is safe to say learning and teaching technologies in 2020 differ dramatically from the paper, pen, and analog clock of earlier education modes of learning. Today there are virtual classrooms and classes with online and hybridized course delivery formats not available 15 years ago. Today online courses are very common across institutions at all levels of academia. The numbers continue to expand with technologies like Massive Open Online Courses (MOOCs). For a sample list of available MOOCs, please follow the link: http://mooc.org/.

While there have been tremendous changes in teaching and learning instruction and technology in the evolution of public education over the last few decades with the IT revolution, the pace of change has quickened yet again. In light of COVID-19 societal interruptions, many school districts, colleges, and universities are preparing contingency plans for course delivery in the virtual and remote teaching format. More and more Californians are either working/teaching from home, or attending school/classes/lectures in the online environment with Learning Management Systems (LMS) like Canvas, Blackboard, or Moodle. We must not only adapt to the transition of great numbers of workers, teachers, and students to the virtual environment, but also assist with novel security threats and vulnerabilities resulting from COVID-19 pandemic response and more working/studying remotely from home.

Given change to public, private, and academic communities in tech/cybersecurity, we need strategies to bring everyone to the table and adapt to the current reality and emphasis on online learning/working. Once together at the table, we can work together to gain a common understanding and situational awareness of underlying problems through the development of a common language by which all cybersecurity education/workforce development key partners and stakeholders engage in the process. After all, coordination is best served and enhanced through statewide partnerships, ways to collaborate moving forward, and strategic communications among key partners and stakeholders.

ENHANCED PARTNERSHIP BETWEEN CYBERSECURITY PROFESSIONALS AND THE ACADEMIC COMMUNITY: DEVELOPING A COMMON VOCABULARY:

There are many linkages and connections in the relationship and interaction between the public sector (government institutions and agencies), private sector (industry/small, medium, large business), NGOs, and education/academic communities in cybersecurity workforce and economic development. Again, a ubiquitous professional field touching many different industry sectors and occupation clusters. The key to resolving modern cybersecurity capability/workforce gap problems involves facilitation, collaboration, and information sharing of major stakeholders and partners across these sectors. Strategies for cybersecurity workforce development and education must include solutions built in conjunction with Industry, Government, and Education/Higher Education. Not information hording nor "siloization." We need partnership and collaboration to design initiatives and innovations to meet diverse hiring needs and working together on viable cybersecurity education and workforce strategies and programs to solve the problem at hand.

For example, it is important to understand IT-Cybersecurity employer needs across economic sectors and industry types. What constitutes relevant qualified workforce knowledge, skills, and abilities for "real world" professional success? Once we understand portable skills (both technical and non-technical) in cybersecurity, we can link and align education programs and workforce development opportunities. Cybersecurity employer needs include; technical cyber skills, problem solving ability, navigating the recruitment and selection process to get the job; what it means to work at a security-based employer; and additional professional responsibilities and duties. This "skills gap" has frequently been an issue between public-private-academia partners and we need to enhance the relationship and better communicate concerns and solutions among work group members.

Do IT-Cybersecurity terms have common meanings and definitions among industry/education/government communities to better understand employer/workforce needs/demands/ supply/capability/programs, etc.? For example cyber resiliency. What does that mean to a cybersecurity professional? An academic? Government agency personnel? Corporations and NGOs? Nonprofit Organizations (NPOs)? **Does this term mean the same thing to everyone?** Unlikely. This is why a common frame of reference and language is useful. Through the process of collaboration and coordination, we can build out common definitions for key terms/concepts among industry and employers (public/private sectors) with academia/education and partners. In this way, we can all speak the same vernacular (language), enhance our common understandings, and sharpen our WDE goals and objectives.

One key step to bringing together the triad of educator-public sector-private sector together is in the development and usage of a common language that binds together our understandings and common objectives to accomplish. Common terms and meanings benefit both educators and the cybersecurity industry community. We can build collaboration by working together in the development and implementation of solid cybersecurity academic programs to graduate quality candidates ready for employment in the field to help meet employer needs. We need a common taxonomy (vocabulary) of meaningful terms with major partners and stakeholders drawn from industry, academics, and the public sector. In meetings to develop the CCEPPP, it was helpful to

define key terms upfront and then move forward with common understanding, language, and drive towards our collective purposes.

There are additional meaningful steps the public and private sectors can take in conjunction with the education/academic community to solve common "cyber insecurity" problems. These steps are based on strategic, decisive actions to enhance statewide cybersecurity education and workforce development activities and deliverables found and discussed throughout this report.

HOW GOVERNMENT, PRIVATE SECTOR, AND EDUCATION/ACADEMIA CAN COLLABORATE ON CYBERSECURITY WORKFORCE/SKILL CAPABILITY GAPS:

Many across the public, private, and NGOs struggle daily with the significant problem of a deepening cybersecurity critical skill capability and workforce gap. Federal, state, local government all struggle finding and retaining qualified cybersecurity professionals to fill available positions. The private sector encompassing many different industries and sized business also struggle to find qualified security personnel. Private sector firms frequently hire experienced public sector cyber professionals away from government service because they can pay salaries agencies are unlikely to beat. NFPs, NGOs, and community/neighborhood organizations also suffer the negative effects of cybersecurity WDE capability and skills gaps.

To meet current and future California cybersecurity education and workforce development needs, we must develop and implement a career education pipeline and pathway. Cybersecurity is a valuable public common and good. We all benefit from enhanced cybersecurity and thus have a vested interest to get major partners and key stakeholders together to work on solutions to meet our collective best interests. Facilitated collaboration is essential in designing workforce development/education programs, courses, and curriculum in partnership with academic institutions, government agencies, private sector, and NGOs to fill skill shortages and gaps.

The following areas of coordination and strategic planning make a big difference and pay a dividend on securing future positive cybersecurity education/workforce development outcomes:

- Align and link Cybersecurity education and workforce development programs at K-12 and Higher Education levels- instructional materials and resources-
- Cybersecurity Model Curriculum and Academic Standards-
- Cybersecurity Extracurricular Activities (Cyber-competitions, After-school activities/ summer camps, hackathons, coding camps, bug bounties, etc.)-
- Cybersecurity Professional and Career Development-
- Workforce Development and Training (Internships, Digital Community Service)-
- Youth Pre- and Registered Cyber Apprenticeship Opportunities (On the Job Training)-
- Cybersecurity Inclusivity and Diversity-
- Military to civilian transition, veterans, and disabled veterans-
- "Soft Start" IT and Cybersecurity Education Programs-
- California Cybersecurity Education Clearinghouse-

- *California Essential Workforce Youth Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework-*

REPORT SECTION SUMMARY:

Before going into further detail on workforce development and education matters, there are CCTF organizational and institutional matters to discuss first. It is essential Cybersecurity Career Education Pipelines and Pathways align and advance California and National Cybersecurity and Homeland Security Strategy, Policy, Mission, and Vision. We discuss CCTF and WDE Subcommittee objectives and linkages in the following section.

As an advisory body, we prepare the *California Cybersecurity Workforce Development and Education Strategy* and recommendations for career education pipeline/pathway development/implementation to guide California towards a more robust cyber posture, enhanced workforce/training/development opportunities, and precise digital situational awareness. This Strategy is further refined by the *California Essential Workforce Youth Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework* found in Appendix 2.

SECTION II- CALIFORNIA CYBERSECURITY TASK FORCE (CCTF) WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE LINKAGES

CCTF WDE SUBCOMMITTEE: CYBERSECURITY CAREER EDUCATION PIPELINE/ PATHWAY FRAMEWORK ALIGNMENT AND LINKAGES

The California Cybersecurity Education Career Pipeline and Pathway Project (CCCEPPP) supports the California Cybersecurity Task Force (CCTF). The CCTF is Co-Chaired by the California Governor's Office of Emergency Services (Cal OES) and California Department of Technology (CDT) and was formed to "act as an advisory board to the State of California Senior Administration in matters relating to Cybersecurity." [9]

As a subcommittee of Cybersecurity Education and Workforce Development Subject Matter Experts (SME) we propose to develop and implement a coordinated and collaborative California Cybersecurity Education Career Pipeline/Pathway Project to prepare 50,000 qualified graduates for entry level employment in California (over a 10- year project period.) Our vision and goal is to develop a competency-based model to meet the critical needs of the State of California as well as key industry stakeholders and major partners. The CCCEPPP seeks to assist in the rapid development of a cybersecurity workforce to meet current and future anticipated statewide needs.

The Workforce Development and Education Subcommittee was requested by the California Cybersecurity Task Force to design and develop a statewide cybersecurity career education pipeline/pathway with the following design components:

- Specified to cover all levels/segments of education (K-12 and Higher Education)
- Includes cybersecurity model curriculum/academic standards, extra-curricular, and professional/career development components.
- Multi-channeled Communication Cyber-hygiene Education Program
- Support mechanisms for transitioning military, veterans, and disabled veterans; encourage women and historically underrepresented backgrounds into the Cyber/Computing/IT fields.

The California Cybersecurity Career Education Pipeline and Pathway Project Aligns and Links with California Cybersecurity Task Force Mission and Vision in the Following Ways:

1. *CCTF Vision* – Advancing California's Cybersecurity Protection.
2. *CCTF Mission* –Acts as an advisory board to State of California Senior Administration in matters relating to Cybersecurity.
3. *California State IT Strategic Plan* – Prepared cybersecurity workforce is essential.
4. *California Homeland Security Strategy-*
5. California Cybersecurity Strategy and Policy – As above.
6. The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework-* (see Appendix 2).

[9] https://www.caloes.ca.gov/cal-oes-divisions/cybersecurity-task-force Accessed electronically 6/21/2020.

Linkages between CTF WDE Subcommittee and CCCEPPP:

1. Share information to foster relationships and increase cyber situational awareness.

2. Increase collaboration and awareness amongst stakeholders on matters of cyber-security.

3.Facilitate and integrate California into national cyber-security efforts- to better share information appropriately and protect it from interference.

4. Enhancing the role and protection of digital privacy.

5. Improving Cyber Education & cultivating a skilled Cyber Workforce.

6. Growing a prosperous California economy.

7. Critical Infrastructure Protection (Cyber and Physical Systems)- there are a variety of ways that cybersecurity education and workforce development are key:

* Reduce State of California exposure and vulnerabilities to cyber-risk.

* Expand state-wide capacity in cyber prevention, response and recovery.

* Shared situational awareness (public, private sectors, and education/academia).

* Overall, increased statewide cyber resilience.

* Create a culture of cybersecurity through heightened education and awareness for the public good and societal best interest.

* Enhance California educational institution incident response and cyber emergency preparedness platform; information sharing coordination, "best practices" and expertise through the creation and operation of a California Education Institution Threat Assessment Center (CEITAC.)

* California Cybersecurity Education Clearinghouse- a collection of all things cybersecurity education, workforce development, professional opportunities, and networking across all key partners and major stakeholders.

***** The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

CCTF Workforce Development and Education Subcommittee Organization and Objectives:

In 2013, Former Governor of California Edmund Gerald "Jerry" Brown, Jr. formed the California Cybersecurity Task Force. The mission was to "act as an advisory board to the State of California Senior Administration in matters relating to Cybersecurity." The CCTF is comprised of five standing subcommittees (please see following).

GCTF Standing Subcommittees

High Tech and Digital Forensics Subcommittee-

Information Sharing Subcommittee-

Legislation and Funding Subcommittee-

Risk Mitigation Subcommittee-

Workforce Development and Education Subcommittee-

In 2015-2016, the Workforce Development and Education Subcommittee was requested to develop a statewide cybersecurity career pathway (to include all levels of education, inclusion of cyber-education hygiene education programs, support mechanisms for military to civilian transition/veterans/disabled veterans and historically underrepresented backgrounds in computing/IT/cyber.) This phase of project activity culminates in the release of this strategy and recommendations report on cybersecurity education and workforce development.

"The Strategic California Cybersecurity Career Pipeline and Pathway for Education and Workforce Development and Educational Institutions Toolkits Framework" draft report was submitted and presented at the CCTF Quarterly Meeting and leadership in August, 2019. That initial draft report discussed the value and importance of a comprehensive, coordinated, and strategic approach to state-wide cybersecurity education and workforce development. However, many updates and revisions have been made to that previous document to yield this polished and comprehensive *California Cybersecurity Workforce Development and Education Strategy.*

California Cybersecurity 4 Year Education Workgroup- this workgroup works on the design and development of undergraduate cybersecurity model curriculum and academic standards for degree and certification programs.

California Cybersecurity Industry Workgroup- this workgroup works on design and development of cybersecurity model curriculum and academic standards to meet industry and employer needs across the public and private sectors.

CCTF Workforce Development and Education Subcommittee Objectives/Status Report:

Objective 1 - Develop a consistent definition and criteria for cyber security expertise to serve the State of California-

STATUS: *This effort was completed in June, 2015. This report recommends (among other things) the creation of a new classification series for Cybersecurity Professionals (and related career ladder for highly skilled staff.*

Objective 2 - Recommend alignment and refinement of the cybersecurity educational pathways inclusive of curricula, competitions, and professional development activities at the high school level of education and higher. There will be focus on ensuring veterans and the underrepresented in the field of cybersecurity are included and are afforded opportunities.

STATUS: *California Cybersecurity Task Force Workforce Development and Education Subcommittee: Recommendations for a Cybersecurity Pathway and Pipeline of Workforce Development and Education Final Report*

(First Draft Released- August 2019. Final version submitted to the California Cybersecurity Task Force Executive Board- August 2020).

Objective 3 - Identify and support opportunities for California to leverage and employ our military veterans in the field of cybersecurity**.**

STATUS: C*alifornia Cybersecurity Workforce Development and Education Strategy: Framework and Recommendations for a Cybersecurity Pathway and Pipeline of Workforce Development and Education Final Report* provides detailed subcommittee recommendations on this objective.

(First Draft Released- August 2019. Final version submitted to the California Cybersecurity Task Force Executive Board- August 2020).

Objective 4 - Align strategic partnerships to create a multi-channel cyber-safe communications campaign for all Californians

STATUS: C*alifornia Cybersecurity Workforce Development and Education Strategy: Framework and Recommendations for a Cybersecurity Pathway and Pipeline of Workforce Development and Education Final Report* provides detailed subcommittee recommendations on this objective.

(First Draft Released- August 2019. Final version submitted to the California Cybersecurity Task Force Executive Board- August 2020).

CCTF Workforce Development and Education Subcommittee Activity to Date:

The CCTF Education and Workforce Development Subcommittee was very active in 2013-2016. The Subcommittee initially divided work into 4 or 5 task groups based on alignment with the objectives listed above. Of note (because it was completed), the Objective 1 Team was assigned the task of "Developing a consistent definition and criteria for cybersecurity expertise to serve the State of California" led by Gary Dias (California Department of Health Care Services). Please see "State of California Cybersecurity Task Force Workforce and Development Document" found at the footnoted link below. [10]

In a nutshell, the WDE Subcommittee Objective 1 Team took a comprehensive look at California (IT Security) cybersecurity positions (both existing and proposed future job classifications) and extracted competencies in various functional framework specialty areas (31 total areas organized into seven categories.) This represents what it takes for a candidate to be appropriately trained for a position in that specific job classification. In the career pipeline/pathway we are interested in the Knowledge, Skills, Abilities, and (additional industry competencies) so qualified candidates are prepared to meet respective minimum/preferred requirements for cybersecurity entry-level professional positions.

California Cybersecurity Task Force Workforce Development and Education Subcommittee: Development of a consistent definition and criteria for cybersecurity expertise to serve the State of California. (Completed June 2015):

Items included in analysis of functional framework specialty areas: cyber education programs/courses/curriculum/ and standards to meet industry workforce needs, gaps, and enhance the quality of candidates within the hiring pool. It is key that career pipelines/ pathways prepare individuals for IT/Cybersecurity workforce with appropriate Knowledge Skills, Abilities (KSAs) for entry-level cybersecurity professional employment. Then we assist candidates navigating the job search process through workforce development opportunities, registered apprenticeships, on the job training; and mentoring for the hiring/selection/promotion process and guidance for long-term professional success within the field.

In the pipeline, cybersecurity competencies map carefully into the model curriculum/academic standards design during the development process. Then we embed relevant professional development opportunities at various education levels. We make additional educational/workforce development recommendations for specific career preparation in select cyber pathway positions. Finally, we follow with recommendations on activities, tasks, deliverables, and timelines for CCCEPPP implementation and statewide roll-out.

[10] https://www.caloes.ca.gov/CybersecurityTaskForceSite/Documents/Workforce%20Objective%201%20Proposal%202015-06.pdf

The California Cybersecurity Workforce Development and Education Strategy Report includes recommendations in the following areas:

(1.) Statewide model cyber-security curriculum/academic standards recommendations at all levels of education in California.

(2.) Statewide extra-curricular activities like statewide cyber-competitions, hackathons, coding camps, and additional structured/organized programs like after school activities and leagues where students hone their skills and practice the skill-set.

(3.) Professional Development Activities – Cyber/IT aptitude testing, introductory courses on getting jobs in this field, professional mentoring and job shadowing, career exploration, registered apprenticeships (on the job training), internships, and related.

(4.) Recruitment and retention of transitioning military, veterans and disabled veterans/spouses; women; and traditionally underrepresented groups in cyber/IT/computer sciences.

(5.) Integration and linkage of cyber hygiene and ethical hacking into education program design/development/implementation.

(6.) IT-Cyber Youth Pre- and Registered Apprenticeship Programs and California Cybersecurity Apprenticeship Centers.

CURRENT CCTF WDE SUBCOMMITTEE ACTIVITY:

1. California Cybersecurity Labor- Market Needs/Demands Update- (please see below)
2. California Cybersecurity Career Education Pipeline/Pathway Project (CCCEPPP) Deliverable Status- Final version of the *California Cybersecurity Career Education Pipeline and Pathway Project: Strategic Framework and Recommendations Report* submitted to CCTF Executive Board, June 2020.
3. Statewide Cybersecurity Training and Education Strategy- Agenda items
4. California Cybersecurity Undergraduate (Upper Division) Model Curriculum and Academic Standards- (please see v7.0 further in the report)
5. California Cybersecurity Essential Workforce Apprenticeship Initiative (Cybersecurity Industry recognized minimum standards linked with NICE Cybersecurity Workforce Framework.)-
6. California Cybersecurity Apprenticeship Centers-
7. California Cybersecurity Education Clearinghouses-
8. California Cybersecurity Education and Workforce Development Road Maps-
9. The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

REPORT SECTION SUMMARY:

The objective of this section of the report is to describe the linkages between the California Cybersecurity Task Force, the Workforce Development and Education Subcommittee, and CCCEPPP and CEWYA strategies. There are a variety of ways in which these strategies align and link with the mission and vision of the CCTF and WDE Subcommittee. Subcommittee objectives (4) are discussed and a status report of the activity completion provided.

In addition, CCTF WDE Subcommittee activities to date are listed, including links provided to previous Subcommittee reports. Finally, this report section briefly describes the organizational framework for the Cybersecurity Workforce Development and Education Strategy and an overview of recommendations covered in greater detail later in this report.

It is important to lay out and discuss linkages and organizational objectives on the front end before going into too much detail on CCCEPPP and CEWYA strategy specifics yet.

SECTION III- CALIFORNIA EMPLOYMENT, CYBERSECURITY WORKFORCE, AND EDUCATION SYSTEMS

CALIFORNIA EMPLOYMENT, CYBERSECURITY WORKFORCE TRENDS, AND STATWIDE WORKFORCE CAPABILITY/GAPS:

The purpose of this report section is a brief look at California state employment/workforce/labor market/occupational information. It is key to look at some numbers and statistics to understand the relative size of current California cybersecurity workforce needs. We analyze and evaluate California cybersecurity related employment and quantify the extent to which a workforce capability gap exists. There are some interesting workforce and occupational trends in the IT-Cybersecurity analysis occurring at the state, regional, and local levels.

Then we provide a brief discussion of the size and organization of the California public education system. We are interested in looking at the size of California education and higher education systems and their tremendous ability to pivot to address "high needs" areas such as cybersecurity. With a basic understanding of statewide workforce capability gaps numbers combined with our innovative California public education/higher education institutions, we should pull together the remaining pieces of a cybersecurity career pipeline/pathway into a cohesive and comprehensive strategy for WDE. In this way, we implement feasible solutions to leverage our workforce/training/skills needs with significant California educational capabilities to square away an urgent and pressing IT-Cyber workforce gap statewide.

Contribution of CCCEPPP to California and U.S. Cybersecurity Workforce Capabilities:

The CCCEPPP objective is to develop 50,000 cybersecurity entry-level professionals over a 10 year period (2020-2030). Meeting this objective in California will be a solid start towards the reduction of national cybersecurity workforce capabilities and gaps as well.

Number of US Residents (2019 Population Estimate)- 328.2 Million. [11]
Number of California Residents (2019 Population Estimate)- 39.5 Million. [12]

The California cybersecurity career education pipeline/pathway serves and effects 39.5 million residents statewide. [13] Total California population represents 12% of total U.S. population (328.2 million residents.) Thus, the CCCEPPP will have a profound impact on California cybersecurity workforce development and education concerns and national impact as well. It is the hope of the report author that additional states, the federal government, and international colleagues and friends benefit from this cybersecurity workforce development and education blueprint and template in their respective location and enjoy great success in solving respective capability and skills gaps as well. If that turns out to be the case, and additional states are able to utilize this cybersecurity WDE framework and blueprint, we could further enhance our collective cyber posture, resiliency, and get people back to work in these high-paying wage positions.

[11] U.S. Census Bureau, Accessed at: https://census.gov/quickfacts/fact/table/US,CA/PSTO45219 on 4/30/2020.
[12] U.S. Census Bureau, Accessed at: https://census.gov/quickfacts/fact/table/US,CA/PSTO45219 on 4/30/2020.
[13] U.S. Census Bureau, Accessed at: https://census.gov/quickfacts/fact/table/US,CA/PSTO45219 on 4/30/2020.

California State Employee Demographics:

State of California Employees (excluding CSUs) appointed to State Controller's Office Employment History Database (July 2019):

Total Number of California Active State Employees- 235,122

Total Number California Full Time Employees- 211,019
Source: https://www.sco.ca.gov/ppsd_empinfo_demo.html

California Statewide IT Workforce Demographics:

State IT Employees 2018: 11,493- 5.06% of State Workforce

State IT Employees 2019: 11,564- 4.95% of State Workforce (note: % of State Workforce for 2019 decreased due to the total statewide employees increasing by 6,498.)

Source: *California Information Technology Annual Report 2019*, California Department of Technology, Accessed at: cdt.ca.gov/wp-content/uploads/2020/02/2019-Annual-Report.pdf

Gender:

State IT Employees 2018: Males- 64%, Females- 36% of State IT Workforce

State IT Employees 2019: Males- 65%, Females- 35% of State IT Workforce

Source: *California Information Technology Annual Report 2019*, California Department of Technology, Accessed at: cdt.ca.gov/wp-content/uploads/2020/02/2019-Annual-Report.pdf

Ethnicity:

State IT Employees 2018: Whites- 43%, Asian- 26%, Latino/Hispanic 13%,

African American- 7%, Other- 11% of State IT Workforce

State IT Employees 2019: Whites- 41%, Asian- 27%, Latino/Hispanic 12%,

African American-7%, Other- 13% of State IT Workforce

Source: *California Information Technology Annual Report 2019*, California Department of Technology, Accessed at: cdt.ca.gov/wp-content/uploads/2020/02/2019-Annual-Report.pdf

CALIFORNIA STATEWIDE POPULATION DEMOGRAPHICS:

Gender 2019- California is 50.3% female and 49.6% male. [14]

Ethnicity 2019- Latino/Hispanic- 39%, Whites- 36.5%, Asian- 15.5%, African American-6.5% [15]

STATE IT WORKFORCE AND POPULATION DEMOGRAPHICS ANALYSIS:

Several important points are found in the analysis of above data and statistics as related to state IT employment and state demographic trends. In terms of state IT sector workforce, women make up 50.3% of the population and 35% are the state IT workforce. This signifies under-representation in the field. To increase the numbers of women entering the IT-cybersecurity sector, we must work towards developing additional recruiting, retention, and outreach programs and initiatives.

In terms of state IT employment numbers and ethnicity, California Latino/Hispanics make up 39% of the population and 12% of the state IT workforce. This also signifies under-representation in the field. To increase the numbers of Latinos and Hispanics entering the IT-cybersecurity sector, we must work towards developing additional recruiting, retention, and outreach programs and initiatives.

While these numbers are drawn from state employment numbers, additional research must be done for private sector employers as well. This analysis supports the importance of diversity and inclusion research and analysis in the IT workforce.

[14] https://worldpopulationreview.com/states/california-population Accessed electronically on 7.01.20.
[15] https://www.census.gov/quickfacts/fact/table/CA/PST045219 Accessed electronically on 7.01.20.

CALIFORNIA CYBERSECURITY LABOR MARKET NEEDS/DEMANDS:

Global demand for computer science, cybersecurity, and information security professionals and personnel has been mounting for decades and nearing a critical point. Burning Glass reports that 13% of all IT jobs are today found in security (2019). The shortage of cybersecurity professionals is well documented and currently includes 72,000+ open job positions in California and 503,000+ positions nationally (https://www.cyberseek.org/heatmap.html). When comparing and state level cybersecurity "open position" (i.e. number of total job openings within the total employed cybersecurity workforce) California has 72,123 cybersecurity related job openings and 111,644 total employed in the statewide cybersecurity related workforce (Cyberseek, 2020). This data indicates significant workforce demand for California cybersecurity professional positions.

It is imperative in this modern and information-rich era to have a strong cadre of qualified and prepared cybersecurity specialists and increasingly specialized workforce (including technicians and managers). Analyzing Cyberseek data, about 88% of these cybersecurity positions specify a bachelor's degree or higher (as listed per job openings from 2/2018 through 10/2019) (Burning Glass, 2019). However, there are also significant moves in government and industry to reduce reliance on 4-year degrees to reduce current cybersecurity workforce capability and gaps. In either case, based on high technology needs of today's digital environment, a series of coordinated and linked education, training, and workforce development is critical to enhanced statewide cyber-security and cyber-resiliency strategies and capabilities.

Cybersecurity education workforce development and education programs must be prepared to guide top talent; upskill students from many different backgrounds, economic sectors and industries; and also provide preparation to a large numbers of individuals with minimal computing academic and technical experience to bring them up to speed for entry-level cybersecurity positions. (Tip: the key is job experience from cyber apprenticeships—see later.)

Table 1: California Cybersecurity Public and Private Sector Job Openings

Sector	Number of total job openings	(%'s)
Public	3,440	5%
Private	68,683	95%

Source: Cyberseek.org/heatmap.html

Of 72,123 current California cybersecurity job openings, 95% are in the private sector. This serves to emphasize the importance of critical engagement, strong ties, and connections with industry to design education and workforce development programs to meet significant workforce needs. In this way, we can better understand what industry seeks from prospective job candidates/valuable skillsets for filling 68,000+ current private sector vacant positions statewide and assist employers to find appropriately prepared job candidates ready for hire.

In terms of public sector job openings, 3,440 openings becomes a bit more significant when we have 209,636 active full time California employees (excluding California State Universities) as appointed to the State Controller's Office Employment History Data Base. [16] The primary takeaway here is the importance of collaborating with the public and private sectors in developing cybersecurity education curriculum/standards and workforce program and apprenticeship opportunity implementation.

In addition to comparing numbers of public and private sector cybersecurity jobs available, we are interested in the geographical/metropolitan area where positions are located (please see Table 2 below.) There are two large clusters of available positions, one in Northern California (35,000) and the other in Southern California (32,000). The remaining 5,000 positions are scattered across the state. Cyberseek data indicates geographic concentration of cybersecurity professionals is higher in California (1.5) than the national average (1.0). Yet, the supply of cybersecurity workforce supply/demand is still much lower in California (1.5) than the national average (2.0). [17]

In other words, there are more cybersecurity positions in California geographically, but we still need to increase cybersecurity related workforce numbers greatly through "supply side" strategies of education and workforce development to meet this expanding need and increase the number of prepared candidates in the cyber job pool statewide.

Table 2: California Cybersecurity Supply/Demand Heat Map 2019-2020 (by Metropolitan Area)

California Metro Areas	Total Cyber Jobs Open
Los Angeles-Long Beach Anaheim	21,957
San Francisco-Oakland-Hayward	18,596
San Jose-Sunnyvale-Santa Clara	13,114
San Diego-Carlsbad	8,429
Sacramento-Roseville-Arden Arcade	3,343
Riverside-San Bernardino-Ontario	1,592
Bakersfield	692
Fresno	441

Source: Cyberseek.org/heatmap.html

[16] State Controller's Office, sco.ca.gov/ppsd_empinfo_demos.html.
[17] (Cyberseek, Accessed electronically on 6.21.2020. Cyberseek.org/heatmap.html

Future Anticipated Cybersecurity Workforce Outlooks/Labor Projections:

The number of cybersecurity job postings has grown 94% since 2013. [18] For each cybersecurity job opening, there was a pool of only 2.3 employed cybersecurity workers for employers to recruit. [19] In terms of future employment projections, 6 of 30 fastest growing occupations are found in computer and mathematical occupations today. Increasing numbers of mobile/smart/connected devices drive demand for application software developers (25.6% job growth projection) and increased need for cybersecurity drive demand for information security analysts (31.6% job growth projection. [20] Cybersecurity is estimated for 28% job growth through 2026. [21]

The cybersecurity workforce and capability gap is going to persist until we have a comprehensive and strategic career pipeline and pathway in progress that significantly increases numbers of qualified entry-level public and private sector personnel for our statewide IT-Cyber employment pool.

[18] (Burning Glass, 2019).
[19] (Burning Glass, 2019).
[20] (U.S. Bureau of Labor Statistics, 2020).
[21] (U.S. Bureau of Labor Statistics, 2020).

SUMMARIZING & UNDERSTANDING THE CALIFORNIA EDUCATION SYSTEM (K-12 and Higher Education):

The purpose of this report section is to provide general information on California cybersecurity workforce and employment trends. We discussed California State and IT-Cybersecurity Workforce and state-regional-metropolitan-local areas of analysis. Now it is important to discuss and analyze the other side of workforce development—the education and academic system side of the equation.

Over the next few pages of the report, we discuss the California K-12 and Higher Education Systems. The number of students in California schools is bigger than the total population of a good number of States. There are a number of interesting questions related to the size of the California Education and Higher Education systems. For example, how many students and teachers attend/work at California Elementary, Middle, and High Schools? How big is the Los Angeles Unified School District (LAUSD)?

Once we get a sense of the enormous size and scale of California K-12 Education, we shift attention to the scope and mission of the Higher Education Community. How many public institutions of higher education are there state-wide? (Hint: 149) How many students attend public colleges and universities? How many faculty/instructors teach at these institutions?

We are interested in the number of students and faculty studying and teaching within the California Community Colleges, California State University, and University of California Systems. These are some of the largest university and college systems in the world.

All these factors and information is essential to keep in mind when developing statewide cybersecurity workforce development/training/education/ strategies. We go into these conversations in the next few pages of the report.

CALIFORNIA K-12 EDUCATION (2019-2020)

This report section provides information on the size of the California K-12 Education System. It is large and encompasses about 12% of the total students nationwide. There are 1,037 school districts statewide and 10,588 schools. [22] These districts served an overall enrollment of 6.163 million students in K-12 public schools in 2019-20 Academic Year (AY). [23] In 2018-19 AY, there were 319,004 teachers in public schools. [24] These numbers are broken down into the following categories:

California Number of Students in Public Schools by Grade Ranges (2019-20 AY)

K-5th- 2,774,703
6-8th- 1,425,109
9-12th- 1,963,189
Total: 6,163,001 Students

California Number of Teachers in Public Schools by Grade Ranges (2018-19 AY)

Elementary Schools- 146,521
Middle/Junior High Schools- 47,374
High Schools- 83,206
Other (Includes Continuation Schools)- 41,903
Total: 319,004 Teachers

Total: 6.482 Million California K-12 Public School Students and Teachers
Source: California Department of Education, Accessed electronically 7/2/20.
https://www.cde.ca.gov/ds/sd/cb/ceffingertipfacts.asp

Los Angeles Unified School District (LAUSD) is the 2nd largest school district in the U.S. with 1,368 schools serving a total estimated enrollment of 673,849 students and 25,418 public school teachers (2019-20 AY). [25] English and 99 other languages spoken in Los Angeles Unified Schools and approximately 4.8 million people live within district boundaries. [26] Approximately 10% of California K-12 students draw from LAUSD.

In terms of the numbers of California K-12 students and teachers attending and working in public schools (6.482 million) is bigger than the 2019 population of 32 other states. [27] As one can tell from California K-12 Education statistics, moving cybersecurity into schools statewide would have a significant impact on state and national education initiatives.

---

[22] California Department of Education, Accessed electronically on 7.2.2020. https://www.cde.ca.gov/ds/sd/cb/ceffingertipfacts.asp
[23] California Department of Education, https://www.cde.ca.gov/nr/ne/yr19/yr19rel27.asp Accessed electronically on 7.2.2020.
[24] California Department of Education, Accessed electronically on 7.2.2020. https://www.cde.ca.gov/ds/sd/cb/ceffingertipfacts.asp
[25] Los Angeles Unified School District, Accessed Electronically on 7.2.2020. https://achieve.lausd.net/site/handlers/filedownload.ashx?moduleinstanceid=52741&dataid=89340&FileName=Fingertip%20Facts%202019-2020.pdfF.pdf
[26] Los Angeles Unified School District, Ibid.
[27] Wikipedia, Rank of States, Accessed Electronically on 7.2.2020. https://en.wikipedia.org/wiki/List_of_states_and_territories_of_the_United_States_by_population

CALIFORNIA PUBLIC HIGHER EDUCATION SYSTEMS:

The previous report section illustrated the large size of the California K-12 education system. This large education system feeds into the California Higher Education System. This section describes California higher education—the California Community Colleges (CCC), California State University (CSU), and University of California (UC) Systems. The objective is to provide information on California Higher Education Systems size and data from Fall 2019.

California Community College (CCC) System- 116 Campuses, (including 1 fully online campus- "Calbright")
2.1 Million Students- (Largest system of higher education in the country) and one in four community college students in the nation attend a California Community College. [28] Fall 2019 statewide search faculty/staff demographics report indicated a CCC employee count of 88,533—with 58,187 academics/faculty and 30,336 educational administrators/classified staff. [29]

California State University (CSU) System- 23 Campuses and eight off campus centers
482,000 Students (Fall 2019)- (Nation's largest four year public university) and one in ten California employees is a CSU graduate. [30] More than 53,000 employees, with 27,682 faculty (48.7% full time, 51.3% part time). [31]

University of California (UC) System- 10 Campuses—newest, UC Merced (2005)
280,000 Students (2019)- More than 227,000 faculty/staff. [32] There are 2.0 million UC alumni living/working around the world. [33]

California Public Higher Education Totals:
California Community Colleges: 2.1 Million Students: 88,533 Faculty/Staff: 2,188,533 Total
California State University: 482,000 Students: 53,000 Faculty/Staff: 535,000 Total
University of California: 280,000 Students: 227,000 Faculty/Staff: 507,000 Total
Total Students/Faculty/Staff: **3,230,533**

In California public higher education, there is a total of 3,230,533 students, faculty, and staff enrolled or working at the CCCs, CSUs, and UCs statewide. On the next page, we combine the education and higher education communities together and perform some brief demographic analysis and discussion.

[28] California Community Colleges, Accessed electronically 7/2/2020. https://www.cccco.edu/About-Us/Key-Facts
[29] California Community Colleges, Accessed electronically 7/2/2020. https://datamart.cccco.edu/Faculty-Staff/Staff_Demo.aspx
[30] California State University, Accessed electronically 7/2/2020. https://www2.calstate.edu/csu-system/about-the-csu/facts-about-the-csu/Documents/facts2020.pdf
[31] California State University, Ibid.
[32] University of California, Accessed electronically 8/2/20. https://www.universityofcalifornia.edu/uc-system
[33] University of California, Ibid.

CALIFORNIA EDUCATION (AND HIGHER EDUCATION) ANALYSIS:

In California K-12 Education and Higher Education, total numbers of students, faculty, and staff are presented below:

Total: 6.482 Million California K-12 Public School Students and Teachers
Total: 3.231 Million California Higher Education System Students/Faculty/Staff
Total: 9.713 Million California Students, Staff, and Faculty

There are more than **9.713** million students, staff, and faculty in California public K-12 and Higher Education in 2019. Approximately **25%** of California residents attend/teach/work at California K-12 and Higher Education institutions. A total of **3%** of the US population is found inside a California K-12/Higher Education classroom/office).

Number of US Residents (2019 Population Estimate)- 328.2 Million. [34]
Number of California Residents (2019 Population Estimate)- 39.5 Million. [35]

This number of public education students, teachers, and faculty in California is larger than the population of 39 states, placing right after Michigan (#10 in national population)! [36]

Thus, it is possible to make a significant impact on state-wide cybersecurity education and workforce development at all levels of California education and higher education. The operation of a California Cybersecurity Career Pipeline/Pathway would also make a significant contribution to national cybersecurity education and workforce development programs. This pool of qualified and prepared prospective employees would increase the number of workforce ready entry-level professionals serving the public and private. In the event there was a fully functional and operational cybersecurity career education pipeline/pathway, it would take a significant bite out of the cybersecurity workforce deficit plaguing the US and California.

Additional Sources of Data:

Educational Data Partnership - http://www.ed-data.k12.ca.us/welcome.asp
California Postsecondary Education Commission - www.cpec.ca.gov
Faculty Association of California Community Colleges - www.faccc.org
University of California - www.universityofcalifornia.edu
California State University – www.csu.edu
Association of Independent California Colleges & Universities - www.aiccu.edu

[34] U.S. Census Bureau, Accessed at: https://census.gov/quickfacts/fact/table/US,CA/PSTO45219 on 4/30/2020.
[35] U.S. Census Bureau, Accessed at: https://census.gov/quickfacts/fact/table/US,CA/PSTO45219 on 4/30/2020.
[36] Wikipedia, Rank of States, Accessed Electronically on 7.2.2020.
https://en.wikipedia.org/wiki/List_of_states_and_territories_of_the_United_States_by_population

SUMMATION THOUGHTS ON THIS REPORT SECTION:

Essential challenges facing California cybersecurity workforce development and education are discussed in this section. We need a strategy that aligns and links increased numbers of California students with cybersecurity industry employers looking for qualified job candidates. How do we enhance cybersecurity workforce development and education for students to, "…educate, recruit, train, develop, and retain a highly qualified workforce?" [37]

What are exciting ways to get students interested in technology, computing, and cybersecurity careers? We seek to guide students through the wide range of marvelous cybersecurity opportunities found through career awareness/preparedness programs found in earlier education phases. In this way, we can curry, support, and reinforce students interested in these fields and domains at all subsequent levels of education in the career pipeline/pathway. Then we continue to add more technical and specialized components and professional development opportunities as they continue and successfully navigate the cybersecurity career education pipeline/pathway. This given the important caveat that not all IT-Cybersecurity is heavy technical work and reliant on significant math/programming skills. "Softer" IT-cyber positions and pathways exist and we need WDE programs and courses to meet those students' needs as well.

An important side note: Lacking coordination and strategic linkage between/across levels of education is one current and significant flaw in state cybersecurity education and workforce development. Thus, we need to enhance seamless and linked transitions from one education program level to the next by moving forward on CCCEPPP recommendations.

In addition, and consistent with education/workforce development recommendations on curriculum and academic standards, we seek a series of cyber educational related experiences to bolster with apprenticeships, internships, hands on experiences, and professional/career development opportunities intended to bring students deeper into the cybersecurity enterprise. All cybersecurity education and workforce development programs and courses (as well as professional development opportunities) in the cyber career pipeline/pathway should be readily available, accessible, and inclusive to all students across California; irrespective of any other factors.

In the program/course design phase, we need visually attractive and engaging model curriculum/academic standards/content/assignments/activities and completely immerse students in tech, computing, cybersecurity and the whole spectrum of related employment. The California Cybersecurity Career Education Pipeline and Pathway operates as a **"Road-map"** of exactly what/how students need to complete (education/experience/necessary skills, etc.) to meet minimum position requirements and get hired in tech somewhere; preferably in the area of cybersecurity. In addition, and explicitly consistent with this cyber pipeline/pathway project, we seek to prepare students as competitive candidates for California entry-level cybersecurity professional positions. This is one of our baseline objectives to fulfill through efficient and

[37] National Cybersecurity Workforce Framework, National Institute for Cybersecurity Education (NICE): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf).

coordinated facilitated CCCEPPP workforce development activities. Consistent with the Road map above, we facilitate and implement collaborative and coordinated curriculum in a variety of educational delivery modes.

Many California Cybersecurity Career Education Pipeline/Pathway programs (including degrees and certificate) and courses (K-12 and Higher Education) recommended later in this report are digitized, virtualized, and available to all students online. By offering courses in an online format, students at all levels of education should have them in their reach (assuming they have a computer and internet access) available, accessible, and inclusive to all California residents. In addition, and consistent and consistent with "best practices" in cybersecurity education/workforce development, we include significant educational experiences, bolster with workforce development opportunities (like apprenticeships and internships with local regional partners/stakeholders), enhanced experience based learning and professional/career development to attract them into the cybersecurity field.

One report recommendation includes utilization of state servers and resources to host cybersecurity educational materials/curriculum/courses and otherwise serve as a clearinghouse for: cybersecurity teaching/learning/extra-curricular activities; professional development/hands-on learning; apprenticeship/internship opportunities; and additional resources all linked into one readily available location. Please see **California Cybersecurity Education Clearinghouse** recommendations and discussion included further in the report. This way, students and their families, instructors/faculty, interested public/private sector industry/NGO employers have access to cybersecurity education and workforce materials and see what is being taught in the programs/courses described here. As often said, cybersecurity WDE issues are coordination based problems—we need to do a better job of preparing these candidates and also a better job of linking program graduates with employers desperately seeking new talent and pool of qualified employees to hire in these high wage positions.

We do not want the siloization of cybersecurity education and workforce development strategies and actions from academia, government (public service) and private sector (industry) to continue. We need to break down this significant barrier and obstacle towards the preparation of a growing number of cybersecurity professionals to meet current/future state workforce development/skills and needs. This is the value of a smoothly functioning and efficiently operating cybersecurity career education pipeline/pathway in resolving pressing workforce development needs/capability gaps. The career pipeline/pathway objective is preparation for entry-level California IT Sector Job classification and technical specialization in cybersecurity/or related information security/engineering area/positions (including necessary KSAs, competencies, and hands-on experience) and 2-Year/4-Year/6-Year degrees and professional certifications (in Cybersecurity, Information Technology, Information Systems, Computer Science, Computer/Electrical Engineering, and related fields).

CYBERSECURITY CAREER EDUCATION PIPELINES AND PATHWAYS

There is still much work to align California State Cybersecurity Workforce/ IT Security Job Classifications and Private Industry/NGO employers (employer need/demand) into career pipeline/pathway programs. A cybersecurity education career pipeline/pathway is an important strategy and feasible plan of action towards resolving continual cyber workforce/skills capability gap issues across the state. Cybersecurity education career pipelines/pathways benefit the residents of California by enhancing the accessibility and availability of cybersecurity education and workforce development programs, opportunities, and resources.

Prior to discussing the details of cybersecurity workforce supply/demand; and strategies to bring workforce numbers into equilibrium (similar numbers of available positions with prospective employees), we introduce several foundational subjects including definitions of key terms.

One topic of discussion and on the role of "pipelines" and "pathways" within education and workforce development is in emerging "high need" areas as cybersecurity. A pipeline is the process of "vertical track" alignment across segments of the education system that is seamless and extraordinarily easy to transition from one level of education to the next. For example, K-12 Education, Community Colleges (2-Year), State Universities (4-Year), Graduate Programs (6-Year), and Advanced Graduate Degrees (Ph.D.'s) education programs linked and aligned together to promote a smooth flow of information and students from program to program.

In addition, IT-Cyber strongly emphasizes the value of Industry Professional Certification/Credentials. We must collaborate with the public, private, and (NGOs) to include "stackable certificates" together with workforce development opportunities to achieve statewide workplace supply/demand equilibrium. The key is coordination and facilitation among major partners and stakeholders here. We focus on making connections and forming collaborative partnerships to help in the coordination process of linking dots together in an otherwise complicated puzzle of cybersecurity education and workforce development. We must develop education programs and workforce opportunities to support many job domains/classifications/types of positions found across the large cybersecurity (and related IT/IS/CS/Information Assurance, etc.) enterprises.

REPORT SECTION SUMMARY

The California Cybersecurity Workforce Development and Education Strategy report is broken up into the following CCCEPPP design, development, and implementation sections:

CCTF WDE Subcommittee Recommendations- Section IV

California Cybersecurity Career Education Pipelines and Pathways- Section V

Cybersecurity Career Education Pipeline/Pathway Systems Architecture- Section VI

California Cybersecurity K-12 Education–Section VII

California Cybersecurity Associate Level Education- Section VIII

California Cybersecurity Bachelors Level Education- Section IX

Undergraduate Cybersecurity Model Curriculum/Academic Standards- Section X

California Cybersecurity Career Education Pipeline/Pathway Project Implementation Tasks/Activities/Deliverables- Section XI

The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

The next report section goes into specifics of the recommendations and strategies to enhance industry's ability and meet workforce demands with properly qualified candidates. We also discuss strategies to enhance the supply of prepared cybersecurity professionals into the field over the next decade (2020-2030) of CCCEPPP program implementation. The Subcommittee hopes these recommendations significantly and strategically enhance California Cybersecurity Workforce Development and Education posture, enhances capabilities, and fills numerous current/future positions with a highly qualified/well-prepared workforce that easily meets/surpasses position minimum and preferred requirements.

SECTION IV- CCTF WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE RECOMMENDATIONS

Recommendations for a California Cybersecurity Career Education Pipeline and Pathway Project:

The California Cybersecurity Task Force (CCTF), Workforce Development and Education Subcommittee proposes the following recommendations to the CCTF Executive Committee and Senior State of California Administration for their consideration of a comprehensive California Cybersecurity Career Education Pipeline/Pathway.

This report lays out a series of Workforce Development and Education Subcommittee recommendations and framework for their completion in the partial fulfillment of our requested Subcommittee duties in service of the California Cybersecurity Task Force and Senior California Government Administration.

As a Subcommittee comprised of cybersecurity education and workforce development Subject Matter Experts (SMEs), the purpose of these recommendations is to guide, assist, and support California Administration Decision-makers and Policy-makers in innovating strategies, policies, and leadership towards significantly enhancing statewide critical cybersecurity and workforce development/education capabilities statewide.

One key Strategy Document objective is to provide a blueprint or template/framework for the CCCEPPP and related tasks/activities. The key to successful career pipelines and pathways is not just a pure reliance on curriculum and academics; but also to include critical "hands on" applied professional learning opportunities as essential components of all cybersecurity education and workforce development programs. However, coordinating and linking all these programs and activities is a true challenge and we speak of these alignments throughout this report.

Recommendations Section Overview:

The purpose of this report section is to provide and discuss CCTF WDE Subcommittee recommendations to design, develop, and implement a statewide California Cybersecurity Career Education Pipeline and Pathway Project (and related Educational Institution Toolkits).

- A Statewide CCCEPPP is an essential tool towards reducing current and future urgent cybersecurity workforce gaps.
- The objective of the Cybersecurity Educational Institutions Toolkit is to assist numerous statewide educational institutions to protect sensitive digital information, harden critical cyber infrastructure, enhance information sharing, and better leverage existing State of California cybersecurity resources.
- California Cybersecurity Education and Workforce Development Clearinghouse (Where all information will be stored and publicly available).
- The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

Recommendation #1- (The California Cybersecurity Career Education Pipeline/Pathway Project (CCCEPPP)

Develop and implement a statewide cybersecurity workforce development career education pipeline pathway to prepare 50,000 cyber-and information security entry-level professionals in a ten-year period (2020 to 2030) to address current and future California critical capability skills/gaps and cybersecurity employment needs.

Project Deliverable #1- The CCCEPPP:

CCCEPPP SCOPE OF WORK:
Phase I Activity- 2019-2022 Cybersecurity Pipeline: Middle School (6^{th}/-7^{th} Grade) through Four-year Undergraduate Degrees (Bachelors of Science/Dual Baccalaureate Cybersecurity Programs); embedded stackable professional certificate program components.

Phase II Activity- 2022-2024 Cybersecurity Pipeline: Pre/Transitional K to Middle School (6^{th} Grade), Advanced Graduate/Doctoral Degrees with stackable professional certificate programs.

K-12 Cybersecurity Education Components:
1. K-12 Education: Develop and Implement Cybersecurity Industry Recognized Certifications- Middle/High School Career Technical Education (CTE).
2. Curriculum Integration of "A-G" Graduation Requirements with CTE courses.
3. California Computer Science and Additional Academic Standards.
4. California Cybersecurity Education and Workforce Development Clearinghouse.

