ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

In addition to postsecondary institutions located in California that offer cybersecurity-related programs and training, there are many accredited and federally recognized institutions outside the state that offer online cybersecurity programs. Examples include Capella University, Kaplan University, Salem International University, University of Phoenix, Utica College, and Walden University.

There are many other providers of cybersecurity training outside of accredited, federally recognized postsecondary institutions, ranging from adult schools to university extensions. Some operate outside of established education institutions, such as "boot camps" and online industry sponsored training. In addition, entities outside of California provide online training that California residents can take. Some universities offer cybersecurity training through their extension or continuing education programs. Examples include UCLA Extension, UC Irvine Division of Continuing Education, California State University Fullerton University Extended Education, and Stanford University Online. These programs are generally fee-based and operate outside of the regular undergraduate or graduate university curriculum.

There are many providers of cybersecurity training outside of accredited, federally recognized postsecondary institutions, ranging from adult schools to university extensions.

The U.S. Military provides cybersecurity training, including at locations in California, such as the U.S. Navy Information Warfare Training Commands in San Diego and Monterey, the U.S. Army Reserve High Tech Regional Training Site in Sacramento, and the Marine Corps Communications and Electronics School in Twentynine Palms. In addition, some adult education schools offer entry-level cybersecurity training. These programs are provided through unified school districts in cities such as Sacramento, Chula Vista, San Diego, and Riverside. These programs are generally low cost compared to alternative cybersecurity training opportunities.

Industry Sponsored Programs

Many industry sponsored programs are offered through high schools or postsecondary institutions. Vendors partner with existing educational institutions to provide training leading to industry certification (which is bestowed by the vendor after students pass specific tests outside of the school or college). It is the role of the partner school/college to provide training to prepare students to pass the industry certification tests, and in exchange the educational institution often receives training materials and gifts of hardware and/or software from the vendor to support the training and promote their products and certifications.

There is no requirement to enroll in or pass a class to qualify for an industry certification. Individuals may be self-taught, may take free or for-pay online classes, may attend a "boot camp" or other short-term training, or any other strategy whereby they can gain the knowledge and competencies to pass the industry certification tests. There are dozens of cybersecurity training providers that are not affiliated with colleges or universities that provide training to prepare students to pass various industry certifications classes. Most if not all provide training online, and many have physical locations for face-to-face classes at various locations in California (including but not limited to the SANS Institute, Fast Lane, LearnQuest, Global Knowledge, ONLC Training Centers, TechData, INFOSEC Institute, Executrain). These training providers tend to be for-profit companies affiliated with one or more industry vendors, and the cost for training ranges from hundreds to thousands of dollars.

ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

Secondary Institutions Programs

To gain a broader understanding of the spectrum of programs serving students, data was gathered on career pathways that exist between community colleges, secondary schools (high schools) and regional occupational center programs (ROCPs), including both formal articulation agreements and informal partnerships and collaborations. The California Statewide Pathways Project is the clearinghouse for formal articulation agreements between occupational courses and programs at high schools, ROCPs, and colleges. Cybersecurity falls under the career path "Information Technology," where there are five disciplines: CIS/Computer Programming, IT Web Design, Web Design, IT Applications, and CIS Cisco/A+. The last two could be considered introductory coursework leading to a cybersecurity career.

Articulation Agreements

There are 140 formal articulation agreements between high schools and colleges registered with the California Statewide Pathways Project, 69 in CIS Cisco/A+ and 71 in IT Applications (Exhibit 32). The majority of these agreements exist in the regional areas of the Inland Empire (Riverside and San Bernardino counties) and the LA/Orange County region (Los Angeles and Orange counties).

Exhibit 32. Formal articulation agreements between regional secondary and postsecondary cybersecurity-related programs

Region	CIS Cisco/A+	IT Applications	Subtotal
Bay Area	10	11	21
Central	4	2	6
Greater Sacramento	5	11	16
Inland Empire	28	28	56
LA/Orange	19	16	35
San Diego/Imperial	2	3	5
South Central	1	0	1
Far North	0	0	0
Total	**69**	**71**	**140**

Source: California Statewide Career Pathways

ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

The colleges with formal articulation agreements with high schools are listed in Exhibit 33. A complete list that identifies the corresponding high schools and ROCPs can be found in Appendix I: Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs.

