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 9, 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 5th/6th 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

Executive Summary 2
Contents 3
Acknowledgements 5
Introduction 7
California Cybersecurity Workforce Development and Education Background.. 9
California Essential Critical Infrastructure Workers and Workforce 11
IT-Cybersecurity Workforce Development and Education Barriers, Obstacles, and Limitations.. 12
Workforce Development Issues Addressed by Pre- and Registered Apprenticeships 12
General Cybersecurity Workforce Development and Education Limitations 12
Education/Higher Education Obstacles 13
Additional Educational Barriers and Obstacles 13
Cybersecurity Workforce Development- Industry Obstacles, Barriers, Limitations 14
Concluding Thoughts on IT-Cyber Workforce Development/Education Barriers, Obstacles, and Limitations 15
Linked Strategies 16
Three Key Pillars 16
Points of Emphasis 16
California IT-Cyber Essential Workforce Pre- and Registered Apprenticeship Program Pipeline and Pathway (CEWYA) Objectives 17
CEWYA Design Methodology and Development Process 18
The Essential Prioritization of California Cybersecurity Workforce Development and Education Initiatives 19
Table 1: California Job Openings/NICE Cybersecurity Workforce Framework Category 20
NICE Framework Work Roles in Key Cyber Workforce Categories 20
Securely Provision (SP) 20
Operate and Maintain 21
Key Support: Security Operations Centers (SOCs) and IT-Cyber-Privacy Offices 21

California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Pipeline/ Pathway Steps/Process.....23

Step 1: Recruiting and Outreach

Step 2: California Cybersecurity Pre-Apprenticeship Program

Step 3: California Cybersecurity Apprenticeship Program

Step 4: Employer Based On the Job Training (OJT)

CEWYA Process Details.....25

California Pre- and Registered Apprenticeship Pacing Guide.....26

5th and 6th Grade.....26

Pre-Apprenticeship Phase and Recommendations.....27

Apprenticeship Phase and Recommendations.....27

Related Higher Education Programs.....28

CEWYA Model IT-Cybersecurity Pacing Guide Milestones and Recommendations.....28

Career Technical Education (CTE) Program Curriculum Component

IT-Cyber Industry Recognized Certification Component

Sample Certifications/Courses/Tracks to Select From

Programming/Coding Component Milestones

Essential Employability "Soft Skills"

On the Job Training Component

Digital Skills, Cyber-Hygiene and Awareness

Pre-Apprenticeship Certification/Courses/Tracks.....29

CEWYA Apprenticeship Level Model.....31

Apprenticeship Certification/Courses/Tracks.....32

Cybersecurity Education and Workforce Development (Post-High School).....34

Certificate Design/Development List to Implement CEWYA.....35

K-12 Cybersecurity (CTE) Industry Recognized Certificate Programs/List of Courses to Develop.....36

Concluding Thoughts: Closing the Barriers, Obstacles, and Challenges of the Apprenticeship Model of Workforce Development.....38

References.....39

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)[1] 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

[1] (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. [2] 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. [3] 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.

[2] (https://www.cyberseek.org/heatmap.html accessed electronically on 7.7.2020).
[3] 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. [4]

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-

[4] (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. [5] 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.) [6]

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.

[5] 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).

[6] 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. [7] 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.

[7] (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 5th/6th 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.

30