Higher Education Cybersecurity Components:
1. Associate Education: Support and enhance Cybersecurity education programs (degree and certifications), engaging/current courses, solid instructional/teaching materials/labs/projects.
2. Bachelors Education: Develop and Implement Cybersecurity education programs (degree and certifications), engaging/current courses, and solid instructional/teaching materials/labs/projects.
3. Cybersecurity Stackable Professional Certificate Programs in "High Demand" Specializations (Entry Level, In-Service)

Additional Cybersecurity Education and Workforce Development Components:
1. Develop and support cybersecurity extracurricular activities (like California Cybersecurity Competition League and affiliated Cyber competitions, Summer Coding Camps, After School Computing activities, etc.).
2. Academic Infrastructure Capacity Support and Growth- Education/Workforce Development and Cyber Program Road Map Preparation and Distribution.
3. Support for: Military-civilian transition, veterans, disabled veterans/spouses.
4. Strategic Initiatives and support for: Underrepresented Backgrounds in Cyber/Tech. Women, Race/Ethnicity, and Socio-Economic Status.
5. California Cybersecurity Apprenticeship Centers.
6. The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

Table 3: Summary CCCEPPP Sources/Numbers of Cyber Pipeline Participants:

Cyber Pipeline/Pathway Sources	Planned Number of Participants	Cumulative Totals
Military-Civilian Transition/ Veterans/Disabled Vets/ Spouses	**17,500** Pipeline Participants	17,500
Associate- 2 Year Degree Program (Cyber, IT, CS) + Apprenticeship	**20,000** Pipeline Participants	37,500
Three year Education +1 year Apprentices (IT-1); 2+2 ed/exp.	**6,500** Pipeline Participants	44,000
Bachelors Level Degree Program (Cyber, IT, CS) + 1 year Apprentices (IT-1/2)	**4,000** Pipeline Participants	48,000
Masters Level Degree Programs (IT-1, IT-2)	**2,000** Pipeline Participants	50,000

The objective of the CCCEPPP is statewide preparation of 50,000 cybersecurity entry-level professionals over a ten-year project period. For planning purposes, the summary chart above describes the anticipated numbers and sources of pipeline participants (including cumulative totals). We discuss all sources of participants in respective report sections. From the numbers provided above, a majority of pipeline participants are coming from California Community Colleges and the many wonderful degree and certificate programs they offer in IT/Computer Science, Cybersecurity, and related fields. Another large number of cyber pipeline participants are transitioning military, veterans, disabled veterans, and spouses. In addition, we rely on students with several years of education and experience, including certificates of completion and apprenticeship programs with 2000 hours on the job training as fully prepared and ready to enter the cybersecurity field.

Whatever the source of pipeline participants may be, it is critical that "road maps" of all essential information (including education programs, workforce opportunities, available apprenticeships/positions, cyber-competitions, hackathons, etc.) is available to guide prospective students into various IT-Cybersecurity specializations. A complete and annually updated dashboard (describing clearly direct paths into employment) will assist with cybersecurity workforce development and education. The "road map" should be available and easily accessible to students of all ages for IT-Cyber career awareness and guidance purposes. Key Roadmap points and components discussed in the following report section on caveats of career education pipelines and pathways.

CRITICAL TAKE-AWAY: The key is not only in facilitating collaboration among all major partners and stakeholders in the eco-system. It is also about communicating to students the process and steps to follow to meet entry-level position minimum requirements (including KSAs and competencies) and graduate from the education component. Then we work with industry and employers to make sure we know what they are looking for in the hiring process. Finally, we network and link program graduates with employers: for either work experience (like apprentices or OJT) or an entry-level position for those appropriately qualified.

Key Caveats for Cybersecurity Career Education Pipelines/Pathways:

1.) Successful career pipelines seamlessly blend, link, and align education segment components. K-12 Education, Associates-level (2 year programs), Bachelors-level (4 year programs), graduate programs (Masters, Doctoral programs), and Professional Certifications/ Workforce Development/Training coordinated and working together in response to critical cybersecurity workforce shortages. Effective and smoothly operating pipelines form a coordinated, comprehensive, and strategic program with the objective of preparing and advancing qualified graduates through the education process with KSAs and competencies to meet employer minimum requirements for cybersecurity positions and employment.

Specific report recommendations facilitate coordination and collaboration at each segment/level of education. In a career pipeline, educational levels closely link and align with the programs and courses coming before and after them. Each level of education continually reinforcing the building blocks of cybersecurity education foundations found earlier; yet also serving as building blocks for more advanced student preparation. This is particularly valuable when looking at the "top end" talent tool in what would otherwise be considered a rigorous STEAM academic discipline with potentially very complex technical skill sets and competencies.

Each level of cybersecurity education and workforce development programs links and networks the education/academic community with the professional industry community. Subcommittee recommendations includes detailed information on objectives, rationale/justification, suggested order of tasks/activities to complete, and project implementation time-frames found below:

K-12 Education Recommendations (see Recommendation #2 and Page #62)

2 Year Associates Level Program s (see Recommendation #3 and Page #65)

4 Year Bachelors Level Programs (see Recommendation #3 and Page #65)

Graduate Programs- Masters, Doctoral (see Recommendation #4 and Page #69)

Professional Certification and Training (see Recommendation #5 and Page #71)

2.) Specific career pipelines/pathways direct students to timely completion of college preparedness and career readiness programs to finish position minimum requirements and competencies and transition into professional positions in cybersecurity. As such, students need to know upfront all necessary minimum/preferred qualifications (education/experience/skills) for specific positions they may be interested in; Cybersecurity Intelligence Analyst, for example. What steps are required for a potential candidate in a particular career pathway to get the desired position? Once students know their career direction/aspirations—it is crucial that students then have the access to available cybersecurity education programs to meet/exceed cybersecurity position minimum requirements and transition successfully into desired positions after graduation.

Because of the technical and specialized nature of the cybersecurity fields, we need to trace career pathways at all segments/levels of education from K-12 through 2- Year/ 4- Year/ Graduate/Ph.D. programs and Professional Certifications to meet the diverse challenges of the cyberspace enterprise moving forward. All information must be clearly conveyed to students in **California Cybersecurity Education and Workforce Development Road Maps** so students can plan their futures with cybersecurity career positions in mind.

3.) An additional complexity with cybersecurity education and workforce development is the essential need for programs to span both academic and applied (experiential) "real world" experiences. In order to complete appropriate preparation and skill/competency mastery in the field of cybersecurity, a variety of "hands-on" learning and practice are critical. Internships, apprenticeships, and digital community service projects are examples of experiential learning opportunities. Generally, "cyber-ranges" develop where students hone and polish skills in a controlled, guided, and supportive learning environment are also helpful to meeting workforce development/education objectives. Other students may need advanced research and lab opportunities to prepare them for their career track.

Cybersecurity education programs should often pair with structured workforce experiences like Pre- and Registered Apprenticeship Programs and On the Job training opportunities. As a note, all OJT mentioned in this report is set at 2000 hours (or one year work year experience) and overseen and administered by **California Cybersecurity Apprenticeship Centers**. This point is covered in additional detail in the *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

4.) To be successful, public and private sector key partners/major stakeholders must collaborate and work together earnestly to design education and workforce development programs that assure prospective employers program graduates can demonstrate the necessary knowledge, skills, abilities, and competencies to get the job done upon graduation. Cybersecurity education programs must address and prepare all segments of the talent pool, through utilization of a Bachelor of Science (B.S.) Degree in Cybersecurity, Dual Baccalaureate Cybersecurity Degree Program (interdisciplinary program linked with any college major and 2000 hour "On the Job" (OJT)), and stackable professional certifications programs supporting public and private sector industry. Many of these education programs are paired with workforce development opportunities.

5.) It is essential to provide a comprehensive, coordinated, and linked series of cybersecurity model curriculum and academic standards at all levels of education to support a "vertical track" of education programs (including degree and industry recognized stackable certifications). In addition, we add significant professional development opportunities and tools necessary to navigate the job selection/hiring process, subsequent professional success, and upward mobility/promotion to increasingly senior positions and management within the organization.

ADDITIONAL SUPPORTING CYBERSECURITY CAREER EDUCATION PIPELINE/PATHWAY RECOMMENDATIONS

In order to achieve the over-arching objectives of recommendation #1 "*The California Cybersecurity Career Education Pipeline/Pathway*," we also include a number of supporting recommendations (#2 to #12) to flesh out the details of specific components of the cybersecurity pipeline/pathway and related support mechanisms. The recommendations provide context, guidance, and structure for the components necessary to integrate together into a comprehensive, coordinated, linked and seamless strategy and network of cybersecurity workforce development and education programs statewide.

Recommendation #14 supports Cyber-hygiene and related education and awareness activities.

Recommendation #15 supports educational institutional cybersecurity incident response, information sharing, and "hands-on" Security Operations Center (SOC) training.

Recommendation #2- (K-12 Cybersecurity Education)

California needs a coordinated, comprehensive, standardized, and accessible series of Cybersecurity education programs at the K-12 segment/level of education. K-12 Cybersecurity education programs, courses, curriculum, extra-curricular activities, cyber competitions, and professional development opportunities must solidly connect and seamlessly transition into college preparedness and career readiness programs found in Higher Education and workforce development (training) programs statewide.

Integral parts of the CCCEPPP include: Program/Course Model Curriculum and Academic Standards, Matriculation/Transfer Agreements. Design cross-walk, and promulgate California Department of Education Career Technical Education (CTE) Information Communications and Technology (ICT)/Public Service (PS) Model Curriculum and Anchor Standards, Computer Science Academic Standards, with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. More information on K-12 Cybersecurity Education found in the next three report sections, but we introduce several key items below.

K-12 Education Program Recommendations included in the report:

1.) Stackable Industry Recognized K-12 Education Cybersecurity Certificate Programs-

The development of a series of Cybersecurity Industry Recognized Stackable Certificates—covering all levels of cybersecurity background (Exploring, Intermediate, and Advanced Cybersecurity) with additional Cybersecurity-related Industry Sectors and occupational clusters like Public Service or for Small/Medium sized Business. Courses developed in the online/remote learning format and virtualized with storage, available cyber range hosted on state servers. As all content is virtualized and available online, schools and districts will not be on the financial hook for purchasing expensive technology for computer labs/computing resources so

students can complete cyber certificate programs and courses. Additionally, as Cybersecurity Certificate Programs are online, these courses will be readily accessible and available to all California students irrespective of geographical location and socio-demographic background. In the name of digital equity, it is important to continue and expand the number of students with a computer and high-speed internet connection at home to reduce the "digital divide" impacting students' ability to study and work from home. The digital divide is an obstacle/barrier discussed in detail shortly.

Additional Information found on K-12 Stackable Certificates found in Section VII- California Cybersecurity K-12 Education

Additional Information found on K-12 Stackable Certificates in Section XI- CCCEPPP Implementation/Tasks/Activities/and Deliverables

2. Cybersecurity "A-G" Course Integration (Academic courses linked with Career Technical Education (CTE) Courses-

We need "Curriculum Integration" of Cybersecurity, Computer Science, and IT topics with "A-G" core graduation requirements and elective courses to assist students on the college readiness track. For students on the STEM college preparedness track in high school, there is not much room for extra coursework to fit into an already tight academic schedule. The purpose of curriculum integration is to link "A-G" graduation requirement courses like Math, English Language Arts, Science classes, with CTE Industry Sector subject materials; in our case, courses with a solid cybersecurity/computer science/IT foundation. The course "integrates" key materials from the academic side ("A-G") with CTE industry sector "vocational" model curriculum/academic standards. Examples linked below.

The net result is that students are meeting graduation requirements and taking core courses carefully aligned and blended with relevant CTE course materials and specialized learning. Course curriculum integration occurs with California Department of Education (CDE) (CTE) Information Communications Technology (ICT) Industry Sector Pathway (and related pathways) and Single Subject Credential educators drawn across state urban and rural school districts.

Sources of Relevant Documentation from NIST and CDE found below:

https://www.cde.ca.gov/ci/ct/sf/documents/infocomtech.pdf

https://www.cde.ca.gov/ci/ct/sf/documents/pubservices.pdf

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

Additional Information on Curriculum Integration found in Section VII- California Cybersecurity K-12 Education

Additional Information on Curriculum Integration found in Section XI- CCCEPPP Implementation/Tasks/Activities/and Deliverables

3. California Computer Science and Additional Academic Standards-

It is important to remember that cybersecurity is a growing and maturing academic discipline and professional field. This is why we need to implement a cybersecurity career education pipeline/pathway in the first place—to enhance and quicken this maturation process and also to develop necessary digital infrastructure to support these educational programs. **However, cybersecurity still falls under the umbrella of Computing and Information Technology on the organization chart. This means that by supporting Computer Science and IT disciplines and fields, we also enhance cybersecurity learning/teaching as well.** One key component of K-12 Education relating to cybersecurity is the State Computer Science Standards recently adopted in 2018. A good deal of information on computer science standards and analysis found in the next sections of the report. For those who would like to see the standards, please follow the CDE link:

https://www.cde.ca.gov/be/st/ss/computerscicontentstds.asp

Additional Information on Computer Science/Academic Standards found in Section VII- California Cybersecurity K-12 Education

Additional Information on Computer Science/Academic Standards found in Section XI- CCCEPPP Implementation/Tasks/Activities/and Deliverables

4. California Cybersecurity Education and Workforce Development Clearinghouse:

Much of the issue with cybersecurity education and workforce development/training is not an absence of quality materials and resources. Rather, it is an issue of coordination, facilitation, access, and ease of availability of a tremendous amount of resources and materials in cybersecurity education and workforce development. To break down potential silos within cybersecurity field amongst education/academia, private/public, we need to bolster the availability, visibility, and awareness of educational/instructional/learning resources in collaboration with major partners and key stakeholders state-wide.

There are a variety of enhancement of academic programs, resources, clearinghouse of best practices in K-12 cybersecurity academic programs, student support, instructional support, instructor toolkits, and resources for educators in elementary, middle, and high schools found under this subcommittee recommendation. There is also additional information to link into a comprehensive California Cybersecurity Education Clearinghouse tied to CCCEPPP.

Additional Information on California Cybersecurity Education and Workforce Development Clearinghouse found in Section VII- California Cybersecurity K-12 Education

Additional Information on California Cybersecurity Education and Workforce Development Clearinghouse found in Section XI- CCCEPPP Implementation/Tasks/Activities/and Deliverables

Recommendation #3- Implement an Associate in Science Cybersecurity Degree (A.D.T. Program) with linked 4 year Bachelors of Science Cybersecurity Degree Program with embedded stacking certificate program specializations.

The third recommendation is the development and implementation of a Cybersecurity Model Transfer Curriculum (MTC) program (short-term objective) and Associate Degree Transfer (A.D.T.) program (long-term objective). In California, the 2- Year/4-Year transferable ADT is the "gold standard" for new and existing degree programs. The true value of an ADT is in the seamless/smooth transition for transferring 2-year to 4-year degree program students.

In the future, it would be ideal to have an Associate Transfer Degree Program (ADT) linking 2-year degree programs (Associate in Cybersecurity) with 4 year degree program (Bachelors in Cybersecurity). Participating California Community College, California State University, and University of California campuses partnering together, coordinating on program/course design, and offering specialized cybersecurity degree and certificate programs would be essential to making this career pipeline/pathway successful, particularly given the large scale of the CCCEPPP (i.e. 50,000 participants over a ten year time frame).

Cybersecurity is often a technical and specialized field; and getting more so every day. Cybersecurity foundations and principles do not fall cleanly into any one current academic discipline. Further technical specialization and tremendous technological innovation draw out a critical need for a distinct cybersecurity degree program to meet substantial and escalating societal needs for computer savvy specialists and analysts. There is a closely related computer science and IT element; and combination of key engineering, science, math, technology, and business fundamentals necessary for success on the technical side of the cyber field. We work closely with academia, public/ private sector, and NGOs to design undergraduate cybersecurity programs/courses to meet critical knowledge, skills, and competencies for current "high demand" specializations and positions.

Implementation Task Activity/Steps: In Progress: Priority: High.

Timeframe of Implementation:

I. **Lower Division Level:** *Computer Science AST Program*- Already Approved.

IT Model Curriculum- Already Approved.

These programs serve as the foundational lower division component of the Bachelors of Science in Cybersecurity Degree program.

Upper Division Level: Cybersecurity Draft Bachelors of Science in Cybersecurity Curriculum: Linked, aligned, and articulated with Associate-level (2 Year degree and certificate programs) mentioned above. Upper division model curriculum/ and academic standards completed in **2020-2021 AY** with local campus curriculum review process.

Further detail on Associate and Bachelor Cybersecurity Model Curriculum and Academic Standards found in later respective report sections.

Recommendation #4- (Graduate Programs, Faculty Research, Teaching, and Service)

Cybersecurity graduate programs should be included as an important component of a career education pipeline/pathway. Not because most entry-level cybersecurity positions require Masters/Doctoral degrees as a required position minimum qualification. Rather, we need graduate programs (at both the Masters, and Ph.D. levels) to advance a variety of critical education, teaching, and research activities directed at cybersecurity in general and specific "high demand" specializations as well. Objectives met by supporting advanced/technical cybersecurity advanced degrees; enhancing faculty teaching and student learning; professional development; and research/community service opportunities. One key reason to support cybersecurity graduate degree programs is that there is where the new instructors, educators, and professors are developed and prepared. As we are discussing a significant boost to the number of new cybersecurity students, we are also going to boost the number of freshly minted educators, instructors, and professors.

This recommendation encourages the growth of cybersecurity education statewide as a blended academic discipline with significant professional workforce development and field applications. This recommendation links and relates to a variety of additional recommendations found in this document. For example, graduate programs and advanced work here translates into more instructors, better-prepared faculty ready for the rigors of teaching cybersecurity in the classroom. Recommendation #4 is a key role and support mechanism of enhancing the numbers of educators and professors teaching in cybersecurity, computer science, IT/IS programs. If we plan to increase the number of students in cybersecurity study statewide, we must also take solid steps and incentives to increase the number of specialized teachers and faculty in educational institutions. We need to take additional steps to support these programs and their further contributions to advance cybersecurity education, research, and collaboration.

Additional Cybersecurity Graduate Program Education information found in report Section XIII.

Recommendation #5- Align Professional Certifications, Workforce Development Training with Education Programs and CAL HR IT Job Classifications

More work and coordination to align cybersecurity education with workforce development, training, and professional certifications with HR departments has been increasing in past years, but still has a way to go. Research has been conducted on HR IT Job Classifications and these findings need to be incorporated into strategies for enhancing state-hiring practices for cybersecurity and information security specialists (along with related positions in state IT Job Classifications). See CCTF, WDE Subcommittee Objective 1 Report link in report Section 2.

The ultimate CCCEPPP objective is to place graduating students (from various exit points in education) into professional cybersecurity entry-level positions. There is much coordination necessary to efficiently align the education/workforce development process with the transition into the professional cybersecurity field and the recruitment/selection/hiring process.

Implementation Task Activity/Steps: In Progress: Priority: High

Recommendation #6- Educational Capacity and Instructor Support Component- simultaneous development of a specialized career pathway intended for cybersecurity educators, instructors, and professors (K-12 and Higher Education);

Discussion: Professional Development- Statewide Educator Capacity/Capability Enhancement and Certificate Implementation:

In addition to model curriculum and academic standards in K-12 cybersecurity education, there are many additional components to keep in mind for an efficient career pipeline. After all, if we are planning on dramatically increasing number of cybersecurity program graduates to quench the fires of a hot skilled cyber labor/workforce demand in a career pipeline; we need to dramatically increase the numbers, resources, and instructional materials to enhance statewide instructor capability and capacity (the academic infrastructure.)

One way this is accomplished is through enhanced instructor professional development. Again, this differs in ways from other model curriculum and academic standards described previously. Instead, this pedagogical focus/discussion is not on "what to teach," but rather "how to best teach" (cybersecurity for our example.) In other words, what are effective cybersecurity instructional practices and how do we promulgate them to a cadre of instructors and then into the classroom? Huge opportunities exist in cybersecurity education professional development. Available cybersecurity resources may help answer the question of "what to teach. However, there is not much evaluative research and available resources on "how to teach" cybersecurity and how students best learn these subjects and skills.

One related idea here is that cybersecurity curriculum providers have already produced much rigorous and relevant content. However, there is little mention of the accompanying instructional strategies based on institutional assessment and student success. So we need to develop, as a part of the cybersecurity career pathway, projects centered on instructor resources, research, and support to effectively deliver cybersecurity instruction at all levels of education. Many of these items are discussed in greater detail in report Section XI on prospective projects, deliverables, timelines, and milestones.

Justification: We are talking about a significant increase in the numbers of students in cybersecurity programs and supporting the career pipeline/pathway. One of the major issues and limitations we have in developing/implementing cybersecurity career pathways is limited numbers of instructors (across all levels of education) who teach the more rigorous math, science, and computing courses. We need to assist instructors (and potential ones) how to master the teaching and learning of cybersecurity, computer science, and information technology.

Increasing cybersecurity educational capacity and support is developed by recruiting and preparing a cadre of cybersecurity educators for strong "teacher training" education and workforce development training programs. Initially, we are describing a **Cybersecurity Education and Teaching Certificate Program** recruiting and retaining quality instructors (please see below.)

Potential Solutions: Certificate program development in Cyber-Computer Science/IS/IT Education (online programs) to support the cyber pipeline for educators. Design creative incentive programs and additional instructor toolkits to increase the number of CTE faculty and instructional staff to teach the larger numbers of students attending cyber (and related) programs. If we are planning to increase numbers of cybersecurity students, we must likewise increase numbers of instructors too.

Implementation Task Activity/Steps:

Phase 1- Cybersecurity (K-12) Education Instructor Certification-

Phase 2- Cybersecurity (Undergraduate) Education Instructor Certification-

Phase 3- Cybersecurity (Graduate) Education Instructor Certification-

Phase 4- Cybersecurity Instructor Incentives Program and Resource Development-

Develop incentive programs, including tuition reimbursement and incentive programs to recruit qualified K-12 and higher education instructors and train them for rigorous cybersecurity academic and career technical education programs. Find ways to attract and recruit additional cybersecurity instructors and professors, such as reduced tuition costs, utilization of V.A G.I. Bill and related student scholarships/stipends/ loan forgiveness to significantly bolster numbers of statewide instructional faculty.

Timeframe of Implementation: Priority: High/Medium

Phase 1- Cybersecurity (K-12) Education Instructor Certification- (2020-2022 High Priority Activity).

Phase 2- Cybersecurity (Undergraduate) Education Instructor Certification- (2021-2023 High Priority Activity). [Designer Note- Build this program in conjunction with the B.S. in Cybersecurity Degree Program and Courses. Launch Simultaneously.

Phase 3- Cybersecurity (Graduate) Education Instructor Certification- (2022-2023 Medium Priority Activity). [Designer Note: this course will be built out when future resources and institutions are ready to move forward on this phase.

Phase 4- Phase 4 implementation priority based on resources secured for this specific recommendation to increase California Cybersecurity Instructor numbers and enhanced capacity.

[General Note Across all Four Phases of Activity: incentive programs should include resources to expand the entire spectrum of IT-Computer Science, IS and related TECH educators, instructors, and professors as well.]

Recommendation #7- Extracurricular Activity Component- (coding camps through cybersecurity competitions); Designation of a State of California Cybersecurity Competition—"the Golden State Cybersecurity Competition."

Justification: What students are most likely to enter cybersecurity education programs, graduate from them, and seek career preparation into the field? Interested students who spend their lunchtime, after school time, and free time on weekends while participating with cybersecurity competitions and the many related tech and computing activities currently available. While cyber learning is often found in curriculum and academic standards, rigorous programs/courses, projects, etc.; there are also many exceptional opportunities outside the classroom to give students an opportunity to practice and hone their skills.

Any extracurricular activity that encourages computer science, IT, coding, bug bounties, hackathons, or similar programs/initiatives/projects needs to be supported as a key component of any comprehensive career education pipeline/pathway and included in **California Cybersecurity Education and Workforce Development Road Maps**. By making current and up-to-date information on cybersecurity extra-curricular activities across the IT-Computer Science, Cybersecurity space, we can expand the level of interest and availability of these programs across California and enhance opportunity for all students and prospective workforce.

Project Deliverable: Extracurricular Activity Component- Designation of a State of California Cybersecurity Competition, "the Golden State Cybersecurity League," California Governor's Cybercompetition Golden Cup; Cybersecurity Competition Cybersecurity Certificate Program Development; -

SCOPE OF WORK: Cyber competitions are an excellent team-based activity shared by students with similar interests and hence a natural area to recruit students into the career education pipeline. Set up a coordinated, organized, and efficient State of California Cybersecurity competition series at the K-12 and Collegiate Education levels accessible and available statewide. While cyber learning is often found in established curriculum and academic standards, rigorous programs/courses, projects, etc.; there are also many exceptional opportunities outside the classroom to give students an opportunity to practice and hone their skills. It is essential to expand extra-curricular activities like cyber competitions across underserved groups and geographic location as well. Participants (students and coaches) need enhanced support and resources to encourage those who may not have had access to these programs previously.

We should model the culmination of the "**California Governor's Cybercompetition Golden Cup"** as the signature annual cyber competition statewide held and awarded every summer. The "Governor's Golden Cup" should be similar to the California Cyberhub Competition held every summer, but we want to encourage all cybercompetion students to participate in these programs. We want all 58 California Counties to submit teams in both K-12 and Collegiate Division Cyber League competitions and activity. We want most California counties represented by 2024.We emphasize cyber competitions as one aspect of the relationship being built (at all levels of cybersecurity education) through the CCCEPPP. Local school districts, CCC, CSU, and

UC campuses statewide should participate and encourage students and faculty to contribute expertise and serve as mentors, coaches, judges, advisors and promote success. We would organize countywide cyber team competitions to function as League Activity in regional competitions rolling up into statewide final rounds.

We organize both a high school and collegiate division. Furthermore, we focus on preliminary round activity as a recruiting activity; assist new teams and coaches to the cybercompetition process and the means to success; yet also retain vigorous competition for advanced and veteran teams.

In addition, cybersecurity competitions assisted/supported by the ***K-12 Cybersecurity Competitions Certificate Program*** (providing team members knowledge, skills, and tools for success in League activities.) Additional information found in additional report sections.

MILESTONES, TIMELINES:

Implementation Task Activity/Steps: Priority: High

Timeframe of Implementation: TBD

County Wide Cyber Team Competitions- League Activity

Regional Cyber Team Competition League Activity

Statewide "Governor's Golden Cup" Statewide Final Rounds-

K-12 and Collegiate Divisions-

New and Advanced Teams Divisions-

Recommendation #8- Professional Development Component (Mentoring, Career Awareness/Preparation, job shadowing, research presentations, soft skills (like oral and written communication, team player, etc.);

In addition to aligning model curriculum and academic standards with extra-curricular activities in cybersecurity, we also need to provide a professional development component to the CCCEPPP. We must provide means of piquing interest in cybersecurity occupations and working in the tech field. These are the careers of the future. We need to begin career awareness and preparation as early in the education process as possible. We frequently hear that middle school preparation is college preparation. Students begin to make these key educational and career decisions in middle school. We must effectively guide them into the right direction starting as early as possible into IT-Computer Science/Cybersecurity pathways.

All cybersecurity professional development programs, projects, initiatives, etc. that encourages computer science, IT needs to be supported as a key component of any comprehensive career education pipeline/pathway and included in **California Cybersecurity Education and Workforce Development Road Maps**.

Implementation Task Activity/Steps: In Progress

Timeframe of Implementation: Priority: High

Recommendation #9- This recommendation has two distinct, yet related components:

I. Cyber Ethos/Ethical Hacking Education Component- Discuss the value of Public Ethos (Serving the Public, Serving the Field)-

II. Ensuring Employability, The Recruiting, Selection, and Hiring Component: Background Investigation for Classified/Public Safety Employment Selection: Character building;

This recommendation concerns the critical candidate recruitment, selection, and hiring processes. We must not only impart cybersecurity technical knowledge and skills to students in a career pipeline/pathway, but also guide them into securing the position as well. One key to success in cybersecurity selection/hiring is to stay away from risky behaviors that may disqualify someone from the job later on down the road. This can include a variety of factors from criminal history, illegal drug and alcohol abuse, credit rating issues, poor employment history, dishonorable discharge from the military, etc. We must find ways to inform students earlier in their academic programs of the potential impact of our decisions and life choices on employment opportunities later on in the future. These subjects of ethics and serving in the cybersecurity profession ethically are found under "soft skills."

In terms of ethical hacking, we must provide good advice and guidance to prospective cybersecurity/information security specialists throughout the entire career pipeline/pathway from start to finish. We do not wish to teach a sensitive knowledge and skills without informing and counseling students of great responsibility and trust that goes along with data and secure systems/computers/etc. Focus on ethics and good online decision-making. Not just in terms of hacking or mischievous online behaviors, but also in utilizing sound personal judgement as well.

This career pathway supports the California cybersecurity workforce development and professional employment pool. It is important to educate students going into the public sector on "Public Service Ethos" and what it means to serve the public. There are enhanced expectations placed on public sector employees in part because public funds support the position. In addition, due to the very sensitive type of work found in select agencies (Public Safety, Defense, Intelligence to name a few) and private firms (defense contractors, life sciences, high tech, financials, biotechnology)—it critical that students are aware of potential employment screening/background investigations. There is value found in solid employment history, personal history statements, good credit, etc. found in the hiring process at some employers and for select highly sensitive positions.

Because of challenges that background investigations pose for classified employers, we dovetail this discussion with *Recommendation #11- Transitioning Military, Veterans, and Disabled Veterans into a cybersecurity workforce pipeline/pathway.*

To meet the spirit of these essential recommendations, we include cyber ethics and the candidate selection/hiring process into all appropriate places throughout CCCEPPP programs, courses, and projects.

Implementation Task Activity/Steps:

Phase 1- Embed Cyber Ethos/Ethical Hacking, Public Ethos, Ensuring Employability, The Selection/Hiring Process, Background Investigations (as necessary), and Character building into WDE components.

Phase 2- Strengthen and enhance ethics and employment resources,; place all related materials online in the California Cybersecurity Education Clearinghouse.

Timeframe of Implementation: Priority: High

Phase 1- (2019-2022 High Priority Activity).

Phase 2- (2021-2023 High Priority Activity).

Recommendation #10- Application of Learning Component: Cybersecurity Professional Development Apprenticeships, Internships, and Project Management;

Cybersecurity is often a very technical field. It relies on the application of learning, knowledge, and skills to complex problem solving. As such classroom learning is important, but what is really lacking is in the coordination of apprenticeships (longer term-1000-2000 hours), internships (short term commitment usually 100-200 hours), and workforce development opportunities. In addition, one common comment heard from industry representatives (both public and private sector) is a lack of focus on project management; both in terms of familiarity with team/group project facilitation, but also in the actual project management process (through all phases of a project, including grant work, planning, implementation, assessment/evaluation, etc.).

Discussion: One key aspect of career pipelines is the linkage with application and experience and real world experience. The same can be said of needs for a prepared and qualified cybersecurity workforce. Any talk of a cybersecurity career pipeline/pathway must also include tight linkage with experiential (applied) learning opportunities outside of the classroom. Thus, one way to support student's professional development efforts and encourage their participation in cybersecurity education programs is through internship and apprenticeship programs and local/regional partnerships with industry. One key subcommittee activity is to collaborate with major partners and key stakeholders towards the objectives of providing paid cybersecurity apprenticeship and internship opportunities across California to support workforce development efforts. The skills and experience gained with substantially augment and enhance student classroom/academic learning found within cybersecurity. Cybersecurity is a "hands on," skill based competency set, and does not rely solely on theoretical and "book" knowledge.

There is a second key strategic point brought to bear here. We need to **assist and support school districts and local campuses to develop cybersecurity programs and public/private partnerships that result in paid local/regional student apprenticeship/ internship opportunities. Education and workforce development programs are expensive, particularly when there is a gap in available cybersecurity infrastructure to overcome as well.**

We look to maximize districts' "buy in" and "participation in cybersecurity education and workforce development and offering lots of CTE opportunities. In other words, use the intern/apprentice component as a coordinating activity to gain multiple funding streams/sources and spread investment costs amongst the beneficiaries of sound regional/local workforce development/training and education programs. A solid and well provisioned employment pool benefits all local and regional employers in areas with chronic cybersecurity workforce shortages and capability/skill gaps.

This recommendation seeks to find strategies to help school districts develop cybersecurity programs and partnerships that result in internship and youth pre- and apprenticeship opportunities for students and consistent with CCCEPPP mission and objectives.

Implementation Task Activity/Steps-Timeline

Phase 1- Regional and Local Cybersecurity Market and Labor Analysis- identify and link cybersecurity education/academics with public and private sector employers.

Identify and recruit business and government to support apprenticeships and internships as part of the labor market analysis.

Phase 2- Develop model K-12/postsecondary transition apprenticeship **PILOT** programs in partnership between educational institutions and public/private sector employers in select regions in California.

Phase 3- Expand K-12/postsecondary transition apprenticeship **PILOT** programs to additional regions in California over time.

Phase 4- Assess and measure impact and benefit of these programs state-wide.

Priority: Variable depending on resource streams.

<u>Recommendation #11- Transitioning Military, Veterans, and Disabled Veterans into cybersecurity workforce career pipeline;</u>

The cybersecurity community, professional field, and workforce development greatly benefit the inclusion of candidates from transitioning military, veterans, and disabled veterans. Thus, the subcommittee recommendation involves strategies and support mechanisms for the recruitment and retention of Military IT MOS into the civilian cybersecurity workforce where they can put their experience in a diverse set of specializations into closely related positions and jobs

throughout California. Individuals with military service are used to working in dynamic environments, using soft skills like oral and written communications, team players, strong leadership, and essential skills with additional employability/selection/hiring traits.

In addition, for positions that involve classified information or highly sensitive data, the active background clearances of transitioning military and veterans could expedite the hiring process and potential advantage in the formal hiring process.

Finally, a third element of this recommendation includes the utilization of their military career experience and training to serve an educational role as teacher, advisor, mentors, and cyber coaches for the increased numbers of students entering and pursuing cybersecurity career education pipelines and pathways.

Implementation Task Activity/Steps- Timeframe: IN PROGRESS

Timeframe of Implementation: Priority: <u>High</u>

Phase 1- (2019-2022 <u>High Priority Activity</u>).

Phase 2- (2021-2023 <u>High Priority Activity</u>).

<u>Recommendation #12- (Strategies to enhance the participation and retention of Women in Cybersecurity and Technological Fields).</u> Building and reinforcing a **s**upportive culture that promotes equity for women in cybersecurity, computing, and IT. This includes the development and implementation of strategies intended for a transformation of cultural and workplace values and related support mechanisms to foster enhanced interest and encourages inclusivity into the field. Furthermore, strategies and policies for career exploration, peer mentoring, and preparation for entry-level cyber employment, recruiting, hiring, retention, and promotions as valued and successful members of cybersecurity (and related) fields.

The inclusion of women into the tech and cybersecurity enterprise is an essential part of closing the California cybersecurity workforce gap. It is imperative to deploy strategies to enhance the numbers of prepared cybersecurity women professionals across industries and sectors. Thus we include separate recommendation for strategies to support and encourage women into the cybersecurity, computing, and IT as well accomplish a significant reduction and elimination of gender disparity existing within this field.

One fundamental CCCEPPP core component is to encourage significant IT-Cyber workforce development and education opportunities for girls and women. To accomplish this objective, we must embed linkages and support mechanisms for gender inclusivity at all stages of a cybersecurity career pipeline/pathway. We start programs early in the education process (Kindergarten--5 years of age) and continue to reinforce them through Associates/Bachelor's Degree (20 somethings) in cyber fields, related extra-curricular activities, and professional/career/ experiences. A variety of strategies embedded into all educational components/ levels to fully support women and girl's entry and success in the academic and professional cybersecurity workforce found in the CCCEPPP.

Thinking of strategies and recommendations that are consistent with all elements of the NICE Workforce Framework Defining Cybersecurity, "…(as) the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce." [38] Strategies must be in place to assist with inclusion, diversity, and evening the playing field with utmost haste in all workforce development and education strategies.

Implementation Task Activity/Steps- Timeline: IN PROGRESS

Timeframe of Implementation: Priority: <u>High</u>

Phase 1- (2019-2022 <u>High Priority Activity</u>).

Phase 2- (2021-2023 <u>High Priority Activity</u>).

<u>Recommendation #13- (Strategies to enhance the participation and retention of Underrepresented Historical Backgrounds in Cybersecurity and Technological Fields).</u> Building and reinforcing a supportive culture that promotes equity for traditionally underrepresented backgrounds in cybersecurity, computing and IT. Furthermore, strategies and policies for career exploration, peer mentoring, and preparation for entry-level cyber employment, recruiting, hiring, retention, and promotions as valued and successful members of cybersecurity (and related) fields.

This includes the development and implementation of strategies intended for a transformation of workplace and related support mechanisms to foster enhanced interest and encourages inclusivity in these fields from underrepresented groups, including persons of color, members of Tribal Sovereign Nations, and persons of varied economic backgrounds across California. Strategies must be in place to assist with inclusion, diversity, and evening the playing field with utmost haste in all workforce development and education strategies.

Implementation Task Activity/Steps- Priority: High

Timeline: IN PROGRESS

Phase 1- (2019-2022 <u>High Priority Activity</u>).

Phase 2- (2021-2023 <u>High Priority Activity</u>).

<u>Recommendation #14- California Cybersecurity Career Education Pipeline/Pathway Cyber-Hygiene Component: Cyber Hygiene "Best Practices" and Linkage with Education/Academic Programs at All Levels-</u>

We have already made recommendations about key elements of the structural education/academic components of the California Cybersecurity Career Education

[38] NICE Cybersecurity Workforce Framework.

Pipeline/Pathway. We discussed the importance of model curriculum/academic standards and professional development ideas/action items for project implementation. However, there is one last key element that we must address at all levels of education—namely the critical skill of practicing "safe computing" and cyber-hygiene for online safety and security.

Networks, systems, and data are only as secure as the users accessing them. By teaching "best practices" in cyber-hygiene we can all be better, safer consumers of information and data; as well as limit exposure to vulnerability and risk that prudent self-cyber security strategies help avoid, prevent, and reduce.

SCOPE OF WORK: One element of the strategy here is the production and distribution of catchy and "fun" PSAs (TV, online, radio spots) to raise statewide cybersecurity awareness of "best practices" in safe computing. In addition to the "cool value," we include outreach and links to cyber education programs, resources, and opportunities found on the California Cybersecurity Education Clearinghouse.

Two areas of interest relating to cyber-hygiene practices:

1. General Public Cyber-hygiene and awareness campaign (focus on the importance and practice of safe computing habits at age appropriate education levels);

2. Link systematic cyber-hygiene best practices into components of cybersecurity career pathway and education programs;

Cyber-hygiene legislation in California:

There is a lot of activity in California related to Cybersecurity and Privacy. Assembly Bill 809 (A.B. 809- Cyber Hygiene Education Bill) supports the movement towards teaching cyber-hygiene in schools (including social media literacy, staying safe online, reducing cyber-bullying, etc.) In the event this bill was to become law and funded, it would be vital to provide school districts with the guidance, resources, and useful curriculum for them to meet this important objective. There are many other items of legislation recently enacted or under consideration. This area of California cybersecurity hygiene and education is ripe for additional research and insight.

Additional Cyber-hygiene Resources to cross-walk with state-wide cybersecurity career education pipelines:

- For cyber hygiene resources for teachers there is the existing group Common Sense Media that houses educator resources https://www.commonsense.org/education/
- DHS's Stop. Think. Connect. Resources could be useful to any teacher since it provides the whole suite of US-CERT publications/agency publications detailing cyber topics: https://www.dhs.gov/publication/stopthinkconnect-parent-and-educator-resources
- Teachingprivacy.org (a project out of UC Berkeley - https://teachingprivacy.org/)

- The UC Berkeley project is a great conversation 9-12 and Be Internet Awesome fits in the K-8 space.
- Google's Be Internet Awesome (https://beinternetawesome.withgoogle.com/en)

The Subcommittee recommends the inclusion of "cyber hygiene" best practices be included in the California Department of Education CTE Anchor Standards. This is an important skillset/area of knowledge for all CTE students across all Industry Sector Model Curriculum/Academic Standards areas and students and their families are strongly encouraged to study best practices and stay safe while computing and online.

Recommendation #15- (Formation of California Educational Institution Threat Assessment Center). Enhanced and shared Educational Institution Cybersecurity, Digital Emergency Management, Incident Response and Information Sharing preparedness, response, recovery, and mitigation capabilities.

Enhance California educational institution incident response and cyber emergency preparedness platform; information sharing coordination, "best practices" and expertise through the creation and operation of a California Education Institution Threat Assessment Center (CEITAC.) CEITAC should naturally be embedded and operate within the California Cybersecurity Integration Center (CAL-CSIC) and California State Threat Assessment Center (STAC). Cal-CSIC serves as the central organizing hub of the State's cybersecurity activities and the STAC serves as the State's primary fusion center. Cal CSIC major capabilities include cyber incident response coordination, cyber threat alerts/advisories, the California Automated Indicator Exchange, and Phishing Email/Malware Analysis. Some great training opportunities found here.

Emergency Operation Center (EOC)- link and activate for Emergency Management issues like wildfires, earthquakes, large power outages, digital emergency/response.

Threat Assessment Center—Joint Fusion Center- collate and analyze LE and Intelligence products with K-12/ Higher Education.

If CEITAC was effective— scale up for utilization as a national model/framework. When effective policy initiatives (like CCCEPPP) begin in one state, they "diffuse" or roll out to other states with similar needs. As cybersecurity information sharing is an international, national, state, and local concern; it would be nice to develop critical infrastructure and architecture in this area.

California Cybersecurity Education Clearinghouse- All related information to be found on the Clearinghouse site for educational institution security controls and "best-practices."

SECTION V: CALIFORNIA CYBERSECURITY CAREER EDUCATION PIPELINES AND PATHWAYS

CALIFORNIA CYBERSECURITY CAREER EDUCATION PIPELINE AND PATHWAY SUMMARY

- Critical need for qualified cybersecurity professionals in California and nationwide.
- Project objective- prepare 50,000 California cybersecurity entry-level professionals in a 10-year period (2020-2030).
- California Cybersecurity Workforce Development-Education-Professional Certification Capability Gap Analysis and Cybersecurity Industry Employment Study (Required/Preferred Job Qualifications.)
- Understand industry needs- public, private, non-government organizations (NGOs).
- Develop Model Curriculum and existing course redesign to meet industry workforce needs.
- Linked, standardized cybersecurity programs at all levels of education:
    - K-12 (in collaboration with California Department of Education);
    - Associates Degrees and Certificates (in collaboration with California Community Colleges);
    - Bachelor's Degree and Certificates (in collaboration California State University and University of California campuses);
    - Graduate Programs (Masters Degrees- Ph.D./Joint Doctoral Degree Programs);
    - Professional Certification- including "stackable certificate" programs either embedded into degree programs or stand-alone certificates aligned with registered apprenticeships and related OJT.
- Importance of pre- and registered apprenticeships, internships, professional development, cyber-competitions, extra-curricular activities, and the selection/hiring process for prospective pipeline/pathway students.
- **California Cybersecurity Apprenticeship Centers-**
- **California Cybersecurity Education Clearinghouses-**
- **California Cybersecurity Education and Workforce Development Road Maps-**
- **The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).**

CYBERSECURITY CAREER EDUCATION PIPELINE/PATHWAY OBJECTIVES:

Design, develop, and implement a coordinated, linked, and seamless state-wide career pathway in Cybersecurity at all levels of education, workforce development, and training (including K-12, Associates, Bachelors, Masters, Doctoral, and Professional Certification), in support of California Cybersecurity Strategy and Policy; and current Industry (Public/Private) Essential Workforce Needs.

To accomplish statewide CCCEPPP objectives, we systematically organize, facilitate, and collaborate on the following points:

1. Industry sector recognized Cybersecurity **Model Curriculum/Academic Standards**;

2. **Extra-curricular activities** (cyber competitions, hackathons, summer coding camps, after school/summer activities, bug bounties, etc.);

3. **Professional Experience opportunities** (i.e. industry apprenticeships and internships);

4. **Professional Development Opportunities** (Mentoring, Career Awareness, etc.)

5. Reinforcement of **cyber-ethos** and **ethical hacking** (including Sandbox/Range Opportunities);

6. An enhanced and leveraged networked enterprise that appropriately prepares graduates with the relevant knowledge, skills, and abilities to meet the minimum (and preferred) qualifications for employment in Cybersecurity/Information security (and related fields);

7. **Cybersecurity Educational Teaching Capacity/**Capabilities- increasing numbers of students in cyber education programs, we must likewise enhance faculty numbers and resources.

8. Enhance California educational institution **incident response and cyber emergency preparedness** platform; information sharing coordination, "best practices" and expertise through the creation/operation of **California Education Institution Threat Assessment Center (CEITAC**); and **California Cybersecurity Education Clearing House**.

9. Implement comprehensive **California Cyber Hygiene and Awareness Plan** and state-wide multi-channel education/awareness campaign to boost safe computing best practices.

10. Statewide **Cybersecurity Pre-and Registered Apprenticeship Pipelines** with **California Cybersecurity Apprenticeship Centers**.

11. **California Cybersecurity Education and Workforce Development Road Maps.**

12. The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

CALIFORNIA CYBERSECURITY CAREER EDUCATION PIPELINE/PATHWAY INTRODUCTION:

There is a critical need to ensure California is able to hire, retain, and promote prepared and qualified cybersecurity professionals. This is a challenge given dynamic change in the contemporary cyber security environment. We have seen a continuing cascading effect of the increasing digital footprint in this age of technology, social media and networking, and the extraordinary value of information today. Thus, our purpose here is to lay out a basic framework to design, develop, and implement a statewide cybersecurity career pipeline/pathway.

One of the first steps of career pathway development is to establish a consistent definition and criteria for cybersecurity expertise. This work was completed by our Workforce Development and Education Subcommittee (June 2015) in a white paper that made three relevant recommendations to our work here: to create a new Cybersecurity Professional classification, IT capital planning and security funding, and Information Security training and awareness for all.

Based on the previous Subcommittee work, we have reformulated our objective to include the development of a **competency-based model** cybersecurity education and workforce development program to help meet critical cybersecurity professionals across California and engage with key industry stakeholders and major partners to assist in the rapid development of cybersecurity workforce education/programs to meet these urgent needs. Colleagues working on the CCCEPPP have brainstormed with many SMEs on innovative and transformative new strategies and ways/means to develop education programs. We asked the following questions:

- What should cybersecurity curriculum and academic standards look like?
- How do we include internships/apprenticeships and what are some best practices here?
- What kind (and where) do we include professional development opportunities, labs/projects, clearinghouse for graduates and industry to meet?
- How do we prepare, recruit, retain, support, and graduate students prepared for cybersecurity professional positions?
- How do we prepare, recruit, retain, and promote faculty in the growing area of cybersecurity education/academics?
- How do we enhance diversity and inclusivity in IT-Cybersecurity?
- Link research opportunities, scholarships and grants, etc.

Furthermore, as a term like "career pipeline" suggests, we must carefully link and coordinate educational programs at all levels; providing a seamless transition of programs from one level to the next (K-12, 2-Year, 4-Year schools, graduate programs, and professional certifications/credentials.) We seek a coordinated, standardized, seamless transition of accessible, available, and inclusive cybersecurity education/workforce development/training programs from kindergarten through graduate degrees and professional training/certifications in the **California Cybersecurity Education Career Pipeline and Pathway**.

One key CCCEPPP outcome/objective is a systematic framework and coordinated process by which California residents anywhere can remotely access a variety of cutting-edge cyber education/academic programs (degree and stackable Industry recognized certifications) to prepare them for future cybersecurity professional positions (as well as private and public sector/NGO employers.) This report discusses and recommends cybersecurity model curriculum/academic standards at all levels of education/academia.

However, there are additional elements of a cybersecurity career pipeline/pathway to note. The purpose of a statewide **cybersecurity career pipeline** is to coordinate between levels of education and establish clear "exit points" from each respective level into corresponding **career cybersecurity pathways** leading to specific and appropriately skilled positions like Security Systems Engineer or Cyber Threat Analyst. Transitions and "exit points" between career pipeline/pathway components/levels of education are plainly laid out and clearly communicated to students interested in the pipeline. In terms of transitions, we mean that students have clear academic pathways from one level of education to the next that are found on **"Road Maps"** available to students interested in cybersecurity pathways. In this way, students can identify and understand their best education/experience path to accomplish their professional objectives and gain entry into the professional field and workforce.

Additionally, we make sure cybersecurity education and workforce development programs all have significant "experiential and applied learning components" embedded to prepare students for **entry-level positions** in cyber/physical security domains. In terms of many cybersecurity domains, we rely on math, science, and oral/written communication academic skills as a firm educational foundation into advanced computing/IT/cybersecurity as well. These students are going to need to be strategic about the programs and courses to best navigate into specializations/domains of their greatest interest.

CALIFORNIA CYBERSECURITY CAREER EDUCATION PIPELINE/PATHWAY PROJECT OBJECTIVES:

The net sum of subcommittee recommendations is the design/development/implementation of a comprehensive, coordinated, and seamless network of linked cybersecurity education and workforce development programs and additional educational institution tools ("Toolkits"). In this report section, we first describe CCCEPPPP project objectives. In the following few pages, we lay out the many complicated facets of cybersecurity pipelines and pathways in terms of additional objectives/sub-objectives/primary learning objectives of these various toolkits to support educational institutions. This information is helpful in understanding project background/overview undergirding Subcommittee recommendations, tasks, activities, timeline and deliverables.

CCCEPPP OBJECTIVES:

OBJECTIVE 1- Implementation of California Cybersecurity Career Education Pipeline and Pathway (covering K-12 through higher education) to prepare 50,000 cyber and information security professionals to serve existing and future State of California entry level (and management) cybersecurity needs and meet the educational component of this technical and specialized professional field and industry sector. This includes the following elements:

Cybersecurity Model Curriculum/Academic Standards-

Cybersecurity Extracurricular (and After-School/ Summer Activities)-

Cybersecurity Professional Development and Socialization Opportunities-

Ethical hacking (and Sandbox/Range Related Opportunities)-

Cyber competitions/Hackathons/Coding Camps-

Cyber Education Program/Outcome Assessment and Evaluation-

Cybersecurity Pre- and Registered Apprenticeship Programs-

Cybersecurity career pipelines/pathways should include a variety of specialized education and training tracks in "high needs areas" ("STACKING CERTIFICATE PROGRAMS") in select areas of cyber-security, cyber-digital forensics (crime), cyber-resiliency, critical infrastructure protection, emergency response, and additional closely related NICE (National Initiative for Cybersecurity Education)/National Institute of Science Technology (NIST) Workforce Framework domains and fields.

OBJECTIVE 2- Development of Cybersecurity Educational Teaching Capacity and Capabilities- (Justification: if increasing numbers of students in cyber education programs, we must likewise enhance the numbers and resources available to instructional staff.)

OBJECTIVE 3- Enhance California educational institution incident response and cyber emergency preparedness platform; information sharing coordination, "best practices" and expertise through the creation and operation of a California Education Institution Threat Assessment Center (CEITAC.)

OBJECTIVE 4- Implementation of a comprehensive California Cybersecurity Hygiene and Awareness Plan including a statewide multi-channel education and awareness campaign to boost safe computing best practices for all residents.

CCCEPPP EDUCATION INSTITUTION TOOLKITS SUB-OBJECTIVES:

(1.) Facilitate and strengthen partnerships, collaboration, and trust between major stakeholders in California cyber-security workforce development and education, including-

Education Institutions (K-12 and Postsecondary Education)- Leverage cyber-security resources and expertise within the California Department of Education, the California Community College, California State University, University of California, and private colleges/universities.

Government Agencies (Local, State, and Federal)- Consult and work together with government agencies at all levels of government to formulate sound cyber-security education and workforce development programs and course curriculum that are consistent with the (NICE) Cybersecurity Workforce Planning Diagnostic Tool.

Private Sector (Large, Mid, and Small Businesses)- Consult and work together with the private sector and industry to formulate sound cyber-security education and workforce development programs and course curriculum that are consistent with their needs as employers of graduates of the career pathway.

Non-Government Organizations (NGOs)- There are many additional organizations that serve as key stakeholders and major partners in the quest for cyber-security and information assurance. It is important to engage with NGOs to make sure their organizational educational and workforce development needs are met with relevant education programs and apprenticeship opportunities.

(2.) Engage and collaborate with key education, government, private sector and NGO partners in the design and development of Cybersecurity Model Curriculum and Academic Standards. It is through partnership, dialogue, and coordination that we can determine baseline needs for inclusion into education/workforce development training program curriculum and standards to meet this generation, and future generations' cybersecurity needs:

- The design and development of Cybersecurity Model Curriculum (The career pathway covers K-12 education through Degree and Certification programs at all levels of

education/training attainment including Associates, Bachelors, Masters, Doctoral, and professional certifications).

- Design and development of Cybersecurity Core Courses and Competencies for Degree and Certification programs at all levels of education/training including Associates, Bachelors, Masters, Doctoral, and professional certifications).
- Student Learning Outcomes (SLOs)- for all courses within the core, breadth, and electives of the Cybersecurity Career Pathway.
- Knowledge Units-
- Develop a state-wide certification for cybersecurity (and related specializations) that could serve as a baseline for training at the various relevant personnel HR classifications.
- Develop a variety of program and course delivery methods/formats- Fully online, hybridized/blending, or traditional offerings-
- Course Instructional Materials, Textbooks, e-textbooks, etc.-
- Standardize relevant programs, courses, and curriculum so as to articulate (transferability) with other programs- (vertical and horizontal track programs).
- Cyber Competitions- enhancing cyber education and professional development through games, exercises, and competitions.
- Cyber-hygiene education program, course design, and development-
- Cyber Summer Camps and Activities (for students and instructors)-
- Strategies to enhance IT-Cybersecurity diversity and inclusion for special populations; to include transitioning military to civilian, veteran, disabled veterans and spouses.
- Strategies to enhance IT-Cybersecurity diversity and inclusion for special populations; to include women, race and ethnicity, and sociodemographic disadvantage.
- **All relevant information included on California Cybersecurity Education and Workforce Development Road Maps.**
- **All education, teaching, and learning materials to be uploaded into the California Cybersecurity Education Clearinghouse.**
- The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

(3.) Develop Incentive structure to leverage program and curriculum implementation between education, government, private sector, and NGOs. How can we connect education and training programs w/ workforce development, employer/agency needs, etc.?

- Academic Education Program Development-
- Career Vocational Program Development-
- Education and Career Training Program Evaluation/Assessment-
- Student Support- Incentives to support students-
- Faculty Support- Incentives to support faculty, teaching, and research-

- Develop Research Initiatives/Partnerships (support Faculty/Students in Basic/Applied research)-
- Strategic Gaming and simulations-

(4.) Expand and enhance Cybersecurity professional development, internship, and volunteer opportunities to support workforce development and education.

- Professional Development and Internships (paid and unpaid)- conduct a capability gap analysis for internship stuff; develop a catalog of internship and volunteer opportunities.
- Volunteer Opportunities-
- Residency Programs-
- Project management and other professional skill development-
- Service Learning Opportunities- Civic engagement to serve the needs of our universities, communities, NGOs.
- The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

(5.) Design and utilize strategies to assist in the preparation, recruitment and retention of a full spectrum of specialized cybersecurity workforce development and education.

- Identify and promulgate pre-professional cybersecurity employment "best practices," including an understanding of the applicant background/security screening process.
- Prepare management and technical side programs to support the full breadth of cybersecurity industry needs.
- *Develop/implement Veterans Cyber-Workforce Plan*- Expedite Veteran transition to Civilian workforce through education and training. Prepare and provide road-maps to veteran's and disabled veterans to support their education and workforce development/upskilling in cybersecurity professional positions to utilize their military training, experience, and hard-work ethic.
- Recruit and retain traditionally under-represented groups in IT-Cybersecurity.

(6.) Design and develop a California Educational Institution (K-12 and Higher Education) Incident Response and Information Sharing Platform (CEITAC).

- Work with all major stakeholders and key partners on the academic/education side in conjunction with government agencies and NGOs and private sector to design CEITAC with the following elements in the overall system design-
- Functions as Educational Institution threat assessment center (connected with the STAC); Emergency Operations Center (EOC: for Emergency Management preparedness, response,

and recovery); Security Operations Center (SOC), and Joint Fusion Center (fusing intelligence between education institutions, public safety/service, and first responder communities).

- Utilize STAC, EOC, SOC, and Joint Fusion Centers for student education and training experiences.
- Utilize the California Cybersecurity Education Clearinghouse to store and deliver all these aforementioned resources and deliverables.
- All relevant information included in **California Cybersecurity Education and Workforce Development Road Maps.**

CCCEPPP-EDUCATION INSTITUTION TOOLKIT PRIMARY LEARNING OBJECTIVES:

1. Design workforce development and education programs, courses, and curriculum in partnership with academic institutions, government agencies, the private sector, and non-government organizations.

Curriculum and instructional materials-

Professional development-

Cyber-competitions-

Auxiliary/education functions-

2. Implement CCCEPPP at all levels of educational attainment and professional certification in a linked and coordinated fashion. Enhance cybersecurity workforce development and education coordination of educational systems and campuses statewide.

3. Assess and evaluate the workforce development and education programs and courses to make sure they are teaching what they need to and stay current with current threats and cyber-security "best practices."

4. Professional development- including cyber competitions, internships, pre- and registered apprenticeships, volunteer opportunities, career mentoring, etc.

5. Share all instructional materials, deliverables, curriculum and related items on the California Cybersecurity Education and Workforce Development Clearinghouse.

STRATEGIES TO SUPPORT CYBERSECURITY WORKFORCE DEVELOPMENT AND EDUCATION FOR UNDERSERVED POPULATIONS

Initiatives in Cybersecurity: Diversity and Inclusivity in Education and Workforce Development

(Strategies to enhance the participation and retention of Women in Cybersecurity and Technological Fields).

SCOPE OF WORK: Building and reinforcing a **s**upportive culture that promotes equity for women in cybersecurity, computing, and IT. This includes the development and implementation of strategies intended for a transformation of cultural and workplace values and related support mechanisms to foster enhanced interest and encourages inclusivity into the field. Furthermore, strategies and policies for career exploration, peer mentoring, and preparation for entry-level cyber employment, recruiting, hiring, retention, and promotions as valued and successful members of cybersecurity (and related) fields.

The inclusion of women into the tech and cybersecurity enterprise is an essential part of any closing of the California cybersecurity workforce gap. It is imperative to deploy strategies to enhance the numbers of prepared cybersecurity women professionals across industries and sectors. Thus we include separate recommendation for strategies to support and encourage women into cybersecurity, computing, and IT as well accomplish a significant reduction and elimination of gender disparity existing within this field.

One fundamental component at the core of the CCCEPPP is to encourage significant workforce development and education opportunities for girls and women. The cybersecurity career pipeline/pathway is intended to start early (Middle School) through Associates/Bachelor's Degree in cyber fields plus all the related professional/career/ experiences. A variety of strategies will need to be embedded into all educational components/ levels consistent to support women fully into the cybersecurity career pipeline/pathway.

MILESTONES, DELIVERABLES:

Timeline: IN PROGRESS

Phase 1- (2019-2022 High Priority Activity).

Phase 2- (2021-2023 High Priority Activity).

(Strategies to enhance the participation and retention of Underrepresented Historical Backgrounds in Cybersecurity and Technological Fields).

Thinking of strategies and recommendations that are consistent with all elements of the NICE Workforce Framework Defining Cybersecurity, "…(as) the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce." [39] Strategies must be in place to assist in these areas with the utmost of haste.

Building and reinforcing a supportive culture that promotes equity for traditionally underrepresented backgrounds in cybersecurity, computing and IT. Furthermore, strategies and policies for career exploration, peer mentoring, and preparation for entry-level cyber employment, recruiting, hiring, retention, and promotions as valued and successful members of cybersecurity (and related) fields.

This includes the development and implementation of strategies intended for a transformation of workplace and related support mechanisms to foster enhanced interest and encourages inclusivity in these fields from underrepresented groups, including persons of color, members of Tribal Sovereign Nations, and persons of varied economic backgrounds across all geographic locations in California.

MILESTONES, DELIVERABLES:

Timeline: IN PROGRESS

Phase 1- (2019-2022 High Priority Activity).

Phase 2- (2021-2023 High Priority Activity).

[39] NICE Cybersecurity Workforce Framework.

STRATEGIES TO SUPPORT CYBERSECURITY WORKFORCE DEVELOPMENT AND EDUCATION FOR UNDERSERVED POPULATIONS

Initiatives in Cybersecurity: Transitioning Military, Veterans, and Disabled Veterans, and Spouses into cybersecurity workforce career pipelines-

The cybersecurity community, professional field, and workforce development greatly benefit the inclusion of candidates from transitioning military, veterans, and disabled veterans. Thus, the subcommittee recommendation involves strategies and support mechanisms for the recruitment and retention of Military IT MOS into the civilian cybersecurity workforce where they can put their experience in a diverse set of specializations into closely related positions and jobs throughout California. Individuals with military service are used to working in the dynamic cybersecurity environment, useful soft skills like oral and written communications, team players, strong leadership and soft-skill development among other desirable hiring traits.

In addition, for positions that involve classified information or highly sensitive data, the active background clearances of transitioning military and veterans could expedite the hiring process and potential advantage in the formal hiring process.

Finally, a third element of this recommendation includes the utilization of their military career experience and training to serve an educational role as teacher, advisor, mentors, and cyber coaches for the increased numbers of students that will be entering and pursuing the cybersecurity career education pipeline and pathway.

MILESTONES, DELIVERABLES:

Timeline: IN PROGRESS

Phase 1- (2019-2022 High Priority Activity).

Phase 2- (2021-2023 High Priority Activity).

CYBERSECURITY CAREER EDUCATION PIPELINE/PATHWAY DESIGN, DEVELOPMENT, AND IMPLEMENTATION ELEMENTS:

Facilitation and coordination of cybersecurity education and training among key partners and major stakeholders. Utilize public-private partnerships to assist educational institutions on the types of information and content necessary to design and develop cyber education and training programs that meet the needs of future employers.

Proposed Model Curriculum Design/Development- (Program, Course, Student Learning Outcomes and related instructor/other course materials/textbooks, etc.) to support K-12 through Advanced Graduate Degree Programs in Cyber-security/resiliency/digital forensics and closely related specializations.

Utilizing California Common Core and Career Technical Education (CTE) Standards when developing K-12 Cyber standards/curriculum as necessary to "fill-in" the holes found in a capability (and skill demand) gap analysis. Focus particularly on the **Next Generation Math and Science Standards** to incorporate STEM (Science, Technology, Engineering, and Mathematics) into the core curriculum and programs.

Cybersecurity Academic Curriculum and Program Development- Once there is a common understanding of the nature and content of the curriculum, necessary courses developed, SLOs established, it is time to develop and implement cybersecurity education and training programs. Programs include K-12, Associates (Transfer Model Curriculum), Bachelors (2+2 programs), Masters, Professional Science Masters Degrees (PSM), Doctoral/Joint-Doctoral Programs, and Professional Certification Programs.

The **Cybersecurity Career Pathway objective** lays out a "**road-map**" for workforce development and education in the fields of IT, Computer Science, Electrical Engineering, etc. and assist students into the cyber-security field. This is done by leveraging partnerships between educational institutions, government agencies, private sector, and NGOs.

These are some primary considerations to keep in mind when designing **effective, seamless, linked** Cybersecurity Career Education Pipeline/Pathways with blended and linked academic, STEAM, CTE based K-12 Education, Degree, and Certificate programs.

REPORT SECTION SUMMARY:

The key to a seamless, comprehensive, and linked career pipeline/pathway is in facilitated collaboration with key stakeholders and major partners (education, public, and private sectors) on the following key elements: model curriculum/academic standards, professional development opportunities (mentoring, career shadowing, apprenticeships), extra-curricular activities (cyber competitions, coding camps), cyber-ethos/ethical hacking.

All these components are aligned together into a networked series of educational/workforce development programs to prepare graduates with relevant knowledge, skills, abilities to meet the minimum (and preferred) qualifications for cybersecurity employment.

More information and details found in the following section on pipeline/pathway design, development, and implementation.

SECTION VI: CYBERSECURITY CAREER EDUCATION PIPELINE AND PATHWAY SYSTEMS ARCHITECTURE

PIPELINE AND PATHWAY SYSTEMS ARCHITECTURE OVERVIEW:

The CCTF WDE Subcommittee prepared a series of recommendations for the design, development, and implementation of statewide career education pipeline in cybersecurity at all levels of education (K-12 through advanced degrees and professional certifications) in the previous report section. This is an ambitious project to develop and implement a comprehensive, effective, and linked statewide Pipeline and Pathway to prepare 50,000 cybersecurity professionals in the next 10 years. The key is on coordination of the many cybersecurity resources, programs, and initiatives statewide and get everything cyber education/workforce development related all in one place; both in terms of road maps and available clearinghouses to store and access this information.

The primary purpose of this page is to provide a graphical format and contextual representation of the variety of complicated elements necessary to synergize and coordinate while facilitating the implementation of a statewide cybersecurity career pipeline and engaging with the public sector, private industry, and all levels of education/academia (and fit into the Road Map.)

K-12 Education
Associate-level Education
Bachelor-level Education
Master-level Education/ Advanced Graduate-level Education
Professional Certifications/Credentials

As a picture tells a thousand words, this section provides details on specific WDE Subcommittee recommendations (found in the previous report section) related to the implementation strategies and action items needed (per respective level of education.) These subcommittee recommendations (in the last report section) are broad and general in scope. In this section, recommendations for each level of education described in further detail. In addition, these specific discussions often contain links to links, more materials, best practices, task items, priorities, timelines, etc.) to complete and fully implement into an operational state-wide cybersecurity career education pipeline/pathway forthwith.

Graphical representation is useful in helping visualize the complicated elements and complex relationships found within this state-wide cybersecurity education and workforce development strategy. It guides and assists synchronization and coordination activities necessary for the preparation of qualified cybersecurity professionals ready for entry-level employment in many different cybersecurity domains/industry sectors. As one can discern from the next few pages, we are talking about blending and coordinating many complex pieces of a puzzle here. Puzzle pieces include, model curriculum, academic standards, extracurricular activities, professional development opportunities, experiential learning (apprenticeships and internships), cyber competitions, and additional strategic components necessary for transformative cybersecurity education and workforce development statewide.

Finally, we emphasize the principle of **"Workforce Ready Workforce Development."** CCCEPPP graduates must be ready to start work day one without significant cybersecurity training or substantial time offline getting up to speed on skills required for the position they were hired for in the first place.

CCCEPPP SUMMARY ORGANIZATION CHART:

Summary California Cybersecurity Career Education Pipeline and Pathway Project "Vertical Track" System Architecture

Please see the following recommendations related to various levels of education found within the cybersecurity career education career pipeline/pathway and included in:

California K-12 Education Cybersecurity Recommendations

Cybersecurity Model Curriculum and Academic Standards-
Specialized Academic Skills-
Extracurricular Activities-
Professional Development Activity-

California Associates-level Cybersecurity Recommendations

Cybersecurity Model Curriculum and Academic Standards-
Specialized Academic Skills-
Extracurricular Activities-
Professional Development Activity-

California Bachelors-level Cybersecurity Recommendations

Cybersecurity Model Curriculum and Academic Standards-
Specialized Academic Skills-
Extracurricular Activities-
Professional Development Activity-

California Graduate-level Cybersecurity Recommendations (Masters/Doctoral Degrees)

Cybersecurity Model Curriculum and Academic Standards-
Specialized Academic Skills-
Extracurricular Activities-
Professional Development Activity-

California Advanced Graduate-level Cybersecurity Recommendations (Doctoral Degrees)

Cybersecurity Model Curriculum and Academic Standards-
Specialized Academic Skills-
Extracurricular Activities-
Professional Development Activity-

California Professional Certification and Training Cybersecurity Recommendations

Cybersecurity Model Curriculum and Academic Standards-
Professional Certifications- (Stackable)
Specialized Academic Skills-
Extracurricular Activities-
Professional Development Activity-

CYBERSECURITY CAREER EDUCATION PIPELINE AND PATHWAY SYSTEMS ARCHITECTURE/SPECIFICATIONS/COMPONENTS:

The larger and over-arching objective of the CCCEPPP is the design, development, and implementation of a career pathway across all levels of education to prepare 50,000 cyber professionals for entry-level employment and assist in qualified workforce development. Each of the following report sections describe/discuss individual education segments in further detail.

PART I- Cybersecurity Education Programs:

The K-12 Education Component is essential bedrock and foundation for any solid education and workforce development strategy. This is particularly true in IT-Cybersecurity as soft skill and technical skills may be quite rigorous. Students are best advised to start early to master IT-Computing skill sets, particularly those seeking more technical skillsets. In cybersecurity, it is essential to begin IT-Computer Science, and related education programs as early in age as possible (or as soon as possible for older children.) This is a new technological age, and tech skills are fast now becoming critical life skills.

Once we complete K-12 Cybersecurity education recommendations and materials, we then discuss cybersecurity higher education components of the career pipeline/pathway. These include Associate-level, Bachelors-level, Master-level, Ph.D. level education programs, courses, and related. The CCCEPPP contains both K-12 and Higher Education program components.

Part II- Cybersecurity Workforce Development and Apprenticeship Programs:

Next, we align and link academic degree programs with professional certifications and industry recognized minimum industry training competencies (standards) with workforce development opportunities through pre- and registered apprenticeship programs and 2000 hour OJT for hands-on experience.

It is important to note here that industry and government have been increasingly concerned about the value of a four-year undergraduate degree program in STEM fields as a predictor/indicator of success within the cybersecurity profession. One alternative education approach is now stackable certificate programs linked with youth pre- and registered apprenticeship programs with 2000 hour on the job training opportunities. These are paid positions calculated at 60% of the prevailing journeyman's wage in a select occupation.

For example, an Information Security Analyst position national prevailing wage (May 2019) was $47.95 an hour ($99,730 per year) with a bachelor's degree the typical entry-level education model. [40] As the WDE model shifts away from a reliance on 4-year degrees, upon

[40] U.S. Bureau of Labor Statistics, Occupation Outlook Handbook 2018-2020 (Updated Through May 2019). https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm Accessed electronically on 7/01/2020.

completion of a Cyber Analyst Certification education program, students could complete an apprenticeship workforce OJT opportunity paying $28.77 (based on 60% national prevailing wage) to start. This is on their way into entry-level work in this occupational cluster (and likely working in a SOC or ISO) where their salary after completion of OJT goes up to the prevailing occupational wage (because they are now 100% trained and ready to work in permanent positions.

Part III- Pulling Everything Together:

At the end of the day, candidates with solid education and experience are more competitive on the job market. We need to make sure graduates are qualified to get the positions they seek. Thus, it is critical that students are exposed to both "book learning" (the education) and "hands-on" experience (the training). Nothing short of this meets the needs/standards for industry and employers. This is also a key reason why major partners/stakeholders need to collaborate on the front end of the design and development process.

California Cybersecurity Education and Workforce Development Clearinghouse-

All cybersecurity education, teaching, and instructional materials (Part I) and Workforce Development and Apprenticeship Program Information (Part II, III) materials uploaded and available in one central public repository.

SECTION VII: CALIFORNIA CYBERSECURITY K-12 EDUCATION

INTRODUCTION TO CALIFORNIA K-12 CYBERSECURITY EDUCATION

K-12 Introduction Prepared by Mr. Erle Hall, CTE Industry Sector Lead for Information and Communications Technology, Education Programs Consultant, Career and College Transition Division, California Department of Education

At a time when the need for cybersecurity education continues to rise, the numbers of students and teachers involved in cyber career preparation continues to lag. The consulting firm Frost and Sullivan forecasted in 2017 that a 2022 shortage of 1.8 million cybersecurity workers would exist (which was a revision upwards of their original 2015 forecast projecting a shortage of 1.5 million workers). [41] This upward trend has existed as long as the occupational field has existed.

The K-12 space in California has dedicated centers of active cyber education programs preparing students to pursue cybersecurity careers after leaving high school. The California Career Technical Education Model Curriculum Standards were updated in 2013 to include the first career pathway standards for cybersecurity by the standards writing team. The Colton-Redlands-Yucaipa Regional Occupation Program (CRY ROP) had the first a-g approved set of courses for cyber security in the state circa 2015 and San Bernardino County Superintendent of Schools ROP has likewise had an a-g approved cybersecurity program since nearly the same timeframe.

The first statewide cybersecurity competition called Cyber Foundations kicked off in the fall of 2011, supported by SANS Corporation, the US Cyber Challenge and the California Department of Education. The California Governor's Go-Biz office, the California Community College, and the California Department of Education launched the California-centric state-wide Cyber Innovation Challenge in 2016 which is now run by CISCO's NetAcademy and The California Cybersecurity Center at Cal Poly San Luis Obispo. The late Harry Talbot of LAUSD's after-school program Beyond The Bell tirelessly worked to expand the enrollment of students in Cyber Patriot as did the California entity known as Cyber Hub (now Cyber Guild) across the state and continues to do so.

All of this is to say that despite years of hard work by educators, administrators, supporters in business and government, the workforce gap still persists because technological change has accelerated and various types of cyber threats have expanded along with the innovations in technologies. Also, barriers exist according to a recent white paper co-written by EdWeek and Cyber.org (formerly National Integrated Cyber Education Research Center – NICERC) and based on a nationwide survey of K-12 educators, which includes the existence of "cybersecurity deserts" which is an absence of business firms engaged in cybersecurity services delivery and/or an absence of Universities engaged in cyber education. [42] In California, it should be added that another contributing factor to cyber security deserts would be an absence of secondary school Career Technical Education (CTE) programs in Information and Communications Technologies (ICT) focused on cybersecurity and a lack of computer science programs which also have cyber security

[41] Frost and Sullivan, 2017 Global Information Security Workforce Study, Accessed electronically on 8/2/2020). (https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

[42] Cyber.org (NICERC) The State of Cybersecurity Education in K-12 Schools, Accessed electronically on 7/18/20). https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

strands in their standards and programmatics. A modest amelioration of this situation has come about due to several successive years of funding from the state Career Technical Education Incentive Grant (CTEIG) starting in state fiscal year 2015-16 (see California Department of Education, CTEIG funding page in references) which has provided sustained, predictable funding for CTE programs across the state. [43]

Other factors affecting the lack of cybersecurity education in the K-12 space includes a lack of knowledge amongst faculty, students being unaware of educational and skill requirements for employment in cyber, and access to cyber education being "infrequent and uneven". Indeed, less than half of the 900 respondents in the Cyber.org survey reported that their district offered cybersecurity education. Worrying trends in the report show that learning about several key cyber-related topics like cyberterrorism, secure programming, secure networking, and hacking/data security is taking place significantly less often in high school versus middle school. The afore-mentioned Cyber Guild, California Community College Information and Communications Technologies – Digital Media division, the Western Academy Support and Training Center (WASTC), and various Career Technical Education and Computer Science programs around the state have been working to accelerate the growth of cyber education and teacher preparation. However, a larger source of sustained support is required from both the public and private sectors.

The latest data from the California Department of Education shows that enrollment in K-12 CTE ICT and Computer Science classes is 82,154 and 22,917 respectively. [44] If we accept these areas of learning as the most likely to possess the aptitude, motivation, and awareness of cybersecurity as a career option but are not necessarily committed to the field, those numbers are still dwarfed by the number of schools who do not have CTE and Computer Science programs. There are 1,016 schools with ICT programs, 376 programs with Computer Science programs out of a total 10,315 California schools. [45] So, even if ICT and CS programs were 100% focused on cybersecurity education, it would still be woefully short of the numbers needed to meet the demand for cyber career preparation. So, there is much left undone to meet this moment in preparing California for the needs of its cybersecurity workforce demand.

[43] California Department of Education, Career Technical Incentive Grant (CTEIG) Funding Years Timeline, (https://www.cde.ca.gov/ci/ct/ig/cteigtimeline.asp, Accessed electronically on 7/18/20).
[44] DataQuest, The California Department of Education, Accessed electronically on 8/2/2020. https://dq.cde.ca.gov/dataquest/dataquest.asp
[45] DataQuest, The California Department of Education, Ibid.

CALIFORNIA K-12 CYBERSECURITY EDUCATION:

K-12 Education Level- All career pipelines and pathways begin here. Career pathways need to begin early in the formal education process. Thus, it is important that we develop sound strategies and "best practices" to get kids interested in cyber as early as possible. We need to initiate a career pipeline/pathway through the blending of academic skill development, career technical education, STEM, and professional/career developments opportunities. Students that do well in STEM fields and academic skill preparation generally go on to college. Once the career cybersecurity education pipeline is in operation, students will have a "road-map" that clearly informs them of all necessary steps to follow for college preparedness/career readiness into the cyber career cluster and job pathway.

CCCEPPP Phase I Activity (2019-2022) begins the road map in middle school (7th grade level) and operates through high school (12th grade) due to a strong Career Technical Education (CTE) and vocational focus.

CCCEPPP Phase II Activity (2022-2024) is where we extend the cybersecurity career pipeline from pre-K/transitional K through 6th grade and significantly enhance the development of digital skills and information literacy at all grades within K-12.

Effective educational strategies are an important step to provide clear cybersecurity college and career awareness to students as they begin to plan for their futures. These strategies must be engaging and foster a learning community to begin and curry and lead interested students into the cybersecurity career pipeline/pathway. And given this engagement, we have prospective students intrigued and curious of all the possibilities in a rich future of tech, computing, and cybersecurity.

Students are also given the necessary, confidence, and resources to succeed in cybersecurity workforce development and education programs. It is essential in the cybersecurity education process, we kick it off with a "Soft Start" to programs and make sure we get everyone up to speed first before sending them down the freeway of cybersecurity workforce development. We must start off slow as to support students from all skill and education backgrounds to master the fundamentals of cybersecurity before getting them involved in increasing advanced subjects and skills. Cybersecurity CTE programs should culminate in a student's ability to enter a profession of choice through completion of quality programs, courses, and experiential opportunities across all levels of the pipeline/pathway. Equally important, it must be available and accessible to all students who may be interested in them.

Summary of CCCEPPP K-12 Cybersecurity Education Components:

In this report section, we add further detail to the K-12 Cybersecurity Education Recommendations previously discussed. This includes cyber model curriculum/academic standards; professional development (as it relates to both student and instructors), enhanced instructor or classroom/computer and cyber-hygiene educational opportunities made available to students and their families with CCCEPPP implementation.

- College and Career Awareness in Cyber, Computer Science, Information Technology, Computer Engineering, and related fields. This includes an understanding of the educational and professional requirements necessary for success in school and/or the professional environment. In other words, what does a student or employee need to know in order to be successful in a particular field? This information is included in a **California Cybersecurity Education and Workforce Development Road Map.**
- Linked learning (blending practical work-based learning with challenging class-based academics and curriculum).
- K-12 Career Technical Education (CTE)- Career Technical Education (CTE) Anchor Standards and Model Curriculum- (Workforce and professional skill development)-
- Crosswalk California Department of Education Career Technical Education Model Curriculum and Academic Standards into "A-G" graduation requirements integrated curriculum with Computer Science/Information Technology/ Cybersecurity Education programs and courses.
- Support California High Schools and Public Service and Safety Academies-
- Combine CTE Information Communications and Technology (ICT), Public Services, Energy Industry Standards with the NICE Workforce Framework in the re-design of California CTE (ICT) Cybersecurity Model Curriculum and Anchor Standards.
- California Next Generation Science Standards- It is important to make sure that these standards are included in both computer science and cybersecurity courses and programs. Computing and cybersecurity share close links to Science, Technology, Engineering, Arts, Mathematics (STEAM) fields.
- Science, Technology, Engineering, Arts, and Mathematics (STEAM)- Enhance STEAM area student skills necessary for success in cyber-security related fields.
- ***Cybersecurity Education Family (and Parent) Roadmap Development.***
- ***California Multi-Channel Cybersecurity Hygiene Awareness Strategy.***
- ***California Cybersecurity Education Clearinghouse.***
- The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

K-12 CYBERSECURITY EDUCATION ACADEMIC COMPONENTS:

Cyber-security education and training programs are based upon, and in turn further reinforce and support the following K-12 Education Model Curriculum/Academic Standards Components:

* California Common Core Standards-

* California Next Generation Science Standards-

* Advanced Placement (A.P.) Computer Science and Honors Courses-

* Career Technical Education (CTE)-

* Academic Skill Development- to support important skills to enhance student success in academic programs (in general) within cyber-security.

* NICE Cybersecurity Workforce Framework- (NIST Special Publication 800-181)

K-12 CYBERSECURITY PROFFESIONAL DEVELOPMENT COMPONENTS:

* Career exploration and exploration

* Extracurricular and summer activities

* Professional Development and Socialization

* Ethical hacking (and Sandbox related opportunities)

* Cyber competitions

* Cyber-hygiene education

* Program and Outcome Assessment

* Youth Pre- and Registered Apprenticeship Programs

K-12 FAMILY ROADMAP RESOURCE FOR CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT COMPONENT:

CALIFORNIA CYBERSECURITY HYGIENE MULTI CHANNEL COMMUNICATION STRATEGY COMPONENT:

K-12 CYBERSECURITY CTE COMPONENTS:

The section objective provides further information and additional details on recommendations and action items in the design, development, and implementation of the K-12 CCCEPPP component. There are many important aspects and components of K-12 Cybersecurity Education discussed on the following pages. This first section discusses the academic components. In addition, these education items are further discussed and described in detail in CCCEPPP Section XI on prospective projects, deliverables, milestones, and timelines.

1. K-12 Career Technical Education (CTE)- Crosswalk California Department of Education Career Technical Education Model Curriculum and Academic Standards into an "A-G" graduation requirement integrated curriculum with Computer Science and Cybersecurity.

- Crosswalk and link California Department of Education (CDE) Career Technical Education (CTE) Information Communication and Technology (ICT), Public Services, Energy/Environment/Utilities CTE Model Curriculum Standards in cybersecurity.

- There are a variety of CDE industry sector CTE standards related to Cybersecurity and found at the following links: For your convenience, relevant Cybersecurity Student Learning Outcomes (SLOs) are found on p. 110 of this document FYI. Note- these and additional cybersecurity related SLOs should all be included together in one location through the creation of a new CTE ICT Industry Sector 5th area pathway "Cybersecurity."

  https://www.cde.ca.gov/ci/ct/sf/documents/infocomtech.pdf

  https://www.cde.ca.gov/ci/ct/sf/documents/pubservices.pdf

  https://www.cde.ca.gov/ci/ct/sf/documents/energyutilities.pdf

It is important to note state-wide CTE Model Curriculum and Academic Standards were approved in 2013. In the past few years, we have seen tremendous advances in technology, computing, and networking. As the curriculum and standards were written some time ago, another in depth thorough review and update of model curriculum and academic standards pertaining to cybersecurity is both warranted and recommended. ICT is a "high need" critical industry sector area and we must have current curriculum and standards available. More details included in the task item list/future activity section (final part) of the report.

New ICT Pathway Sector in Cybersecurity-

Review and revise Curriculum-

Curriculum Integration- (CTE and Academic Course Blending)- see the University of California Curriculum Integration (UCCI) website at ucci.ucop.edu for existing cybersecurity

integrated courses in the Information and Communications Technologies Sector. Existing UCCI curriculum integration courses with cybersecurity/related content include Area A- History/Social Science, Area C-Mathematics, and Area D- Science.

2. K-12 Cybersecurity Industry Recognized Certificate Program Development:

Cybersecurity K-12 Stackable Industry Recognized Certificates/Credentials-

We look to enhance elementary computing/IT at earlier levels in K-12 Education. We also seek to add cybersecurity certificate programs at all levels of skill/mastery (from beginning through advanced) in Career Technical Education (CTE) programs and curriculum. Enhanced K-12 Cybersecurity education boosts and enhances student academics and vocational learning. By teaching "elementary" IT-Cyber skills earlier in the education process, it will allow 2 year /4 year Cybersecurity pipeline programs to focus on advanced topics/specializations and move past the "basic digital skills" being taught at younger and younger ages.

We recommend creation of a variety of Cybersecurity Industry Recognized Pre-Certifications for middle and high school CTE to cover levels of cyber skills and preparation (Exploring, Intermediate, Advanced) reflecting a wide range of cybersecurity education academics and workforce development interests. These certificate programs are also linked with youth Pre- and Registered Apprenticeship opportunities (see the pacing guides located near the end of Appendix 2 for more detail on these linkages and connections).

California Department of Education CTE Certifications consist of three course sequences:

1. Introduction Course-
2. Connector Course-
3. Capstone course- linked with an internship, apprenticeship or some Service Learning (SL) based opportunities.

In addition to skill based cybersecurity certificates, certificate programs linked with other CTE Industry Sectors like; Public Service, Health Science/Medical Technology, Transportation, and Business & Finance are needed and in demand. Completion of three-course sequence for any CTE Industry Sector or Skill Mastery Certificate to be awarded.

Cybersecurity Skill/Mastery Certification Programs:

Exploring Cybersecurity Certificate Program- (ICT-Basics & Fundamentals)

Essentials of Cybersecurity Certificate Program- (ICT- Intermediate skills-link with Internship/Community Service hours requirements, possible industry certifications per below).

Advanced Cybersecurity Certificate Program- (ICT- Advanced skills-link with Internship/Community Service hours requirements, industry certifications per below).

Discussion: Talking about CTE ICT certification programs, we seek to emphasize three different levels of mastery. An **Exploring Cybersecurity Certificate Program** is general and broad, not too technical, and looking to get students without a strong background interested and engaged with computing/IT/Cyber. Some exploring cyber students may not even be exactly sure what cybersecurity is all about yet. This certificate program serves as an easy dive into the field. It also can recruit and provide outreach and support to prospective new students who may never have thought about entering the IT-Cyber field before.

We want a medium-level **Essentials Cybersecurity Certificate Program** for intermediate cybersecurity skill development. We should have at least one academic course here, but the other two courses should be experience/application driven courses. Ideally, high schools students pick up their first Industry Recognized Certification in advance of high school graduation. This course sequence includes other vendor/industry certifications attached to basic skill cybersecurity principles; for example, CISCO Network Academy courses, COMP-TIA IT Fundamentals+, SCAN, Oracle, Microsoft, and others.

Advanced Cybersecurity Certificate Program- More technical and specialized, and Industry/vendor certifications are the focus here. For example, CompTIA A+/ Network+/ Security+ sequence; CISCO Network Academy courses, SCAN, Oracle, Microsoft, and others.

This plan and pacing guide gets "elementary cybersecurity" coursework (and certifications!) squared away by the time of high school graduation. Students transferring to 2 year/4 year cybersecurity programs (or IT/Computing) would be in a prime position to move into advanced cybersecurity education and workforce development academic programs or beginning tech positions.

While we mention three levels of cyber mastery/ skill based certificates below, there are numerous other areas of potential certificate program development within the cyber domain.

For further information on K-12 Cybersecurity certificate programs and component courses, please see Section XI on CCCEPPP Projects and Deliverables.

3. CALIFORNIA K-12 EDUCATION COMPUTER SCIENCE STANDARDS AND CYBERSECURITY EDUCATION:

In addition to model curriculum that serves as the foundational basis for the study of cybersecurity, we need to find a way to link the theoretical with the practical and real world applications. "The California Computer Science Standards are based on computer science core concepts and core practices, aligned to the K12 Computer Science Framework." [46] This

[46] Source: https://sites.google.com/sfusd.edu/cs-sac

information is also available at the following California Department Education link: (https://www.cde.ca.gov/be/st/ss/computerscicontentstds.asp.) The latter includes an 11x17 matrix we used to review and the former includes an "Awesome Table" that allows for standards to be easily sorted, filtered, and reviewed. The State Board of Education formally approved California K-12 Computer Science Standards in 2018 (links and additional information found at:)

Computer Science Standards Guidelines Source:
https://www.cde.ca.gov/be/st/ss/compsciguidelines.asp

The California Computer Science Standards include the Following **Critical Subconcepts** at age appropriate levels (in grade bands found on the following page):

Computing Systems Devices-
Computing Systems Hardware & Software-
Computing Systems Troubleshooting-
Network & The Internet Network Communication and Organization-
Network & The Internet Cybersecurity-
Data & Analysis Storage-
Data & Analysis, Collection, Visualization, and Transformation-
Data & Analysis Inference & Models-
Algorithms & Programming Algorithms-
Algorithms & Programming Variables-
Algorithms & Programming Control-
Algorithms & Programming Modularity-
Algorithms & Programming & Program Development-
Impacts of Computing Culture-
Impacts of Computing Social Interactions-
Impacts of Computing Safety, Law, and Ethics-

The California Computer Science Standards include the Following **Practices**:
P1- Fostering and Inclusive Computing Culture
P2- Collaborating Around Computing
P3- Recognizing and Defining Computational Problems
P4- Developing and Using Abstraction
P5- Creating Computational Artifacts
P6- Testing and Refining Computational Artifacts
P7- Communication about Computing
(Please see K-12 CS Framework (k12cs.org) for related **Subpractices**

Source: Computer Science Standards Guidelines:
https://www.cde.ca.gov/be/st/ss/compsciguidelines.asp

K-12 EDUCATION COMPUTER SCIENCE STANDARDS GRADE BANDS:

Grades K-2: The above Subconcepts, Practices, and Subpractices found in this age appropriate level of understanding.

Grades 3-5: The above Subconcepts, Practices, and Subpractices found in this age appropriate level of understanding.

Grades 6-8: The above Subconcepts, Practices, and Subpractices found in this age appropriate level of understanding.

Grades 9-12: The above Subconcepts, Practices, and Subpractices found in this age appropriate level of understanding.

Source: Computer Science Standards Guidelines:
https://www.cde.ca.gov/be/st/ss/compsciguidelines.asp

Cybersecurity K-12 Education:

This section provides a brief description of the K-12 Education Cybersecurity component for context and understanding on related components and activities.

K-5th Grade- Focus on computing basics, coding, and a heavy dose of cyber-hygiene and cyber-bullying best practices.

K-8th Grade- Include recommendations directed at enhanced academic skills (math/science, oral/written communication), computer awareness, cyber hygiene, and exploration/awareness of Computing/IT/Cyber and related STEM fields.

6th- 8th Grade- Basic programming skills in middle school. Courses taught in Distance Learning environments and supplemented by virtual tutors from the CCC/CSU/UC systems. This increases the skillsets of youth entering the pipeline while providing college students a venue for education supplement through expanded tutoring opportunities.

These tutoring opportunities must be provided in a controlled environment (e.g. conducted at a campus library or education center) isolating direct contact opportunities between the student and tutor. The process should be a round-robin experience where a student loges info for assistance and the next random tutor with the skillset is provided.

9th to 12th Grade- Focus on academics (college prep track, advanced math/computer science courses, more students taking and passing A.P. Math/Comp Sci tests) as well as Career Technical Education (in the ICT and related CTE Industry Sectors) and engagement in extra-curricular activities like cyber competitions, coding camps, hackathons, etc. Discussions to include materials and resource on social engineering, human social factors, privacy, cyber-hygiene.

K-12 Career Technical Education (CTE) in ICT and related CTE Industry Sectors; enhanced student/faculty engagement including extra-curricular activities like cyber competitions, coding camps, hackathons, etc. In addition, we need to link all levels of K-12 Education with

professional development (experiential learning/real world application) through internships, pre- and registered apprenticeships, lab based learning, projects serving the public good, and to give students on the job experience and college preparedness/ workforce readiness.

The cybersecurity pipeline/pathway pushes "basic" cyber knowledge, skills, and abilities into middle and high school CTE programs. Courses to be digitized, virtualized, and delivered fully online. Because of pushing more "elementary" cybersecurity skills into CTE and enhanced vocational opportunity (pre-apprenticeship programs for example), we anticipate better-prepared and more knowledgeable prospective students entering higher education programs. [47]

"Too many alternatives leads to decision paralysis and anxiety. When a huge alternatives space is partitioned into a small number of archetypal choices, paralyzed people can comfortably begin exploration, starting with a small focused set of alternatives. MyVerse uses psychometrics to suggest 5 careers likely to interest the visitor and further helps them determine how to prepare or apply to jobs available in each industry they explore."

Founder - Wayne Sharp.

With more CTE exposure and better understanding of their potential career aptitudes/professional/employment, students can dive right into these disciplines and not rehash intro/elementary stuff previously covered. This is the true value of a career pipeline/pathway. Innovations at one level of education become infused into the curriculum/academic standards at more and more campuses; which in turn impacts curriculum/best practices/courses taught in other segments of education as well. This speaks to the importance of linked and aligned programs in "vertical" education and workforce development in complex pathways and potentially lengthy learning curves (depending on how technical one wanted to get.)

In summation, K-12 education CTE programs align nicely with community college workforce development and apprenticeship opportunities. Some students enter the workforce and others pursue undergraduate and graduate degree programs (and then enter the workforce). There is a very gentle onramp "Soft Start Component" to get students interested in cybersecurity employment when they are younger, have a roadmap that explains all relevant steps in the process, and show them concrete steps to take so they can get the job they are looking for! Also, the understanding that all cybersecurity programs, courses, and workforce opportunities are inclusive, diverse, and equitable and serve the needs of everyone who may be interested in pursuing/entering these career fields.

All CCCEPPP program and course content is aligned and "shakes hands" with the education programs that come before and after them. In other words, one class picks up where the last one ends, all the way through the educational process. Then all education programs lead into workforce development opportunities. As we are talking about a vocational model (i.e. CTE) —in many cases, we would like to see the addition of an apprenticeship opportunity and cybersecurity related on the job training. In this way, education programs lead to workforce development

[47] (like Computing/IT/IS/Electrical/Computer Engineering, and Cybersecurity programs.)

opportunities like registered apprenticeships, which leads to On the Job Training (OJT) and qualification for entry-level professional careers in cybersecurity.

California Career Technical Education (CTE) Cybersecurity Related Model Curriculum and Anchor Standards: (7th to 12th Grade)

California Department of Education CTE Standards for California public school information found at the following link: https://www.cde.ca.gov/ci/ct/sf/ctemcstandards.asp

On this link, one finds at least three different CDE CTE Industry Sectors with some aspect of Cybersecurity model curriculum and academic standards. This is an important observation as cybersecurity continues to be an area of significant economic growth and impacts multiple industry sectors. Many (if not all) industry sectors need cybersecurity controls, information security office, security operations center, work with managed service providers, or other form of outsourcing. As technology and IT continues to grow and affect our computer-oriented society, it is just a matter of time before all CTE vocational sectors interface regularly with tech, data, e-communication, networks, etc. through IT, cybersecurity, computer science, and privacy model curriculum and academic standards. Cybersecurity is a "nexus profession" as IT touches all industry sectors.

However, just as there are different industry sectors with existing cybersecurity related curriculum (3 examples below) and additional sectors including these relevant items in future revisions, there is another key point here. We need to not only view cybersecurity model curriculum and academic standards in slices found across in CTE Industry Sectors; but also holistically as its own standalone ICT CTE Sector Pathway itself. This makes sense in the integral nature of cybersecurity in the big picture and net sum of contribution to future education and workforce development programs in this space. **One recommendation is to pull together, consolidate cybersecurity CTE model curriculum/academic standards into one new ICT Pathway, and have all related cybersecurity items together in one location.**

In the future, we need to find a way to pull these model curriculum/academic standards into their own ICT Pathway, revise, and update to 2020 and beyond.

STANDARDS FOR CAREER READY PRACTICES-

These career standards are considered so vital to all industry sector model curriculum and academics they are known as "Career Ready Practices." As IT and computing become further embedded into our education system and schools, we need to include security and privacy and cyber-hygiene into CDE Standards for Career Ready Practices. These "new collar" skills are becoming more essential to all career readiness and college preparedness tracks. The modern digital world is rapidly transforming the kinds of skills in demand for all types of employment and across industry sectors. We should consider including more IT, computing, and soft skills into these standards in future revisions.

California Department of Education, CTE ICT Industry Sector,
B.) Networking Pathway, standards:

B8.0 Identify security threats to a network and describe general methods to mitigate those threats:

B8.1 Identify and define command network security threats: hackers, crackers, viruses, worms, and Trojan horses.

B8.2 Describe the importance of classifying appropriate monitoring devices and procedures for quick identification and prevention of security violations.

B8.3 List the policies and procedures for routine administration, such as user agreement, incident reporting, and recovery for users.

B8.4 Identify common potential risks and entrance points, including internal and external risks, and the tools used to neutralize them: firewalls; monitoring; and antivirus, spyware, and spam protection.

B8.5 Identify and apply common techniques for disaster prevention and recovery

California Department of Education, CTE Public Services Sector,
A.) Public Safety Pathway, Standards:
A2.0 Describe the history, shared mission, and roles of public safety agencies and professionals at the national, state, and local government levels:

A2.3 Describe public safety agency roles in preventing terrorism, enhancing security, managing border security, securing cyberspace, and preparing for and responding to emergencies and disasters.

A7.0 Demonstrate an understanding of the major elements and career opportunities within the United States Department of Defense (DOD), including the Army, Navy, Marine Corps, Air Force, and Coast Guard.

A7.6 Describe the need for, and the responsibilities of, the following functions within the DOD: armored security, maritime security and welfare, air superiority, space operations, and cyber security.

A8.0 Demonstrate an understanding of the functions and career opportunities within the U.S. Department of Homeland Security (DHS).

A8.6 Understand the role of cyber-security professionals within the homeland defense community and the methods and techniques used to combat public and private cyber-attacks.

California Department of Education, CTE Energy, Environment, and Utilities Sector, C.) Telecommunications Pathway Standards:

C6.0 Consider privacy and security issues of the telecommunications systems.

C6.1 Understand switching, routing, and security systems and technologies for wireless and Internet networking.

C6.2 Explain the need and strategies for network security and integrity.

C6.3 Demonstrate appropriate applications of network and user data mining and behavior profiling.

Source: California Department of Education, Career Technical Education: https://www.cde.ca.gov/ci/ct/sf/ctemcstandards.asp Accessed electronically on 6/16/2020.

DEVELOPING CALIFORNIA K-12 INSTRUCTOR CAPACITY IN COMPUTING, IT, AND CYBERSECURITY:

Cybersecurity Professional Development (Instructor-level)

In addition to the model curriculum and academic standards related to cybersecurity in K-12 Education (and higher education), there are many additional components to keep in mind for an efficient career pipeline/pathway. If we plan to increase the number of tech and STEM students/graduates annually to stoke the fires of a career pipeline/pathway, we need to increase instructor numbers and capabilities as well. One way this is accomplished is through enhanced instructor professional development; and again, in ways that differ from curriculum and standards and those types of resources. Instead, the focus is not just on "what to teach," but more important, "how to teach?" In other words, what are effective cybersecurity instructional practices and how do we promulgate them to our cadre of instructors and educators?

Huge opportunities exist in the cybersecurity education and teaching areas of professional development. Available resources may help answer the question of "what to teach," however, there is not much evaluative research on cyber education and not many available resources on "how to teach". The idea is that curriculum providers have produced rigorous and relevant content, but there is often little mention of instructional strategies or teaching materials.

Develop as a component of the cybersecurity career pathway; a project centered on researching and creating resources to support effective cybersecurity instruction and program/teaching assessment. This information to be included in the **California Clearinghouse for Cybersecurity Education and Workforce Development** for CCCEPPP education and teaching materials. These courses support instructors and cybersecurity education programs. They also contribute to the enhanced infrastructure necessary for smooth scaling of additional programs.

In addition, as a key strategy to build statewide cybersecurity CTE instructors, we need to partner with Master's Degree granting intuitions in Cybersecurity to educate and prepare instructors ready to teach cyber and computing at the K-12 and community colleges. Building instructional capacity will be key to significantly enhancing the number and capability of future cybersecurity students and ultimately, professionals in the field. In this indirect way, more emphasis placed on cybersecurity graduate education can actually reap more rewards on the tail end—more educators, instructors, and professors prepared to teach IT-Computer Science-Cybersecurity (and related tech subjects).

In addition to collaborating with California public institutions of higher education in this area of great need (i.e. limited number of instructors), we must partner with private institutions across the state like National University (and other graduate programs) to prepare future educators and instructional capacity to teach in cybersecurity specialization and CTE. With a Master's Degree in hand, instructors can teach courses in K-12 Education (with appropriate teaching credentials), in California Community Colleges, or as adjuncts/lecturers at California State University and University of California campuses. Doctoral degrees are traditionally necessary to teach in 4-year degree programs, but there are notable examples like a Masters of Fine Arts (M.F.A.) terminal degree program.

Professional Development- Cybersecurity Pre-Apprentices, Registered Apprenticeship Programs, and Internships

One key aspect of career pipelines is the linkage with application and experience. The same can be said for a qualified cybersecurity workforce. Any talk of a cybersecurity career pipeline must include a tight linkage with experiential learning opportunities. Thus, one way to support student's professional development efforts and encourage their participation in cybersecurity education programs is through internships and apprenticeships. One key activities to work towards is finding ways to gain paid apprenticeship and internship opportunities to augment student classroom and academic learning in IT-Cyber.

The final related issue concerns the selection and hiring process for cybersecurity professionals. One of the keys to success in the area of cybersecurity selection and hiring is to stay away from risky behaviors that may disqualify someone from the job later on down the road. This can include a variety of factors from criminal history, drug and alcohol abuse, credit rating issues, poor employment history, dishonorable discharge from the military, etc. It is important that we focus on ethics, not just in hacking, but in our personal lives as well. In terms of ethical hacking, these are the kinds of things that we must really provide some good advice and guidance to prospective career pipeline students. We do not wish to teach sensitive knowledge and skills without informing them of the great responsibility and trust that goes along with that information.

Cybersecurity Pre- and Registered Apprenticeship Programs:

California has a long and rich history of supporting apprenticeship programs. California today has more apprentices than most states and in many varied professions, sectors, and fields as well. Apprenticeships are found in many industries and occupations and there is a growing realization among the public and private sector that this strategy may be helpful in the cybersecurity space as well. One reason why cybersecurity is an excellent candidate for registered apprenticeship program development is the "hands-on" practical skills necessary for professional success. The learn by doing model is well supported by industry and we must work carefully with employers to develop solid apprenticeship programs that are closely linked to the education programs we have been discussing in this strategy report. These apprenticeship programs include a classroom related instruction component (RTI) plus a 2000 hour OJT with employers.

For those who are interested in Cybersecurity Apprenticeships, they would be administered and coordinated at **California Cybersecurity Apprenticeship Centers found** at participating college and university campuses.

Additional information on Cybersecurity Youth Pre-Apprenticeships and Registered Apprenticeships found in Appendix 2 of this report.

Family Roadmap Resource for Cybersecurity Education and Workforce Development:

Education of family of cybersecurity students- much of the general discussion of cybersecurity education has only discussed the role of students and educators in the career education pipeline/pathway process. However, this philosophy leaves out a key component of K-12 learning and education—the family, parents, siblings, and extended family. If IT-Cyber education is tough for interested students, how difficult is it for family members (particularly those without these skills and experiences themselves) to understand different ways they can show support and provide encouragement to their cyber kids?

Thus, we must also reach out to and educate the family and parents of prospective career education pipelines/pathways students. Many in our society do not understand much about cybersecurity and tech as we would prefer. We should provide resources to allow family and parents of prospective cybersecurity students to understand what they can to do to encourage their kids in tech-cyber and support their success in these programs. This is particularly true for parents who may not have much formal education or a tech background themselves.

The message parents must hear is that their students can complete cybersecurity education programs, complete workforce development opportunities, and ultimately be successful in the profession. The parents and family can in turn encourage and assist their children in being successful in these programs. What information is included in the Family Roadmap Resource?

1. **Family Roadmap Resource for Cybersecurity Education and Workforce Development**- illustrates and explain what parents/family need to know about program basics, expectations, and what to expect. Family needs to know this is achievable stuff and how they can participate and help out in their role of supportive parents.

2. Communicate tips and advice on how parents can encourage, support their students, and help them to succeed in cybersecurity education and workforce development programs.

3. “Soft start” education programs will assist to bring students up to speed in fundamentals and additional skills for the profession.

4. Provide parents, family, and students with additional resources and links to get more information and assistance to help with program completion.

CALIFORNIA CYBERSECURITY HYGIENE MULTI CHANNEL COMMUNICATION STRATEGY COMPONENT: CYBER-HYGIENE:

We have already spoken about key elements of the K-12 component of the California Cybersecurity Career pipeline. We have discussed model curriculum and academic standards; and also professional development ideas/action items/prospective recommendations for our Workforce Development and Education Subcommittee to promulgate. However, there is one last key element that we must address at this, and other levels of education—namely the critical skill of practicing "safe computing." Our networks, systems, and data are only as secure as the users that access these items. By teaching "best practices" in cyber-hygiene, we can be better and safer consumers of information and data. We can limit our cyber risk to ourselves and our families, educational institutions, workplaces, and other sensitive aspects of our lives that prudent self-cyber security strategies would reinforce and help secure.

One may ask, how important is cyber-hygiene and related issues here in California? Assembly Bill 809 (A.B. 809- Cyber Hygiene Education Bill) would support the movement towards teaching cyber-hygiene in schools (including social media literacy, staying safe online, reducing cyber-bullying, etc.) In the event this bill was to become law and also funded, it would be vital to provide school districts with the guidance, resources, and useful curriculum for them to meet this important objective.

For cyber hygiene resources for teachers there is the existing group **Common Sense Media** that houses educator resources https://www.commonsense.org/education/

DHS's Stop. Think. Connect. Resources could be useful to any teacher since it provides the whole suite of US-CERT publications/ other agency publications detailing cyber topics: https://www.dhs.gov/publication/stopthinkconnect-parent-and-educator-resources

Teachingprivacy.org (a project out of UC Berkeley - https://teachingprivacy.org/)

- The UC Berkeley project is a great conversation 9-12 and Be Internet Awesome fits in the K-8 space.

Google's Be Internet Awesome (https://beinternetawesome.withgoogle.com/en)

K-12 CYBERSECURITY ADDITIONAL RECOMMENDATIONS AND ACTIVITY:

1. Update CTE Model Curriculum relating to Cybersecurity. We recommend that the CDE update the ICT anchor standards and pathway model curriculum from "4" to "5," to include the creation of a Cybersecurity ITC Sector Pathway and related standards and curriculum.

2. Work towards the design of an "efficient" A-G Integrated Curriculum and courses for statewide approval in support of Computer Science/Information Technology/Cybersecurity

3. Recommend new "Cybersecurity" specific courses to link ICT CTE with GE; key caveat—make courses accessible and interesting to attract broader student interest in these type of courses.

4. Prepare template letter of support and "formal recommendation to the CDE for the design and development of a specific cybersecurity pathway. Secure support across the GCTF.

5. Recommendation to create and implement CALPADS codes for cybersecurity pathways.

6. Develop cybersecurity education metrics for program/course assessment validity and evaluation.

7. Study and analyze current and future California legislation for cyber education and workforce development activity.

SECTION VIII: CALIFORNIA CYBERSECURITY HIGHER EDUCATION

Important Reasons to Enhance Cybersecurity Higher Education Workforce Development:

In the previous report section, we discussed California K-12 Education and recommendations for preparation of students in ICT-Cybersecurity pathways. Cybersecurity academic preparation, CTE, career/professional exploration/development, apprenticeships, cybersecurity competitions, and meaningful education opportunities exist or in development to serve as the educational bedrock for solid workforce development. However, there is an issue with the cybersecurity field as rather specialized and technical sometimes. Few graduating high school seniors likely have the skill/experience/education level to directly transition into cybersecurity workforce right after graduation from high school. We seek to change that as part of this transformative cybersecurity career pipeline/pathway.

In terms of cybersecurity workforce development and education career pathways, there are relatively few "on-ramps" into the cybersecurity profession from secondary schools. This means the cybersecurity career pipeline must align seamlessly and transition effortlessly from high school into higher education via California Community Colleges, California State University, and University of California, as well as private and not for profit colleges and universities.

This takes us to a second and related point. Cybersecurity is a rapidly growing and maturing professional field based on significant global and societal needs and demands. Being an extraordinarily dynamic field and industry, it has been a challenge keeping up with rapidly evolving workforce needs, industry certifications, new programming languages, and teaching of up to date tech/skills/competencies/ and digital environment.

Analyzing Cyberseek data, about 88% of these cybersecurity positions specify a bachelor's degree or higher (as listed per job openings from 2/2018 through 10/2019) (Burning Glass, 2019). However, at this time, there are no four year public institutions in the State of California that offer a Cybersecurity Degree program. Thus, while many positions require four-year degrees, these standards are beginning to rapidly change in industry and government circles.

There is much change in industry, also as a nascent and burgeoning academic discipline to educate, train, and prepare this increasingly specialized and valuable resource. So in relations to academics, there is a tremendous amount of siloization going on within the higher education community. Computer Science, IT/IS, Computer and Electrical Engineering all have their own specific questions and concerns related to the role of cybersecurity within their discipline. However, there are many commonalities of need shared between cybersecurity professionals from domains and irrespective of specific fields/disciplines. Thus, we want to focus on commonalities of Computing/IT/Engineering disciplines and not subsume cybersecurity as a "minor role" in them.

To make sure we utilize all relevant sources of cybersecurity curriculum/standards together into an evolving and growing cybersecurity discipline/sub-discipline, we align and link with Computer Science, IT/IS, and Electrical/Computer Engineering (and closely related academic fields.) Curriculum and standards included for cybersecurity degree and certificate programs in high demand industry sectors and specializations:

- Stand-alone Cybersecurity Degree Programs-

- Dual Baccalaureate Cybersecurity Degree Programs (with linked apprenticeships)-
- Stackable Certificate Programs embedded into various degree programs representing key cybersecurity specializations. These fall into two categories:
    - "**Professional certifications"** for entry-level employment;
    - **"In-service"** cybersecurity certificate programs for those currently employed and wish to up-skill/re-skill.

Cybersecurity Student Learning Outcomes (SLOs) are curriculum mapped thematically into the following types of higher education courses:

Core Course Requirements-

Major Course Requirements-

Electives/Specializations Courses-

Capstone (Culminating Experience) Courses-

Cybersecurity Curriculum Mapping Discussion and Process:

As Cybersecurity SMEs, we rely on statewide faculty to prepare a list of recommended courses (and the SLOs that have been competency mapped into them). We work with employers (public and private) and education/higher education statewide to design education programs that meet the needs of all major stakeholders and partners. We find out what SLOs are necessary to demonstrate various KSAs and core competencies necessary for the appropriate preparation of minimum requirements for various entry-level cybersecurity professional positions. Our objective is to make sure current KSAs and competencies are included in the curriculum map above in essential workforce positions. Completed KSA mapping demonstrates exactly how the needs of major stakeholders (public, private, and education/academic communities are met and where in the curriculum. These mapping exercises become an integral part of the CCCEPPP and related model curriculum at all levels of education

Cybersecurity Model Curriculum and Academic Standards: Program Delivery- the Multi Campus Consortium Model:

We rely on the "hub and spoke model" of cybersecurity program and course offerings. Large multi campus consortiums working together to offer multiple sections of cybersecurity core and major requirements online (as a shared resource across educational systems/campuses.) In addition, and depending on institutional and faculty strengths/teaching/research specializations—we develop a catalog of cybersecurity courses (core, major requirements, and elective) drawn from participating campuses and involved faculty members.

The B.S. in Cybersecurity Degree Program included in the Model Curriculum and Academic Standards Report Section (version 7.0) on page 152 is a general cybersecurity program model. In the undergraduate degree model curriculum and academic standards sample, we see a new variant undergraduate degree program curriculum with space to include 12-unit (4 course) embedded stackable certificates as specialized offerings. We are also interested in the Dual Baccalaureate Cybersecurity Degree Program as well (interdisciplinary program to be added to college major across campus in combination with a 2000 OJT apprenticeship opportunity.

Multi-Campus Consortium Organization:

The extent of need in California is very great right now and expected to continue well into the future. As such, we are going to need to build cybersecurity workforce development and education programs to scale. In this way, it is foolish to believe that any single campus or small group of campuses is going to be able to graduate enough cyber students by themselves. We are going to need to leverage all the higher education institutions across California, both public and private to help out here. Thus, when we are talking about a California Cybersecurity Career education Pipeline/Pathway—we are going to need to build significant campus ties, infrastructure, and communications to collaborate and coordinate activity and program development. Based on the nature of the program, contributing campus consortiums will vary greatly. However, their organization chart example is found below:

Lead Institutions-

Participating Campuses-

Campuses-based Specializations for embedded "stackable" certificate programs-

THE CYBERSECURITY ASSOCIATE LEVEL EDUCATION COMPONENT

In the previous section of the report, we discussed a series of recommendations related to the framework for an important foundation of IT-Cybersecurity in K-12 academics, career technical education (CTE), and extra-curricular and professional development opportunities. Once we have elementary and introductory computing, IT, and cybersecurity skills embedded into accessible and available K-12 education programs, courses, and opportunities, we need students to quickly and seamlessly articulate and transfer into higher education programs. The first step for many graduating high school seniors is the California Community Colleges. With over 2.1 million students system wide, and as previously noted, the largest higher education system in the world.

The third subcommittee report recommendation is the development and implementation of a Cybersecurity Model Transfer Curriculum (MTC) program (short-term objective) and Associate Degree Transfer (A.D.T.) program (long-term objective) in California higher education. The 2-Year/4-Year transferable ADT is the "gold standard" for new and existing degree programs. The true value of an ADT is in the seamless/smooth transition for transferring students—exactly what is necessary in an efficient career pipeline/pathway.

INTRODUCTION TO CALIFORNIA ASSOCIATE LEVEL CYBERSECURITY EDUCATION

Associate Level Cybersecurity Introduction Prepared by:

Markus Geissler, Ph.D., Professor of Computer Information Science, Cosumnes River College and Chair of the C-ID Information Technology/Information Systems Faculty Discipline Review Group.

Richard Grotegut, Regional Director/Employment Engagement, ICT Digital Media Sector for the Bay Region; Lecturer, San Jose State University; Computer Science Professor Emeritus, Ohlone College; Director, Western Academy Support & Training Center (WASTC)

Olivia Herriford, DM, M.B.A. Regional Director/Employment Engagement, ICT Digital Media Sector, Bay Area Community College Consortium

The California Community Colleges (CCC) were the first postsecondary institutions to offer Cybersecurity education in our state, and they continue to significantly contribute to building California's Cybersecurity workforce. When Cosumnes River College began offering the first degree in Information Assurance in 2004, it started what has become a solid array of postsecondary Cybersecurity-related programs at public two-year institutions throughout California. Today, thanks to various efforts to guide curriculum development and recruit individuals of all ages and backgrounds, about one-half of California's 116 community colleges are helping their communities' by preparing qualified Cybersecurity professionals who will help their employers defend technology and other assets against unauthorized access, use, or damage.

Community colleges have traditionally offered a lot of technology education and training for both recent high school graduates and working professionals who are changing careers. Through their many programs in Computing disciplines, including Computer Science, Information Technology, and Information Systems, they continue to enable students from a great diversity of backgrounds to advance professionally and improve their livelihoods.

Model Curricula for Computing Disciplines

Developing model curricula has been one of the successful strategies used to broaden academic programs in the Computing disciplines. The faculty-driven C-ID initiative, by which the Academic Senate for California Community Colleges (ASCCC) and the Academic Senate for the California State University (ASCSU) created a supra-course numbering system to identify common courses offered at California Community Colleges and California State Universities has served as a platform for faculty collaboration around creating and maintaining model curricula since 2011. Faculty Discipline Review Groups (FDRG) consisting of six faculty members appointed by the ASCCC and ASCSU have created numerous Transfer Model Curricula (TMC) to serve as a foundation for Associate's Degrees for Transfer (ADT) awarded by CCCs and accepted by many CSUs in fulfillment of lower division requirements for common majors.

In 2013 the Computer Science FDRG implemented a TMC which is based on the ACM's globally accepted curricular guidance for introductory Computer Science courses (CS1, CS2, etc.), and has since made minor modifications to allow more CCC's to implement the ADT in Computer Science. Around the same time the Information Technology and Information Systems (ITIS) FDRG launched an effort to create an Information Technology TMC in 2013, but, due to the low number of upper-division transfer programs at the CSUs, the proposed TMC had to be converted to the IT Model Curriculum (ITMC). The ITMC is based on recommendations by the U.S. Department of Labor and ACM and has since been implemented at approximately 50 CCCs. In 2018 the ITIS FDRG used the same process to create an IT Cybersecurity Model Curriculum (IT Cyber MC) which is currently awaiting approval by the C-ID's Intersegmental Curriculum Workgroup (ICW). In the meantime, however, about 30 CCCs have already begun implementing Cybersecurity courses based on the draft descriptors.

Keeping model curricula current, which is especially important in the IT and Cybersecurity disciplines as they continue to evolve, has been a substantial challenge in an environment where more traditional majors are only reviewed every five years. Notwithstanding substantial delays in the appointment process for its members, the ITIS FDRG continues to regularly meet to develop new descriptors and update existing ones. And while, due to a lack of trained evaluators, the assessment of new Course Outlines of Record submitted by CCCs to map to model curriculum descriptors has stalled, Computing programs at CCCs continue to successfully prepare students for transfer to a baccalaureate program or for starting an entry-level position in IT or Cybersecurity.

Apprenticeships

California Community Colleges have been instrumental in the expansion of apprenticeship opportunities to Computing disciplines, including Cybersecurity, by offering the Related and Supplemental Instruction (RSI) classroom component to complement the hands-on training provided by employers.

Supported by the California Apprenticeship Initiative (CAI), a grant opportunity offered by the California Community College Chancellor's Office (CCCCO) to support the creation of new apprenticeships and pre-apprenticeship training programs, City College of San Francisco (CCSF) and Coastline College now deliver cybersecurity apprenticeship programs registered with the California Division of Apprenticeship Standards and the Department of Labor Office of Apprenticeship. Both colleges have earned designation as Centers of Academic Excellence (CAE2Y) in accordance with the guidelines set forth by the National Security Agency and Department of Homeland Security.

The CCSF Information Security Analyst (ISA) Apprenticeship is an 18 month paid program for 32 hours per week with stepped wages toward the journeyworker hourly pay at the end of the program. Applicants must have a CompTIA Security+ or CCNA certification or have successfully completed an equivalent sequence of CC courses. Participating employers select from a vetted pool of candidates. During the apprenticeship, apprentices receive a minimum of 157.5 hours of advanced related instruction and must complete at least 2000 hours of OJT, supported by a ”journeyperson”/mentor to help develop skills for proficiency in the required work processes. The CCSF ISA Apprenticeship uses Urban Institute’s Competency-Based Occupational Framework for Cybersecurity Support Technician for registered apprenticeship developed for the DOL OA to define the work processes. Employers may customize the work processes and related instruction to fit their needs. Upon completion of the program, apprentices are not only certified by the DOL and DAS, they are prepared to take the CISSP Associate exam.

The Coastline College apprenticeship is a 2-year, cohort-based program. Applicants must have the CompTIA A+ certification. The initial related instruction begins before apprentices are placed at employers and includes significant job-readiness training and additional CompTIA certifications (Network+, Security+, Server+). Once placed, 2000 hours of OJT is required, with apprentices working 30 hours per week to allow more time to complete training along one of two tracks (Cybersecurity or Cisco Networking). Upon completion of the program, apprentices are not only certified by the DOL and DAS, apprentices also earn CompTIA Linux+, PenTest+, and Cybersecurity Analyst+ certifications.

Relationship with Industry

Since many technology companies are based in California, our state has unique opportunities to forge relationships between leading tech companies and the education sector. The community colleges have a long history of solid public-private partnerships. Early engagement with leading tech companies like Microsoft and Cisco Systems through their “Academy” programs, dating back over 20 years, as led to a fruitful partnership and an advantage for community college students to acquire the tech skills that industry has demanded. Aligning IT/Cyber course curricula with industry certification is an ongoing and reliable undertaking.

To date CCC faculty have implemented course materials developed by several key technology companies into the Cybersecurity courses they offer:

- **Cisco Systems**
  - Cisco Network Academy
- **Palo Alto Networks**
  - Cybersecurity Academy
- **Microsoft**
  - Azure Development tools for Teachers
  - Microsoft Imagine (software sharing)
- **Amazon Web Services (AWS)**
  - AWS Academy and AWS Educate
- **Google**
  - Google IT Support Certificate
  - Google Cloud Foundations
- **Dell/VMware**
  - VMware Academy
- **IBM/Red Hat**
  - Red Hat Academy
  - IBM Open P-TECH Cybersecurity Badges
- **CompTIA**
  - Vendor-agnostic industry certifications

"Cisco Networking Academy courses are an outstanding fit for community colleges in a variety of ways. Learners can prepare for industry-recognized certifications, earn credits towards a 2-year degree, and prepare for a transfer to a 4-year university. In today's world, staying on top of evolving technology brings economic opportunities to individuals and their communities. We are extremely proud of partnering with community colleges across the United States."

Rebecca Chisolm, North America Network Academy Regional Manager, Cisco Systems

Intersegmental Educational Partnerships

California Community Colleges are integral parts of their communities. And as such, many of them serve as activity hubs not only for their own students but also for members of the community at large. Since effective Cybersecurity efforts must involve the education and training of all community members, exposing students to Cybersecurity-related topics as early as elementary school will not only teach them to safeguard their own personal assets and privacy, but it also helps to prepare them for joining the Cybersecurity workforce after they have completed various levels of education.

Over the past several years, many CCCs and members of the ICT/DM Sector Team of Regional Directors have sponsored Cybersecurity-related activities on CCC campuses and in virtual environments. Activities included:

- Cyber camps for middle and high school students, with some camps especially targeted at girls and underrepresented populations,
- Cybersecurity competitions, such as Cyberpatriot, National Cyber League, the Bay Cyber League (BCL), and the California Mayors' Cyber Cup.

- "Cybersecurity Day" events to help raise awareness about better Cybersecurity practices throughout the community.

Strong Workforce and K-12 Strong Workforce funds, which are administered by the CCCCO and awarded by the regional CCC consortia, have played a major role in allowing CCCs to not only ensure that their own instructional programs are current, but also to collaborate with regional industry and education partners in creating effective Cybersecurity-related academic pathways and pipelines.

California community colleges have been at the forefront of Cybersecurity education in our state for a long time. They will continue to serve our state as a whole, and their communities in particular, as hubs for Cybersecurity-related information, training, and workforce preparation for many decades to come.

Current California Community College Degree Programs Related to Cybersecurity: Existing Lower Division Model Curriculum/Academic Standards/Programs:

The first step in the student cybersecurity undergraduate education process is securing Associate Degrees and Certifications from California Community Colleges. There are two current associate level tracks useful for undergraduates to transfer into a prospective upper division cybersecurity degree program. There are numerous certifications available at many CCCs as well.

Computer Science Associate Transfer Degree Program- Already Approved.

IT Model Curriculum Degree Program- Already Approved.

The two lower division programs are currently available and increasingly offered at a growing number of CCC campuses statewide. These two tracks are for students to take in preparation for transfer into upper division multi campus university consortiums based on B.S. Cyber Degree/Dual Baccalaureate Degree Programs. It is important to take this opportunity to enhance CCC capacity and capability in cybersecurity education and workforce development. Because many of these programs and courses have been around for a while, it would be ideal to provide CCC Faculty the opportunity to redesign/update courses that advance cybersecurity in computer science, IT, and electrical/computer engineering courses. Also key to fully integrate CCC faculty into workgroups and activities with K-12 and CSU and UC campus colleagues.

(See the following samples of the Computer Science Associate Science Transfer Degree Program and Information Technology Model Curriculum on the next page.)

Associates Level Cybersecurity Education Components

1. **Associate Degree Model Curriculum (MC)/ Transfer Model Curriculum (TMC) in Cybersecurity** in conjunction with Colleagues from the California Community College, California State University, University of California.

Information Technology Model Curriculum (ITMC)

Key Current California Undergraduate Cybersecurity Program Limitation: ITMC— current A.S. programs lack 4-Year academic partners to develop Transfer Model Curriculum (TMC) and Associate Transfer Degree (AST) programs in cybersecurity. This is a current limitation to a career pipeline in cybersecurity and "disconnect" between 2 year and 4 year schools.

2. **Associates level Cybersecurity Stacking Certificate Professional Certifications**- The California Cybersecurity Career Education Pipeline/Pathway includes specialized education and training tracks across "high needs areas" through the development of **("STACKING CERTIFICATE PROGRAMS")** in select areas:

- Including, cyber-security, cyber-digital forensics (crime), cyber-resiliency, critical infrastructure protection, emergency response, and additional related NICE Cybersecurity Workforce Framework fields.

- An additional list of prospective higher education cybersecurity certifications and specializations are found at the end of the draft B.S. Cybersecurity Degree Program Course list in several pages.

AST COMPUTER SCIENCE REQUIREMENTS-

***** Two Quick Notes Here:**

A. Traditional Computer Science (CS) to Cyber is the "traditional" pathway for top end talent model.

B. Additional exposure to CS students to the security environment. Important to get students (and others) thinking about security as a fore thought on the front end. We want our CS/IT/Engineers, etc. to think security first, not as a passing or after-thought.

Future Activity: California Cybersecurity Associate Transfer Degree Program Development and Implementation:

In the future, it would be ideal to have an Associate Transfer Degree Program (ADT) linking 2 year degree programs (Associate in Cybersecurity) with 4 year degree programs (Bachelors in Cybersecurity). Participating California Community College, California State

University, and University of California campuses partnering together and offering specialized cybersecurity degree and stacking certificate programs.

SCOPE OF WORK: There are 116 CCCs in California (115 campuses and one fully online campus known as "Calbright"). The CCCEPPP needs to work collaboratively with all of them. CCC's work closely in conjunction with high schools and 4- year universities across the state to align academic programs, articulation agreements, etc. from one education level/segment to the next. Much coordination, alignment, and linkage must occur for cybersecurity career pipelines/pathways to function/operate efficiently. It becomes a matter of coordination and facilitation to make sure Cybersecurity Associate Level programs and courses receive the support they and their students need for academic success.

One key to Associate cybersecurity component success is building degree/certificate programs, courses, instructional/student materials, and road maps for instructors/students to achieve a solid foundational baseline for workforce development and education.

Cybersecurity Associates Level (Degrees/Certifications) Objectives:

Develop an 18-21 Unit Associate of Science Degree Program in Cyber-Security (Fully transferrable and articulated Model Transfer Curriculum (MTC) 2+2 degree program:

Computer Science A.S.T. Programs- Articulation agreements with proposed 4 Year Cybersecurity Bachelor of Science Degree Program.

Information Technology Model Curriculum (ITMC)- Articulation agreements with proposed 4 Year Cybersecurity Bachelor of Science Degree Program.

Lower division General Education Cybersecurity Courses-

A.B. 1440/440 Model Transfer Curriculum- A.S.T. Degree Program in Cybersecurity

Associates level Cybersecurity Stacking Certificate Professional Certifications-

TOP/CIP Codes- Need to develop ones for cybersecurity academic programs.

Cybersecurity Course Identification Descriptors (CID) Development-

Current California Community College Degree Programs Related to Cybersecurity: Existing Lower Division Model Curriculum/Academic Standards/Programs:

Cybersecurity Lower Division Course Work:

The first step in undergraduate education is securing an Associate Degree and Certifications from the California Community College.

Associate of Science Transfer Degree Program in Computer Science (AST)-

Information Technology Model Curriculum (ITMC)-

Electrical/Computer Engineering-

Associate of Science Transfer Degree Program in Computer Science (AST)- Please see the attached example courtesy of a AST Degree Program in Computer Science Coursework from Santa Ana College [48]:

Required Core (29 units) Units

Computer Science 121, Programming Concepts 3

Computer Science 131, Data Structures Concepts 3

Computer Science 129, Introduction to Computer Organization 4

Computer Science 140, Discrete Structures for Computer Science 3

Mathematics 180, Analytic Geometry and Calculus I —OR — Mathematics 180H, Honors Analytic Geometry and Calculus I 4

Mathematics 185, Analytic Geometry and Calculus II 4

Physics 217, Engineering Physics I 4

Physics 227, Engineering Physics II 4 Total 29

[48] https://www.sac.edu/StudentServices/Counseling/articulation/Documents/Computer%20Science%20AST.pdf

Information Technology Model Curriculum (ITMC)-

Source: "AS Degree in IT (Fall 2015) Ohlone College Case Study" presentation prepared by Dr. Richard Grotegut.

ITMC PROGRAM STUDENT LEARNING OBJECTIVES

1. Apply fundamental knowledge of computing and the current use of technology techniques, skills, and tools necessary for the computing practice.
2. Demonstrate the ability to locate, critically evaluate, and solve business problems with technology solutions using qualitative and quantitative information.
3. Demonstration a fundamental ability to identify and analyze user needs in the selection, creation, evaluation, and administration of computer-based systems.
4. Provide information technology technical assistance to computer and network users.
5. Demonstrate application of the IT career field and the need to be lifelong learners.

INFORMATION TECHNOLOGY MODEL CURRICULUM

Total Program Units: 22-23
Required Core Courses: __13___units

Title (units) C-ID Designation Certification Prep

Information & Communication Technology Essentials (4)- ITIS 110 Certification Prep: CompTIA A+

Business Information Systems, Computer Information Systems (3)- ITIS 120

Introduction to Programming Concepts and Methodologies (3)- IT IS 130 or COMP 112

Computer Network Fundamentals (3) ITIS 150- Certification Prep: CompTIA Network+

Select 6 units or 2 courses from the following:

Introduction to Systems Analysis and Design (3)- ITIS 140

Routing and Switching Essentials (3) ITIS 151- Certification Prep: Cisco CCENT

Systems and Network Administration (3) ITIS 155- Certification Prep: CompTIA Server+

Introduction to Information Systems Security (3)- ITIS 160- Certification Prep: CompTIA Security+

Introduction to Cybersecurity: Ethical Hacking (3)- ITIS 164-

Digital Forensics Fundamentals (3)- ITIS 165

Introduction to Database Management Systems (3)- ITIS 180

Business Communication (3)- BUS 115

Select 3 - 4 units or 1 course from the following:

Introduction to Statistics (3) MATH 110 Also fulfills CSU GE Area B4

Finite Mathematics (3) MATH 130 Also fulfills CSU GE Area B4

Business Calculus (3) MATH 140 Also fulfills CSU GE Area B4

Single Variable Calculus I Early Transcendentals (4)- MATH 210 Also fulfills CSU GE Area B4

Cybersecurity General Education (G.E.) Lower Division Courses:
(For All Majors across Campus)-

Before we discuss specific details of a specialized upper division cybersecurity program model curriculum and academic standards (major), we want to mention an area in which many students from across the entire campus can benefit from these education programs/courses. General Education pattern courses are found as additional requirements to graduation and are drawn from all academic units on a campus and intended to broaden and widen the student's educational experience (and thus known as General Education, or GE courses.) It would be ideal to have a non-technical yet informative course for students to explore the professional cybersecurity field a bit; as well as provide students with timely cyber-hygiene/online safety materials to enhance cyber awareness/security posture in their personal and professional lives. Of additional benefit is that GE (and writing courses) courses tend to "double count" in the major. GE and writing courses are thus very efficient when designing new academic programs such as these.

Cybersecurity General Education (G.E.) Lower Division Courses

We are interested in the following lower division cybersecurity undergraduate General Education (G.E.) Courses:

Cybersecurity General Elective (G.E.) Courses (For All Majors across Campus)- There are a variety of G.E. pattern courses to develop):

Lower Division G.E Courses- Cybersecurity Awareness course - online 3-unit elective course for any major. Introduction to Information Security would be such Cybersecurity Awareness course. The difference would be in the scope, time, delivery (online only), targeted audience (any major, instead of specifically IT).

Human factors of cybersecurity (including UI/UX, and social engineering attacks)-

Cyber-Competition Team Courses-

Lower Division General Education (G.E.) Courses-

Cybersecurity Awareness- (3.0 units)

Catalog Description: Exploration of practical computer security in everyday life for non-majors. Covering security principles, technologies and tools used to secure computers, cyber space, and keep ourselves 'digitally' secure, including: AntiVirus and Malwares, E-mail security, Firewalls, Data security, Cryptography, Web security, Wireless security, Password management, Authentication, Access Control, Privacy and Anonymity, Privacy Regulation, US Constitution.

Student Learning Outcomes:

Upon completion of this course, students will be able to:

1. Critically evaluate scopes and vulnerabilities of Cyber Space.

2. Determine security principles, technologies, and tools used in cyber space.

3. Employ current security tools that are available in cyber space to protect oneself.

4. Understand privacy rights and regulations.

Area E (G.E.) Learning Outcomes (Sample below; determined by local campuses)
1. Develop intellectual, practical, and/or physical skills and abilities that will serve them throughout their lives.

2. Apply their learning to other pursuits within and outside of the classroom.

3. Demonstrate the capacity to make informed and ethical decisions.

Human factors of cybersecurity (including UI/UX, social engineering attacks)- (3.0 units)
COURSE BUILDOUT- Public Sector, Industry, Higher Education

Catalog Description: Understand human factors, motivations, and psychology driving good and bad actors in the cyber space. Role and impact of social engineering on offensive and defensive cybersecurity practices. Analyze risk aversion and other key psychological and behavioral traits.

Student Learning Outcomes:
By the end of this course, students will be able to:
1. Identify and describe various motivations of cyber bad actors.
2. Demonstrate the effectiveness of social engineering attacks.
3. Compare and contrast UI/UX.
4. Develop and test theories related to bad actor human factors.
5. Apply cyber risk mitigation and risk aversion activities for individual.

Area E (G.E.) Learning Outcomes (Sample below; determined by local campuses)

1. Develop intellectual, practical, and/or physical skills and abilities that will serve them throughout their lives.

2. Apply their learning to other pursuits within and outside of the classroom.

3. Demonstrate the capacity to make informed and ethical decisions.

CYBERSECURITY BACHELOR'S LEVEL EDUCATION COMPONENT

CYBERSECURITY BACHELOR'S LEVEL EDUCATION PROGRAMS

Bachelor's Degree Cybersecurity Education/Workforce Development and Coordination: (Including Planning, Administration, and Management)-

SCOPE OF WORK: There are 116 CCCs, 23 CSUs and 10 UC campuses currently in California. The CCCEPPP needs to work collaboratively with all of them. CCC's work closely in conjunction with high schools and 4- year universities across the state to align academic programs, articulation agreements, etc. from one education level/segment to the next. Much coordination, alignment, and linkage must occur for cybersecurity career pipelines/pathways to function/operate efficiently. It becomes a matter of coordination and facilitation to make sure that the Cybersecurity Bachelors Level programs and courses receive the support they and their students need for academic success. One key to Bachelors Cyber component success is building degree/certificate programs, courses, instructional/student materials, and road maps for instructors/students to achieve a solid foundational baseline for cybersecurity education/workforce development.

Bachelors of Science (B.S.) in Cybersecurity Degree Program (offered as Multi-campus Consortium)

SCOPE OF WORK: Bachelors of Science (B.S.) Cybersecurity Degree Program Model Curriculum and Academic Standards design, development, and implementation.

Cybersecurity is often a technical and specialized field; and getting more so every day. Cybersecurity foundations, principles, skills, and tools do not fall cleanly into any one current academic discipline. Newer and more specialized degree programs are needed. Because California currently needs over 72,000+ cyber professionals in the workforce, it is clear that a campus or two is hardly going to provide the economy of scale to make much of a dent on that large amount of workforce needing development. Thus, it is critical to develop a significant number of participating campuses (also known as a multi campus consortium) of California Community Colleges (CCC), California State Universities (CSU), and University of California (UC) to implement a 2 Year/4 Year transferable Bachelors/Dual Baccalaureate Cybersecurity Degree Program. The program to be offered as a multi-campus consortium of participating California higher education institutions (CCC, CSU, and UC campuses and private colleges/universities).

Further technical specialization and tremendous technological innovation draw out the critical need for a distinct cybersecurity degree program to meet substantial and escalating demand for computer savvy specialists and analysts. Computer science and IT elements remain as the basis for the expanding cybersecurity specialization. Cybersecurity education programs also contain a combination of engineering, science, math, technology, and business fundamentals necessary for success in the field. We leverage existing academic and institutional strengths to develop and offer cybersecurity undergraduate degree programs (to scale) across a significant number of participating CSU and UC campuses. After all, 65-70% of cybersecurity/information security have 4 year degrees (in a closely related field). State of California H.R. I.T-1 Job Classification requires a combination of 4 Years Education/Related Experience, so we will need to run a good number of students per program cohort to meet this capability/workforce gap.

Bachelor of Science Degree in Cybersecurity (with Embedded Stackable Industry Certification Programs and Specialized Courses) and Dual Baccalaureate Cybersecurity Degree Programs-

Design and develop a Bachelor's of Science Degree Program in Cybersecurity fully linked and articulated with 2-year degree programs under A.B. 1440/440 guidelines and policy. This transfer degree program will initially follow as a Model Transfer Curriculum (MTC) where students receive 2 years of education in the California Community College System directly into the California State University System (Degree completion programs (60/60 or 2+2 programs).

Build a multi-campus consortium to host the cybersecurity pathway. The Consortium includes partnering institutions from K-12, Associates, Bachelors, and Graduate programs.

Hub and spokes model: select campuses offer the program core. Additional supporting institutions offer specific tracks or "specializations" in all the relevant areas of cyber security/forensics/resiliency and additional areas of interest/demand. Additional information on the B.S. in Cybersecurity Task/Activity/Project found in the next report section.

California Multi Campus Consortiums in Cybersecurity-

Utilize the "Hub and spokes model" where lead campuses coordinate to develop and offer cybersecurity core, major requirement, and elective/specialization courses for undergraduate degree programs. In addition, other partnering campuses will develop embedded stackable certificate programs that will "plug into" the Bachelors of Science Degree Program in Cybersecurity and Dual Baccalaureate Degree Program in Cybersecurity. In this way, campuses can contribute and work together to offer these specialized certificate programs (4 course, 12 units) in high demand areas of cybersecurity, like privacy, cybersecurity for small-medium sized businesses, transportation cybersecurity, maritime domain cybersecurity, and numerous additional areas of faculty interest, disciplinary expertise, and campus institutional strengths.

Bachelors Level Professional Cybersecurity Certification Programs-

The development of "Stackable Certifications" is a key design feature of our 4 Year Degree Cybersecurity Career Education Pipeline/Pathway. Stackable certificates are flexible small groups of clusters that really add specialization into their degree program. Students can pursue relevant certifications they need in variety of cybersecurity domains. Students take these certifications in conjunction with the program common core requirements. Now the degree program becomes a very specialized degree program individually tailored to meet individual student career interests. This is a very flexible approach to education program development, particularly in an area like cybersecurity with many specializations found within the maturing professional field and nascent academic discipline.

CCCEPPP CYBERSECURITY UPPER DIVISION MODEL CURRICULUM/ACADEMIC STANDARDS DESIGN AND DEVELOPMENT METHODOLOGY/PROCESS:

This section purpose is to describe the methodology and process by which CCCEPPP cybersecurity model curriculum and academic standards were initiated, designed, and developed.

In April 2019—we reached out to computing faculty across the California State University System (over 950+ faculty/admin/staff) for a call to serve on the **California Cybersecurity Four Year Education Workgroup** also to collect/analyze course syllabi for the development of statewide upper division undergraduate model curriculum and academic standards. This Workgroup has meet about every month to six weeks since then.

This preliminary Cybersecurity model curriculum/academic standards was presented at the Silicon Valley Cybersecurity Executive Roundtable Meeting with influential senior cybersecurity industry leaders/professionals to discuss career pipeline/pathway components. **Miki Bellon** (Mikology) and **Jimmy Sanders** (President, SF Bay ISSA) did a fantastic job of organizing/co-facilitating the event at **the Silicon Valley Education Foundation (San Jose**). Subcommittee Colleague **Dr. Markus Geissler** attended and represented the California Community Colleges. The primary purpose of the meeting was to collaborate with the cybersecurity industry and gain feedback on the design and development of our Bachelors of Science Cybersecurity Degree and Dual Baccalaureate Degree Programs.

CCCEPPP Colleagues have brainstormed with SMEs on innovative and transformative new strategies and ways/means to develop education/degree/workforce development programs. We asked the following questions:

- What should the curriculum and academic standards look like?
- How do we include internships/apprenticeships and what are some best practices here?
- What kind (and where) do we include professional development opportunities, labs/projects, clearinghouse for graduates and industry to meet?
- How do we prepare, recruit, retain, support, and graduate students prepared for cybersecurity professional positions?
- How do we prepare, recruit, retain, and promote faculty in the growing area of cybersecurity education/academics?
- Link research opportunities, scholarships and grants, etc.

The methodology to develop the cybersecurity model curriculum and academic standards has been through facilitated discussion and conversations with IT-Cybersecurity Industry leaders and Higher Education Colleagues in a back and forth iterative discussion and curriculum review process. In this Strategy Report, the Model Curriculum and Academic Standards version 8.0 was utilized. Cybersecurity curriculum and standards should be updated annually to make sure it remains crisp, current, and up to speed.

CCCEPPP CURRICULUM RELATED MEETINGS AND PRESENTATIONS:

Cybersecurity career pipeline/pathway model curriculum/academic standards design/ development is a complicated and involved process. This is due in part because we include all levels of education in the CCCEPPP. But also because we work in collaboration with the public sector, Industry, and Non-Government Organizations (NGOs) on cybersecurity design and development. We like to acknowledge and thank the following for their work in organizing, facilitating, and presenting at meetings involving cybersecurity model curriculum and academic standards with key partners and major stakeholders in California Cybersecurity Education and Workforce Development.

1. California Commission on Peace Officer Standards and Training (POST) Cybersecurity Curriculum Meeting (9.6.19): Sacramento, CA

Meeting Organizers/Co-Facilitators:
Phil Caporale, POST
Charles Evans, POST
Greg Kyritsis, POST

2. Cybersecurity Workforce Development and Education Pipeline Roundtable

State of California Cybersecurity Education Summit 2019 (10.9.19): Sheraton Grand, Sacramento, CA

Panel Co-facilitators: Brenda Bridges-Cruz (California Department of Technology), Keith Clement, California State University, Fresno

Education Panelists:
Olivia Herriford, City College of San Francisco
Markus Geissler, California Community College Chancellors Office
John Dolan, University of California, Davis
Teana Fredeen, SynED
Brandon Hardy, Microsoft
Jamie Keledjian, Magnolia High School, Anaheim
Sandra Cano, Los Angeles Unified School District

3. Silicon Valley Cyber Executive Roundtable (12.17.19):
Silicon Valley Education Foundation, San Jose, CA

Meeting Organizers/Co-Facilitators:
Miki Bellon, Mikology
Jimmy Sanders, Netflix DVD (President, SFBay ISSA)
Keith Koo (Guardian Insight, Silicon Valley Insider Radio and Podcast)

4. WASTC Winter ICT Educators Conference Meeting (1.07.20): CISCO HQ
"The Transformation of California Cybersecurity Education and Workforce Development through Career Education Pipeline/Pathway" San Jose, CA

Presented by: Markus Geissler (California Community College Chancellors Office), Richard Valdez (California DAV), Tolgay Kizilema (University of California, Merced), Keith Clement (California State University, Fresno)

5. California Cybersecurity Task Force Workforce Development and Education Subcommittee Workshop. (2.27.20) Lockton. San Diego, CA

Presented by: Keith Clement (California State University, Fresno)

Hosted and Facilitated By: San Diego Cybersecurity Center of Excellence, RADM (RET) Kenneth Slaght CCOE Chair & President

6. "PaCE Cybersecurity Deep Dive May 26, 2020" (5.26.2020) California State University, Professional and Continuing Education (PaCE) Leadership Council Virtual Meeting

Presentation by: Keith Clement (California State University, Fresno)

7. Silicon Valley Cyber Executive Roundtable II (6.8.20): Virtual Meeting

Meeting Organizers/Leads/Co-Facilitators/Presenters/Speakers: Miki Bellon (Mikology), Jimmy Sanders (Netflix DVD, President, SFBay ISSA), Nathan Chung (EY), Jessica Savage (Cisco TV), Keith Koo (Guardian Insight, Silicon Valley Insider Radio and Podcast), Kelly Mackey (Division of Apprenticeship Standards), Keith Clement (California State University, Fresno), Manny Barbara (Silicon Valley Education Foundation), Lakshmi Hanspal (Box), Caroline Wong (Cobalt.io).

Cybersecurity Education Program Facilitation-

Cybersecurity Diversity and Inclusion-

IT-Cybersecurity Pre- and Registered Apprenticeships Panel-

8. California Cybersecurity 4 Year Education Workgroup, Professional Certification Model Curriculum Feedback and Input (6.9.20): June Virtual Meeting.

Meeting Organizer/Lead/Facilitator: Keith Clement (Fresno State University).

9. Silicon Valley Cyber Executive Roundtable III (6.29.20): Virtual Meeting.

Meeting Organizers/Leads/Co-Facilitators/Moderators/Presenters: Miki Bellon (Mikology), Jimmy Sanders (President, SFBay ISSA), Nathan Chung (EY), Jessica Savage (Cisco TV), Keith Koo (Guardian Insight, Silicon Valley Insider Radio and Podcast), Kelly Mackey (Division of Apprenticeship Standards), Keith Clement (California State University, Fresno), Diane Delaney (IBM), John Dunn (California Labor and Workforce Development Agency), Michael Nathan (5G Open Innovation Lab), Shalini Pahwa (IBM Global Business Services/IBM IGNITE ASD inclusivity program, and Porter Wong (New Solar, Inc.).

10. California Cybersecurity 4 Year Education Workgroup, Professional Certification Model Curriculum Feedback and Input II (6.30.20): Virtual Meeting.

Meeting Organizer/Facilitator: Keith Clement (California State University, Fresno).

11. California Cybersecurity Industry Convening (9.2.2020): Virtual Meeting.

Meeting Organizers/Leads/Co-Facilitators/Presenters: Many.

Keynote Speakers:

Mark Ghilarducci, Director, California Governor's Office of Emergency Services- Confirmed

Julie Su, Secretary of the California Labor and Workforce Development- Confirmed

Shamla Naidoo, Chief Information Security Officer, IBM-Global- Confirmed

12. California Cybersecurity Model Curriculum/Academic Standards (9.10.2020): Virtual Meeting.
Meeting Organizer/Lead/Facilitator: Keith Clement (California State University, Fresno)
Meeting Presenters: TBD

Representation from key partners and major stakeholders across the Public Sector, Private Sector, and K-12 Educators/Higher Education colleagues from California Community Colleges, California State University, and University of California to discuss and review CCCEPPP model curriculum and academic standards.

13. The University of California Cyber Security Summit (10.15.2020): Virtual Meeting

"The California Cybersecurity Career Education Pipeline and Pathway Project."

Invited Presentation: Keith Clement (California State University, Fresno)

California Cybersecurity Industry Convening 2020 Draft Invitation

Tech is the engine of a modern economy and society and cybersecurity is an essential and critical workforce. Yet 72,000+ (and growing) private and public sector cybersecurity positions currently exist unfilled in California. To meet and address state current/future/ growing cybersecurity education and workforce development challenges, the California Cybersecurity Taskforce invites your attendance and participation at the **2020 California Cybersecurity Industry Convening Virtual Meeting.**

Industry Convening When/Where: September 2, 2020- Videoconference

Convening Purpose: Link, connect, and network key state-wide IT-Cybersecurity industry employers, educators, and government partners to discuss state-wide education and workforce development strategies and digital innovation initiatives to prepare 50,000 California cyber professionals for entry-level employment (2020-2030) in critical "high demand" industry sectors.

1. Cybersecurity Education program development (degree and stacking professional/ academic certificates) with participating California Community College, California State University, University of California campuses, and Private Colleges/Universities.

2. Cybersecurity Workforce Development through California "Essential Workforce" Pre- and Registered Apprenticeship Program Pipelines supporting pandemic first responder sectors, including Cybersecurity and related Healthcare/Medical, Civil Services (including Public Safety/Service, Emergency Responders), and Small/Medium Sized Business.

Industry Convening Agenda Items Include

- California Cybersecurity Career Education Pipeline and Pathway Project
- California Cybersecurity Model Curriculum and Academic Standards
- State-wide Cybersecurity Industry Training Criteria
- Registered "Essential Workforce" Pre- and Registered Apprenticeship Pipeline
- Linking Employers with apprentices and "On the Job Training" opportunities
- Ensure upward mobility in cybersecurity for all Californians
- Network and socialize with public/private industry colleagues at the "Water Cooler"
- Leading Industry Speakers and Collaboration, IBM Global, and others (TBD)

State of California Cybersecurity Industry Convening Partners

California Government Operations Agency (GovOps)
California Governors Office of Policy and Research (OPR)
California Governor's Office of Business and Development (GoBIZ)
California Governor's Office of Emergency Services (Cal OES)
California Department of Technology (CDT)
California Labor and Workforce Development Agency
California Workforce Development Board (CWDB)
California Department of Industrial Relations, Division of Apprenticeship Standards (DAS)

Cybersecurity Undergraduate Program Strategy (Across All Levels of Talent)

Cybersecurity Upper Division Program Learning Objectives:

1. Critical, creative, and curious thinking.

2. Build an appreciation, culture, and skillset for life-long learning and curious inquiry.

3. Effective communication skills in oral, written, and media.

4. Collaborative and team-work based ethos and approach to problem solving.

5. Support and encourage the success of special populations in IT-cybersecurity; including members of historically disadvantaged groups, and transitioning military to civilians, veterans, disabled veterans, and all spouses.

6. Demonstrate comprehensive understanding of one or more computer programming languages.

7. Demonstrate the importance of professional certifications in cybersecurity and complete one or more industry recognized certification.

8. Act with professional ethics and integrity consistent with the security field.

9. Understand the value of a cybersecurity culminating experience, internship, research project, project management, and service learning experience.

Part 1- California Cybersecurity Model Curriculum and Academic Standards:

In the design/development process with public sector, industry, and education/higher education communities. In terms of Cybersecurity Education Program development and implementation, we are talking about three undergraduate programs in this strategy document. All three programs are designated “High Priority Emerging Cybersecurity Areas” of Workforce Development and Education and demands our full attention in 2020. Top priority. This designation is warranted as the cybersecurity workforce and capability gap rises to critical and exigency related levels across the state and nation. We discuss specific executive-level general information for specified cybersecurity undergraduate level education programs, including program target population, programmatic overview, and miscellaneous program notes. These items are included:

Cybersecurity Course Description-

Cybersecurity Course Student Learning Objectives (SLOs)

Course Knowledge Units (course content aligned with hours of instruction)

Part 2- California Cybersecurity Registered Apprenticeship Program Alignment:

One challenge of cybersecurity education and workforce development is the direct experience requirements found on the job. Two of three strategy cybersecurity education and workforce development programs (the Dual Baccalaureate and Professional Certifications) have a registered apprenticeship component to them.

In document Part 2, we discuss statewide cybersecurity minimum industry standards/requirement development. Their relationship and linkages to the Part 1 Model Curriculum/Academic Standards (above) and National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework documentation found at the following site: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf. These linkages enhance portability and value of cybersecurity education programs, related job skills, and contribute to statewide and national workforce development.

Cybersecurity Statewide Industry Minimum Standards/Requirements

Cybersecurity Apprenticeship Standards and Demonstrable Skill Checklist

NICE Framework Domains organized by Course Knowledge Units and Skill Checklist

Through the registered apprenticeship process, we design and develop the essential "hands-on" skillsets, tools, and experience moving forward into the professional cybersecurity workforce. Apprenticeships go well beyond most traditional volunteer experiences, short-term internship hours, or additional professional experiences like cyber-competitions and cyber boot camps. These are critical components of cybersecurity education and workforce development as well. But, to be perfectly clear—there is little better than a year of on the job training/experience to start a professional career off right. Plus, a solid way to assist learning the art and craft of cybersecurity.

Part 1- California Cybersecurity Model Curriculum and Academic Standards

1. Bachelors of Science (B.S.) in Cybersecurity Degree Program-

Target Population: Top Cybersecurity talent preparation for public and private sector positions. Transitioning military, veterans, disabled veterans and spouses. Students from underserved backgrounds in technology and computing.

Program Overview: 4 Year math and science heavy (STEM/STEAM) B.S. degree program. Preparation for cybersecurity generalists. Solid background preparation into growing variety of related specializations for advanced workforce development. Blending of key Computer Science, Business/IT/IS, Electrical/Computer Engineering (ECE), and Social Science principles related to cyber and information security.

PROGRAM NOTES:

a. Tough major and program. Similar to success in STEM/STEAM and hard math science disciplines. Students must have solid academic preparation, particularly strong science/math and a basic to intermediate technical background. This program would have strong connections to graduate programs in cybersecurity.

b. Timing concerns. Formal approval and offering of these Cyber B.S. Degree Programs are 2-3 years away (Fall 2022 or Fall 2023) due to development time and the lengthy curriculum and academic review at participating local campuses, the CSU Chancellor's Office, and Western Association of Schools and Colleges (WASC). Timing also depends on funding availability. The cyber workforce gap (i.e. 72,000+ available positions) is already tough. Waiting around is counterproductive to the serious exigency unfolding in cybersecurity workforce gaps and shortages and we move forward on this program ASAP.

c. This would be the top echelon of education and workforce development. The B.S. Program has a capstone Cybersecurity Research Project as well. Graduating program candidates start at entry-level positions when transitioning into cyber public sector workplaces with 4 Year degrees (State of California IT-1 job classification) and prepared for a wide range of positions within industry across a variety of economic sectors.

2. Cybersecurity Dual Baccalaureate Degree Program-

Target Population:

Interdisciplinary program for students of all college/university majors. Emphasis on cybersecurity paid apprenticeship opportunities. Transitioning military, veterans, disabled veterans and spouses. Students from underserved backgrounds in technology and computing.

Program Overview:

Industry indicates that 4 year "technical" or STEM degree programs only go so far in assisting them find prepared cyber and information security personnel. While students excel in theory and research, they may not have exposure to current cybersecurity principles, tools, skills, and work experience. Rather, Industry indicated a preference these days to finding prospective cybersecurity job candidates based on a variety of factors outside of 4 Year degree completion rates and otherwise technical degree programs. Instead, industry seeks critical thinkers, security minded types of persons/personalities, superior communicators (oral and written), and ethical collaborative/team members oriented to fit within tech/cyber workplace ecosystems.

The Dual baccalaureate degree program is less technical, interdisciplinary, and attractive to students from across the college/university campus. The program will be added onto existing degree programs of study. Not as deep a dive as the B.S. in Cybersecurity Degree Program (academically speaking.) For example, there are no additional major requirements with a dual baccalaureate degree program as with the B.S. Cyber program. In addition, less science and math as well in a dual baccalaureate degree program. This means we attract a broader and more diverse student group than STEM focused/heavy B.S. degree programs. Students from across campus to be found in interdisciplinary cybersecurity programs like Colleges of Social Sciences, Business, Engineering, Arts and Humanities, Science and Math, Education, and Agriculture.

Students retain their traditional academic discipline/major/degree program, but we add a 6-8 course sequence to serve academic minor, concentration, emphasis, or certificate program depending on local campus interests, policies, and academic programs terms/vernacular. In this way, we provide the education side of cybersecurity fundamentals, skillsets, and preparation for the real-world experiences to follow. There is a good degree of flexibility here as to how we arrange the specifics of the program structure and how to fit in into the university and college master academic plan for the implementation phase.

There is a trade off with the dual baccalaureate degree program for reduced cybersecurity academic coursework. Instead, students complete 2000 Hour OJT Cybersecurity Registered Apprenticeship Program in conjunction with employers statewide (public, private, Non-Government Organizations (NGOs), and non-profits. In this way, students can hone and polish their skills and toolsets from the classroom instruction component of the dual baccalaureate program. (Please see **California Cybersecurity Apprenticeship Initiative** details in this section.)

PROGRAM NOTES:

a. Less academically demanding and rigorous. Instead, focus is on Career Technical Education (CTE) and professional experience through completion of registered cybersecurity apprenticeships utilizing statewide Industry recognized minimum standards.

b. Timing concerns. Formal approval and offering of these Cyber B.S. Degree Programs are 2-3 years away (Fall 2022 or Fall 2023) due to length of time to conduct curriculum and academic review at local campus, CSU, and WASC. Timing also depends on funding availability. The cyber workforce gap (i.e. 72,000+ available positions) is already tough. Waiting around is counterproductive to the serious exigency unfolding in cybersecurity workforce gaps and shortages and we move forward on this program ASAP.

c. Registered Cybersecurity Apprenticeship Program: 20 Hours- Completion of Cybersecurity Apprenticeship Security and Orientation Program + 1980 hours 0JT.

3. Cybersecurity Certificate Programs-

Target Population:

Students from across a college/university campus in an interdisciplinary program emphasizing cybersecurity and interested in paid apprenticeship opportunities. Transitioning military, veterans, disabled veterans and spouses. Students from underserved backgrounds in technology and computing.

Program Overview:

Certificate programs are designed into 6-8 course sequences (18-24 units) depending on the nature, content, and objectives of various "in demand" specializations. Program completion: one academic year (2 semester's equivalency.) Students to complete 2000 Hour "On the Job Training" Cybersecurity Registered Apprenticeship Program in conjunction with employers statewide (public, private, Non-Government Organizations (NGOs), and non-profits. In this way, students can hone and polish their skills and toolsets from the classroom instruction component of the dual baccalaureate program. (Please see **California Cybersecurity Apprenticeship Initiative** details in Part 2 of this document.}

a. Registered Cybersecurity Apprenticeship Program: 20 Hours- Completion of Cybersecurity Apprenticeship Security and Orientation Program + 1980 hours 0JT.

Timing:

First round of professional certification programs target date: Fall 2020-Spring 2021.

CCCEPPP Cybersecurity Certificate Programs fall into two general categories:

I. Professional Cybersecurity Role Certifications- certificate programs to support narrow cyber functions/job classifications that are currently and growing in demand within the current IT ecosystems. We want to assume an absolute minimum of program candidates (i.e. basic skills, minimum pre-requisites, modest technical skillset) and we bring them up to speed over the course of one Academic Year (AY) (i.e. 9 months/or two semesters equivalency) to succeed in the practical apprenticeship opportunity.

1. Intelligence Threat Analyst-
2. Cyber Forensic Investigations-
3. IT Cybersecurity Systems, Architecture, Vulnerability Analysis-
4. Cybersecurity Generalist- directed at **small-medium sized businesses** where the certificate program holder may be the sole security department/personnel on staff at any given time.

II. Professional Cybersecurity for Key Economic Sectors- modular based certificate programs where all sectors receive general units that are followed up by industry specifics and best practices on security related to their specific economic sector. There are about many industry economic sectors, and cyber/information security plays a particularly key role in the following:

Financials/Banking/Insurance-

Advanced Manufacturing-

Critical Infrastructure Protection (CIP)-

Elections Security-

Healthcare/Medical-

Energy-

Transportation-

Defense-

Agriculture and Water-

Tourism and Hospitality-

Part 2- California Cybersecurity Apprenticeship Program Alignment:

Our primary objective here is to collaborate and coordinate with all key stakeholders and major partners statewide to develop cybersecurity education and workforce development programs to reduce and mitigate critical gaps and shortages in this workforce. In Part I, the education program CCCEPPP component was discussed, including standardization of California Cybersecurity "common" model curriculum and academic standards. A variety of cybersecurity degree and certifications are going to have an apprenticeship opportunity to complete as well.

In terms of California economic impact, there are many significant economic benefits to a statewide California Cybersecurity Apprenticeship Program. From the student's perspective, apprenticeship programs are amazing because the program cost (i.e. tuition") is not paid by them; but will come directly and indirectly from other sources. Secondly, both students and employers will benefit from the paid apprenticeship opportunities (a minimum of $16.00 per hour with select cost of living adjustments.) **If 50,000 CCCEPPP participants completed a 2000 hour On Job Training (OJT) component (@$16 p/h) that would translate into $1.2 billion dollars in California economic growth (over 10 years).** Apprenticeships would be a mix of in-person and remote based locations to promote the geographical diversity and inclusivity of these programs.

There is close linkage between cybersecurity education programs (curriculum and academic standards) with registered apprenticeships (minimum industry recognized standards/requirements). The alignment between the two is crucial. In terms of the administration, management, and administration of cybersecurity apprentices statewide, we will utilize **California Cybersecurity Apprenticeship Centers** formed at participating California Community College, California State University, and University of California campuses.

Of additional importance is the liaison and maintenance of strong collaborations amongst all key partners and major stakeholders from the public sector, Industry, and education/higher education communities. So we are in the process of gathering feedback and input from many participants across all interested communities (and is anticipated to be 300-500 contributors and industry representatives by the end of the design/development process.) Many participants whom provided feedback and input recognized in the acknowledgements pages. Participants include representatives from industry, the public/private sectors, and educators/academicians and reflect diverse interests in curriculum/academic standards and minimum industry standard training development and promulgation.

State, Regional, Local, Tribal, Special District Government-

Professional/Trade Associations/Organizations-

Big Employers- Fortune 50, 500

Tech Companies-

Small, Medium, Large Industry across economic sectors-

Cybersecurity Firms-

SECTION XI: CALIFORNIA CYBERSECURITY UPPER DIVISION MODEL CURRICULUM AND ACADEMIC STANDARDS

(VERSION 8.0) Revised 8-2-2020

Cybersecurity Upper Division General Education (G.E.) and Writing Courses-

Like many Science, Technology, Engineering, Arts, Mathematics (STEAM) programs, including those in the College of Business, fitting an entire course of study in under 120 units is a definite challenge. As such, we can rely on some new CSU curriculum and academic standards to boost the efficiency of core cybersecurity curriculum and courses. One way this is done is through the utilization of a key California State University (CSU) academic policy that was effective Fall 2018, CSU General Education Breadth Requirements; Executive Order (EO) 1100. (https://calstate.policystat.com/policy/6741976/latest/, Accessed 12/22/2019.)

CSU Executive Order 1100 allows the practice of "double counting" of Upper Division General Education and Writing Courses within a major. We add a few extra courses to an otherwise constrained STEM based undergraduate major program (limited by a 120 unit maximum credit for graduation requirement.) STEAM programs often struggle with the 120-unit limit and prefer program unit counts set higher (i.e. the 123-125 unit range.)

Upper Division General Education (GE) Course-

***Human Factors and Psychology of Cybersecurity*- (3.0 units)- UDGE Area D**

COURSE BUILDOUT- Public Sector, Industry, Higher Education

Catalog Description: Understand human factors, motivations, and psychology driving good and bad actors in the cyber space. Role and impact of social engineering on offensive and defensive cybersecurity practices. Analyze risk aversion and other key psychological and behavioral traits.

Student Learning Outcomes:
By the end of this course, students will be able to:
1. Identify and describe various motivations of cyber bad actors.

2. Demonstrate the effectiveness of social engineering attacks.

3. Compare and contrast UI/UX.

4. Develop and test theories related to bad actor human factors.

5. Apply cyber risk mitigation and risk aversion activities for individual.

Area E (G.E.) Learning Outcomes (Sample below; determined by local campuses):

1. Develop intellectual, practical, and/or physical skills and abilities that will serve them throughout their lives.

2. Apply their learning to other pursuits within and outside of the classroom.

3. Demonstrate the capacity to make informed and ethical decisions.

Upper Division Writing "W" Course

Business Communication and Writing in Cybersecurity (3 units)

COURSE BUILDOUT- Public Sector, Industry, Higher Education

Catalog Description: Application and demonstration of effective business communication and writing in the field of cybersecurity.

Student Learning Outcomes
By the end of this course, students will be able to:
1.

2. Prepare professional e-mail, business letters.

3.

4.

5.

COURSE BUILDOUT TIMEFRAME- SPRING 2021

Cybersecurity Bachelor of Science Degree Program Model Curriculum (Upper Division Component): version 8.0

Lower Division- 12 units major (Computer Science-AST and Information Technology-MC programs (described in Associate-level section from above).

Upper Division Core- (9 courses- 25 units)

Professionalism in Cybersecurity- (1 units)
Learning the Art of Cybersecurity- (3 units)
Human Factors and Psychology of Cybersecurity- (3 units) *** double count UDGE
Introduction to Cybersecurity- (3 units)
Technical Principles of Cybersecurity- (3 units)
Network Security- (Foundations similar to Network+)- (3 units) ***course substitution for major requirement if student achieved Network+/ or closely related professional certification
Computer Security- (Topics similar to Security+)- (3 units) ***course substitution for major requirement if student achieved Network+/ or closely related professional certification
Cybersecurity Risk Management- (3 units)
CAPSTONE COURSE: Cybersecurity Senior Capstone Project/Management (3 units)
Total: 25 units-3 units double counted = total 22 units core major requirements

Upper Division Major Requirements- (8 Courses: 24 units)

Introduction to Computer Science- (3 units)
Computer Programming Language- (3 units)
Cybersecurity Policy, Privacy, and Legal Context- (3 units)
Business Communication and Writing in Cybersecurity- Upper Division Writing "W" Course- (3 units) *** double count UD Writing Requirement/Major
Information Technology Infrastructure, Vulnerability, and Security- (3 units)

Select 3 courses- (9.0 units minimum) from below:
Securing Platforms and OS Operations: Windows, Linux, Unix LAB Class- (Practice Oriented)- (3 units)
Digital Forensics, Cybercrime, and Incident Response- (3 unit lecture/1 unit lab, 4 total)
Cybersecurity Risk and Ethical Hacking (linked with next course)- (3 units)
Information Security and Assurance [related to previous course]- (3 units)
Cloud Computing Architecture, Security, and Design- (3 units)
Pen testing- (3 units)-
Digital Logic (3 units)-
Programming and Cybersecurity (3 units)-
Total: 24 units-3 units double counted = total 21 units major requirements

Upper Division Electives- (6 units minimum)

Cryptography- (3 units)
Cyber Intelligence and Analytics- (3 units)

Internet-of-Things Security (updates, loopholes, password)- (3 units)
Introduction to Wireless and Mobile Security- (3 units)
Smart Device Security- (3 units)
Secure Software Development/Software Security (Analysis and development of secure software and protocols)- (including design and SSDLC, malware and vulnerabilities analysis) (3 units)
Vulnerability Analysis (3 units lecture, 1 unit lab, 4 units total)
Cybersecurity Operations (SecOps)/ Application Security and Secure Development (DevOps) (Hands On course)
Fundamentals of Machine Learning (ML)

Cybersecurity B.S. Degree Program Unit Count:

Upper Division Core- 25 units, 3 units double counted- 22 units total

Upper Division Major Requirements- 24 units, 3 units double counted- 21 units total

Upper Division Electives- 6 units

Program- 55 units
Major-W/UDGE Courses- (-6 units) double counted in major= 49 UNITS

Dual Baccalaureate Cybersecurity Degree Program (Upper Division):

Version 8.0

Project Deliverable #4: Dual Baccalaureate Cybersecurity Degree Program (4-year degree program linked with 2000 hour Apprenticeship (on job training) at CCC/CSU/UC Campus Cybersecurity Apprenticeship Centers:

SCOPE OF WORK: One key aspect of career pipelines is the linkage with application, experience, and real world application for a prepared and qualified cybersecurity workforce. Cybersecurity is often a technical field. It relies on the application of learning, knowledge, and skills to complex problem solving. One CCCEPPP objective is an operational statewide Baccalaureate Cybersecurity Degree Program. The Dual Baccalaureate Degree Program includes a Registered Apprenticeship (2000 hour "On the Job Requirement" (OJT) and 145 minimum hours of classroom/instruction time). To cover the 145 hour instructional element of the apprenticeship, we develop a 12 unit (4 course sequence) Cybersecurity Apprenticeship Certification Program for necessary competencies, skills, tools, and orientation for success in the placement.

A cybersecurity career pipeline/pathway must include tight connections with experiential (applied) learning opportunities outside of the classroom. We utilize Cybersecurity Apprenticeship Centers located at participating CCC/CSU/UC campuses (these cost components are discussed in further detail later in this funding proposal). One way to support student's professional development efforts and encourage participation in cybersecurity education is through apprenticeship programs and local/regional industry partnerships. Skills and experience gained will significantly enhance student cybersecurity classroom/academic learning. Cybersecurity is a hands on, skill based set, and does not rely solely on theoretical or "book" knowledge.

Professional Development Component: Mentoring, Career Awareness/Preparation, job shadowing, research presentations, soft skills (like oral and written communication, team player, and orientation for success at the apprenticeship placement.)

MILESTONES, TIMELINES: 2020-2021 ACADEMIC YEAR ACTIVITY:

Dual Baccalaureate Degree Program Curriculum:

Professionalism in Cybersecurity- (1 units)
Learning the Art of Cybersecurity- (3 units)
Human Factors and Psychology of Cybersecurity- (3 units) *** double count UDGE
Introduction to Cybersecurity (3 units)
Technical Principles of Cybersecurity- (3 units)
Cybersecurity Risk Management- (3 units)

Professional Industry Certification (Basic or Intermediate certificate/exam) (3 units)

19 Upper Division Units- Dual Baccalaureate Program

-3 units double count= 16 units program total

ADDITIONAL DUAL BACCALAUREATE CYBERSECURITY DEGREE PROGRAM NOTES:

What exactly is a cybersecurity dual baccalaureate degree program? These programs combine education program with the workforce development component of registered apprenticeship on the job training. There are a variety of advantages to this type of education program/workforce development opportunity. It is an interdisciplinary degree intended to be taken with other colleges' majors across the campus. This dual baccalaureate degree program fits with many majors with the kinds of skills and backgrounds that industry and employers frequently seek. For example, critical thinking of superior oral/written communicated based majors could utilize the cybersecurity fundamentals and technical background to serve as the classroom instruction component in preparation for 2000 hour OJT (One year equivalent work experience). Upon completion of a four year degree (including a cybersecurity major) with a minimum of 1 year work experience and 1 industry certification under their belt would make a solid pool of prospective entry level cyber professionals for the public and private sectors.

- Registered Apprentices need 145 hours of classroom instruction in preparation for the apprenticeship On the Job Training Hours (2000).

- Additional Requirement: Completion of "Success in Cybersecurity Apprenticeship Orientation"- 20 hours dedicated OJT to understanding the workplace and tips on how to succeed from professionals in the field of cybersecurity.

- Additional Requirement: 2000 hours On the Job Training administered at participating California Community College, California State University and University of California campuses.

Cybersecurity Bachelors of Science Degree Program Upper Division Courses

We are interested in discussing Cybersecurity undergraduate programs and courses in this section. Please see the following draft list of proposed upper division courses currently planned for the Cybersecurity B.S. Degree Program. The following set of criteria is the outline for the Dual Baccalaureate Degree Program curriculum and academic standards. **CCTF WDE Subcommittee's 4 Year Cybersecurity Education Workgroup** and many participants have been working on the B.S. in Cybersecurity and assisted in the development of the following upper division Core, Major Requirements, and Electives.

UNDERGRADUATE CYBERSECURITY DEGREE PROGRAM #1

Bachelors of Science Cybersecurity Degree Completion Program: Upper Division Course Sequence Model Curriculum

CORE UPPER DIVISION CYBERSECURITY COURSES:

1. Professionalism in Cybersecurity- (1.0 unit)

Catalog Description: Introductory survey course on the academic discipline and professional field of cybersecurity/information technology security. Discuss various specializations/ functional domains, technical, human elements, management/policy, privacy, and cyber ethics. Modeling simulations. Guidance on professional cyber preparation, field experience, discussion of roadmaps to careers, specializations, certifications, and apprenticeship work in this area.

COURSE BUILDOUT- Public Sector, Industry, Higher Education

Student Learning Objectives/Outcomes:
By the end of this course, students will be able to:
1. Define and explain cybersecurity.

2. Identify and describe cybersecurity specializations and functional domains.

3. Define and explain the NIST/NICE Framework (s) and 31 NIST Specialty Areas.

4. Identify and describe basic cybersecurity technical terms and concepts.

5. Discuss the human element of cybersecurity.

6. Demonstrate ethical cyber and digital ethics.

7. Analyze and evaluate the role of management and policy in cybersecurity.

8. Promulgate the concept of trust and understand its ramifications and consequences.

9. Student self-assessment of professional field preparation work and requirements.

10. Evaluate and analyze the importance of professional cybersecurity certifications and their familiarity (basic, intermediate, and advanced).

11. Prepare students for professional experience opportunities like apprenticeships, internships, and digital community service.

2. Learning the Art of Cybersecurity- (3.0 units)

Catalog Description: Interdisciplinary approach to enhancing student cybersecurity learning. Cybersecurity environment, threats, and vulnerabilities change daily. Effective learning strategies, emphasis on critical thinking, and understand risks when troubleshooting/remediating security issues. Course emphases teaching students strategies on "how to learn" the art and craft of cybersecurity by becoming continuous and effective life-long learners. Course topics include, gamification, information literacy, and strategies for learning cybersecurity as an art, craft, and science.

COURSE BUILDOUT- Industry Request: Higher Education

Student Learning Objectives/Outcomes:
By the end of the course, students will be able to:
1. Demonstrate gamification skills through completion of student course learning outcomes and digital badges for successful completion of key skills and course.

2. Describe and explain "how to think like a cyber/data thief."

3. Identify, map patterns, and "anti-patterns" in terms of normal/anomalies.

4. Demonstrate troubleshooting skills, like the identification of compensatory measures and controls including risk assessment and management.

5. Application of cyber logic in development of "plan B" contingencies in digital table-tops and simulations.

6. Teach students through the gamification process the power of risk and risk-taking as potential solutions for problems.

7. Utilize and harness curiosity and non-traditional ways of learning and critical thinking.

8. Design and evaluate a framework of ethical thinking and behavior in the cyber environment.

9. Demonstrate Information Literacy skills and find relevant educational resources in the solution of security problems.

3. Human Factors and Psychology of Cybersecurity- (3.0 units)

{Preparation Note: Course intended as upper division G.E. Course- will double count within the major to free up 3.0 units for utilization elsewhere in the program).

COURSE BUILDOUT- Public Sector, Industry, Higher Education

Catalog Description:

Student Learning Objectives/Outcomes:
By the end of the course, students will be able to:
1.

2.

3.

4.

5.

COURSE BUILDOUT TIMEFRAME- FALL 2020

4. Introduction to Cybersecurity (3.0 units)

{Preparation Note: Utilize similar existing upper division Introduction to Cybersecurity courses currently available on university campuses today).

COURSE BUILDOUT- Public Sector, Industry, Higher Education

Catalog Description:

Student Learning Objectives/Outcomes:
By the end of the course, students will be able to:
1.

2.

3.

4.

5.

COURSE BUILDOUT TIMEFRAME- FALL 2020

5. Technical Principles of Cybersecurity- (3.0 units)

COURSE BUILDOUT- Public Sector, Industry, Higher Education

Catalog Description: Provides key cybersecurity technical and operational principles, scope and vulnerabilities of Cyberspace, the problem of identity, privacy, malicious software, data security, cryptography, authentication in distributed systems, e-mail security, network security, wireless security, offensive security. Programming assignments and review of literature.

Student Learning Objectives/Outcomes:
Upon completion of this course, the student will be able to:
1. Apply Cyber security requirements to security applications.

2. Utilize security applications and tools to creatively solve security problems.

3. Recognize and distinguish the mechanisms, components and architecture of cyber security systems.

4. Analyze Cyber security problems, and identify and define the resources and requirements needed for its solution.

5. Demonstrate communication skills in both written and oral form, and work in a team environment and Independently/collaboratively acquire new Cyber security skills through analysis of current literature and industrial practices.

6. Network Security (Foundations similar to Network+)- (3.0 units)
[Note: ***course substitution for major requirement if student achieved CompTIA Network+/ or closely related professional certification]

Catalog Description: Fundamentals of network and computer security. Security services and mechanisms, models, cryptography, network and wireless security, digital forensics, security threats and vulnerabilities, risk analysis and management models, security attacks and policies, and legal and regulatory issues. Programming projects. Practical hacking and defense techniques.

STUDENT LEARNING OUTCOMES
By the end of the course, students will be able to:
1. Describe key network security requirements

2. Present main concepts of symmetric cryptography (DES, AES algorithms)

3. Present main concepts of a symmetric cryptography (RSA, Diffe-Hellman, ECC)

4. Present an overview of basic structure/usage of cryptographic hash functions (SHA-1, MD5)

5. Present an overview of techniques for remote user authentication using symmetric encryptions (Kerberos)

6. Describe Web security threats and security approaches

7. Present an overview of Secure Socket Layer (SSL/TLS)

8. Present an overview of the operation of PGP (Pretty Good Privacy)

9. Understand the functionality of S/MIME and security threats it addresses

10. Present an overview of IP security (IPsec)

11. Present an overview of Firewalls, Viruses and Intrusion Detection Systems

12. Practice different Hacking Techniques

13. Apply critical thinking and problem solving skills by analyzing security problems, designing solutions, and evaluating results.

14. Demonstrate communication skills in both written and oral form, and work in a team environment. (WIKI, EP and Discussion group activities)

15. Independently and collaboratively acquire new network sec security skills through analysis of current computer science literature and industrial practices. (EP)

7. Computer Security- (Topics similar to Security+)- (3.0 units)

[Note: ***course substitution for major requirement if student achieved CompTIA Security+/ or closely related professional certification]

Catalog Description: Examination of practical computer security concepts in everyday life. Covering the principles, technologies and tools used to secure the Internet and keep ourselves 'digitally' secure, including: privacy and anonymity, web and data security, cryptography, malware, authentication and access control. This course will also introduce basic programming concepts in Python to demonstrate hands-on applications of computer security.

Student Learning Objectives:
By the end of the course, students will be able to:

1. Demonstrate a general knowledge of, and be able to differentiate between, core computer security principles.
2. Approach claims of security with an informed sense of skepticism, as well as develop an ability to intelligently critique those claims.

3. Recognize that information we store digitally can have real value, but can also be valued differently, warranting different protections.
4. When considering the value of digital assets, identify the common and emerging threats to those assets, and identify the appropriate techniques for protecting those assets.
5. Gain confidence, develop good intuitions, and integrate into their own lives the best practices and behaviors to keep secure in daily life.
6. Establish, in addition to computational thinking skills, an ability to think "counterfactually" and "adversarial" about systems, allowing students to protect these systems against adversaries thinking about them in the same way.
7. Be provided with the core programming and problem solving skills to be successful in basic computer security.

8. Cybersecurity Risk Management- (3.0 units)

Catalog Description: Covers fundamentals of cybersecurity primarily focusing on its technical (and some managerial) aspects. There is large industry demand for seasoned cybersecurity skills and it is definitely a perfect time to consider it as a life-long career path. Cybersecurity itself is a very large knowledge domain and a successful career demands understanding in computer networking and programming. In this course, a comprehensive overview is offered on a large array of technical concepts. To realize learning outcomes, this course relies on various pedagogical approaches: reading assignments, classroom lectures, classroom hands-on exercises, and individual and/or group assignments. Special focus placed on technical experience via hands-on exercises.

COURSE OBJECTIVES/LEARNING OUTCOMES:
By the end of the course, students should achieve the following:
1. Possess general knowledge of threats, vulnerabilities, and their remediation approaches.

2. Understand issues and methods of host, application, data, and network security.

3. Describe various cryptography technologies.

4. Explain various access control and identity management methods.

5. Discuss elements of risk mitigation, compliance, and auditing.

6. Become familiar with various security tools to analyze data, and control network and system threats and vulnerabilities.

7. Be familiar with the creation and usage of virtual machines.

8. Demonstrate competency with tabletop and simulation exercises.

9. Demonstrate "best practices" of business continuity and resilience.

9. Cybersecurity Senior Capstone Project/Management (3.0 units)

[Designer Notes: Capstone Course Requirement will be a choice among Cybersecurity

Internships, Cybersecurity Undergraduate Research Project, Cybersecurity Service Learning

/Community Project)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Catalog Description- Students will design and complete all facets of a senior project within the broad field of cybersecurity. The project must be done in conjunction with an external partner; including public sector, private sector, Non-Government Organization (NGO), and Not for Profit Organization related to the broadly defined field of cybersecurity and various specializations.

Student Learning Objectives/Outcomes:
By the end of the course, students will be able to do:
1.
2.
3.
4.
5.
6.
7.

COURSE BUILDOUT TIMEFRAME- FALL 2020

UPPER DIVISION CYBERSECURITY MAJOR REQUIREMENTS:

1. Cybersecurity Policy, Privacy, and Legal Context- (3.0 units)

Catalog Description: Cybersecurity has a profound impact on governance, policy, regulation, and compliance. This course analyses the role of policy and development in cybersecurity, including the protection of privacy and data, many faceted legal context of laws/regulations, and ongoing issues related to compliance in this increasingly bureaucratized and legislated area of IT and security.

Student Learning Objectives/Outcomes:

1. Describe and explain policy design, development, implementation, and evaluation processes of national and state cybersecurity statutes, laws, and requirements.

2. ADD Cybersecurity Regulations, Auditing, and Compliance.

3. Describe and discuss the importance of CISO Top 20 Controls.

4. Identify and explain privacy.

5. Identify types of data and describe data protection.

6. Analyze and evaluate current privacy legislation, regulation, and legal protection.

7. Define and synthesize a legal framework for analysis of cybersecurity issues.

8. Relate course learning outcomes to the development of a cyber-ethical framework (illustrate right versus wrong in cyber ethos).

9. Inform ethical individual and organizational decision-making practices.

2. Business Communication and Writing in Cybersecurity- Upper Division Writing "W" Course- (3.0 units)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Student Learning Outcomes/Objectives:
By the end of this course, students will be able to:
1.

2.

3.

4.

5.

COURSE BUILDOUT TIMEFRAME- SPRING 2021

3. Information Technology Infrastructure, Vulnerability, and Security- (3 units)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Catalog Description:

Student Learning Objectives/Outcomes:
By the end of this course, students will be able to:
1.

2.

3.

4.

5.

6.

COURSE BUILDOUT TIMEFRAME- SPRING 2021

4. Securing Platforms and OS Operations: Windows, Linux, Unix LAB Class- (Practice Oriented)- (3 units)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Course Description:

Student Learning Outcomes:

By the end of this course, students will be able to:
1.

2.

3.

4.

5. OS Based Malware and Forensic Analysis.

COURSE BUILDOUT TIMEFRAME- SPRING 2021

5. Digital Forensics, Cybercrime, and Incident Response- (3 unit lecture/1 unit lab, 4 total)

Catalog Description: Investigative techniques, evidence handling procedures, forensics tools, digital crime reconstruction, incident response, ethics, and legal guidelines within the context of digital information and computer compromises. Hands-on case studies cover a range of hardware and software platforms and teach students how to gather evidence, analyze evidence, and reconstruct incidents. **Prerequisite: None, but equivalent experience in the Unix/Linux command-line environment is strongly recommended.**

Prerequisites by Topic
Experience in the Unix/Linux command-line environment strongly recommended.
Knowledge of how to install, configure, use, and troubleshoot Windows and/or Unix/Linux useful.

Student Learning Outcomes
This course covers the following ACM/IEEE CS2013 (Computer Science) Body of Knowledge student learning outcomes:

CS-IAS/Digital Forensics
CS-IAS/Security Policy and Governance
CS-OS/Security and Protection
CS-SP/Professional Ethics
CS-SP/Security Policies, Laws and Computer Crimes

ABET Outcome Coverage
The course maps to the following performance indicators for Computer Science (CAC/ABET):
3e. An understanding of professional, ethical, legal, security, and social issues and responsibilities.
3i. An ability to use the current techniques, skills, and tools necessary for computing practice.

6. Cybersecurity Risk and Ethical Hacking- (linked with next course) (3 units)

Catalog Description: This course is an introduction to risk management with modern ethical hacking as a technique for penetration testing, finding security vulnerabilities, incident handling, and system's security audit processes. Areas of instruction include evolution of ethical hacking; penetration testing for risk assessment; the basics of cryptology for information security; foot printing; vulnerability scanning and exploit; wireless, web, and database attacks; malware and system exploit; traffic analysis; incident response; and defensive technologies and internal controls. In this course, students will learn how to discover vulnerabilities and types of security attacks, how to defend systems, how to respond to attacks, and how to identify and design controls to prevent future attacks. The assigned homework is a practice component of the course. It is designed to re-enforce understanding of Information Security risk management concepts and knowledge using ethical hacking tools and techniques.

Major Instructional Areas

1. Evolution of computer hacking threats and risks
2. The role of information security professionals
3. Ethical hacking tools and techniques affecting internal controls
4. Risk vulnerabilities and threats exploited by hackers
5. Incident response and continuity and disaster recovery planning
6. Controls and defensive technologies

Additional risk specific topics:

- The Role of the Law and Ethical Standards (see Ch. 1)
- Risk assessment (see Ch. 9 and other chapters)
- The Role of Business Continuity Plans and Planning for Disaster and Recovery) (see Ch. 14)
- The Role of Controls (see Ch. 15)
- Operations security and security program development are discussed in view of potential vulnerabilities and attacks.

Course Learning Objectives:

1. Explain the history and current state of ethical hacking and penetration testing, including ethical and legal implications.
2. Describe fundamental TCP/IP concepts and technologies related to networking.
3. Describe cryptology.
4. Identify common information-gathering tools and techniques.
5. Identify system ethical hacking, and web and database attacks.
6. Analyze vulnerabilities exploited by hackers and the resulting risks.
7. Identify common types of malware and the threats they pose.
8. Describe network traffic analysis and sniffing by using appropriate tools.
9. Describe incident handling, continuity and disaster recovery planning by using appropriate methods.
10. Identify security controls and defensive technologies.

7. Information Security and Assurance [related to previous course]- (3 units)

Catalog Description: Broad coverage of theoretical, conceptual, methodological, and practical foundations of information security and assurance in selected domains within the Common Body of Knowledge (CBK) developed by the International Information Systems Security Certification Consortium (ISC2) (see https://www.isc2.org/) for Certified Information Systems Security Professionals (CISSP) such as: access control, asset security, security engineering issues, use of cryptography, communications and network security, identity management, application security.

Homework designed to reinforce and assess understanding of Information Security management concepts and knowledge. This course is paired with and a continuation of **previous Security Risk [Management and Ethical Hacking Course**.]

Course Learning Objectives:

1) Apply theoretical ideas in information security to real world situations.

2) Understand the role of policy development in mitigating risks.

3) Demonstrate a broad-based understanding of security essentials such as Network Security Fundamentals, Cryptography, Security Models, Access Control, Architectural Approaches to Defense in Depth, Cyber Attacks, Vulnerability Assessment and Management.

8. Cloud Computing Architecture, Security, and Design- (3 units)

Catalog Description: Course provides ground-up coverage on high level concepts of cloud landscape, architectural principles, techniques, design patterns and best practices applied to Cloud service providers/consumers/ and delivering secure Cloud based services. Cloud security architecture and guiding security design principles, design patterns, industry standards, applied technologies and addressing regulatory compliance requirements critical to design, implement, deliver and manage secure cloud based services. Delves into secure cloud architectural aspects of identifying and mitigating risks, protection and isolation of physical & logical infrastructures including compute, network and storage, comprehensive data protection at all OSI layers, end-to-end identity management & access control, monitoring and auditing processes and meeting compliance with industry and regulatory mandates. Leverages cloud computing security guidelines set forth by ISO, NIST, ENISA and Cloud Security Alliance (CSA).

Student Learning Objectives/Outcomes:
By the end of the course, students will be able to:
1. Understand fundamentals of cloud computing architectures based on standards, protocols, and best practices for delivering Cloud based enterprise IT services/business applications.

2. Identify known threats, risks, vulnerabilities and privacy issues with Cloud based IT services.

3. Understand concepts and guiding principles for designing/implementing appropriate Safeguards/countermeasures for Cloud based IT services

4. Design cloud services to meet essential Cloud infrastructure characteristics – on demand computing, shared resources, elasticity, and measuring usage.

5. Design security architectures to assure secure isolation of physical and logical infrastructures; including compute, network and storage, comprehensive data protection at all layers, end-to-end identity/access management, monitoring/auditing processes, and compliance with industry and regulatory mandates.

6. Understand industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.
Syllabus Source: CSCI-E49-CloudSecurity-Syllabus-RameshNagappan (Accessed 12/12/19)

UPPER DIVISION CYBERSECURITY ELECTIVE/SPECIALIZATION COURSES:

1. Cryptography- (3.0 units)

Catalog description: Traditional ciphers; background of number theory and finite fields; symmetric key cryptography (block ciphers, stream ciphers, message authentication codes); asymmetric key cryptography (RSA, ElGamal, digital signature, Diffie-Hellman key exchange); cryptanalysis; security protocols (IPsec and TLS/SSL); other related topics. Encryption and blockchain. Students who are looking to specialize in the field of cryptography and computer network security are encouraged to consider this elective course.
Prerequisites: Knowledge of Programming Languages

Student Learning Outcomes:

By the end of the semester, students will be able to:

1. Cryptographic theory with applications to data security.

2. Classical Encryption techniques such as Substitution, Transposition Techniques, Steganography, Block ciphers and DES, AES, Triple DES, Blowfish, RC5, RC4.

3. Confidentiality with Symmetric Encryption.

4. Publickey Encryption and Hash Functions: RSA, Diffe-Hellman Key exchange, Elliptic Curve Cryptography, Message authentication, MD5, SHA, RIPEM-160, HMAC.

5. Digital Signatures and authentication Protocols.

2. *Cyber Intelligence and Analytics*- (3.0 units)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Course Description:

Student Learning Objectives:

1.

2.

3.

4.

5.

COURSE BUILDOUT TIMEFRAME- SPRING 2021

3. *Internet-of-Things Security*- (3.0 units)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Catalog Description: This course covers security topics related to both home and industry IoT devices. Areas of instruction include risks, vulnerabilities, privacy concerns and best practices to harden home and industry IoT devices. Students will have a hands-on learning opportunity to create their own smart home device and then analyze that device's network traffic. Next, students will work with a home router to create a simple intrusion detection system based on the network traffic of their smart home device.

Student Learning Objectives:

By the end of the term, students will be able to:

1. Describe the architecture and ecology of the Internet of Things

2. Describe the concept of a smart home

3. Describe the risks associated with the insecure use of a smart home devices

4. Describe the impact of home network vulnerabilities

5. Recognize the need for smart home device privacy

6. Explain best practices for hardening smart home devices

7. Differentiate and analyze some typical attacks against industry IoT

8. Demonstrate techniques for testing and analyzing the security of industry IoT devices

9. Translate the cybersecurity principles of confidentiality, availability, and integrity in the IoT environment

10. Have a good working understanding of the current industry IoT best practices

11. Discuss the impact of standardization of industry and smart home IoT devices

12. Analyze the threat of IoT botnets

13. Create a simple smart home device

14. Identify smart home device traffic

15. Program a simple intrusion detection system on a home router

4. *Introduction to Wireless and Mobile Security*- (3.0 units)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Catalog Description: Comprehensive topics in Wireless, Mobile, Grid and Pervasive computing, including IEEE 802.11 Wireless security, Security in Mobile Telecom Networks (CDMA200, UMTS (3GPP)), MANETs, VANETs , WSNs, Bluetooth, VoIP, Grid, Cloud and Mobile Agents Security. Practical hacking and defense techniques in wireless environments.

Student Learning Objectives:
By the end of the term, students will be able to:
1. Describe key Wireless Network security requirements
2. Analyze IEEE 802.11i Security protocols (WEP, TKIP, CCMP and Key Management)
3. Understand security requirements of MANETS
4. Analyze Secure Routing Protocols in MANETS (ARAN, ARIADNE etc)
5. Analyze Secure Data Forwarding Protocols in MANETS (Hommorphic Encryptions and Threshold Cryptography)
6. Understand security requirements of WSN
7. Analyze Security protocols in WSN (SNEP, TINY SEC, TESLA)
8. Understand security requirements of CLOUD Computing
9. Analyze Security protocols in CLOUD Computing
10. Understand security requirements of UMTS & CDMA 2000
11. Analyze Security architecture of UMTS & CDMA 2000
12. Understand security requirements of VANETS
13. Analyze Security architecture of VANETS
14. Understand security requirements of VoIP
15. Analyze Security architecture of VoIP
16. Understand security requirements of Mobile Agents
17. Analyze Security architecture of Mobile Agents
18. Practice Different Wireless Hacking Techniques
19. Apply critical thinking and problem solving skills by analyzing security problems, designing solutions, and evaluating results.
20. Demonstrate communication skills in both written and oral form, and work in a team environment.(WIKI, EP and Discussion group activities)
21. Independently and collaboratively acquire new network sec security skills through analysis of current computer science literature and industrial practices. (EP)

5. *Smart Device Security*- (3.0 units)

Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Catalog Description: Presents the concepts and techniques associated with designing, developing, and testing secure smart devices, such as smartphones, smartwatches, and implantable medical devices. Smart devices usually have limited computing resources but may send data to cloud computing data centers. Topics include preventing hackers from stealing our password by measuring them physically from our devices, selecting appropriate encryption algorithms for resource-constraint devices, and understanding the limit in protecting your secret data during wireless network transmission. Particular attention focuses on the study of hardware security in smart embedded systems.

Student Learning Objectives/Outcomes:

1. Know the security considerations of a smart device.

2 Understand the differences between a general purpose computer and an embedded computer.

3. Understand security vulnerabilities in a smart computing device.

4. Understand the countermeasures of most typical attacks.

Course Outcomes

By the end of the term, students shall be able to:

1. Select and deploy an appropriate cipher for an edge computing device under given scenarios.

2. Analyze secrecy capacity in wireless channels.

3. Carry out differential power analysis to decipher secret keys.

4. Integrate randomness from the device environment for security.

5. Model basic physical unclonable function units.

6. Secure Software Development/Software Security (Analysis and development of secure software and protocols)- (including design and SSDLC, malware and vulnerabilities analysis)

Course Title: *Vulnerability Analysis* (3 units lecture, 1 unit lab, 4 units total)

Catalog Description: Identification and quantification of security weaknesses, primarily in source code and executables. Topics include professional ethics, source code auditing, common source code errors, the runtime stack and memory systems, common attacks against executables, risk assessment, vulnerability classification, static binary analysis, and mitigation techniques.

Prerequisites: Knowledge of an assembly language (Intel, MIPS, etc.)
Knowledge of the runtime stack and basic memory layout
Knowledge of programming languages in the C/C++ family
Knowledge of formal computer language grammar
Basic understanding of computer language translation from source code to binary

Student Learning Outcomes
This course covers the following ACM/IEEE CS2013 (Computer Science) Body of Knowledge student learning outcomes:

CS-IAS/Foundational Concepts in Security
CS-IAS/Principles of Secure Design
CS-IAS/Defensive Programming
CS-IAS/Threats and Attacks
CS-PL/Static Analysis
CS-SE/Software Construction

ABET Outcome Coverage
The course maps to the following performance indicators for Computer Science (CAC/ABET):
4. An ability to recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

Professional ethics and legal issues are integrated into this course and students will complete at least one homework assignment related to this topic.

6 [CS]. An ability to apply computer science theory and software development fundamentals to produce computing-based solutions.

Homework and laboratory assignments investigate how vulnerabilities in source code can arise from common mistakes, lack of understanding about the details of the high-level language, valuing optimization over security, and other causes. Through this intensive investigation, students will gain the awareness and skills to produce more secure code.

7. Cybersecurity Operations (SecOps)/ Application Security and Secure Development (DevOps) (Hands On course)
Syllabus/Source: GOVT INDUSTRY/EDUCATION COLLABORATION BUILD

Catalog Description:

Student Learning Objectives/Outcomes:

1.

2.

3.

4.

5.

COURSE BUILDOUT TIMEFRAME- SPRING 2021

8. Fundamentals of Machine Learning (ML)

Catalog Description: Machine learning uses interdisciplinary techniques such as statistics, linear algebra, optimization, and computer science to create automated systems that can sift through large volumes of data at high speed to make predictions or decisions without human intervention. Machine learning as a field is now incredibly pervasive, with applications spanning from business intelligence to homeland security, from analyzing biochemical interactions to structural monitoring of aging bridges, and from emissions to astrophysics, etc. This class will familiarize students with a broad cross-section of models and algorithms for machine learning, and prepare students for research or industry application of machine learning techniques. Simulation of machine learning algorithms with either Python or Matlab will be experimented.

Course Description: Linear regression, SSR, gradient descent, overfitting and complexity, training, validation, test data classification problems, decision boundaries, nearest neighbor methods, probability and classification, Bayes optimal decisions, linear classifiers, neural networks, decision tree, ensemble methods, clustering, supervised and unsupervised learning, PCA, SVM.

Course Topics:
• Class overview: Class organization, topics overview, software etc.
• Introduction: what is ML; Problems, data, and tools; Visualization; Matlab
• Linear regression; Sum of Squares Regression (SSR)
• Gradient descent; closed form; normal equations; features
• Overfitting and complexity; training, validation, test data, and introduction to Phyton
• Classification problems; decision boundaries; nearest neighbor methods
• Probability and classification, Bayes optimal decisions
• Naive Bayes and Gaussian class-conditional distribution
• Linear classifiers
• Bayes' Rule and Naive Bayes Model
• Logistic regression, online gradient descent, Neural Networks
• Decision tree
• Ensemble methods: Bagging, random forests, boosting
• A more detailed discussion on Decision Tree and Boosting
• Unsupervised learning: clustering, k-means, hierarchical agglomeration
• Advanced discussion on clustering and EM
• Latent space methods; Principal component analysis (PCA).
• Text representations; naive Bayes and multinomial models; clustering and latent space models
• VC-dimension, structural risk minimization; margin methods and support vector machines (SVM) 2
• Support vector machines and large-margin classifiers
• Time series; Markov models; autoregressive models

Student Learning Outcomes: Based on ABET Criterion; ones applied to course highlighted in bold.

1. "An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics"

2. "An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors"

3. "An ability to communicate effectively with a range of audiences"

4. "An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts"

5. "An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives"

6. "An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions"

Student Learning Objectives:

After successfully completing the course, students will be able to:

1. Understand the different fields of machine learning, such as supervised and unsupervised learning, and identifying scenarios where it makes sense to apply machine learning for real-world problem-solving.

2. Design and implement machine learning techniques for solving real-world problems.

3. Apply those techniques for data analysis.

4. Recognize and implement various ways of selecting suitable model parameters for different machine learning techniques.

5. Be aware of the cutting edge areas relevant to machine learning.

6. Use advanced mathematical simulation tools e.g. Python, Matlab, to simulate and/or solve practical machine learning problems.

ADDITIONAL SOURCES TO INCLUDE/CROSSWALK INTO THE CURRICULUM:

ABET accreditation- follow Criterion 5 minimum curriculum requirements.

The Centers of Academic Excellence in Cyber Defense/Information Assurance.

CAE in Cyber Operations programs- extensive lists of knowledge-area requirements for degrees seeking one of those designations.

ACM/IEEE also has recommendations for cybersecurity programs.

NICE Cybersecurity Workforce Framework

California Interagency Advisory Committee on Apprenticeships (IACA), Division of Apprenticeship Standards (DAS)- Minimum Industry Training Criteria (MITC)

*** One challenge for a 4-year degree program in the CSU is mapping all major requirements, plus CSU's general education requirements, into 120 semester units. This is particularly challenging for the Computer Science based programs, since there are also requirements on the CS side. Business or MIS/IT based programs would not have the ABET or ACM/IEEE concerns.

UNDERGRADUATE CYBERSECURITY PROGRAM #2

Dual Baccalaureate Degree Program Upper Division Courses

The first undergraduate program discussed in this document was a generalist degree program in cybersecurity. It is intended a stand-alone degree program with linkages and connections to many different disciplines across campus (Business, Science/Math, Engineering, Social Sciences) through interdisciplinary core, major requirement and electives. The 4 year Baccalaureate Cybersecurity Degree Program includes the following:

Registered Apprentices need 145 hours of classroom instruction in preparation for the apprenticeship On the Job Training Hours (2000).

Dual Baccalaureate Degree Program Curriculum:

Professionalism in Cybersecurity- (1 units)
Learning the Art of Cybersecurity- (3 units)
Human Factors and Psychology of Cybersecurity- (3 units) *** double count UDGE
Introduction to Cybersecurity (3 units)
Technical Principles of Cybersecurity- (3 units)
Cybersecurity Risk Management- (3 units)

Professional Industry Certification (Basic or Intermediate certificate/exam) (3 units)

19 Upper Division Units- Dual Baccalaureate Program

-3 units double count= 16 units program total

*** Additional Requirement: Completion of "Success in Cybersecurity Apprenticeship Orientation"- 20 hours dedicated OJT to understanding the workplace and tips on how to succeed from professionals in the field of cybersecurity.

*** Additional Requirement: 2000 hours On the Job Training administered at participating California Community College, California State University, and University of California campuses.

DUAL BACCALAUREATE CYBERSECURITY DEGREE PROGRAM

CORE COURSES

(Please see Core B.S. in Cybersecurity Major Requirements for Course Details):

UNDERGRADUATE CYBERSECURITY EDUCATION SPECIALIZATIONS AND CERTIFICATIONS OF INTEREST:

Question: Any "Specializations/Options/Emphases/ Concentrations" that should be included within a Bachelor's of Science Degree Program in Cybersecurity?

Stackable Certificate Programs are 12-24 units (lower/upper division) depending on a variety of institutional and curricular factors/regulations:

Amazon Cloud Computing (Pathway, Certificate, Specialization for 2/4 yr. programs)

Software Specialization

Hardware Specialization

Ethical Hacking and Countermeasures-

Cybersecurity Offense and Defense

IoT Product Security

Machine Learning/AI Cybersecurity Specialization

Have the curriculum broken down into 4 domains or concentrations, (Infrastructure & DevOps, AppSec, Ethics and Compliance, Analytics)

Hardware, Cryptography, Cloud, IT/Endpoint:

Secure Software/Engineering Management

Embedded Security

Network (and Infrastructure) Security (and Implementation)-

Networking/Wireless Security-

Mobile Security Specialization-

Application Security/Secure Development-

Cybersecurity Security Operations (SecOps)-

Cybersecurity Policy, Law, Privacy, and Risk Management-

Cybersecurity Intelligence and Analytics-

Cyber and Computer Forensics and Incident Response-

IT Security-

Business-based- Business programs might offer concentrations in policy and management, such as compliance with security regulations in health care, banking, and so on.

MIS/IT-Based Programs- MIS/IT programs to offer concentrations in compliance, system hardening, firewalls, and other defenses/skills useful for system administrators and IT staff.

Computer Science Based Programs- CS-based programs might offer more theoretical options for developers and researchers like secure programming, reverse engineering, cryptography, etc.

Human Aspects of Cybersecurity-

Emergency Cyber Response-

Cryptosystems-

Auditing and Compliance-

Legal Implementation-

Cybersecurity Workforce Development for California Essential- Critical Industries-

Advanced Manufacturing

Agriculture

Banking/Financials

Civil Service

Critical Infrastructure

Energy

Geographic Information Systems (GIS) Cybersecurity-

Healthcare/Medical

Life Sciences and Biotech

Public Service and Safety

Transportation

Travel and Hospitality

Water

FUTURE UPPER DIVISION CYBERSECURITY CURRICULUM/COURSES

CURRICULUM DEVELOPMENT AND IMPLEMENTATION NEXT STEPS:

Continue to engage with public sector, industry, and education/higher education community with industry roundtables and focus groups to sharpen and polish the draft cybersecurity model curriculum and academic standards.

In late summer 2020, we are planning an Education/Higher Education Summit with K-12 Educators and colleagues from across the California Community Colleges, California State University, and University of California to discuss and formalize the model curriculum and academic standards for:

- Bachelor of Science Cybersecurity Degree Program.
    - With Embedded Stacking Cybersecurity Certificate Programs and Specializations

- Dual Baccalaureate Cybersecurity Degree Program (degree program linked with 2000 hour- On the Job Training apprenticeship.)

- Stacking Professional Cybersecurity Certification Programs linked with 2000 hour- On the Job Training apprenticeship.)

Future Cybersecurity Courses/Topics:

Any Interest/Need for development of the following courses. If so, what course (s)? Where does it fit into the program curriculum? Core, major requirement, elective? What is the priority for course development (high/medium/low?) Whom should we go to for assistance in designing/building the course?

Artificial Intelligence (in Cybersecurity)-

Data and Analytics-

Cybersecurity Automation- (course is on Industry radar for development)-

Programming in Cybersecurity-

Cybersecurity Controls-

Cybersecurity Auditing and Compliance-

Quantum Computing and Security-

Web Security-

CYBERSECURITY MASTERS LEVEL EDUCATION:

Cybersecurity Masters level education is a key component of the career education pipeline and pathway. For those interested in management (mid-level or executive) in IT-Cyber, a master's degree would be very useful. In addition, masters programs are key in the training and development of new IT-CS-Cybersecurity instructors and educators. There are a variety of degree and certificate programs at the master's degree level of education that will have value for workforce development purposes. There is quite a bit of materials found on this level of education found throughout the rest of this Strategy Report.

ADVANCED CYBERSECURITY GRADUATE DEGREE (Ph.D.) PROGRAMS:

Cybersecurity is an emerging and maturing professional field and a nascent and evolving academic discipline. In terms of analyzing State of California need for advanced cybersecurity graduate degree programs (i.e. Ph.D.'s/E.D.D., etc.), the current priority level for the design, development, and implementation is "medium."

In short, this priority level is earned because there is currently a lacking feeder pattern of 2 year and 4 year Cybersecurity colleges and universities to fully capitalize on a doctoral cybersecurity program quite yet. There are some issues of lacking coordination of cybersecurity model curriculum, academic standards, matriculation agreements at the Associates/Bachelor's degrees level and limited cybersecurity courses and options statewide that need to occur as a precursor to any advanced degree development and implementation. (Please see the above discussion on undergraduate cybersecurity education programs in California). Pathways into Cybersecurity doctoral programs are reduced these days as the number of "feeder institutions" is only now beginning to strengthen and mature.

In the middle and longer terms (3-5 years), however we need to have a Ph.D. in Cybersecurity Degree Program with the courses properly curriculum mapped, aligned, and linked with Undergraduate and Master's Degree cybersecurity education academic programs. If cybersecurity wishes to achieve solid status as a core academic discipline at the college and university level, it is going to need to significant increase instructor capacity as well. This is clearly where cybersecurity doctoral programs can boost the numbers of cybersecurity professors, educators, and teachers at all levels of education.

In other words, one solid strategy to significantly impact numbers of California cybersecurity instructors and educators (across all levels of education and academia) is to increase the numbers of Cybersecurity Doctoral Students in the pathway and on the way to freshly minted Ph.D.'s. In this way, we increase the number of qualified and prepared cybersecurity educator, researchers, and those that engage in university based community service. While a Ph.D. Program in Cybersecurity does not solve all the instructor related capacity issues (which is a very significant problem) it will be useful to open up and mature the future academic discipline and professional field of cybersecurity.

Additionally, the codification of cybersecurity knowledge, theories, methodologies, analytics, tools into core academic programs and courses as well as the advanced teaching of pedagogy would be essential for additional academic discipline development. Research opportunities, both basic and applied derived from these doctoral programs would provide an additional level of experience and seasoning to future cybersecurity educators/academicians and assist professionals within the field.

Advanced Cybersecurity Graduate Degree Program Implementation Task Activity/Steps:

Phase 1: Program Needs/Industry Labor Demand Survey

Phase 2: Facilitation of Academia, Public Sector, Private Sector and Non-Government Organizations (NGOs) major stakeholder meetings to establish program objectives, courses and curriculum/academic standards, develop research and scholarship opportunities; provide university and community cybersecurity service opportunities.

Phase 3: Implement Multi Campus Consortiums to support Ph.D. Cybersecurity Degree and Specializations in High Need Domains.

Phase 4: Support Cybersecurity Student Teaching/Scholarship, Faculty Research Service.

Phase 5- facilitate enhanced cybersecurity education, academic programs, research, teaching, and service opportunities with University of California & California State University.

Phase 6- Program Evaluation and Assessment

Timeframe of Implementation: Priority: <u>Medium,</u> 3-5 year timeframe: 2023-2025

Phase 1- 2021
Phase 2- 2022
Phase 3- 2023
Phase 4- 2023- As Long As Needed
Phase 5- 2023- Collaboration ongoing
Phase 6- 2025- Program/course evaluations and assessments ongoing

PROFESSIONAL CYBERSECURITY CERTIFICATIONS/CREDENTIALS-

One way in which the professional field of cybersecurity differs from many other fields is in the importance of certifications, or taking of tests that demonstrate mastery in a particular domain or area of tech and cybersecurity. In terms of the "gold standard" for cybersecurity professionals, it is the CISSP Certification—requiring 5 years of professional/related experience within the field. However, there are many, many additional certifications, and levels of certifications that can be also be mastered and contribute in significant ways to the greater cybersecurity enterprise.

The key (the trick) from an education and workforce development perspective is the linkage of cybersecurity certificate/credential programs (that develop skills and abilities) with a solid academic background (knowledge) and experiential learning/professional development opportunities into a prospective program graduate.

While the majority (65-70%) of the cybersecurity professional field has a bachelor's degree in related computing/IT/engineering discipline, some critics think it unfortunate that the 4 year degree/experience minimum job classification requirements are inflexible, burdensome, and keeps employers from hiring otherwise capable staff (because they cannot meet blanket position degree minimum requirements). This may be true even when the candidate may otherwise have a solid background in requisite skills through the completion of industry recognized stackable certificates common throughout the computing, tech, and cybersecurity fields. We need to integrate professional certification requirements into the cyber career pipeline/pathway.

Priority: High

Implementation Task Activity/Steps Timeline:

Phase 1- 2021- Cross-walking with other curriculum sources and additional needs as found in the educational capability gap analysis.
Phase 2- 2022-
Phase 3- 2024-
Phase 4- 2024- As Long As Needed
Phase 5- 2025- Program/course evaluations and assessments are ongoing

SECTION XI: Examples of California Cybersecurity Education and Workforce Development Partnerships

There are many exciting cybersecurity education programs, extracurricular activities, and workforce development opportunities existing (and in development) in California. If you have any such programs to be included in updates to this report, please send the report author an e-mail so it can be included in future resources. In addition, please see the following examples of cybersecurity centers and education programs in California.

San Diego Cyber Center of Excellence (CCOE) is a non-profit that focuses on regional planning and program implementation in order to address cybersecurity workforce, economic development and infrastructure challenges through collaboration with industry, academia and government agencies. CCOE was created to support the growth of the cyber industry, promote cybersecurity in San Diego and provide a template to mobilize other regions.

Our primary goals are to:

Attract and retain cybersecurity talent
Create new opportunities for business
Foster collaboration through the cyber community

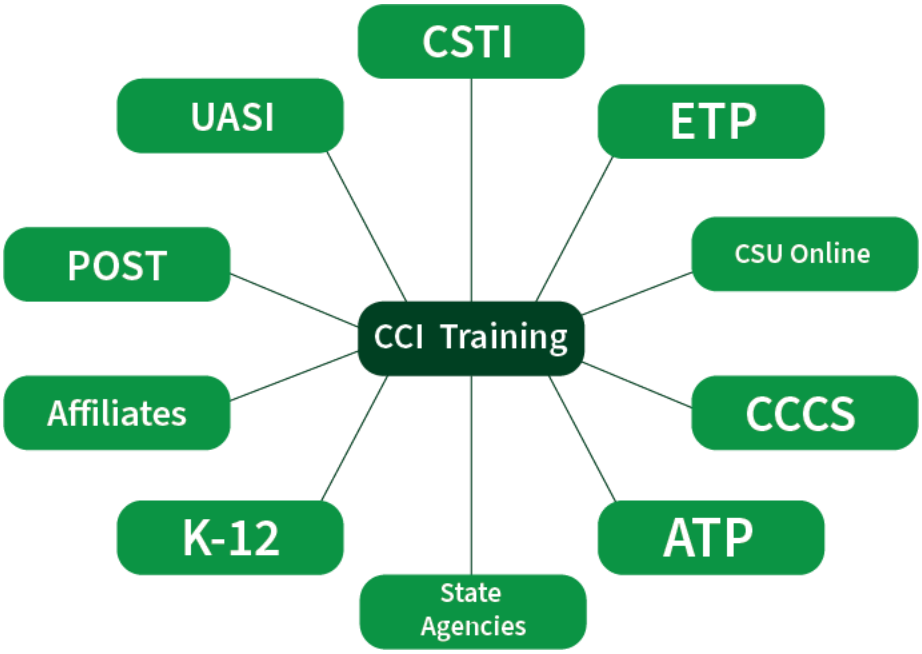
Based on these pillars, CCOE strives to develop best practices and recommendations that can be used as frameworks for other regions to seed the talent pipeline, drive cybersecurity innovation and protect our nation's infrastructure.

CCOE represents a consortium of key leaders from the commercial and defense industries, academia, non-profits, government and the military and intelligence community. Together, we pool resources and lead unified efforts to move the needle on key challenges and opportunities facing the industry. CCOE's programs and resources include the Cyber Career Center, Economic Impact and Workforce Studies, and Cyber Insiders Podcast Series.

The California Cybersecurity Institute

Teaching Californians to Protect California

The California Cybersecurity Institute (CCI) is engaged in multiple campaigns throughout the state, from working with California's urban area security initiatives funded by the Department of Homeland Security (DHS) to hosting the California Cyber Innovation Challenge for the fourth year in a row for middle and high school students. The CCI continues to grow its research initiatives: election security, critical infrastructure, e-learning, digital literacy, innovation, anti-human trafficking, and expanding its portfolio of training through strategic public-private partnerships. The diagram below provides an overview of the existing relationships, training, and programs ongoing for cybersecurity research and training.



To learn more about the CCI, please visit www.cci.calpoly.edu or contact CCI Program Manager Martin Minnich at mminnich@calpoly.edu

CAL POLY
California Cybersecurity Institute

California State University, San Bernardino

Leading the Way in Creating the Next Generation Cybersecurity Workforce

Executive Summary:

California State University, San Bernardino (CSUSB) is a leader in developing applied and innovative approaches to creating curricula that meets the needs of the next generation of cybersecurity leaders, preparing the nation to address the exponential threat that cybersecurity represents to the global economy.

CSUSB's cybersecurity program provides cutting edge skill sets and was one of the first-ever colleges and universities in California to offer a baccalaureate degree with a cybersecurity focus. Offerings in the field now include five master's degree programs, including an advanced degree in cybersecurity and national security studies, as well as a 3 bachelor's programs.

As the nation grapples with the urgent, un-met need of cybersecurity experts in the workforce, it is critical to understand that the future workforce requires cyber experts who are not solely in the engineering field, but bring a broader array of skills representative across every aspect of our public and private sectors. CSUSB is leading the way to ensure that diverse candidates can succeed in this key area.

Key Statistics:

CSUSB brings a unique set of successes that few other colleges or universities have in the field of cybersecurity educational programs, including:

- One of only two Cybersecurity National Resource Centers in the U.S. funded by the National Security Agency and the Department of Homeland Security.
- One of three institutions leading the National Cybersecurity Training & Education Center (NCYTE) an NSF funded Advanced Technology Education Center.
- The lead institution for the Center of Academic Excellence (CAE) in Cybersecurity Community, coordinating more than 350 universities and colleges in the U.S. that have earned the hard-won CAE designation from NSA and DHS. (caecommunity.org)
- Developed and hosts the NICE Challenge Project, a national cyber range that serves some 450 colleges, universities, and high schools. (nice-challenge.com)
- The university is one of five in the country piloting a community college pipeline program with a focus on retraining military veterans (C3P).
- CSUSB's NSF-funded CyberCorps: Scholarships for Service (SFS) program is in the top five in the nation in terms of the output of new cyber talent for the federal workforce, and it is first for diversity. CSUSB also offers the Department of Defense Cybersecurity Scholarship Program (DoD CySP). (cyber.csusb.edu)

Overview of Programs:

Through our various partnerships, initiatives, and designations we have created unique curriculum and programs that customize the skill set of our students. These include:

- **Scholarship for Service:** CSUSB's National Science Foundation (NSF) funded CyberCorps: Scholarships for Service (SFS) program is in the top three in the nation in terms of the output of new cyber talent for the federal workforce, and it is ranked first for diversity.[49] Students who receive these scholarships do so with the understanding they will serve in a federal agency for two to three years after graduation.[50] CSUSB successfully competed for a $4.3 million grant that now is in its fourth year, and this is the third such grant CSUSB was awarded.

- **Center of Academic Excellence in Cyber Defense:** CSUSB is a lead institution among **the NSA/DHS** CAE's in the cybersecurity community, and in this role it coordinates more than 350 universities and colleges that have earned CAE designation. CSUSB developed and hosts the **NICE Challenge Project,** a national cyber range that serves some 450 colleges, universities, and high school**s** throughout the nation to bring real-world cybersecurity challenges straight to students. These help to strengthen students' knowledge and test their skills before joining the cyber workforce in federal government and the private sector.

- **National Cybersecurity Resource Center**: CSUSB helps to expand the quantity and quality of cyber programs across the nation by advising other colleges and universities seeking designation from the Department of Homeland Security (DHS) and the National Security Agency (NSA) as Centers of Academic Excellence (CAE) in Cyber Defense Education. CSUSB is a National Cybersecurity Resource Center, one of only two in the U.S.

- **Cybersecurity Workforce Pathway Programs**: CSUSB is a leader in developing the cybersecurity workforce through pathway programs along the educational continuum. The university is one of five in the country piloting a community college pipeline program with a focus on retraining military veterans to serve in cyber careers. Also, CSUSB hosts the largest GenCyber Camp in the country. Since 2015, this summer program has served more than 1,200 middle school and high school girls, helping to build the workforce pipeline of cyber professionals by introducing these students to the study of cybersecurity careers fields.

- **Information Security Research and Education (INSuRE):** The INSuRE collaborative is a network of National Centers of Academic Excellence in Cyber Defense Research (CAE-R) universities that cooperate to engage students in solving applied cybersecurity research problems. CSUSB runs the infrastructure and coordinates this critical program that pairs universities with technical directors from defense and national labs to work on complex cyber security problems. Roughly 270 project reports on roughly 130 separate problems through Spring 2020. Approximately 750 students from 30 universities have participated.

[49] More than 40 percent of SFS recipients are female and 52 percent are from minority backgrounds.
[50] To date, CSUSB has produced more than 100 SFS cyber graduates.

NSA/DHS NATIONAL CENTERS OF ACADEMIC EXCELLENCE (CAE) IN CYBER DESIGNATED INSTITUTIONS (IN CALIFORNIA)

California State Polytechnic University, CAE-CD 2014-2021

California State University, San Marcos, CAE-CD 2019-2024

California State University, Sacramento, CAE-CD 2017-2022

California State University, San Bernardino, CAE-CD 2014-2021

City College of San Francisco, CAE-2Y 2019-2024

Coastline Community College, CAE-2Y 2019-2024

Cypress College, CAE-2Y 2018-2023

Long Beach City College, CAE-2Y 2018-2023

National University, CAE-CD 2014-2020

Naval Postgraduate School, CAE-CD 2014-2021

CAE-R 2014-2021

Ohlone College, CAE-2Y 2019-2024

Sierra College, CAE-2Y 2019-2024

University of California, Davis, CAE-CD 2014-2021

CAE-R 2014-2021

University of California, Irvine, CAE-R 2019-2024

CAE-CDE- National Centers of Academic Excellence in Cyber Defense Education

CAE-2Y- National Centers of Academic Excellence in Cyber Defense 2-Year Education

CAE-R- National Centers of Academic Excellence in Cyber Defense Research

Source: National IA Education & Training Programs, iad.gov/NIETP/reports/cae_designated_institutions.cfm, accessed on 9.6.2020.

***

SECTION XII- CALIFORNIA CYBERSECURITY CAREER EDUCATION PIPELINE/PATHWAY PROJECT IMPLEMENTATION TASKS/ACTIVITIES, AND DELIVERABLES

California Cybersecurity Task Force Workforce Development and Education Subcommittee Project Task List/Activities/Deliverables:

In addition to the series of subcommittee cybersecurity education and workforce development recommendations, we are working on priority action steps on the task list below to implement key components of the cybersecurity career education pipeline/pathway.

The following report section discusses CCTF Workforce Development and Education Subcommittee Task List/Activities/Deliverables as related to implementation of the CCCEPPP.

The following tasks, activities, and deliverables relate to the completion and efficient operation of the California Cybersecurity Career Pipeline and Pathway. A list of actions items for implementation in conjunction with our recommendations contained previously in this document.

CYBERSECURITY K-12 EDUCATION COMPONENT PROJECTS: DELIVERABLES, SCOPE OF WORK, MILESTONES, TIMELINES:

This section discusses K-12 Task List/Activities/Deliverables/Timelines/Details on CCCEPPP education development and implementation. The project delivers a coordinated, comprehensive, standardized, and accessible series of Cybersecurity education programs at the K-12 segment/level of education through the following tasks, activities, and deliverables:

1. K-12 Education Program/Course Model Curriculum and Academic Standards-
2. Extra-curricular activities, cyber competition-
3. Professional development opportunities- seamlessly transition into college preparedness and career readiness programs found in Higher Education and workforce development (training) programs statewide-
4. Matriculation/Transfer Agreements. Design/Cross-walk California Department of Education Career Technical Education (CTE) Information Communications and Technology (ICT)/Public Service (PS) Model Curriculum and Anchor Standards, Computer Science Academic Standards, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework- Functional Domains.
5. Cybersecurity Education Family (and Parent) Roadmap Development.
6. California Multi-Channel Cybersecurity Hygiene Awareness Strategy.
7. California Cybersecurity Education Clearinghouse.

A summary of prospective projects to undertake in the development, implementation, and evaluation of the CCCEPPP are found throughout the rest of this report section. On the following page or two, is a summary list of cybersecurity education and workforce development projects, scope of work, timelines, milestones, and additional information. The final table in this section lays out the task list related to various projects/initiatives/programs.

SUMMARY LIST: CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT PROJECTS for CCCEPPP-

Project Deliverable #1- The California Cybersecurity Career Education Pipeline and Pathway Project (CCCEPPP).

K-12 CYBERSECURITY EDUCATION PROJECTS AND DELIVERABLES:

Project Deliverable #2- Stackable Industry Recognized K-12 Career Technical Education Cybersecurity Education Certificate Programs/Courses.

Project #3- Cyber workforce development and education programs for career prep/college readiness of high school students. Specifically, we need to enhance computer science college preparedness as a support mechanism for cybersecurity as well.

Project #4- Develop, and implement cybersecurity certificate education programs and related curriculum, education toolkits, apps and build everything out on dedicated servers (cloud-based); virtualized, offered online/on demand across California.

Project #5: Cybersecurity K-12 Education "A-G" Academic Course Curriculum Integration (Academic-CTE Based Courses).

Project #6: K-12 Cybersecurity Instructor/Student Resource/Teaching/Lab/Project/ Instructional Material Development.

Project #7: K-12 Cybersecurity Education and Workforce Development Road Map Production and Distribution (Online/Print).

Project #8- K-12 Cybersecurity Education and Workforce Development- Instructor Recruiting, Development, and Training.

HIGHER EDUCATION CYBERSECURITY EDUCATION PROJECTS AND DELIVERABLES:

Project #9- Associate Transfer Degree Program (A.S. to B.S.) Cybersecurity Degree Program.

Project #10- California Cybersecurity Education/Higher Education and Workforce Development Annual Summit. Featuring: California Department of Education, California Community College- California State University-University of California, private and independent colleges and universities.

Project #11- Develop and Implement California Cybersecurity Education Instruction Certificate Programs and Educator Resources.

Project #12- Statewide Cybersecurity Education and Workforce Development Advisory Board and Annual Meeting.

Project #13: Educational Capacity and Instructor Support Component- simultaneous development of a specialized career pathway intended for cybersecurity educators, instructors, and professors (K-12 and Higher Education).

Project #14: Extracurricular Activity Component- Designation of a State of California Cybersecurity Competition, "the Golden State Cybersecurity League," California Governor's Cybercompetition Golden Cup; *Cybersecurity Competitions Certificate Program.*

Project #15- Initiatives in Cybersecurity: Transitioning Military, Veterans, and Disabled Veterans, and Spouses into cybersecurity workforce career pipelines.

Project #16- Initiatives in Cybersecurity: Diversity and Inclusivity in Education and Workforce Development.

* Strategies to enhance the participation and retention of Women in Cybersecurity and Technological Fields-

* Strategies to enhance the participation and retention of Underrepresented Historical Backgrounds in Cybersecurity and Technological Fields-

Project #17: California Cybersecurity Career Education Pipeline/Pathway Cyber-Hygiene Component: (Cyber Hygiene "Best Practices" and Linkage with Education/Academic Programs at all levels of education).

Project #18: California Cybersecurity Education and Workforce Development Clearinghouse.

Project #19: California Cyber Range Development and Implementation.

Project #20: California Cybersecurity Education Apprenticeship Centers.

PROFESSIONAL CYBERSECURITY TRAINING AND AWARENESS- SPECIFIC CRITICAL INDUSTRY PROJECTS AND DELIVERABLES:

Project #21- Develop workforce development and employee training programs and certificates (including CEU credits) in key industry sectors, critical infrastructure protection.

Project #22- Cyber/Information Security Online Training Programs. Develop and implement for employee training state-wide (including CEU credits.)

PROSPECTIVE K-12 CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT PROJECT DETAILS:

Project Deliverable #2- Stackable Industry Recognized K-12 Career Technical Education Cybersecurity Education Certificate Programs/Courses-

SCOPE OF WORK: Preparation and promulgation of 8 Cybersecurity Industry Recognized Stackable Certificates with offerings for 7th to 12th Grade Career Technical Education (CTE) Cybersecurity Stackable Industry Certification Programs utilizing California Department of Education (CDE) CTE key Model Curriculum and Anchor Standards; recently adopted Computer Science Standards; and cross-walked with NICE/NIST Framework documentation and matrixes.

I. Implement 8 Cybersecurity Industry Recognized Certification for middle/high school students (three course sequences each for certificate completion= 24 "new" courses):

Middle School Cybersecurity Career Technical Education (CTE) Industry Recognized Pre-Certification Programs:

1. Exploring Cybersecurity Certificate Program- (ICT-Basics & Fundamentals)

2. Essentials of Cybersecurity Certificate Program- (ICT- Intermediate skills-link with Internship/Community Service hours requirements, possible industry certifications per below).

High School Cybersecurity Career Technical Education (CTE) Industry Recognized Pre-Certification Programs:

Exploring Cybersecurity Certificate Program- (ICT-Basics & Fundamentals)

Essentials of Cybersecurity Certificate Program- (ICT- Intermediate skills-link with Internship/Community Service hours requirements, possible industry certifications per below).

Creation of Cybersecurity Industry Recognized Pre-Certification for high school students (three course sequences each for certificate completion= 15 "new" courses):

3. Advanced Cybersecurity Certificate Program- (ICT- Advanced skills-link with Internship/Community Service hours requirements, definite industry certifications per below).

4. Cybersecurity and Public Service/Safety Certificate Program- (ICT and Public Service/Safety)- Formation of academy and industry certifications and work in conjunction with other agencies/organizations to implement. Work in conjunction with California Public Safety and Service Academies to develop digital forensics/eCrimes courses/ and related pre-industry certifications.

5. Cybersecurity and Digital Forensics Certificate Program- (ICT and Public Service/Safety)- Formation of academy and industry certifications and work in conjunction with other agencies/organizations to implement. Work in conjunction with California High Schools and Public Safety and Service Academies to develop digital forensics/eCrimes courses/ and related pre-industry certifications.

6. Cybersecurity Competition and Leagues Certificate Program- (ICT/other sectors)- support cybersecurity students, teams, and coaches in cyber competitions. Recruit and work to build skills and tools at the novice level and advance to veteran cybersecurity competitor. Preparation for high school and collegiate division cyber competitions. Digital Badging for participants and for completion.

7. Women in Cybersecurity Certificate Program- Support, encourage, and prepare girls and women for careers and opportunities in the IT-Cyber enterprise. Detailed understanding of the field, different career pathways, strategies and best practices to education programs and workforce opportunities. Emphasize career preparation, hiring/selection, how to secure positions in the field, retention, promotion and career success. Mentoring and peer group work on individual strategies to chart for success in the IT-Cyber Profession.

8. Cybersecurity for Underserved Backgrounds Certificate Program- Support, encourage, and prepare students from undeserved backgrounds for careers and opportunities in the IT-Cyber enterprise. Detailed understanding of the field, different career pathways, strategies and best practices to education programs and workforce opportunities. Emphasize career preparation, hiring/selection, how to secure positions in the field, retention, promotion and career success. Mentoring and peer group work on individual strategies to chart for success in the IT-Cyber Profession.

Project #3- Cyber workforce development and education programs for career prep/college readiness of high school students. Specifically, we need to enhance computer science college preparedness as a support mechanism for cybersecurity as well.

Discuss strategies and enhanced resources to increase the number of schools with A.P. Computer Science (C.S.) Courses. Discuss strategies and enhanced resources to increase numbers of students taking A.P. C.S. tests annually, increase A.P. C.S. exam passage/success rate. Enhance diversity and inclusion outreach and recruiting strategies for greater equity and success rates for all students.

Project #4- Develop, and implement cybersecurity certificate education program and related curriculum, education toolkits, apps and build everything out on dedicated servers (cloud-based); virtualized, offered online/on demand across California.

SCOPE OF WORK: Courses developed online and virtualized with storage and cyber-range hosted on state servers. By utilizing virtualization (and the cloud), local schools and districts do not need to invest significant amounts of money into the otherwise necessary technology and computers labs on campus. Content is virtualized. Schools and districts will not need to purchase additional expensive technology for computer labs/computing resources so students can complete the courses and certificate programs.

Cybersecurity Certificate Programs are in an online format. These courses will be readily accessible and available to all California students with a computer and internet connection. This will enhance cybersecurity education/workforce development program accessibility and availability and overcome geographic obstacles. In addition, to recruit/train/support historically disadvantaged students whom would not otherwise have access to cybersecurity/computer science, IT educations programs locally.

Furthermore, this is a helpful mechanism to coordinate and ensure standardization of cybersecurity curriculum. We can make sure education programs are up to date and cutting edge for today's threat vectors, high skill need areas, and gaps/vulnerabilities.

PROPOSED K-12 CYBERSECURITY (CTE) INDUSTRY RECOGNIZED CERTIFICATE PROGRAMS/ LIST OF COURSES TO DEVELOP:

To ensure all potential student/learner skill needs/levels are met through K-12 CTE Industry Recognized Certificate Programs, we recommend the development of **8** Cybersecurity Certificate Programs. Each certificate program consists of a 3 course sequence; all courses digitized, virtualized, and available online/cloud-based to students across California. We anticipate building 2 certificate programs an academic year over a 4 year time period.

1. Exploring Cybersecurity Industry Recognized Certification Program:
Introduction course: Introduction to Cybersecurity Understanding and Awareness
Connector course: Foundations of Cybersecurity
Capstone course: Cybersecurity Skill and Projects

2. Essentials of Cybersecurity Industry Recognized Certification Program:
Introduction course: Cybersecurity Principles and Fundamentals
Connector course: Cybersecurity Tools, Skills, and Lab
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

3. Cybersecurity Advanced Bridge Industry Recognized Certification Program:
Introduction course: Advanced Cybersecurity Essentials
Connector course: Advanced Cybersecurity Tools, Skills, and Lab
Capstone course: Cybersecurity Mentoring, Apprenticeship, and Internship Professional Development [Cybersecurity Apprenticeship/Pre-Apprenticeship Preparation]

4. Cybersecurity Competition Industry Recognized Certificate Program:
Introduction course: Introduction to Cybersecurity Competitions
Connector course: Cybersecurity Competitions Tools, Skills, and Lab
Capstone course: Cybersecurity Competition Leadership and Management

5. Cybersecurity-Public Service/Safety Industry Recognized Certificate Program:
Introduction course: Introduction to Cybersecurity and Public Service/Safety
Connector course: Cybersecurity/Public Safety Tools, Skills, and Lab
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

6. Cybersecurity-Public Service/Safety Digital Forensics-Investigation Certificate Program:
Introduction course: Introduction to Cyber Digital Forensics and Investigations
Connector course: Digital Forensics and Investigations Tools, Skills, and Lab
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

7. Women in Cybersecurity Certificate Program:
Introduction course: An Introduction to Girls and Women in Cybersecurity
Connector course: Tools, Skills, and Projects for Success in Cybersecurity
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

8. Cybersecurity for Underserved Backgrounds Certificate Program:
Introduction course: An Introduction to the Exciting World of Cybersecurity
Connector course: Tools, Skills, and Projects for Inclusivity in Cybersecurity
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

MILESTONES, TIMELINES:

Implementation of 2 CTE Industry Recognized Certification Programs/x 4 years

Project #5: Cybersecurity K-12 Education "A-G" Academic Course Curriculum Integration (Academic-CTE Based Courses)

SCOPE OF WORK: Second, we need curriculum integration of Cybersecurity, Computer Science, and IT with "A-G" core graduation requirements/elective courses. This will assist students on the college readiness track fit into cybersecurity courses into their already tight academic schedule with solid cybersecurity/computer science/IT foundations. Course curriculum integration in conjunction with California Department of Education (CDE) Career Technical Education (CTE) Information Communications Technology (ICT) Industry Sector Pathway (and

related Pathways); Single Subject Credential educators drawn across state urban and rural school districts. Sources of CDE CTE Model Curriculum/Academic Standards Documentation include:

https://www.cde.ca.gov/ci/ct/sf/documents/infocomtech.pdf
https://www.cde.ca.gov/ci/ct/sf/documents/pubservices.pdf
https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

K-12 CYBERSECURITY CURRICULUM INTEGRATION COURSES TO DEVELOP:

English (9th Grade): Cybersecurity, and Digital Privacy (ICT CTE Sector)-
English (10th Grade): Digital Writing/Cybersecurity Communications (ICT CTE Sector)
Math: Algebra for Cyber and Information Security (ICT CTE Sector)
American Government: Digital Governance, Cybersecurity, Policy (ICT CTE Sector)
Foreign Language: Technology and Cybersecurity in Spanish (ICT CTE Sector)
World/American History: History of Technology, Computing, and Cybersecurity
Science 1: 9th Grade Science (ICT CTE Sector)-
Science 2: 11th Grade Science (ICT CTE Sector)-
Elective 1: Cybersecurity Awareness (ICT CTE Sector)-

Annual Cybersecurity Education Curriculum Integration Conference- curriculum alignment, development, review, and assessment across levels of education. CDE model curriculum/academic standards were approved for state-wide utilization in 2013. In the past 7 years, we have seen significant advances in technology, computing, networking, and security. Curriculum. A new review/update of curriculum/standards is needed and can occur at the curriculum integration meeting. Additionally, discussion of "best practices and pedagogy," instructor preparation/ networking; sharing of instructional materials/resources, with a state-level and regional focus: North, South, and Central/Inland California.

MILESTONES, TIMELINES: Might need to add as separate project;
None established at this time.

Project #6: K-12 Cybersecurity Instructor/Student Resource/Teaching/Lab/Project/ Instructional Material Development-

SCOPE OF WORK: One key aspect of K-12 Education Cybersecurity Education is in the engagement and involvement of students in various certificate programs and courses. We need to make sure the courses, class materials (instructor, student), projects/labs are all visually appealing, academically rigorous, and "fun" to enhance and maintain student interest/success. It is key to include the efforts of talented instructional designers/developers to add these critical elements into the cybersecurity courses under development.

MILESTONES, TIMELINES: None established at this time.

Project #7: K-12 Cybersecurity Education and Workforce Development Road Map Production and Distribution (Online/Print)-

SCOPE OF WORK: One key problem associated with current cybersecurity education and workforce development is that many students do not know the various education/experience/ extra-curricular activities that frequently serve as position minimum requirements within the many specializations of the field. We develop "road maps" to clearly illustrate to middle/high school students the specific steps taken at each level of education to secure entry level cybersecurity positions upon completion of cyber pipeline/pathway education/experience components.

In order to better guide and shepherd students through the cybersecurity education and workforce development pipeline and process, we need detailed "Road Maps" to lay out the clear and necessary preparation steps for entry-level employment in cybersecurity. Road Maps lay out specific education/experience minimum requirements to gain cybersecurity employment upon pipeline/pathway completion. Road maps must be clear, direct, supported by a variety of additional resources, kept up to date; and include the following information (found on the next page.)

California Cybersecurity Career Pipeline/Pathway Roadmap Templates

"Road Map Template" link/align the following elements of each level/segment of education; as well as across education levels/segments to fulfill CCCEPPP objectives/goals. The information below serves as the framework template for a "road map" of essential cybersecurity knowledge, skills, abilities (KSAs) and program areas:

1. Cybersecurity Model Curriculum and Academic Standards-
   - K-12 Education-
   - Associates Level Education- Bachelors Level Education
   - Graduate Level Education-
   - Professional Certifications-

2. Extra-Curricular Cybersecurity Activities- Cyber competitions, Summer/After School Coding Camps, Workshops/labs/projects-
   - K-12 Education-
   - Associates Level Education- Bachelors Level Education-
   - Graduate Level Education-
   - Professional Certifications-

3. Professional Experience- (Registered Apprenticeships, Internships, Digital Community Services/Badges-
   - K-12 Education-
   - Associates Level Education- Bachelors Level Education-
   - Graduate Level Education-
   - Professional Certifications-

4. Professional Development Opportunities- Career exploration/awareness/guidance, mentoring, leadership, networking support, life/work balance, etc.

K-12 Education-
Associates Level Education- Bachelors Level Education-
Graduate Level Education-
Professional Certifications-

MILESTONES, TIMELINES:
Road Map Template Design and Development- Online distribution
Cyber Ed Program and Resource Inventory Collection, Links,

(Relevant Information uploaded to the California Cybersecurity Education and Workforce Development Clearinghouse)

Project #8: K-12 Cybersecurity Education and Workforce Development- Instructor Recruiting, Development, and Training

SCOPE OF WORK: One key to success in the K-12 cyber pathway/pipeline component is in the building of instructor/educator capacity to develop/deliver cybersecurity, computing, and IT programs and courses. This is already a dire need (for cybersecurity instructors) in the K-12 Education segment. As we move greater numbers of students into the cybersecurity pipeline/ pathway, we need to recruit and retain significant numbers of new teachers. This is a problem at all levels of academics, but K-12 educators face many unique challenges to the teacher preparation and certification process. The following proposed funds will secure sub-time and travel monies for cybersecurity educators, recruit new interested instructors, and provide in-service education and teaching resources and opportunities to enhance the number and quality of instruction.

MILESTONES, TIMELINES: None established at this time.

ADDITIONAL K-12 EDUCATION ITEMS

Miscellaneous CTE ITC/PS Model Curriculum/Academic Standards Discussion:

Problem/Concern Related to Students Taking Professional Certification Courses: It is important that students not only take preparatory courses but complete the certification exam as well. One barrier to student success is the cost to take certification exams. They do not complete the Certification exam due to cost. We need to find an avenue to fund students' costs to take the relevant certification exams as to minimize the impact of high school student financial issues related to certification test taking.

Solution: One way to defray student costs for certifications is to provide them with vouchers that allow them to take the exams for no-cost. There are organizations and individuals engaged in these voucher based programs. Perhaps have sponsors provide the resources for vouchers if we were unable to provide voucher through funding projects.

HIGHER EDUCATION CYBERSECURITY EDUCATION PROJECTS AND DELIVERABLES:

Project #9- ASSOCIATE TRANSFER DEGREE PROGRAM (A.S. to B.S.) in Cybersecurity Degree Program:

Associates/ Stackable Training Certifications- Develop Transferable Model Curriculum Degree Program component of Cybersecurity-related Lower Division Degree Program; Completion of Industry Recognized Professional Certification (lower division) Programs.

Objective: Transferable A.S.T. Cybersecurity Degree and Certificate Programs for development and offerings throughout the California Community College System.

Bachelors/Stackable Training Certifications- Link 2 Year- 4 Year Bachelor of Science Cybersecurity Degree Program; Completion of upper division Industry Recognized Certificates and Credentials programs:

1. Meet the entry level employment requirements for State of California IT job classification (for Cyber/Information Security (and related) positions.)

2. Find efficient ways to blend and link learning domains, NIST list framework and additional sources of curriculum/standards/related best practices to innovate new innovative cybersecurity curriculum and professional development opportunities based on critical "high need" domains and functional specializations.

Curriculum development and implementation to be conducted within a large multi-campus consortium. We are talking about developing a cybersecurity career education pipeline/pathway intended to prepare 50,000 cybersecurity professionals through a lengthy workforce development/education process. There is simply no way for a few cybersecurity education programs at a few colleges and universities able to turn out the tens of thousands of graduates over the ten year pipeline/pathway project to meet all cybersecurity workforce needs for California.

We rely on the "hub and spoke model" of cybersecurity program and course offerings: large multi campus consortiums working together to offer multiple sections of cybersecurity core and major requirements online (as a shared resource across educational systems/campuses. In addition, and depending on institutional and faculty strengths/teaching/research specializations—we would develop a catalog of courses (core, major requirements, and elective) drawn from all participating campuses and involved faculty members.

Finally, it is key to establish a future educational standard for all prospective 4 Year Cybersecurity Education Degree Program graduates to uphold: Workforce Ready Workforce: **"Ready to step directly into entry level cybersecurity professional positions upon graduation."** In other words, 4 Year Cybersecurity Program Graduates will be trained on skills needed by employers in the field right now. Such qualified graduates would not need significant additional training, or employers taking new staff off-line for a lengthy period to train them/bring them up to speed on the job. Public and private sector employers raise these comments and concerns frequently. This issue needs to be resolved through the efficient and streamlined operation of a California Cybersecurity Career Education Pipeline/Pathway.

Implementation: Facilitate and bring the academic/education community together with the public and private sector for program and course specification and design. Please see the K-12 Education, Associates, and Bachelors' levels of education discussion of the Cybersecurity Systems Architecture (of this document) for additional materials on this project.

PRIORITY: HIGH-

TIMELINE: CURRENTLY IN PROGRESS

Project #10- California Cybersecurity Education/Higher Education and Workforce Development Annual Summit. Featuring: California Department of Education, California Community College- California State University-University of California, private and independent colleges and universities.

Another step in the collaborative and facilitative education process is Project #10. The *Cybersecurity Education- Higher Education and Workforce Development Summit* should be interdisciplinary in nature with specific tracks addressing key domains and disciplinary areas: Computer Science, IT/IS Computer and Electrical Engineering, Forensics, and other areas of general interest to CDE, CCC, CSU,UC participants.

It should not only be a working session of presentations, roundtables, and workshops; but also include significant social activities to strengthen the bonds and deepen the ties between cybersecurity (and related) educators, researchers, and digital community service statewide.

PRIORITY: HIGH- Schedule to synchronize activity and program/courses/resources between the CDE, CCC, CSU, and UC on Cybersecurity Education and Workforce Development.

LOCATION/TIMEFRAME: Alternating in Northern, Southern, Central California annually. Spring planning activity; Summit Date/Location- TBA.

Project #11- Develop and Implement California Cybersecurity Education Instruction Certificate Programs and Educator Resources:

K/12 Education- Cybersecurity Instructor Professional Certification-

Higher Education- Cybersecurity Instructor Professional Certification-

California Community Colleges-

California State University Campuses-

University of California Campuses-

Problem: Recruit, hire, and retain capable C.S./I.T./Cybersecurity instructors. In terms of finding additional instructors with capacity to teach C.S./I.T./Cybersecurity courses, we must have a roundtable meeting with all key stakeholders and major partners and find substantial ways of increasing C.S./I.T./ Cybersecurity instructor numbers, capabilities, and resource opportunities state-wide across all levels of education.

Solution: Bring veterans (IT MOS) and proficient family members with excellent computing and security backgrounds to lend a hand in the classroom, assume posts as cybersecurity competition coaches, and other critical professional development opportunities for our students.

Priority Level: High Priority: Critical Note: We must increase the number of cybersecurity/CS/IT K-12 and Higher Education instructors and professors to teach across California. Due to the critical nature of increasing and supporting additional cybersecurity educations/professor numbers (and corresponding resources); we need a deeper dive into expanding the initiative to increase cybersecurity instructor numbers (and available teaching resources) in a variety of innovative ways and thoughtful strategies.

SCOPE OF WORK: Professional Development- Statewide Educator Capacity/Capability Enhancement and Certificate Implementation: Certificate program development in Cyber-Computer Science/IS/IT Education (online programs) to support the cyber pipeline for educators. Design creative incentive programs and additional instructor toolkits to increase the number of CTE faculty and instructional staff to teach the larger numbers of students attending cyber (and related) programs. These programs translates directly into more instructors, better prepared faculty, ready for the rigors of cybersecurity in the classroom. This a key role and support mechanism of enhancing the numbers of educators and professors teaching in cybersecurity, computer science, IT/IS and closely related programs. .

Project #12- Statewide Cybersecurity Education and Workforce Development Advisory Board and Annual Meeting-

SCOPE OF WORK: Annual statewide meeting for cybersecurity educators (at all levels of education) in conjunction with representatives from the public and private sector. The emphasis will be on keeping up with innovation in the field and upgrading education/workforce needs /skills to speed. Curriculum/Best Practices on the agenda. Annual meeting tied to statewide Cybersecurity Education and Workforce Development Advisory Board activities and functions.

Project #13: Educational Capacity and Instructor Support Component- simultaneous development of a specialized career pathway intended for cybersecurity educators, instructors, and professors (K-12 and Higher Education)-

SCOPE OF WORK: Professional Development- Statewide Educator Capacity/Capability Enhancement and Certificate Implementation: Develop incentive programs, including tuition reimbursement and incentive programs to recruit qualified K-12 and higher education instructors and train them for rigorous cybersecurity academic and career technical education programs. Find ways to attract and recruit additional cybersecurity instructors and professors, such as reduced tuition costs, utilization of V.A G.I. Bill and related student scholarships/stipends/ loan forgiveness to significantly bolster numbers of instructional faculty here

In addition to model curriculum and academic standards in K-12/higher education, there are additional components necessary for an efficient statewide cyber career pipeline/pathway. We seek to facilitate and encourage the growth of cybersecurity education statewide as a blended academic discipline/professional field. If we plan on dramatically increasing number of cybersecurity program graduates in skilled cyber labor/workforce career pipeline; we need to dramatically increase the numbers, resources, and instructional materials to further enhance statewide instructor capability and capacity as well.

Huge opportunities exist in cybersecurity education professional development. We need to develop, as a part of the cybersecurity career pathway, a project centered on instructor resources, research, and support to effectively deliver cybersecurity instruction at the various levels of educational instruction.

Justification: We are talking about a significant increase in the numbers of students in cybersecurity programs and supporting the career pipeline/pathway. One major issue and limitation in developing/implementing cybersecurity career pathways is the limited number of qualified instructors (at all levels of education) to teach rigorous computing courses. We need to assist instructors (and potential ones) how to master the teaching and learning of cybersecurity, computer science, and information technology.

Increasing cybersecurity educational capacity and support is developed by recruiting and preparing a cadre of cybersecurity educators for strong "teacher training" education and workforce

development training programs. We develop a **Cybersecurity Education and Teaching Certificate Program** recruiting and retaining quality instructors at each segment of education.

MILESTONES, TIMELINES: TBD

Project #14: Extracurricular Activity Component- Designation of a State of California Cybersecurity Competition, "the Golden State Cybersecurity League," California Governor's Cybercompetition Golden Cup; *Cybersecurity Competitions Certificate Program*

SCOPE OF WORK: Set up a coordinated, organized, and efficient cyber competition series at the K-12 and Collegiate Education levels that are accessible statewide. While cyber learning is often found in established curriculum and academic standards, rigorous programs/courses, projects, etc.; there are also many exceptional opportunities outside the classroom to give students an opportunity to practice and hone their skills. Cyber competitions is an excellent team-based activity shared by other students who share the same types of interests. We should model the culmination of "California Governor's Cybercompetition Golden Cup" as the big cyber competition statewide held and awarded every summer. The purpose of this funding is to ensure that a majority of California counties will be represented by 2023 statewide Cyber League/competitions activity. It is essential to expand extra-curricular activities like cyber competitions across underserved groups and geographic location. Participants (students and coaches) need enhanced support and resources to encourage those who may not have had access to these programs in the past.

We emphasize cyber competitions as one aspect of the relationship being built (at all levels of cybersecurity education) through the CCCEPPP. We work with local school districts, CCC, CSU, and UC campuses statewide to assist with organizing countywide cyber teams for competition/league activity in regional competitions that roll up to state-wide final rounds. Furthermore, we organize high school and collegiate divisions; and to focus on preliminary round activity as recruiting and assisting new teams/coaches to the process; yet also retain vigorous competition for veteran teams. In addition, cybersecurity competitions will be assisted/supported by the *Cybersecurity Competitions Certificate Program* (providing team members knowledge, skills, and tools for success in League activities.)

MILESTONES, TIMELINES: TBD

Project #15- Initiatives in Cybersecurity: Transitioning Military, Veterans, and Disabled Veterans, and Spouses into cybersecurity workforce career pipelines-

The cybersecurity community, professional field, and workforce development greatly benefit the inclusion of candidates from transitioning military, veterans, and disabled veterans. Thus, the subcommittee recommendation involves strategies and support mechanisms for the recruitment and retention of Military IT MOS into the civilian cybersecurity workforce where they can put their experience in a diverse set of specializations into closely related positions and jobs throughout the State of California. Individuals with military service are used to working in the dynamic cybersecurity environment, useful soft skills like oral and written communications, team players, strong leadership and soft-skill development among other desirable hiring traits.

In addition, for positions that involve classified information or highly sensitive data, the active background clearances of transitioning military and veterans could expedite the hiring process and potential advantage in the formal hiring process.

Finally, a third element of this recommendation includes the utilization of their military career experience and training to serve an educational role as teacher, advisor, mentors, and cyber coaches for the increased numbers of students that will be entering and pursuing the cybersecurity career education pipeline and pathway.

MILESTONES, TIMELINES: High Priority: TBD

Projects #16- Initiatives in Cybersecurity: Diversity and Inclusivity in Education and Workforce Development

(Strategies to enhance the participation and retention of Women in Cybersecurity and Technological Fields).

SCOPE OF WORK: Building and reinforcing a **s**upportive culture that promotes equity for women in cybersecurity, computing, and IT. This includes the development and implementation of strategies intended for a transformation of cultural and workplace values and related support mechanisms to foster enhanced interest and encourages inclusivity into the field. Furthermore, strategies and policies for career exploration, peer mentoring, and preparation for entry-level cyber employment, recruiting, hiring, retention, and promotions as valued and successful members of cybersecurity (and related) fields.

The inclusion of women into the tech and cybersecurity enterprise is an essential part of any closing of the California cybersecurity workforce gap. It is imperative to deploy strategies to enhance the numbers of prepared cybersecurity women professionals across industries and sectors. Thus we include separate recommendation for strategies to support and encourage women into the cybersecurity, computing, and IT as well accomplish a significant reduction and elimination of gender disparity existing within this field.

(Strategies to enhance the participation and retention of Underrepresented Historical Backgrounds in Cybersecurity and Technological Fields).

Thinking of strategies and recommendations that are consistent with all elements of the NICE Workforce Framework Defining Cybersecurity, "…(as) the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce." (NICE Framework). Strategies must be in place to assist on all these areas with the utmost of haste.

Building and reinforcing a supportive culture that promotes equity for traditionally underrepresented backgrounds in cybersecurity, computing and IT. Furthermore, strategies and policies for career exploration, peer mentoring, and preparation for entry-level cyber employment, recruiting, hiring, retention, and promotions as valued and successful members of cybersecurity (and related) fields.

This includes the development and implementation of strategies intended for a transformation of workplace and related support mechanisms to foster enhanced interest and encourages inclusivity in these fields from underrepresented groups, including persons of color, members of Tribal Sovereign Nations, and persons of varied economic backgrounds across all geographic locations in the State of California.

MILESTONES, TIMELINES: TBD

Project #17: California Cybersecurity Career Education Pipeline/Pathway Cyber-Hygiene Component: (Cyber Hygiene "Best Practices" and Linkage with Education/Academic Programs at all levels of education)-

SCOPE OF WORK: There is one last key element that we must address at all levels of education—namely the critical skill of practicing "safe computing" and cyber-hygiene for online safety and tech security. Networks, systems, and data are only as secure as the users accessing them. By teaching "best practices" in cyber-hygiene we can all be better, safer consumers of information and data; as well as limit exposure to vulnerability and risk that prudent self-cyber security strategies help avoid, prevent, and reduce. One element of the strategy here is the production and distribution of catchy and "fun" PSAs (TV, online, radio spots) to raise statewide cybersecurity awareness of "best practices" in safe computing. In addition to the "cool value," we include outreach and links to cyber education programs, resources, and opportunities found on the Cyber Clearinghouse (the following project deliverable #21).

Project #18: California Cybersecurity Education and Workforce Development Clearinghouse-

SCOPE OF WORK: All educational materials related to K-12/Higher Education cyber workforce and professional development will be uploaded into the Clearinghouse. Useful as we begin to implement cybersecurity instructor/student instructional materials and education initiatives. Dramatically increase the availability in a "one-stop" location of cyber academic/CTE related/ Cyber/IT/Comp Sci. material collection and availability. A clearinghouse is particularly important given the quick speed of innovations/change in the field of cybersecurity. We must have up to date and cutting edge materials developed and made available.

In addition to the cybersecurity education and workforce development materials and resources made available above, there is another key aspect of Clearinghouse activity—having a networking/exchange section where we place prospective employers in touch with potential cybersecurity job applicants seeking positions.

MILESTONES, TIMELINES: TBD

Project #19: California Cyber Range Development and Implementation:

SCOPE OF WORK: Cyber range to accompany all the education and workforce development and programs, etc. contained elsewhere in this funding proposal. Train instructors/students how to use the cyber range effectively and where to find all the tools and resources.

MILESTONES, TIMELINES: TBD

Project #20: California Cybersecurity Education Apprenticeship Centers

SCOPE OF WORK: In conjunction with California Department of Education, California Community Colleges, California State University, and University of California campuses- launch a series of Cybersecurity Education Apprenticeship Centers with local industry and public sector employers. CCCEPPP campuses will have students in education programs linked to apprenticeship opportunities. Centers to be a campus wide mix of Student Services/Career Development, Individual Academic units, and Veteran's Affairs offices across campuses/educational systems.

MILESTONES, TIMELINES: TBD

PROFESSIONAL CYBERSECURITY TRAINING AND AWARENESS SPECIFIC CYBERSECURITY CRITICAL INDUSTRY PROJECTS

Project #21- Develop workforce development and employee training programs and certificates (including CEU credits) in key industry sectors, critical infrastructure protection.

As many public and private agencies, corporations, and organizations struggle with cybersecurity training and workforce development, we need to step in and assist. We need to develop a program that provides information on best practices for cybersecurity at the workplace relevant to key sectors (including financials, energy, aviation, health care, transportation, etc.).

Emerging Areas Include: Elections Systems, Energy, Water, Agriculture

Project #22- Cyber/Information Security Online Training Programs. Develop and implement for employee training state-wide (including CEU credits.)

This project #9 differs from project #8 in at least one critical way. This training program is not intended to be workforce development as folks are already employed somewhere in the field (agencies, firms, NGOs, and others.)

Key sectors could utilize training programs to prepare new staff on key cybersecurity/information security essentials to a specific field. Lawyers, Insurance, Bankers, Accountants are all looking for professional cyber-side training, but not necessarily super technical (or extraneous) information to that field or position. Provide online and in-person training formats.

Emerging Areas Include: Elections Systems, Energy, Water, Agriculture

Note: Not cybersecurity train the trainers programs. Intended to enhance worker training and knowledge in these critical sectors.

CCCEPPP and Educational Institution Toolkit Task List/Activity Deliverables

Deliverable/Activity #1- California Cybersecurity Career Education Pipeline/Pathway-

Deliverable/Activity #2- Cybersecurity A.D.T Degree Program (Associates to Bachelor's Degree in Cybersecurity with Multiple Embedded Stackable Certificates);

Deliverable/Activity #3- Develop Career Technical Education (CTE) Cybersecurity Industry Recognized Certifications; Educator/Instructor Certificate Programs—K/12 and Higher Education/ Higher Education- Lower and Upper Division areas.);

Deliverable/Activity #4- California Cyber Hygiene and Awareness Plan; California Multi-Channel Cybersecurity Hygiene Awareness Campaign Strategy Vision and Design Framework.

Deliverable/Activity #5- Framework/basic specification architecture for development and implementation of California Education Institution Threat Assessment Center (CEITAC);

Deliverable/Activity #6- Framework/basic specification architecture for development and implementation of California Cybersecurity Education Clearinghouse;

Deliverable/Activity #7- Diversity and Inclusivity in IT-Cyber Report

Deliverable/Activity #8- California Cybersecurity Education and Workforce Development Roadmap.

Deliverable/Activity #9- California Cybersecurity Education Family (and Parent) Roadmap Development.

Deliverable/Activity #10- The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*- (see Appendix 2).

REFERENCES

Burning Glass Technologies. "Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring." Accessed at: https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf electronically on June 2019.

California Community Colleges, Accessed electronically 7/2/2020. https://www.cccco.edu/About-Us/Key-Facts

California Community Colleges, Accessed electronically 7/2/2020. https://datamart.cccco.edu/Faculty-Staff/Staff_Demo.aspx

California Computer Science Standards, source: https://www.cde.ca.gov/be/st/ss/computerscicontentstds.asp Accessed electronically on 8/04/18.

California Employee Demographics, Accessed electronically on 8/04/18. https://www.sco.ca.gov/ppsd_empinfo_demo.html

California Department of Education, Accessed electronically on 7.2.2020. https://www.cde.ca.gov/nr/ne/yr19/yr19rel27.asp

California Department of Education, Accessed electronically 7/2/20. https://www.cde.ca.gov/ds/sd/cb/ceffingertipfacts.asp

California Department of Education, Accessed electronically on 7.2.2020. https://www.cde.ca.gov/ds/sd/cb/ceffingertipfacts.asp

California Department of Education, Career Technical Incentive Grant (CTEIG) Funding Years Timeline, (https://www.cde.ca.gov/ci/ct/ig/cteigtimeline.asp, Accessed electronically on 7/18/20).

California Department of Education, Career Technical Education, Accessed electronically on 6/16/2020. https://www.cde.ca.gov/ci/ct/sf/ctemcstandards.asp

California Department of Education, Accessed electronically on 8/04/18. https://www.cde.ca.gov/ci/ct/sf/documents/infocomtech.pdf

California Department of Education, Accessed electronically on 8/04/18. https://www.cde.ca.gov/ci/ct/sf/documents/pubservices.pdf

California Department of Education, Accessed electronically on 8/04/18. https://www.cde.ca.gov/ci/ct/sf/documents/energyutilities.pdf

California Cybersecurity Integration Center (Cal-CSIC), Accessed electronically on 8/01/19. https://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/california-cybersecurity-integration-center

California Information Technology Annual Report 2019, California Department of Technology, Accessed electronically at: cdt.ca.gov/wp-content/uploads/2020/02/2019-Annual-Report.pdf

California State Employee Demographics (State Controller's Office), Accessed electronically on 2.15.20. sco.ca.gov/ppsd_empinfo_demos.html

California State University, Accessed electronically 7/2/2020. https://www2.calstate.edu/csu-system/about-the-csu/facts-about-the-csu/Documents/facts2020.pdf

Cyberseek Heat Map, Accessed electronically on 6/21/2020. https://www.cyberseek.org/heatmap.html

DataQuest, The California Department of Education, Accessed electronically on 8/2/2020. https://dq.cde.ca.gov/dataquest/dataquest.asp

Economy of California, Wikipedia, Accessed electronically on 7.1.2020. https://en.wikipedia.org/wiki/Economy_of_California#:~:text=The%20economy%20of%20California%20is,of%20India%20and%20behind%20Germany.

Frost and Sullivan, 2017 Global Information Security Workforce Study, Accessed electronically on 8/2/2020. https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

Information Technology Model Curriculum (ITMC)-
"AS Degree in IT (Fall 2015) Ohlone College Case Study," Prepared by Richard Grotegut.

Los Angeles Unified School District, Accessed Electronically on 7.2.2020. https://achieve.lausd.net/site/handlers/filedownload.ashx?moduleinstanceid=52741&dataid=89340&FileName=Fingertip%20Facts%202019-2020.pdfF.pdf

Massive Open Online Courses, Accessed electronically on 8/16/19. http://mooc.org/

(National Cybersecurity Workforce Framework, National Institute for Cybersecurity Education (NICE). Accessed electronically on 7/1/19. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center

National IA Education & Training Programs, iad.gov/NIETP/reports/cae_designated_institutions.cfm, Accessed electronically on 9.6.2020.

Santa Ana College, source- Accessed electronically on 8/20/19. https://www.sac.edu/StudentServices/Counseling/articulation/Documents/Computer%20Science%20AST.pdf

U.S. Bureau of Labor Statistics. Accessed electronically on 2/16/2020. https://www.bls.gov/news.release/pdf/ecopro.pdf

U.S. Bureau of Labor Statistics, Occupation Outlook Handbook 2018-2020 (Updated Through May 2019). Accessed electronically on 7/01/2020. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

United States Census Bureau, Accessed electronically on 7/15/19. https://www.census.gov/glossary/#term_Populationestimates

United States Census Bureau, Accessed electronically on 7/15/19. https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk

University of California, Accessed electronically 8/2/20. https://www.universityofcalifornia.edu/uc-system

Wikipedia, Rank of States, Accessed Electronically on 7.2.2020. https://en.wikipedia.org/wiki/List_of_states_and_territories_of_the_United_States_by_population

APPENDIX 1-

Contributions, Acknowledgements, and Participants

The CCCEPPP initiative was developed with the support of many dedicated Colleagues from government agencies, labor and workforce development agencies, cyber employers (public and private), and education/higher education communities. Academic disciplines related to cybersecurity, information technology, and computer science were key participants. The following individuals, organizations/institutions, and firms are to be acknowledged in this appendix. The acknowledgements, contributions, and participants were initially included at the beginning of this report in earlier iterations. However, the list just continued to grow and is worthy of inclusion as its own report appendix.

PUBLIC SECTOR AGENCY COLLEAGUES

Darin Bournstein, California Governor's Office of Emergency Services

Marc Glenn, California Governor's Office of Emergency Services

Adam Crawford, California Governor's Office of Emergency Services

Nyssa Fulmer, California Governor's Office of Emergency Services

Ted Johnson, California Governor's Office of Emergency Services

David Lane, California Governor's Office of Emergency Services

Helen Lopez, California Governor's Office of Emergency Services

Karen Navarro, California Governor's Office of Emergency Services

Eli Owen, California Governor's Office of Emergency Services

Kyle Trembley, California Governor's Office of Emergency Services

Douglas Burt, California Governor's Office of Policy and Research

Emily Desai, California Governor's Office of Business and Economic Development (GO-Biz)

Isabel Casillas Guzman, California Governor's Office of Business and Economic Development (GO-Biz)

Poonum Patel, California Governor's Office of Business and Economic Development (GO-Biz)

Kaina Pereira, California Governor's Office of Business and Economic Development (GO-Biz)

Julie Whitten, California Government Operations Agency (GovOps)

Michael Todd, California Department of Technology

Ema Roberts, California Department of Technology

Brigadier General Robert A. Spano, California Military Department

James Parsons, California Military Department

Kenneth Foster, California Military Department

Edward Chao, California Military Department

Jaeson White, California Highway Patrol

Dr. Scott Howland, California Highway Patrol

Pam Greeley, California Highway Patrol

Cindi Beck, California Department of Education

Erle Hall, California Department of Education

Gary Page, California Department of Education

Dr. Jeffrey Mrizek, California Community College Chancellor's Office

Sheneui Weber, California Community College Chancellor's Office

Dr. Maureen White, California Community College Chancellor's Office

Dr. Steve Wright, California Community College Chancellor's Office

Dr. Linda Vaughn, South Bay Regional Public Safety Training Consortium

Dr. Sheila Thomas, California State University, Office of the Chancellor, Professional and Continuing Education (PaCE)

Shannon Jackson, California State University, Office of the Chancellor, Professional and Continuing Education (PaCE)

Sorann Sing, California State University, Office of the Chancellor, Professional and Continuing Education (PaCE)

Dr. Marshall Thomas, California State University, Office of the Chancellor

David Rusting, University of California Office of the President, CISOs Office

Robert Smith, University of California Office of the President, CISOs Office

Matthew Linzer, University of California Office of the President, CISOs Office

Monte Ratzlaff, University of California Office of the President, CISOs Office

Mark Bisbee, Cal Fire, Office of the State Fire Marshal, State Fire Training Division

Greg Kyritsis, California Commission on Peace Officer Standards and Training (POST)

Phil Caporale, California Commission on Peace Officer Standards and Training (POST)

Charles Evans, California Commission on Peace Officer Standards and Training (POST)

Brian Rohde, County of Madera

Stephen Pollitt, California Office of Statewide Health Planning Development (OSHPD)

Stacie Walker, California Office of Statewide Health Planning Development (OSHPD)

Gary Dias, California Department of Health Care Services (DHCS)

Miguel San Mateo, San Francisco Area InfraGard

Robert Morgester, California Department of Justice

Howard Ballin, California Department of Justice

Randi Kay Stephens, Institute for Local Government (ILG)

CALIFORNIA LABOR & WORKFORCE DEVELOPMENT COLLEAGUES

Secretary Julie Su, California Labor and Workforce Development Agency (LWDA)

Under-Secretary Stewart Knox, California Labor and Workforce Development Agency (LWDA)

Michael Younger, California Labor and Workforce Development Agency (LWDA)

Tim Rainey, California Workforce Development Board (CWDB)

Aida Cardenas, California Workforce Development Board (CWDB)

Robert Meyer, California Employment Training Panel (ETP)

Heather Miguel, California Employment Training Panel (ETP)

Eric Rood, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Glen Forman, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Kelly Mackey, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Paul Giacomotto, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Linda Mount, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Tsegay Arefaine, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Helen Bui, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Laura Thompson, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Adriana Salmoran, California Department of Industrial Relations, Department of Apprenticeship Standards

Vinz Koller, Social Policy Research Associates (SPRA)

Terri Carpenter, Sacramento Employment Training Agency (SETA)

Jo Marie Diamond, East County EDC

Will McCoy, Ed Tech Authority

Molly (Mary) Uzoh, Rightvarsity Technologies, LLC

INDUSTRY COLLEAGUES

The California Cybersecurity Workforce Development and Education Strategy includes participants and colleagues contributing from industry (both public and private). The CCCEPPP objective is cybersecurity model curriculum and academic standards reviewed by 100+ industry representatives to ensure it meets workforce and sector needs.

Darin Andersen, CyberTECH Network

Simon Bain, Ten Dot Zero

Manny Barbara, Silicon Valley Education Foundation

Ray Bareiss, Socratic Arts, Inc.

Ibinabo BobManuel, Mylestone

Vicki Brannock, Biocom Institute

Tony Bryan, CyberUp

Immanuel Chavoya, Intuitive

Rebecca Chisholm, Cisco Systems

Pat Choy, Abbott

Thomas Chow, Pubmatic

Chris Cochrane, Marqeta

Brian Collins, Mission Critical Institute

Joe Collinwood, CySure

Tristen Cooper, ReCog LLC

Kathy Cruz, KPMG

Nick Curry, Amazon

Marcela Denniston, Cyber Lantern

Deidre Diamond, CyberSN

Phil Dillard, Global Minds Work Local

Diane Delaney, IBM

Stephen Dodd, IBM-Public Partnerships

Shamla Naidoo, IBM Global

Jon Donovan, Malwarebytes

Howard Duck, ISACA Sacramento Chapter

John Armantrout, NAVWAR

Lisa Easterly, Cyber Center of Excellence

Janet Fouts, Nearly Mindful

Liz Fraumann, synED/Cyber-Guild

Matt Gardner, California Technology Council

Adam German, ISACA, Sacramento Chapter

Davood Ghods, Direct Technology

Stephen Gilfus, Mission Critical Institute

Debbie Gordon, Cloud Range

Maurilio Gorito, Palo Alto Networks Education Team

Lakshmi Hanspal, Box

Brandon Hardy, Microsoft

Brian Horton, Breadcrumb Cybersecurity

Tori Hughes, Cloud Range

Harsh Jadhav, ACERA

Karen Jensen, Saaby Consulting

Lars Jenson, Adaptable Security

Richard Jones, NAVWAR

Sean T. Jones, groupsense.io

Pratul Kant, Metropolitan Transportation Commission

Peter Kardel, Clever Ducks

Amy Kaufman, CEO Leadership Alliance Orange County

Paul Keener, Viasat

Vinz Koller, SPRA

Benjamin Kushner, ICF

Cameron Law, Social Venture Partners of Sacramento

Brandon Leck, Biocom Institute

Peter Liebert, Liebert Security, LLC

Dr. Alexander Loew, CEO Data-Warehouse, Munich; Member, Cybersecurity Council Germany

Chuck Lott, EMC Corporation

Dr. Tony Lopez, Indus Technology, Inc.

Kevin McNally, Booz, Allen, Hamilton

Marian Merritt, National Initiative for Cybersecurity Education (NICE)

Donna Milgram, Institute for Women in Trades, Technology, and Science

Richard Miller, Sentek Global

Andres E. Jimenez Montoya, Latino Institute for Corporate Inclusion (LICI) -- Americas

Dr. Coleen Morehead, CLEAR Strategies, LLC

Michael Morgan, Foster Farms; California State University, Stanislaus

Dan Myers, Palo Alto Networks Education Team

Meer Nazir, accenture

Michael Nathan, 5G Innovation Lab

Dennis Noone, techwire

Aidan O'Leary, SentinelOne

John Owen, Next Gen Cyber Ed

Jamie Parenteau, 42

Nital Patel, Cisco

Amy Kardel, CompTIA

Mark Plunkett, CompTIA

Dr. Nader Qaimari, ISACA

Lou Rabon, SecOps

Nick Rodrigues, Hewlett Packard Enterprise

Esperanza Romero, NAVWAR

Mimi Rosado, NIWC Pacific

Vanessa Russell, Love Never Fails

Jessica Savage, CiscoTV

Robert Shaw, Dell SecureWorks

Steve Shaw, McMillan Consulting

Stacy Sherman, Genomics Institute of the Novartis Research Foundation

Scott Sibley, Journeys Map

Jim Skeen, Lockton San Diego

Michael Specchierla, SLO Partners & SLOCOE

Karen Stanton, Western Academy Support and Training Center

Lauren Strauss, searchable.com

Todd Thiel, Undisclosed

Karen Tinucci, ISACA, Sacramento Chapter

Alex Torres, Sierra College, Hewlett Packard Enterprise

Thomas Trevethan, Palo Alto Networks Education Team

Trisha Turlington, Red Hat

Lawrence Wagner, Spark Mindset

Tohru "TJ" Watanabe, FireEye

Joy Weed, Southern California Edison

Nicola Whiting, Titania

Caroline Wong, Cobalt.io

Porter Wong, Lawrence Livermore National Laboratory

Monte Young, Young Technologies

Scott Young, SynED, Cyber-Guild

Stephen Zalewski, Levi Strauss & Co.

Benny Zhao, Box

Rami J. Zreikat, xTerraLink, Inc.

CYBERSECURITY EDUCATION/HIGHER EDUCATION COLLEAGUES

Cybersecurity model curriculum and academic standards documents were prepared utilizing the contributions of many within the education and higher education communities. We would like to recognize the following educators, university/college faculty, and administration/staff who contributed to the design, development, and implementation of the Cybersecurity Model Curriculum/Academic Standards. Participation included a variety of activities, including submitting course syllabi, assisting and fostering linkages with additional colleagues, serving as Cybersecurity Subject Matter Experts (SMEs), and attending regular meetings/ teleconferences. Thanks to the following:

Dr. Reza Abdolee, California State University, Channel Islands

Dr. Ali Ahmadinia, California State University, San Marcos

Dr. Leslie Albert, San Jose State University

Dr. Mehrdad Aliasgari, California State University, Long Beach

Professor Fred Allen, Grossmont-Cuyamaca Community College District

Dr. Joseph Allen, National University System

Dr. Sami Al-Salman, California State University, Channel Islands

Kit Alvarez, San Bernardino County Office of Education

Jaime Anderson, Yucaipa-Calimesa Joint Unified School District

Dr. Brent Auernheimer, California State University, Fresno

Dr. Pamela Avila, Porterville High School, Porterville Unified School District

Dr. Ahmed Azam, California State Polytechnic University, Pomona

James J. Baker, California Polytechnic State University, San Luis Obispo

Gretchen Bliss, University of Colorado

Veronica Boe, California Maritime Academy

Dr. Debra Bowen, National University

John Callahan, San Diego State University

Winnie Callahan, San Diego State University

Sandra Cano, Los Angeles Unified School District

Dr. Thomas Carter, California State University, Stanislaus

Dr. Alfred Castillo, California State Polytechnic University, San Luis Obispo

Dr. Stephen Choi, California State University, Fresno

Dr. Mark Clark, California State University, San Bernardino

Dr. Rita-Marie Conrad, University of California, Berkeley

Dean Kris Costa, West Hills College

Dr. Tony Coulson, California State University, San Bernardino

Dr. Jeffrey Cummins, California State University, Fresno

Dr. Melissa Danforth, California State University, Bakersfield

Dr. Henry Danielson, California Polytechnic State University, San Luis Obispo

Dr. Bruce Edward DeBruhl, California Polytechnic State University, San Luis Obispo

Dr. Harjit Dhillon, California State University, Northridge

John Dolan, University of California, Davis

Dr. Haysaam El-Razouk, California State University, Fresno

Dr. Peter English, California State University, Fresno

Dr. Levant Ertaul, California State University, East Bay

Dr. David Falconer, California State University, Fullerton

Dongweng Fang, California Polytechnic State University, San Luis Obispo

Melissa Fish, American River College

Jeffrey Forrest, College of the Canyons

Dr. Eric Frost, San Diego State University

Dan Ganzow, National University

Dr. Muhammed Ghanbari, California Polytechnic State University, San Luis Obispo

Dr. S. Jimmy Ghandi, California State University, Northridge

Dr. Mikhail Gofman, California State University, Fullerton- College of Engineering and Computer Science Center for Cybersecurity

Dr. Mark Gondree, Sonoma State University

Dr. Jiang Guo, California State University, Los Angeles

Dr. Babita Gupta, California State University, Monterey Bay

Dr. John Halpin, City College of San Francisco

Carl Hansen, Humboldt State University

Paula Hodge, College of the Canyons

Dr. Emma Hughes, California State University, Fresno

Dr. Mohammed Iftekhar Husain, California State Polytechnic University, Pomona

Dr. Shih-Hsung (Alex) Hwu, San Francisco State University

Dr. Alicia Iriberri, California State University, Fresno

Professor Sevada Isayan, California State University, Northridge

Janine Johnson, National University

Dr. Matt Johnson, California State University, East Bay

Dr. Nancy Jones, Coastline Community College

Professor William Kearney, Clovis Community College

Jamie Keledjian, Magnolia High School, Anaheim

Jeff Klaben, Santa Clara University

Dr. Hovannes Kulhandjian, California State University, Fresno

Dr. Ojoung Kwon, California State University, Fresno

Dr. Shui Lam, California State University, Long Beach

Orlando Leon, California State University, Fresno

Dr. Ming Li, California State University, Fresno

Qianqian Lin, TEALS k-12

Professor Carlos Martinez, California State University, Fresno

Dr. Nahid Majd, California State University, San Marcos

Dr. Stanley Maloy, San Diego State University

Dr. Dan Manson, Desert Research Institute

Dr. Patricia McQuaid, California Polytechnic State University, San Luis Obispo

Dr. Kathleen Meehan, California State University, Chico

Martin Minnich, California Cybersecurity Institute, California Polytechnic State University, San Luis Obispo

Dr. Sinjini Mitra, California State University, Fullerton

Dr. Stephanie Mizrahi, California State University, Sacramento

Professor Dennis Mohle, Fresno City College

Dr. Marina Mondin, California State University, Los Angeles

Amanda Elledge Moore, James C. Enochs High School

John Mummert, Foothill College

Dr. Ani Nahapetian, California State University, Northridge

Dr. Ygnacio "Nash" Flores, Rio Hondo College

Dr. Vincent Nestler, California State University, San Bernardino

Professor Craig Neumann, El Camino College

Dr. Ram Nunna, California State University, Fresno

Professor Kathy Oborn, Los Angeles Pierce College

Dr. Kazunori Okada, San Francisco State University

Dr. Joseph Otto, California State University, Los Angeles

Professor John Owen, San Francisco State University

Dr. Pramood Pandya, California State University, Fullerton

Carey Peck, Los Angeles Unified School District

Mario Perez, Los Angeles Mission College

Dr. Ron Pike, California State Polytechnic University, Pomona

Dr. Matin Pirouz Nia, California State University, Fresno

Josef Preciado, American River College

Dr. Frank Quiambao, University of California, Los Angeles

Dr. Anne-Louise Radimsky, California State University, Sacramento

Dr. Raeza Raisi, California State University, Fresno

Professor Edward Rangel, California State University, Bakersfield

Dr. Kenneth J. Ryan, California State University, Fresno

Sheryl Ryder, Placer County Office of Education

Jeremy Rosenberg, University of California Berkeley

Dr. Kevin Sampson, Coastline Community College, Fullerton College

Dr. Chandrika Satyavolu, California State University, Monterey Bay

Dr. Hossein Sayadi, California State University, Long Beach

Dr. Lutfus Sayeed, San Francisco State University

Dr. Peter Schuerman, University of California, Merced

Dr. Harald "Otto" Schweizer, California State University, Fresno

Professor Puneet Sharma, California State University, Channel Islands

Professor Ron Sha, Ohlone College

Dr. Bongsik Shin, San Diego State University

Dr. Christopher Simpson, National University

Janet Sloan, Fresno County Office of Education

Dr. Ludwig Slusky, California State University, Los Angeles

Laurie Smith, OC STEM Initiative

Dr. Michael Soltys, California State University, Channel Islands

Dr. Steven Stepanek, California State University, Northridge

Dr. Aaron Stillmaker, California State University, Fresno

Professor Richard Taha, City College of San Francisco

Dr. Shahab Tayeb, California State University, Fresno

Dr. Megan Thomas, California State University, Stanislaus

Professor Javad Varzandeh, California State University, San Bernardino

Dr. Balaji Venkatraman, San Jose State University

Dr. Sameer Verma, San Francisco State University

Dr. Rafael Villegas, California State University, Fresno

Professor Senhua Yu, California State University, Northridge

Dr. Hao Yue, San Francisco State University

Diane Walker, Antelope Valley Union High School District

Dr. Zhaohong Wang, California State University, Chico

Annette Webb, University of California, Riverside Extension

Professor Tobi West, Coastline Community College

Dr. Todd Wilson, California State University, Fresno

Donna Woods, Canyon Springs High School/ Moreno Valley Unified School District

Dr. Timothy Woods, Fresno City College

Professor Richard Ning Wu, City College of San Francisco

Dr. David Zeichick, California State University, Chico

In addition to other colleagues whom have graciously volunteered their time and assisted on CCCEPPP and enhancing statewide cybersecurity education and workforce development and model curriculum/academic standards design and development. Thanks!

APPENDIX 2-

The California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Model Talent Pipeline

The California Cybersecurity Essential Workforce Youth Pre- and Registered Apprenticeship Talent Pipeline (CEWYA) Strategy and Framework

Strategy Paper and Recommendations

Prepared by:

Keith Clement, Ph.D., Professor, California State University, Fresno,
California Cybersecurity Task Force, Workforce Development-Education Subcommittee Chair;
California Interagency Advisory Committee on Apprenticeship (IACA) IT Subcommittee Chair;
Chair, Public Safety Education Advisory Committee (PSEAC) of the California Community Colleges

Kelly Mackey, Regional Director of Strategic Partnerships, Department of Industrial Relations, Apprenticeship and Workforce Innovation

Erle Hall, Education Programs Consultant, Career Technical Education Leadership Office, Career and College Transition Division, California Department of Education

Mario F. Garcia, CISSP, Deputy Commander, California Cybersecurity Integration Center (Cal-CSIC), Homeland Security Division, Governor's Office of Emergency Services (Cal OES)

September 3, 2020

EXECUTIVE SUMMARY

Global demand for cybersecurity and information security professionals and personnel has been mounting for decades. Well-prepared cybersecurity professionals are essential given the dynamic change in scope and breadth of threats and vectors in today's cybersecurity environment. Based on the reliance of technology in the digital environment, we need coordinated and linked education, training, and workforce development programs to increase statewide cybersecurity capabilities and enhance cyber-resiliency. In order to meet current and future critical state-wide cybersecurity "high needs areas" and workforce/skills gaps; comprehensive, coordinated, and strategic academics/education and professional workforce training programs are in heavy demand.

The ***California Essential Workforce Youth Pre- and Registered Apprenticeship Talent Pipeline Strategy and Framework*** **("CEWYA")** describes a statewide comprehensive and collaborative model of education programs and workforce development opportunities into a coordinated IT-Cyber sector apprenticeship pathway. The IT-Cyber youth pre- apprenticeship and registered apprenticeship pathway advances students from $5^{th}/6^{th}$ grade through career readiness and college preparedness programs. This includes education programs and workforce development opportunities aligned to select IT-Cyber career entry points as well as linkages with college/ university two-year/four-year degree programs and professional/industry recognized certificates.

The CEWYA Apprenticeship Pipeline is a four-step process: 1. Outreach and Recruiting; 2. Pre Apprenticeship step; 3. Apprenticeship Program step; 4. Employer Based "On the Job Training" (OJT) step. Spanning these four steps, we find six critical components woven together into the CEWYA Process: these include education programs, industry recognized certification components, essential employability "soft skills," OJT, and Cyber-Hygiene-Awareness components. This report discusses how these components relate to the CEWYA process and steps; as well as, cybersecurity model curriculum, academics standards, extra-curricular activities, cyber-competitions, professional/career development, and additional activities (like Model Industry Training Competency (MITC) design and promulgation.

The cybersecurity career pathway includes a variety of specialized education programs and specialized tracks in "high need domains/areas" including degree and certificate programs (see "Stacking Certificate Programs" later in the report). In addition, it is key to align and link with National Initiative for Cybersecurity Education (NICE) Workforce Framework domains. Finally, it is critical all education programs and workforce development opportunities are available to everyone irrespective of geographic location or socioeconomic status/background.

We seek innovative ways to meet key stakeholder workforce needs with rigorous academic/professional curriculum and standards, enhanced student access to quality, cost-efficient, and aligned IT-Cyber programs statewide. This paper describes the CEWYA Apprenticeship Pipeline, the broader *California Cybersecurity Workforce Development and Education Strategy*, and how an apprenticeship vocational model is key to reduce current/future state cybersecurity workforce capability skills/gaps. The Strategy Report provides **recommendations** for a framework, blueprint, and template to develop and implement the California Cybersecurity Career Education Pipeline and Pathway Project (CCCEPPP) to prepare 50,000 entry-level cybersecurity professionals from 2020-2030.

CONTENTS

ACKNOWLEDGEMENTS

Tsegay Arefaine, Strategic Business Analyst, California Department of Industrial Relations, Division of Apprenticeship Standards (DAS)

Miki Bellon, Mikology/Silicon Valley Roundtable

Helen Bui, Strategic Business Analyst, California Department of Industrial Relations, Division of Apprenticeship Standards (DAS)

Brenda Bridges Cruz, Deputy Director, Office of Professional Development, California Department of Technology (CDT)

Stephen Dodd, IBM Certified Project Executive, IBM Public Partnerships, IBM

Paul Giacomotto, Deputy Regional Director of Strategic Partnerships, Department of Industrial Relations, Apprenticeship and Workforce Innovation

Amy Kardel JD, Vice President, Strategic Workforce Relationships, CompTIA

Keith Koo, Managing Partner, Guardian Insight Group and Host, Silicon Valley Insider Radio Show

Marian Merritt, Lead for Industry Engagement, National Initiative for Cybersecurity Education (NICE)

Shamla Naidoo, Managing Partner of IBM Security, former Chief Information Security Officer, IBM Global

Jonathan Nunez, Commander, California Cybersecurity Integration Center (Cal-CSIC)

Palo Alto Networks Education Team

Vitaliy Panych, State Chief Information Security Officer (Acting), Office of Information Security, California Department of Technology

Mario Perez. Data Communications Specialist/CSIT Professor, Los Angeles Mission College

Mark Plunkett, Senior Director, Global Custom Training Solutions, Operations, and Business Development, CompTIA

Eric Rood, Chief, California Department of Industrial Relations, Department of Apprenticeship Standards (DAS)

Wayne Sharp, Founder/President, MyVerse.com

Julie Su, Secretary, California Labor and Workforce Development Agency (LWDA)

Trisha Turlington, Senior Business Development Manager RHA, Red Hat

Kyle Trambley, California Governor's Office of Emergency Services (Cal OES)

Julie Whitten, Assistant Deputy Secretary of Innovation and Accountability, Government Operations Agency

Donna Woods, Instructor, CTE Cyber Academic Pathway, Canyon Springs High School/Moreno Valley Unified School District, CyberPatriot Teams Advisor/Coach

California Cybersecurity Integration Center (Cal-CSIC)

California Community Colleges (CCCs)

California Department of Education (CDE)

California Department of Technology (CDT)

California Division of Apprenticeship Standards (DAS)

California Governor's Office of Emergency Services (Cal OES)

California Government Operations Agency (GovOps)

California Interagency Advisory Committee on Apprenticeship (IACA)

California Labor and Workforce Development Agency (LWDA)

National Initiative for Cybersecurity Education (NICE)

The California State University (CSU)

The University of California (UC)

INTRODUCTION:

Faced with unemployment rates and economic conditions reminiscent of the Great Depression, we must get Californians back to work in high need, high wage essential professional jobs immediately. Curiously and simultaneously, many high paying tech jobs remain currently and critically unfilled in California cybersecurity fields (i.e. 72,000+ positions)[51] as well as many more in IT. Vigorous action today is necessary to prepare tomorrow's workforce in IT-Cyber specializations. Moving forward in a rapidly evolving digital and technological transformation, it is key to fill numerous and rapidly growing numbers of available tech and security positions. In an information-rich era, it is imperative to have a solid cadre of qualified and prepared IT-Cyber specialists and specialized workforce (from technicians through managers) with key skills and experience flowing regularly into the statewide labor pool.

In this strategy report, we seek to collaborate and develop a framework and template to help alleviate statewide IT-Cyber employment, workforce, economic, critical infrastructure, security objectives and concerns. This strategy paper examines an IT-Cyber pipeline/pathway apprenticeship model approach to enhance California workforce development and education capacities. We seek to answer the following questions in this report.

1. How do we design IT-Cyber career pipelines/pathways with an immense and thorough recruiting and outreach process to include all state residents; and focused on serving and driving upward social mobility for all?

2. How do we develop and implement a career pipeline with coordinated, comprehensive, seamless transitions from one level of the education process so that all students may access it through virtualization and digitalization?

3. Where are the critical "hands on" and vocational learning elements of IT-Cyber workforce development? How do we prepare a specialized IT-Cyber workforce to meet current Industry job minimum requirements and Knowledge, Skills, Abilities (KSAs) and professional competencies?

4. How do we get candidates the necessary educational preparation and work experience critical to getting the "big job" in the professional field?

5. How do we match prepared candidates with employers looking to hire in these fields with well-paying entry-level positions?

The most direct solution to these questions is the formation of an Essential Workforce Pre- and Registered Apprenticeship Talent Model and Pathway. This model has key short-medium-and long-term strategy components and implications that are discussed. One strategy report objective is linking education, workforce (and other components) together into a coordinated, seamless, and linked apprenticeship model culminating in qualified and prepared IT-Cyber workforce to serve

[51] (https://www.cyberseek.org/heatmap.html accessed electronically on 7.7.2020).

California. These "pipeline/pathway" strategies yield a highly trained and experienced IT-Cyber workforce with key skills ready for entry-level positions and moving the needle on getting the state back to work in the burgeoning "new-collar" economy.

A second CEWYA strategy report objective is a brief discussion of the scope and extent of California cybersecurity workforce development/education needs and capability/skills gaps. The *California Cybersecurity Workforce Development and Education Strategy* facilitates and coordinates a statewide pipeline/pathway at all levels of education (K-12, Associates, Bachelors, Graduate, and Professional Certifications). About 1/8 of all IT jobs (about 12-15%) are found in the specialized field of cybersecurity and we are currently experiencing significant workforce and skill capability gaps in both.

A third report objective is a discussion of various obstacles, limitations, and barriers found in IT-Cyber workforce development and education. It is important to understand these critical limitations and concerns so we can work collaboratively towards viable solutions. IT-Cyber workforce development issues currently confronting industry, public sector, and academic communities are profound. In some cases, these education concerns and workforce capability gaps/ skill shortages date back decades. However, pre-existing IT-cyber workforce and skill gaps are exacerbated by the further transformation to a digital and social media era.

While critical shortages of prepared and qualified IT-Cyber candidates existed before COVID 19, the pandemic response has only exacerbated already substantial and chronic workforce and skill shortages. Many students and employees today work and study remotely from home on unsecured (or under-secured) computers and networks. When conducting organizational business virtually at home, many are not working with usual workplace office IT and network security. These additional vulnerabilities and risks illustrate the ever changing and opportunistic nature of security concerns found in the transition to working/studying remotely.

IT-Cyber workforce needs for emergency responders, health, medical, life sciences, public safety/service and health officials, airlines, tourism/hospitality, small/medium sized business and other heavily impacted sectors is also concerning. Industry and employers (and "Essential Workforce") are impacted given quarantines, shelter in place orders, and potential customers staying at home. We face today the twin pressing concerns of growing IT-Cyber workforce development capacity/infrastructure shortages; further exacerbated by COVID-19 pandemic response/global supply chain and economic disruptions. These significant events themselves have in turn exposed additional cybersecurity threats and risks across the global economy; including vulnerabilities discovered in the new "work from home" workplace.

While we have many residents seeking jobs right now due to economic upheaval, there is simultaneously a large pool of well-paying and available positions in IT-Cyber to upskill, reskill, or begin to skill. Towards this objective, we lay out and discuss issues confronting IT-Cyber workforce development and education. These issues impact industry (employers public and private), the public sector (government), and Education/Higher Education communities. These obstacles are often similar and important commonalities for us to build on. The value here is in information sharing and building upon common purpose, goals, mission, and objectives. In this

way, we encourage and facilitate IT-Cyber education and workforce development coordination, collaboration, communication, better-informed partners, and stronger resulting partnerships.

What is the solution to a California cybersecurity workforce/capability/skill gap problem? We discuss specifics and details of solutions to include an IT-Cyber pre- and registered apprenticeship talent model at all levels of education. How do participants move through phases of the apprenticeship talent model from outreach/recruiting through education, work experience, and entry-level career positions? Through an IT-Cyber framework structure for career preparedness and college readiness programs and initiatives. Additional details found in the "Pre-Apprentice and Registered Apprenticeship Pacing Guide" near the end of this report. The IT-Cyber pacing guide describes the four-step pre- apprentice and registered apprenticeship pipeline process. For each step of the apprenticeship pathway process, we recommend key objectives, timelines, and milestones in the education/workforce development pathway.

In addition to the steps of the *California IT-Cyber Pre- and Registered Apprenticeship Talent Pipeline Model*, we include an IT-Cyber "Road-map" for related education and workforce development coordination, information, and planning purposes. An IT-Cyber Education Roadmap clearly describes all education and experience necessary to meet position minimum qualifications; knowledge, skills, abilities, and competencies for entry-level IT-Cyber employment in select occupations/related industry sectors. The Roadmap covers each level of education and provides a variety of recommendations to enhance all aspects of the talent pool. Some students may need degree programs and others certificate programs. Roadmaps provide the central hub and conduit for strategic communication so we can share and match prepared workers with hiring employers. Thus, we link IT-Cyber education program graduates with Industry (both public and private) to meet the needs of major stakeholders and key partners. However, before we get too far ahead on discussing potential workforce development and education solutions, we should provide relevant background to the matter at hand.

California Cybersecurity Workforce Development and Education Background:

There are 504,000 cybersecurity positions available in the U.S. and over 72,000+ in California. [52] Available cybersecurity positions are expected to continue and increase due to greater reliance on tech in COVID-19 pandemic emergency response as students and employees study/work remotely from home. As of 9.01.20, California has 712,052 positive cases and 13,163 deaths. [53] Essential public and private workforce concerns and COVID-19 emergency pandemic response, as well as pressing cybersecurity education and workforce development needs exist to justify the design, development, and implementation of a statewide comprehensive cybersecurity career education pipeline and pathway forthwith.

[52] (https://www.cyberseek.org/heatmap.html accessed electronically on 7.7.2020).
[53] California Department of Public Health, https://www.cdph.ca.gov/Programs/CID/DCDC/Pages/Immunization/ncov2019.aspx, Accessed electronically 9.3.2020.

The *California Cybersecurity Workforce Development and Education Strategy: Framework and Recommendations for a Career Pipeline and Pathway Project* objective is to prepare 50,000 entry-level IT-Cyber professionals over a 10 year time frame (2020-2030). This innovative and coordinated strategy was designed by the California Cybersecurity Task Force (CCTF) Workforce Development and Education (WDE) Subcommittee in collaboration and partnership with statewide public sector, industry, and education/higher education communities. In addition to cybersecurity education programs aligned, linked, and seamlessly transitioning from one segment to the next, we are also keenly interested in vocational/workforce preparation.

IT-Cybersecurity workforce development initiatives and projects are widely anticipated to have a significant role in the upcoming California economic recovery. Getting people skilled/reskilled/upskilled to work in high demand, well paying, and essential career positions is a key step in enhancing the state economy and improving the personal finances of participating candidates and their families. IT-Cyber is a "hands-on" professional field and prospective job candidates significantly benefit from registered apprenticeships, work experience, and On the Job Training (OJT) opportunities. Public and private sector employers greatly benefit from apprenticeship programs in many ways as discussed shortly.

The California Cybersecurity Task Force, WDE Subcommittee partners extensively with IT-Cyber employers (both public and private sector), Non Government Organizations (NGOs), Government agencies and organizations, and education/higher education communities. Collaboration and enhanced coordination exist in the following areas: model curriculum, academic standards, extra-curricular activities (like cyber competitions, coding camps), and vital workforce development opportunities (like pre- and registered apprenticeships).

Including all of these components (and others described in the pacing guide at the end of this document) to develop an efficient and comprehensive career pipeline is critical. CEWYA begins in the 5th/6th grade and continues through college readiness and career preparedness programs as consistent with California Career Technical education (CTE) programs in Middle and High Schools.

The smooth and efficient operation of a cybersecurity (and related) career education pipeline/pathway to support the California economy is timely and critical to meet the multi-faceted pandemic and related challenges to our workforce/employment talent pool, security, and society.

To enhance California Cybersecurity Workforce Development and Education Strategy, we include the *California Cybersecurity Essential Workforce Youth Pre- and Registered Apprenticeship Pipeline* component to balance and reinforce model curriculum/academic standards for IT-Cyber education programs, courses, and instructional content as well as workforce/career opportunities.

California Essential Critical Infrastructure Workers and Workforce:

The *California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Pipeline* supports Governor Newsom's March 19, 2020 Executive Order N-33-20 and State Public Health Officers' designated "Essential Critical Infrastructure Workers. [54]

Important to note that in a modern economy, all industry sectors have a direct link and connection tied to IT-Cyber. Tech is very pervasive in our lives and organizations today. Because of this nexus, we must coordinate and design clear pathways and pipelines for many different industry sectors; and provide a clear road map for cybersecurity education and workforce development opportunities that are accessible and available. We must provide guidance and advice for pathway students to navigate and onboard with "open high demand jobs" through workforce and education programs with professional experience opportunities to enhance economic and social mobility for all.

The following Industry Sectors are identified/included as "Essential Workforce."

1. Healthcare/Public Health-

2. Emergency Services Sector- (including Law Enforcement, Public Safety, and First Responders, and Public Works)-

3. Food and Agriculture-

4. Energy- (including Electricity Industry, Petroleum Workers, Natural and Propane Gas Workers)-

5. Water and Wastewater-

6. Transportation and Logistics-

7. Communications and Information Technology-

8. Other Community-Based Government Operations and Essential Functions-

9. Critical Manufacturing-

10. Hazardous Materials-

11. Financial Services-

12. Chemical-

13. Defense Industrial Base-

[54] (https://covid19.ca.gov/img/EssentialCriticalInfrastructureWorkers.pdf, Accessed electronically on 7/05/2020).

IT-Cybersecurity Workforce Development and Education Barriers, Obstacles, and Limitations:

Workforce Development Issues Addressed by Pre- and Registered Apprenticeships:

There are a variety of current barriers, obstacles, and limitations in current cybersecurity workforce development and education practices. These problems contribute in part to large numbers of available job openings and difficulty finding qualified talent to hire and onboard. Significant obstacles include accessible statewide cybersecurity education programs/courses; available workforce development/experiential learning opportunities; and diversity, inclusivity, and equity of special populations in IT-Cyber. Industry, the Public Sector, and Academic communities have common problems that require mutual solutions. However, each arm of the triangle has their own respective considerations to handle within their own sphere of activity as all have their own interests and objectives at the heart of their strategic activity.

Once we understand the underlying problems commonly associated with cybersecurity workforce development and education, we can work towards implementing solutions, both within each major stakeholders, but also holistically across the entire ecosystem. Solutions to cybersecurity workforce development and education are found when eliminating these barriers and limitations; and hence forms the basis of CEWYA project objectives found below. Clearly, workforce development opportunities like a pre- and registered apprenticeship programs will go a long way to address the following key capacity and supply side limitations and issues.

General Cybersecurity Workforce Development and Education Limitations:

Workforce barriers, obstacles, and limitations briefly described below:

IT-Cybersecurity crosses the public (across all levels of government) and private sectors (small, medium, large sized business); across all industrial and economic critical infrastructure sectors, and most occupations and professions found in an interconnected modern digital world.

IT-Cybersecurity is a very ubiquitous field. As tech is deeply ingrained everywhere in our organizational and individual lives, we all become tech specialists. We are behooved to start thinking like cyber professionals and safeguarding our computers, devices, data, networks, social media presence.

One key consequence of the pervasive presence of IT-Cyber is in many specializations, sub-fields, and numerous occupation clusters found in this field; from networking, mainframes, software design, database/cloud management, AI, programming, machine learning, augmented/virtual reality, hacking/pentesting, big data/analysis, and many others.

Education/Higher Education Obstacles:

In a recent white paper co-written by EdWeek and Cyber.org (formerly National Integrated Cyber Education Research Center – NICERC) and based on a nationwide survey of K-12 educators, several obstacles and trends that limited progress in cyber education were identified. [55] The most daunting of these is the situation identified in the paper as "cybersecurity deserts". This circumstance is characterized by an absence of business firms engaged in cybersecurity services delivery and/or an absence of Universities engaged in cyber education.

In California, it should be added that a contributing factor to cybersecurity deserts would be an absence of secondary school Career Technical Education programs in Information and Communications Technologies focused on cybersecurity since their existence is not necessarily dependent upon the presence of business firms and universities due to several successive years of funding from the state Career Technical Incentive Grant (CTEIG) starting in state fiscal year 2015-16 (see California Department of Education, CTEIG funding page.) [56]

The white paper also notes the absence of cybersecurity education taking place in undersized and high needs school districts and especially in high poverty rural districts where no cybersecurity resources exist. Other factors affecting the lack of cybersecurity education in the K-12 space include a lack of knowledge amongst faculty, students being unaware of educational and skill requirements for employment in cyber, and access to cyber education being "infrequent and uneven". Indeed, less than half of the 900 respondents in the survey reported that their district offered cybersecurity education. Worrying trends in the report show that learning about several key cyber-related topics like cyberterrorism, secure programming, secure networking, and hacking/data security is taking place significantly less often in high school versus middle school.

Additional Educational Barriers and Obstacles:

Coordinated alignment and linkage between cybersecurity industry (private/public sector) employer needed curriculum/skills with salient and accessible education/higher education programs (certificates, degrees) and courses.

Many entry and exit points available/needed to fulfill the workforce needs in the very diverse, ubiquitous, and specialized IT-Cyber profession and numerous sub-fields.

IT-Cyber is a "hands on" experiential "learn by doing" field. The role of work experience is essential for recruiting, hiring, and advancement in the field, particularly when discussing more technical and specialized IT-Cyber sub-fields.

[55] Cyber.org (NICERC) The State of Cybersecurity Education in K-12 Schools, (https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf, Accessed electronically on 7/18/20).

[56] California Department of Education, Career Technical Incentive Grant (CTEIG) Funding Years Timeline, (https://www.cde.ca.gov/ci/ct/ig/cteigtimeline.asp, Accessed electronically on 7/18/20).

One key limitation found in cybersecurity education and workforce development programs and workforce development opportunities is in coordination and information sharing functions. Coordination and communication are critical in any effective career pipeline/pathway and linked/aligned/articulated across multiple (or all) segments/levels of education.

Assuming the development of a vast series of cybersecurity education programs and courses and linked pre- and registered apprenticeship opportunities, how do we manage and administer and liaise between educational institutions (and students and faculty) and local employers in the field? We need an organized strategy and approach on how to initiate, maintain, and communicate with a strong network of statewide, regional, and local employers that serve as OJT providers, mentors, and ultimately the employers of successful pre- apprentices and registered apprentices at the end of the workforce development process.

Cybersecurity Workforce Development- Industry Obstacles, Barriers, and Limitations:

In terms of IT-Cyber workforce development and education, there are a variety of unique current barriers, obstacles, and limitations faced by industry (both public and private) employers in finding prepared/qualified professional employees.

The ideal cybersecurity program provides a balanced emphasis on what educational institutions teach with the current "in-demand" mastery of skills, knowledge, and abilities sought by public and private employers. Equilibrium and balance must be found somewhere here. This mix of education/industry/government needs implemented throughout education and workforce development pave the way for substantial growth in this multi-sector workforce. In other words, is what employers think needs to be taught in IT-Cyber what is actually taught in the classroom? If the answer is no—we have a significant problem here.

IT-Cyber are extremely dynamic professional fields given rapid changes in technology. Predicting future workforce capability and skills is a challenging task in newly emerging and rapidly evolving industry sectors and occupations.

Routine changing of necessary workplace skills and professional demands due to evolving security threats, risks, and vulnerabilities on a near daily basis require an emphasis on "life-long learning." It is more important to keep up with the current environment than static and dated knowledge, skills, and abilities that lose relevance over time. Always keeping up on timely new skills and knowledge is key to success in this profession.

There is a lack of understanding and resulting disconnect in industry HR recruiting, selection, and hiring of many IT-Cyber professionals. Significant steps must be taken to streamline and enhance this process so we can onboard greater numbers of newly minted cybersecurity professionals ready for work. While HR departments may do an excellent job hiring many classifications of employees, it is a much greater challenge when dealing with IT-Cyber fields. Writing job descriptions, recruiting diverse groups, and the interviewing process are examples of where the HR Department could enhance IT-Cyber hiring practices.

Today's cybersecurity job candidate must consider the quality of their educational background and substantial exposure to tech and computing (usually) at earlier ages than previous generations and excel in both their academic and vocational (career technical) achievements. Employers seek these qualities today.

The creation of many IT-Cyber career entry/exit points are necessary to prepare all segments and specializations within the talent pool. The entire talent model needs feeder programs to support the entire spectrum of prospective candidates seeking these positions. In this occupational cluster, some entry points are basic and lead to relatively unskilled entry-level positions. Candidates utilizing these entry points will need access to additional skills development and preparation to advance to the next level within the IT-Cyber field. Other segments of the entry-level talent pool need more complex, technical, perhaps programming heavy, specialized knowledge, and additional skills well beyond capabilities of most tech users. In any case, all segments of the talent pool must have clear road maps provided to direct them to education/experience needed for professional success in IT-Cyber.

Contrary to conventional and public misperceptions of cybersecurity, there are many non-technical positions such as in social engineering or privacy found within the large number of IT-Cyber based occupations. This indicates different strategies and workforce development/ education models must be utilized and encouraged to prepare all segments of the cyber talent pool.—technical or not. In addition, support must also be provided to assist IT-Cyber professionals across different industry sectors, types of organizations, and spanning the org chart from entry level to executive.

We must work towards strategies and ways to enhance diversity, inclusion, and equity in the IT-Cyber workforce. Education programs, workforce development opportunities, and mentoring of students are examples of these strategies to include new groups of students who may not have had access to these programs previously.

Concluding Thoughts on IT-Cyber Workforce Development/Education Barriers, Obstacles, and Limitations:

As one can see, there are many barriers, obstacles and limitations with current IT-Cyber workforce development and education challenges. Finding prepared cybersecurity professionals statewide is daunting with 72,000+ current available positions; robust future occupational growth outlook; and record numbers of baby-boomers retiring from the workforce monthly. These concerns point to significant employment challenges down the road. Given all barriers and obstacles to IT-Cyber workforce development and education, California needs a comprehensive strategy and innovative digital/technology initiatives to overcome potential limitations.

To help overcome these significant challenges, we are working on both a comprehensive long- term strategy (covering 2020-2030), as well as immediate steps, and short-term strategies, tactics, and actions to secure an enhanced and prepared IT-Cyber Essential Workforce moving forward into the future.

As such, we rely on two carefully linked California IT and cybersecurity workforce development and education strategies:

I. The *California Cybersecurity Workforce Development and Education Strategy: Framework and Recommendations for a Career Pipeline and Pathway Project*- (discussed under separate cover).

II. *California Cybersecurity Essential Workforce Youth Pre- and Registered Apprenticeship Pipeline (CEWYA)*

With Three Key Pillars:

I. IT-Cyber Education Programs at all levels of education.

II. Workforce Development Opportunities- Pre-Apprenticeships and Registered Apprenticeships across IT-Cyber employer/industry sectors and occupations.

III. Diversity, Inclusion, and Equity in IT-Cyber supporting all special populations into the field including: military-civilian transitioning, veterans, disabled veterans and their spouses; as well as historically underrepresented groups: including women, minorities, and those with physical/neurological differences.

Points of Emphasis (Contributed by Mario Perez, Professor, LA Mission College)

This proposed program emphasizes competitive job skills that are useful and employable.

The program aligns to the needs of the industry (both public and private sector).

The program provides value and outreach to the community.

Students are taught to think critically (also creativity, curiosity, inquisitive, passion).

California IT-Cyber Essential Workforce Pre- and Registered Apprenticeship Program Pipeline and Pathway (CEWYA) Objectives:

1. Enhance partnership and communications with key partners and major stakeholders of cybersecurity workforce development and education.

2. Build a coalition of interested public sector, industry, and education partners into a network of coordinated action on California cybersecurity workforce development and education.

3. Design, develop, and implement cybersecurity education programs, courses, and relevant content in coordination with major partners and key stakeholders to support the pre-apprenticeship and registered apprenticeship program pipeline/pathway.

4. Collect, analyze, and organize cybersecurity education Student Learning Objectives (SLOs) from middle school (6^{th} grade) through 4 year undergraduate degree programs and embedded stackable certificate programs in high need essential workforce specializations.

5. Establish and promulgate cybersecurity model curriculum and academic standards to support all phases of the pre-apprenticeship and registered apprenticeship pipeline education process.

6. Work with key partners and major stakeholders to develop competencies to support apprenticeship program Minimum Industry Training Criteria (MITC) for key high demand IT-Cyber occupations (linked to specific O*Net Classification codes and positions).

7. Outreach and relationship building with IT-Cyber employers and additional key industry sectors to develop employer-apprentice connections and provide available job positions.

8. Utilize California Cybersecurity Apprenticeship Centers on participating California Community Colleges, California State University, and University of California campuses to administer and manage employer-apprenticeship logistics, training, and coordination. Develop and implement education programs that meet the needs of their local workforce. Serve as liaison between employers and apprenticeship students, faculty, and staff.

9. Enhance diversity, inclusion, and equity of IT-Cyber and encourage the participation of students from traditionally disadvantaged backgrounds in the IT-Cyber Pre-Apprenticeship and Registered Apprenticeship Pipeline/Pathway Program.

10. CEWYA Program assessment and evaluation.

11. Link and align CEWYA with the NICE Cybersecurity Workforce Framework.

CEWYA Design Methodology and Development Process:

The California Cybersecurity Task Force (CCTF) Workforce Development and Education (WDE) Subcommittee consists of subject matter experts from California agencies/departments, the private sector (including small, medium, and large sized firms) and K-12 Education/Higher Education community. The California Department of Education (CDE) administers K-12 education statewide; and on the higher education side, campuses are drawn from California Community Colleges (116), California State University (23), and University of California (10).

As many in the workforce development and education professions know, the key to success is found in the facilitating collaboration and coordination among industry, government, and education/higher education communities. In other words, bringing prepared job candidates (i.e. with solid qualifications) together with firms looking to hire people with a particular set of skills/education/experience. Based on the variety of barriers, obstacles, and limitations found in this space, it is clear we have much to do to bring everyone together under one roof and handle these issues collaboratively.

Towards this end, the CCTF WDE Subcommittee initiated discussions in 2013 on the design and development of a comprehensive cybersecurity career education pipeline and pathway. Since 2017, the subcommittee generally met for monthly teleconferences, quarterly in person meetings at CCTF Quarterly Meetings and presentations. In addition, Subcommittee members have made many professional conferences, meetings, presentations across the state to support IT-Cyber and CEWYA design, development, and implementation phases. We have met in Northern, Southern, and Central California and draw on participants across the state.

Over the course of the career pipeline/pathway design and development process, we relied on the input and feedback of hundreds of participants. This includes assisting on the development of model curriculum, academic standards, and workforce development opportunities. Many participated because they are acutely aware that we need to increase our workforce capacity and build up these ranks. It is difficult to provide sufficient security and necessary vigilant posture over extended periods without sufficient staffing and full IT-Cyber teams. One clear element contributing to cybersecurity vulnerability and risk these days is not having enough qualified and prepared IT-Cyber personnel. In terms of organizational structure, workforce and capability gaps (shortages) found across all ranks and key positions in all our respective organizations is perhaps the ultimate obstacle here.

To address these various issues, the California Cybersecurity Workforce Development and Education Strategy acknowledges hundreds and hundreds of participants who contributed in some way to the objective of reducing critical IT-Cyber chronic workforce shortages. Please see Appendix 2 of that document for a comprehensive list of participants. One way in which many participants helped was in the design and development of statewide cybersecurity undergraduate model curriculum and academic standards process. The model curriculum and additional items are also found in the aforementioned report.

The Essential Prioritization of California Cybersecurity Workforce Development and Education Programs and Initiatives:

Due to great demand for current and future IT-Cyber workforce, we need to triage and take care of where the job demand is the highest and most essential. While COVID-19 has redefined how we work/study remotely from home, it have also shifted cyber threats and vulnerabilities to take advantage of increased remote access. We need prepared IT-Cyber professionals to handle the uptick in malicious activity. In terms of workforce development, we should play the numbers to expeditiously reduce critical statewide gaps. We begin with an understanding of where the jobs/opportunities exist in the cybersecurity enterprise.

When looking at the Cybersecurity Supply/Demand Heat Map, some interesting information pops out. Of the 72,123 available cybersecurity positions in California (according to Cyberseek) the majority of positions (43,056) or (60%) have job requirements that map to the "Operate and Maintain" category wand 37,758 positions map to "Securely Provision" from the NICE Cybersecurity Workforce Framework. [57] This demonstrates the complexity of a typical open position in cybersecurity, with each practitioner needing to master many workforce category skills. The cybersecurity workforce is malleable and flexible, and many positions map into multiple workforce categories.

In any case, if we concentrate our workforce development and education activities on building cybersecurity career education pipelines /pathways with aligned essential workforce pre- and registered apprenticeship opportunities—we need to focus on where the available positions are found to move the needle forward quickest. Please see the following table 1 (next page) listing NICE Cybersecurity Workforce Categories and California Cybersecurity Job Openings.

[57] (https://www.cyberseek.org/heatmap.html accessed electronically on 7.7.2020).

Table 1: California Job Openings/NICE Cybersecurity Workforce Framework Category:

NICE Framework Category	California Cybersecurity Job Openings (Cyberseek data)
Securely Provision (SP)	37,758
Operate and Maintain (OM)	43,056
Oversee and Govern (OV)	9,360
Protect and Defend (PR)	20,579
Analyze (AN)	9,971
Collect and Operate (CO)	4,719
Investigate (IN)	293

NICE Source: (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf) accessed electronically on 7.7.2020).

Cyberseek Source: (https://www.cyberseek.org/heatmap.html accessed electronically on 7.7.2020).

In order to maximize the efficiency and impact of California cybersecurity workforce development strategies and initiatives, we focus on NICE framework categories underlying the majority of available cybersecurity job openings. Two key NICE Framework work roles discussed below are where a majority of positions are currently available with demand expected to continue into the foreseeable future. If we focus on Securely Provision (SP) and Operate and Maintain (OM) NICE framework categories; we can make significant progress on reducing current California IT-Cyber workforce skills and capability gaps. It is important to note that Cyberseek data indicates many cybersecurity positions span multiple workforce framework categories. Again, with a statewide deficit of 72,000+ cybersecurity professional positions—when you analyze relevant NICE framework categories, we see many cybersecurity positions cross various workforce categories (i.e. positions falling into two or more categories).

NICE Framework Work Roles in Key Cyber Workforce Categories-

Securely Provision (SP)-

Authorizing Official/Designating Representative-
Security Control Assessor-
Software Developer-
Secure Software Assessor-
Enterprise Architect-
Security Architect-
Research and Development Specialist-
Systems Requirement Planner-
Systems Testing and Evaluation Specialist-
Information Systems Security Developer-
Systems Developer-

Operate and Maintain (OM)-

Database Administrator-
Data Analyst-
Knowledge Manager-
Technical Support Specialists-
Network Operations Specialist-
System Administrator-
Systems Security Analyst-

NICE Source: (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf accessed electronically on 7.7.2020).

Key Support: Security Operations Centers (SOCs) and IT-Cyber-Privacy Offices

Effective strategies to include "high demand" cyber workforce occupational roles is essential to reducing California IT-Cyber gaps and bolstering essential workforce development and job preparation numbers. In addition to preparing solid numbers of qualified candidates in these two categories, we discuss another key workforce development strategy in this report as related to Security Operation Centers (SOCs). We discuss these perspectives and innovations in this report section.

Today, many IT-Cyber functions are embedded in SOCs, Information Security Offices, and other IT-Security-Privacy Offices/Divisions. There are many types of valued work and vocational experience in today's modern information security layers. One great source of IT-Cyber employment and opportunities these days is working in SOCs found pervasively in the public and private sectors. Many companies, government agencies, and educational institutions already have them and more are in the "set-up" process. As SOCs are numerous and continuing to grow in importance, it would be a natural fit to include an educational track leading to employment here.

As the SOC is where a large source of available job positions exist in many geographical areas and multiple industry sectors (both public and private), this makes an excellent place to embed significant education program and workforce development opportunities. Pre-apprenticeship and registered apprenticeship opportunities can help support the IT-Cyber enterprise by serving a variety of roles during OJT to include time (even the briefest) in SOCs. (SOCs), Cyber Integration Centers (Cal CSIC) or other OP center is where we find cybersecurity technicians, research analysts, security engineers, and layers of management personnel. Rotating apprentices amongst technicians, analysts, engineers, and managers to support various IT-Cyber functions and roles could greatly benefit apprentice and employer.

In addition, we want to make sure pre-apprentices and registered apprentices have the opportunity to move around the organization a bit and see different aspects of the business. We want apprentices to understand the business model and its linkages to real-world business practices and process. It is important that apprentices have an opportunity to rotate about the organization and try new things from different departments and divisions. This of course with the caveat that

the needs of sponsoring employers is paramount and how various apprenticeships are structured is done in conjunction with participating prospective employers. In terms of IT-Cyber positions, they range all the way up the organizational chart through the C-Suite and executive decision makers.

***Important Note: It is also prudent to note that not all employers are going to be open and flexible with staffing in their SOCs/ISOs. We must make sure to have additional departments/areas for apprentices to secure their respective OJT hours.

Relevant Offices Often Include:

Information Security Office (CISO)- Public, Private Sector

Chief Information Office (CIO)- Public, Private Sector

Chief Technology Office (CTO)- Public, Private Sector

Privacy and Compliance Office (CPO)- Public, Private Sector

Cybersecurity Resiliency Services/Centers- Public, Private Sector

Cybersecurity Fusion/Threat Centers- Public Sector

California Cybersecurity Essential Workforce Youth Pre-Apprenticeship and Registered Apprenticeship Pipeline/Pathway Steps/Process:

Tech hubs enjoy engaged partnerships with industry and education community as vigorous workforce programs benefit career seekers and employers. However, our proposal delivers a comprehensive statewide youth apprenticeship strategy and framework to expand access to all Californians irrespective of geographical region or socio-demographic background.

STEP 1- Recruiting and Outreach: Wide and extensive outreach and recruiting activities at the front-end of the workforce development funnel. In this way, we can bring interested participants together to learn more about IT-Cyber education and workforce development programs and ways of getting involved in this career cluster. Outreach and recruiting efforts directed towards finding apprenticeship candidates, prospective employers, and participating educational institutions and campuses. All key partners and major stakeholders should work collaboratively for the CEWYA apprenticeship talent model pathway to function at peak efficiency and maximized utility.

Mentoring, support, encouragement, engagement activities at the state, regional, local, and neighborhood level of recruiting and outreach is essential. We must reach out on a neighborhood basis to attract and recruit talent that may not have been historically reached through tech recruiting and outreach. To accomplish recruiting and outreach objectives, it is essential to collaborate with NGOs and Not-for-Profit (NFP) community and youth organizations at the state, regional, local, and neighborhood levels. Furthermore, as all jobs and educational institutions serve local areas, we must be prepared to conduct significant outreach and recruiting initiatives within our communities and neighborhoods to attract talent into the IT-Cyber workforce and apprentice pool.

With major stakeholders (including industry and employers) involved in ongoing and continuous recruiting and outreach, we are in business so to speak. At this point, we would have interested apprenticeship pathway students, employers that are seeking to hire and train workforce, and educational institutions offering numerous IT-Cyber academic programs. The next step in this process is to enroll students, employers, and schools together into the California Cybersecurity Pre-Apprenticeship Program.

STEP 2- California Cybersecurity Pre-Apprenticeship Program-

We include the following components into the Pre-Apprenticeship phase of the CEWYA talent model. Education programs and certifications (both academic and vocational) will make up the formal classroom/learning component of Related Teaching and Instruction (RTI). In addition, there is a recommended pre-apprenticeship On the Job Training (OJT) 40-50-hour commitment that ideally would occur several months during summer break. More details on OJT and RTI are found on the IT-Cyber pacing guide (in several pages.)

Education Programs (RTI) Classroom Component-

Numerous Career Technical Education (CTE) Certification Programs- (see pacing guide)

Aligned Pre-App Workforce OJT- (40-50 hour target range)

Propose 48 hour Pre-App OJT- 12x4 hour: summer/school year

Coordinated by California Cybersecurity Apprenticeship Centers on participating campuses.

Cyber Competitions- link and align closely for students interested in participating.

Cyber- Hygiene and Awareness- Helping students stay aware and safe while computing.

STEP 3- California Cybersecurity Apprenticeship Program-

When effective at recruiting and retaining students, employers, and schools into the IT-Cyber pre-apprenticeship program, and as students complete the program, they need to transition into registered apprenticeship programs. Students will now generally be high school students

Education Programs (RTI) Classroom Component- Remote Delivery

Numerous 2-year and 4-year Cybersecurity Degree and Stackable Certificate Programs.

FALL 2020 Essential Workforce Priority-

Cybersecurity Generalist- Supporting Small and Medium Sized Business

Cybersecurity for Life-Sciences (including BioTech, Health/Medical)

Aligned Registered Apprenticeship Workforce OJT- (20 hour apprentice orientation, 1980 hours OJT)

Cyber Competitions

Cyber- Hygiene and Awareness

STEP 4- Employer Based on the Job Training-

Model Industry Training Competencies (MITC) development and promulgation for high-demand cybersecurity occupations. For example, Cyber Analyst is in demand from both the public and private sectors. A specific registered apprenticeship program track must be developed to meet such high-demand cybersecurity occupations.

CEWYA PROCESS DETAILS:

PHASE 1- RECRUITMENT AND OUTREACH PROCESS

Work with local state and workforce development boards; economic development groups; industry and trade groups, community and neighborhood groups, not-for profits.

Public Service Announcement (PSAs) Campaign

Cyber Competitions Linkage

Cyber- Hygiene and Awareness Component

PHASE 2- California Cybersecurity Pre-Apprenticeship Program-

Education Programs and Certifications

Workforce Development Opportunities and OJT

Cyber Competitions Linkage

Cyber- Hygiene and Awareness Component

PHASE 3- California Cybersecurity Registered Apprenticeship Program-

Education Programs and Certifications

Workforce Development Opportunities and OJT

Cyber Competitions Linkage

Cyber- Hygiene and Awareness Component

PHASE 4- Employer Based on the Job Training-

Cyber Competitions Coach/Mentor

Cyber- Hygiene and Awareness Component

Developing Business Model/Process/Skills

***additional notes- these phases are described in further details below in the CEWYA pacing guide. The pacing guide visually illustrates the steps in the process by which individuals would travel all the way through the pre- and registered apprenticeship talent pipeline. Students start out in the recruitment and outreach phase for IT-Cyber and then provided education and workforce development opportunities all the way through the career pipeline/pathway. When students have

completed the education components, they are moved into workforce development opportunities to get them working upon the completion of their 2000 hour on the job training.

*** It is important to keep in mind throughout all stages of the process, we focus on diversity, inclusivity, and equity. We want to even the playing field for IT-Cyber education and workforce development opportunities for all residents across California.

California Pre- and Registered Apprenticeship Pacing Guide:

There are several key assumptions made when discussing education and workforce development pacing guides. The first is that industry recognized certificate programs and other educational programs are a key step in the apprenticeship process. Therefore, a good part of the talent pool is going to secure these certifications on their way to OJT and into the workforce.

Second, California vocational education is "Career Technical Education" (CTE) begins in the Seventh Grade, continues through high school and into the community college system. Given these key assumptions, we provide a basic pacing guide (below) describing the timing and manner in which students progress through a IT-Cyber youth Pre-Apprenticeship and Registered Apprenticeship talent pipeline/pathway.

Third, a segment of the IT-Cyber talent pool is going to need more higher education and less focus on workforce development. As many say, "college begins in middle school." This staying recognizes the common understanding that academic preparation for college and success begins (and heavily reinforced) in middle school years. Good study habits, solid academics, and knowledge/skills are developed in middle school for further advanced study in high school and the college/university. Academic and literacy skills are essential and we do not wish to leave them out of pacing guides for IT-Cyber Pathway students/apprentices.

5th-6th Grade: In advance of CTE vocational education, we administer a variety of professional/ career awareness/interest/psychomotor skills tests. Students with STEM/STEAM interests are introduced and encouraged to participate in the IT-Cyber Pre-Apprenticeship Program Pathway. In addition, we enhance support for related computer science, information communications technology, digital media, and related pursuits. This is also a key age to familiarize students with extracurricular activities including cybersecurity competitions, coding camps, hackathons, etc.

PRE-APPRENTICESHIP PHASE

7th Grade: Year 1 Cybersecurity Certificate Program Course

8th Grade: Year 2 Cybersecurity Certificate Program Course

9th Grade: Year 3 Cybersecurity Certificate Program Course

PRE-APPRENTICESHIP PHASE AND RECOMMENDATIONS

Complete 1st CTE Cybersecurity Certification Program/

Certificate Award and Digital Badging

Completion of Pre- Apprenticeship RTI

Completion of CompTIA IT Fundamentals+ Certificate Program and Exam

Summer after Freshman Year- 40-50 hours Pre Apprenticeship OJT

Cyber Competitions Alignment

Cyber- Hygiene and Awareness Component-

REGISTERED APPRENTICESHIP PHASE

10th Grade: Year 1 Cybersecurity Certificate Program Course

11th Grade: Year 2 Cybersecurity Certificate Program Course

12th Grade: Year 3 Cybersecurity Certificate Program Course

REGISTERED APPRENTICESHIP PHASE AND RECOMMENDATIONS

Complete 2nd CTE Cybersecurity Certification Program/

Certificate Award and Digital Badging

Completion of Registered Apprenticeship RTI

Completion of CompTIA IT Network+, Security+

(or, other relevant training certifications, CISCO Networking for example)

Summer after Senior Year- Begin Apprenticeship OJT

Career Readiness and College Preparedness Tracks-

Cyber Competitions Alignment

Cyber- Hygiene and Awareness Component-

*****Transfer to California Community College, California State University, or University of California campuses upon completion of high school graduation requirements and campus admissions standards.**

RELATED HIGHER EDUCATION PROGRAMS

California Community Colleges- Computer Science-IT-Electrical/Computer Engineering-Cybersecurity Degrees and Certificates

California State University- Computer Science-IT- Electrical/Computer Engineering-Cybersecurity Degrees and Certificates

University of California- Computer Science-Electrical/Computer Engineering-Cybersecurity Degrees and Certificates

Private College/Universities: Computer Science-IT- Electrical/Computer Engineering-Cybersecurity Degrees and Certificates

CEWYA MODEL IT- CYBER PACING GUIDE MILESTONES AND RECOMMENDATIONS

CEWYA PRE-APPRENTICESHIP LEVEL: (Middle School/High School)

By the time a student has completed the IT-Cyber pre-apprenticeship level of the CEWYA pipeline process, they should have fulfilled the various components discussed below:

1. CAREER TECHNICAL EDUCATION (CTE) PROGRAM CURRICULUM COMPONENT:

(Select one that corresponds to skill and experience level; in part identified by the psycho-metric/career/professional interests testing taken in 5^{th}/6^{th} grade). We assume that most students will fit well into either the Exploring or Essentials Certificate Program; and we do not want to hold advanced learners back if they have exceptional skills, talent, and/or experience.

Exploring Cybersecurity Certificate Program- (ICT-Basics & Fundamentals)

Essentials of Cybersecurity Certificate Program- (ICT-Intermediate)

Advanced Cybersecurity Certificate Program- (ICT- Advanced skills).

***design notes: High School Courses: We design one course from each sequence as a CTE-Curriculum Integrated Course: ("A-G" Requirements like math, English Language Arts, science course, etc.); and one course dual enrollment- high school/college credit) to make for efficient utilization of the curriculum here.

*** design notes: in addition to securing a CTE Pre-Industry Recognized Certification, students can complete IT-Cyber recognized professional courses, exams, and certifications as well. At the pre-apprenticeship level, we are generally working on the foundational courses to complete the actual certification and exam around the time of high school graduation.

2. IT-CYBER INDUSTRY RECOGNIZED CERTIFICATION COMPONENT: (PRE-APP)

In addition to CTE education programs above, we recommend pre-apprentices to complete industry recognized certification programs as a baseline for more advanced certification work at the CEWYA Apprenticeship pathway stage. It is key to start IT-Cyber pathway participants with fundamentals (in middle school) or as early as possible. We recommend completion of CompTIA IT Fundamentals course (vendor neutral) or related basic course/certificate for IT-Cyber pre-apprenticeship students (ideally in the 7th to 9th grade band).

PREAPPRENTICESHIP CERTIFICATION/COURSES/TRACKS:

IBM-

Pre-Apprentice Security Program-

CompTIA-

IT Fundamentals (ITF+)- (Pre-App) (vendor neutral certification, and serves as foundation course before many vendor specific offerings)

CISCO, Networking Academy CCNA:

Get Connected (Pre App)

IT Essentials (Pre App)

Introduction to Networks (Pre-App)

Palo Alto Networks-

Cybersecurity Essentials (Network Security Essentials) (Pre-App)

Red Hat/Linux- Red Hat Academy-

Fundamentals of Red Hat Enterprise Linux (Pre-App)- leading to Systems Administration 1 at the Apprenticeship level)

3. PROGRAMMING/CODING COMPONENT MILESTONES: (PRE-APP)

(for more technical types of programs)

Exploring IT-Cyber Program (Basic): Scratch- (basic principles/foundations)

Getting started with Raspberry Pi, Arduino

Essentials IT-Cyber Program (Intermediate): Python, Java

Advanced Projects- Raspberry Pi, Arduino

Advanced IT-Cyber Program (Advanced): Python, HTML, Javascript, C++

4. ESSENTIAL EMPLOYABILITY “SOFT SKILLS”: (PRE-APP)

- Problem Solving
- Collaboration/Team Work
- Critical Thinking/Analytical Skills/Attention to Detail
- Adaptability/Ability and willingness to learn new skills
- Communication Skills

5. ON THE JOB TRAINING COMPONENT: (PRE-APP)

All pre-apprenticeship students should complete a 48-50 hour OJT experience at a public, private, or non-profit organization upon completion of the education and certification program requirements. It is understood these students would have minimal exposure to employer security activities, but would rather benefit from their first general work experience in the IT-Cyber space. The rate of pate in 2020 should start at $15/hour. We want to instill upon our CEWYA students the understanding that NO ONE in the IT-Cyber fields makes minimum wage. Ever. Even as freshman or sophomores in high school.

6. CYBER-HYGIENE AND AWARENESS: (PRE-APP)

Cyber hygiene- staying safe online.

Cyber awareness- being aware and prepared.

Cyber resiliency- quick response, recovery, and continuity in the event of a cyber incident or breach.

CEWYA APPRENTICESHIP LEVEL MODEL (High School)

By the time a student has completed the IT-Cyber apprenticeship level of the CEWYA pipeline process, they should fulfill the various components discussed below at approximately the same time as graduation from high school.

1. CAREER TECHNICAL EDUCATION (CTE) PROGRAM CURRICULUM COMPONENT:

(Select one that corresponds to skill and experience level; in part identified by the psycho-metric/career/professional interests testing taken in $5^{th}/6^{th}$ grade). We assume that most students will fit well into either the Exploring or Essentials Certificate Program; and we do not want to hold advanced learners back if they have exceptional skills, talent, and/or experience.

Exploring Cybersecurity Certificate Program- (ICT-Basics & Fundamentals)—[hopefully completed as a PRE-APP already)

Essentials of Cybersecurity Certificate Program- (ICT-Intermediate)—[following the pathway pacing guide, most high school students would move from pre-app program into this skill/experience level]

Advanced Cybersecurity Certificate Program- (ICT- Advanced skills)-- following the pathway pacing guide, a good number of high school students would move from pre-app program into this skill/experience level]

***design notes: High School Courses: We design one course from each sequence as a CTE-Curriculum Integrated Course: ("A-G" Requirements like math, English Language Arts, science course, etc.); and one course dual enrollment- high school/college credit) to make for efficient utilization of the curriculum here.

Cybersecurity and Public Service/Safety Certificate Program- (ICT and Public Service/Safety CTE Sectors)-

Cybersecurity and Digital Forensics Certificate Program-

Cybersecurity Competition and Leagues Certificate Program-

Women in Cybersecurity Certificate Program-

Cybersecurity for Underserved Backgrounds Certificate Program-

2. IT-CYBER INDUSTRY RECOGNIZED CERTIFICATION (APP) COMPONENT:

In addition to the CTE education programs above, we would recommend to have pre-apprentices complete the following industry recognized certification programs as a baseline for more advanced certification work at the Apprenticeship stage of the CEWYA pipeline.

APPRENTICESHIP CERTIFICATIONS/COURSES/TRACKS:

CompTIA-

A+ Course and Certification-

Network+ Course and Certification-

Security+ Course and Certification-

CISCO, Networking Academy

CCNA: Introduction to Networks Course

CCNA: Switching, Routing, and Wireless Essentials Course

CCNA7: Enterprise Networking, Security, and Automation

Cisco Certified Network Associate (CCNA) Exam

Palo Alto Networks- Completion of 3 course sequence= PCCSA Cert

Cybersecurity Essentials (Network Security Essentials) (Pre-App)

Cybersecurity Gateway (Network Security Fundamentals) Course (APP)

Cybersecurity Foundations (Introduction to Cybersecurity) Course (APP)

Palo Alto Networks Certified Cybersecurity Associate (PCCSA)

Red Hat/Linux- Red Hat Academy

Red Hat Systems Administration 1- Course

Preliminary Exam in System Administration (leads to a student certification ID)

Red Hat Systems Admin 2- Course

Leads to the Red Hat Certified System Administrator Exam

3. PROGRAMMING/CODING (APP) COMPONENT MILESTONES:

The more technical and specialized cybersecurity professionals are going to need some programming/coding experience. This is not to say that all cybersecurity and privacy positions or professionals necessarily need these skills. However, a solid background and some experience here will unlock a variety of interesting and exciting opportunities for those with these useful and employable skills.

Exploring IT-Cyber Program (Basic): Scratch- learning the basic principles/foundations:

Getting started with Raspberry Pi, Arduino

Essentials IT-Cyber Program (Intermediate): Python, Java

Raspberry Pi, Arduino

Advanced IT-Cyber Program (Advanced): HTML, Javascript, C++

4. ESSENTIAL EMPLOYABILITY "SOFT SKILLS (APP) COMPONENT-

- Problem Solving
- Collaboration/Team Work
- Critical Thinking/Analytical Skills/Attention to Detail
- Adaptability/Ability and willingness to learn new skills
- Communication Skills

5. ON THE JOB TRAINING (APP) COMPONENT:

All apprentices complete a 2000 hour OJT experience at a public, private, or non-profit organization upon completion of education and certification program requirements. It is understood these students would have exposure to significant employer security activities because of completion through the certification/course sequence: The rate of pay should start at $15/hour (2020). We want to instill upon CEWYA students the understanding that NO ONE in the IT-Cyber fields makes minimum wage. Ever. Even as freshman or sophomores in high school.

6. CYBER-HYGIENE AND AWARENESS: (APP)

Cyber hygiene- staying safe online.

Cyber awareness- being aware and prepared.

Cyber resiliency- quick response, recovery, and continuity in the event of a cyber incident or breach.

CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT (POST-HIGH SCHOOL)

IT-Cyber spans many economic sectors, industries, and occupations. To meet these needs, students are going to have two options to prepare themselves after high school graduation.

OPTION A: CAREER READINESS- For students who have completed all recommendations of the pre-apprentice and registered apprenticeship level pipelines, they are cleared to perform their 2000 hour OJT with participating employers. Once completed with the education component and OJT—they should be prepared for entry-level IT-Cyber positions in public/private sectors.

OPTION B: COLLEGE PREPAREDNESS- For students who complete all recommendations of the pre-apprentice/registered apprenticeship pipelines, they are cleared to perform 2000 hour OJT with participating public and private sector employers. However, some students may prefer the college track. These students will complete the following IT-Cyber Education programs with select programs having a registered apprenticeship 2000 hours OJT.

IT-Cyber Education Programs:

Computer Science Associate Transfer Degree Program (California Community College)

Information Technology Model Curriculum Degree Program (California Community College)

Bachelors of Science in Cybersecurity Degree Programs (STEM based)- Design/Develop

Dual Baccalaureate Degree Program in Cybersecurity (Interdisciplinary with Registered Apprenticeship with 2000 hour OJT)- Design/Develop

Cybersecurity Professional Certifications (w/ linked registered apprenticeship 2000 hour OJT)

Cybersecurity Academic Certifications

Apprenticeship Programs:

OPTION 1: 2000 Hours OJT- Completed in conjunction with 2-year degrees and certificate programs at California Community Colleges.

OPTION 2: 2000 Hours OJT- Completed in conjunction between 2-year and 4-year degree and certificate programs at California Community Colleges and California State Universities/University of California participating campuses:

Lower Division OJT- 1000 hours- California Community College campuses

Upper Division OJT- 1000 hours- CSU/ UC campuses.

*** Important note: Pipeline registered apprentices administered and managed at California Cybersecurity Centers at participating public and private colleges/universities.

CERTIFICATE DESIGN/DEVELOPMENT LIST TO IMPLEMENT CEWYA

I. Implement 8 Cybersecurity Industry Recognized Certification for middle/high school students (three course sequences each for certificate completion= 24 "new" courses):

Middle School Cybersecurity Career Technical Education (CTE) Industry Recognized Pre-Certification Programs:

1. Exploring Cybersecurity Certificate Program- (ICT-Basics & Fundamentals)

2. Essentials of Cybersecurity Certificate Program- (ICT- Intermediate skills-link with Internship/Community Service hours requirements, possible industry certifications per below).

High School Cybersecurity Career Technical Education (CTE) Industry Recognized Pre-Certification Programs:

Exploring Cybersecurity Certificate Program- (ICT-Basics & Fundamentals)

Essentials of Cybersecurity Certificate Program- (ICT- Intermediate skills-link with Internship/Community Service hours requirements, possible industry certifications per below).

Creation of Cybersecurity Industry Recognized Pre-Certification for high school students (three course sequences each for certificate completion= 15 "new" courses):

3. Advanced Cybersecurity Certificate Program- (ICT- Advanced skills-link with Internship/Community Service hours requirements, definite industry certifications per below).

4. Cybersecurity and Public Service/Safety Certificate Program- (ICT and Public Service/Safety)- Formation of academy and industry certifications and work in conjunction with other agencies/organizations to implement. Work in conjunction with California Public Safety and Service Academies to develop digital forensics/eCrimes courses/ and related pre-industry certifications.

5. Cybersecurity and Digital Forensics Certificate Program- (ICT and Public Service/Safety)- Formation of academy and industry certifications and work in conjunction with other agencies/organizations to implement. Work in conjunction with California High Schools and Public Safety and Service Academies to develop digital forensics/eCrimes courses/ and related pre-industry certifications.

6. Cybersecurity Competition and Leagues Certificate Program- (ICT/other sectors)- support cybersecurity students, teams, and coaches in cyber competitions. Recruit and work to build skills and tools at the novice level and advance to veteran cybersecurity competitor. Preparation for high school and collegiate division cyber competitions. Digital Badging for participants and for completion.

7. Women in Cybersecurity Certificate Program- Support, encourage, and prepare girls and women for careers and opportunities in the IT-Cyber enterprise. Detailed understanding of the field, different career pathways, strategies and best practices to education programs and workforce opportunities. Emphasize career preparation, hiring/selection, how to secure positions in the field, retention, promotion and career success. Mentoring and peer group work on individual strategies to chart for success in the IT-Cyber Profession.

8. Cybersecurity for Underserved Backgrounds Certificate Program- Support, encourage, and prepare students from undeserved backgrounds for careers and opportunities in the IT-Cyber enterprise. Detailed understanding of the field, different career pathways, strategies and best practices to education programs and workforce opportunities. Emphasize career preparation, hiring/selection, how to secure positions in the field, retention, promotion and career success. Mentoring and peer group work on individual strategies to chart for success in the IT-Cyber Profession.

K-12 CYBERSECURITY (CTE) INDUSTRY RECOGNIZED CERTIFICATE PROGRAMS/ LIST OF COURSES TO DEVELOP:

To ensure all potential student/learner skill needs/levels are met through the California Cybersecurity Essential Workforce Pre- and Registered Apprenticeships Education process, we recommend the development of K-12 CTE Industry Recognized Certificate Programs. Each certificate program (8) consists of 3 course sequences. All courses digitized, virtualized, and available online/cloud-based to students across California. We anticipate building 2 certificate programs an academic year over a 4 year time period.

1. Exploring Cybersecurity Industry Recognized Certification Program:
Introduction course: Introduction to Cybersecurity Understanding and Awareness
Connector course: Foundations of Cybersecurity
Capstone course: Cybersecurity Skill and Projects

2. Essentials of Cybersecurity Industry Recognized Certification Program:
Introduction course: Cybersecurity Principles and Fundamentals
Connector course: Cybersecurity Tools, Skills, and Lab
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

3. Cybersecurity Advanced Bridge Industry Recognized Certification Program:
Introduction course: Advanced Cybersecurity Essentials
Connector course: (select 1 from below)
Advanced Cybersecurity Tools, Skills, and Lab
Professional Certification Course (w/ vouchers for students to test for free)

Capstone course: (select 1 from below)
Cybersecurity Mentoring, Apprenticeship, and Internship Professional Development
[Cybersecurity Apprenticeship/Pre-Apprenticeship Preparation]/
Professional Certification Course (w/ vouchers for students to test for free)

*****students in this program will be able to complete up three certifications in advance of high school graduation depending on the courses/track they selected.**

4. Cybersecurity Competition Industry Recognized Certificate Program:
Introduction course: Introduction to Cybersecurity Competitions
Connector course: Cybersecurity Competitions Tools, Skills, and Lab
Capstone course: (select 1 from below)
Cybersecurity Competition Leadership and Management
Professional Certification Course (w/ vouchers for students to test for free)

5. Cybersecurity-Public Service/Safety Industry Recognized Certificate Program:
Introduction course: Introduction to Cybersecurity and Public Service/Safety
Connector course: Cybersecurity/Public Safety Tools, Skills, and Lab
Capstone course: (select 1 from below)
Cybersecurity in Public Service/Safety
Professional Certification Course (w/ vouchers for students to test for free).

6. Cybersecurity-Public Service/Safety Digital Forensics-Investigation Certificate Program:
Introduction course: Introduction to Cyber Digital Forensics and Investigations
Connector course: Digital Forensics and Investigations Tools, Skills, and Lab
Capstone course: (select 1 from below)
Digital Forensics in Public Service/Safety
Professional Certification Course (w/ vouchers for students to test for free).

7. Women in Cybersecurity Certificate Program:
Introduction course: An Introduction to Girls and Women in Cybersecurity
Connector course: Tools, Skills, and Projects for Success in Cybersecurity
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

8. Cybersecurity for Underserved Backgrounds Certificate Program:
Introduction course: An Introduction to the Exciting World of Cybersecurity
Connector course: Tools, Skills, and Projects for Inclusivity in Cybersecurity
Capstone course: Professional Certification Course (w/ vouchers for students to test for free).

Concluding Thoughts: Closing the Barriers, Obstacles, and Challenges of the Apprenticeship Model of Workforce Development:

We appreciate our education system and schools for teaching key academics and knowledge in student preparation for both the college and career preparedness tracks respectively. We also appreciate the role of industry on describing their workforce needs and capabilities so the education/higher education community can develop appropriate curriculum, academic standards, programs, courses, and content. This report previously discussed a variety of limitations related to the coordination of education/industry communities and related concerns on the transmission of relevant skills and competencies in the IT-Cyber space.

There are obstacles and challenges facing workforce development and apprenticeship strategies in IT-Cyber to address. It is true that many assume the apprenticeship "vocational model" to be an enlightened European approach to traditional training for traditional "blue and white collar" employment in public and private sector "high need" occupations and industries. These are some issues to face as we advance the apprenticeship vocational model as an increasingly viable and important source of innovative digital workforce development.

REFERENCES:

California Department of Education, Career Technical Incentive Grant (CTEIG) Funding Years Timeline, (https://www.cde.ca.gov/ci/ct/ig/cteigtimeline.asp, Accessed electronically on 7/18/20).

California Department of Public Health, (https://www.cdph.ca.gov/Programs/CID/DCDC/Pages/Immunization/ncov2019.aspx, Accessed electronically 7.16.2020).

California Essential Workforce Sectors, https://covid19.ca.gov/img/EssentialCriticalInfrastructureWorkers.pdf Accessed electronically on 7/05/2020).

Cisco Networking Academy, (https://www.netacad.com/ Accessed electronically on 8/17/2020).

CompTIA, (https://www.comptia.org/home Accessed electronically on 8/17/2020).

Cyberseek, (https://www.cyberseek.org/heatmap.html Accessed electronically on 7.7.20200.

Cyber.org (NICERC) The State of Cybersecurity Education in K-12 Schools, (https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf, Accessed electronically on 7/18/20).

NICE Cybersecurity Workforce Framework, (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf accessed electronically on 7.7.2020).

Palo Alto Networks, (https://www.paloaltonetworks.com/services/education accessed electronically on 8.17.2020).

Red Hat, https://www.redhat.com/en/services/training/red-hat-academy?sc_cid=701600000011vjtAAA accessed electronically on 8.17.2020.

Wikipedia, https://en.wikipedia.org/wiki/Economy_of_California, Accessed electronically 7.18.2020.

APPENDIX 3- All Abbreviations

ABBREVIATIONS

Academic Senate for California Community Colleges (ASCCC)
Academic Senate for the California State University (ASCSU)
Academic Year (AY)
Amazon Web Services (AWS)
Artificial Intelligence (AI)
Associate Degree Transfer Program (ADT)
Association for Computing Machinery (ACM)
Bachelors of Science Degree Program (B.S.)
Bay Cyber League (BCL)
California Apprenticeship Initiative (CAI)
California Community Colleges (CCC)
California Community College Chancellor's Office (CCCCO)
California Cybersecurity Institute (CCI)
California Cybersecurity Integration Center (Cal-CSIC)
California Cybersecurity Task Force (CCTF)
California Department of Education (CDE)
California Department of Industrial Relations (DIR)
California Department of Technology (CDT)
California Division of Apprenticeship Standards (DAS)
California Education Institution Threat Assessment Center (CEITAC)
California Essential Workforce Pre-and Registered Apprenticeship Pipeline Talent Model (CEWYA)
California Government Operations Agency (GovOps)
California Governor's Office of Business and Economic Development (GO-Biz)
California Governor's Office of Emergency Services (Cal OES)
California Labor and Workforce Development Agency (LWDA)
California Longitudinal Pupil Acheivement Data Systems (CALPADS)
California State Threat Assessment Center (STAC)
California State University (CSU)
California State University (CSU) Professional and Continuing Education (PaCE)
California Workforce Development Board (LWDA)
Career Technical Education (CTE)
Career Technical Incentive Grant (CTEIG)
Centers of Academic Excellence (CAE)
Chief Information Officer (CIO)
Chief Information Security Officer (CISO)
Chief Privacy Officer (CPO)
Chief Technology Officer (CTO)
City College of San Francisco (CCSF)
Computer Science (CS)
Continuing Education Unit (CEU)
Critical Infrastructure Protection (CIP)
Career Technical Education Incentive Grant (CTEIG)
Course Identification Descriptor (C-ID)

C-ID's Intersegmental Curriculum Workgroup (ICW)
Colton-Redlands-Yucaipa Regional Occupation Program (CRY ROP)
Cybersecurity and Infrastructure Security Agency (CISA)
Department of Defense (DOD)
Department of Homeland Security (DHS)
Disabled American Veterans (DAV)
Doctorate of Philosophy (Ph.D.)
Emergency Operations Center (EOC)
Ernst & Young (EY)
Faculty Discipline Review Groups (FDRG)
Federal Education Records Protection Act (FERPA)
General Education (GE)
Health Insurance Portability and Accountability Act (HIPAA)
Information Communication and Technology (ICT)
Information Communication and Technology and Digital Media (ICT-DM)
Internet of Things (IOT)
Information Security (IS)
Information Security Analyst (ISA)
Information Technology (IT)
Information Technology and Information Systems (ITIS)
Knowledge, Skills, Abilities (KSA)
Learning Management System (LMS)
Los Angeles Unified School District (LAUSD)
Machine Learning (ML)
Massive Open Online Courses (MOOC)
Master of Fine Arts (MFA)
Model Transfer Curriculum (MTC)
National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE)
National Centers of Academic Excellence in Cyber Defense 2-Year Education (CAE-2Y)
National Centers of Academic Excellence in Cyber Defense Research (CAE-R)
National Integrated Cyber Education Research Center (NICERC)
National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology (NIST)
Non-Government Organizations (NGO)
Nonprofit Organizations (NPO)
On the Job Training (OJT)
Professional and Continuing Education (PaCE)
Professional Science Masters Degrees (PSM)
Public Services (PS)
Rear Admiral (RADM)
Regional Occupation Program (ROP)
Registered Apprenticeship Programs (RAP)
Related and Supplemental Instruction (RSI)
Retired (RET)
Return on Investment (ROI)
Security Operations Center (SOC)

Science, Technology, Engineering, Arts, Mathematics (STEAM)
Science, Technology, Engineering, Mathematics (STEM)
Student Learning Objectives (SLOs)
Subject Matter Expert (SME)
U.S. Bureau of Labor Statistics (BLS)
United States Department of Homeland Security (DHS)
United States Department of Labor (USDOL)
United States National Security Agency (NSA)
University of California (UC)
University of California Curriculum Integration (UCCI)
University of California Office of the President (UCOP)
Western Academy Support and Training Center (WASTC)
Workforce Development and Education (WDE)

30