Exhibit 33. Articulation agreements between colleges and high schools

Bay	Central	Greater Sacramento	Inland Empire	LA/Orange	San Diego Imperial	South Central	Far North
San Jose City College	Bakersfield College	Sacramento City College	Chaffey College	Los Angeles Pierce College	Imperial Valley College	Moorpark College	Yuba College
Santa Rosa Junior College	College of the Sequoias	Folsom Lake College	College of the Desert	Mt. San Antonio College	Palomar College		
College of San Mateo		Woodland College	Crafton Hills College	Saddleback College	Southwestern College		
Evergreen Valley College			Mt. San Jacinto College	Coastline College			
Los Medanos College			Riverside CCD	Golden West College			
Mission College			San Bernardino Valley College	Rio Hondo College			
Ohlone College							
Skyline College							
Solano College							

While articulated programs exist between secondary and postsecondary schools, it appears enrollment is low at the high school level. At California public high schools, IT-related coursework is not a part of the core curriculum, and falls under the broad course subject area of "other" along with elective courses such as yearbook and life skills.

There are a few cybersecurity-related introductory courses in the public high school curriculum—two courses that can be identified as cybersecurity related and four that could be considered possibly pre-cybersecurity. These six courses are taught at 521 high schools, which represents approximately 15% of all public high schools in California. For a list of the courses and their descriptions, see Appendix J: List of Cybersecurity-related and Pre-cybersecurity Secondary Courses at California Public High Schools.

ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

Cybersecurity High School Enrollment

High school enrollment in cybersecurity-related coursework totaled 1,901 in 2016-2017 (Exhibit 34). In the same year, pre-cybersecurity enrollment totaled 23,216 for a combined total of 25,117. As total high school enrollment reached nearly 2 million that year, cybersecurity-related and pre-cybersecurity courses comprised only 1% of those enrollments.

Exhibit 34. Enrollment in high school cybersecurity-related and pre-cybersecurity courses

Course Name	Course Code	Number of Schools	Courses Taught	Number of UC/ CSU Courses	Total Enrollment
Cybersecurity Related		**82**	**163**	**29**	**1,901**
Network Engineering	4604	55	107	17	1,643
Network Security	4646	27	56	12	258
Pre-Cybersecurity		**439**	**1199**	**422**	**23,216**
Database Design and SQL Programming	4631	8	11	8	222
Computer Repair and Support	4633	121	319	15	2,971
Exploring Computer Science	4634	284	821	353	18,741
CTE AP Computer Science A	4641	26	48	46	1,282
Total		**521**	**1362**	**451**	**25,117**

Source: California Department of Education

Note: Data are from 2016-2017, the most recent year available.

High school enrollment in cybersecurity-related and pre-cybersecurity courses is low, which indicates the formal articulation agreements may not function effectively to bring high school students into a cybersecurity pathway to further education and training, and ultimately employment. However, in addition to formal articulation agreements, many less formal and informal partnerships and collaborations exist with high schools.

There are many industry partnerships with high schools (CISCO, Oracle, CompTIA, Microsoft) that exist outside of formal articulation agreements with postsecondary institutions. Other programs, such as the CyberPatriot program, aim to create interest in cybersecurity among high school students. High schools may also have cybersecurity-related clubs on campus with the same aim.

The California Cyberhub is a recent development with the goal of coordinating cybersecurity training efforts in California to decrease duplication of effort and confusion. Started in 2017, the California Cyberhub is an interagency and interdepartmental collaborative including representation from K-12, California Community Colleges, California State Universities, CompTIA, Hewlett Packard, Amazon, Bust Buy, California Department of Technology, California Office of Emergency Service, Governor's Office, and others. This new organization sponsors faculty professional development and training, summer "Cyber Camps" for students, and competitions held throughout the state. The competitions have the goal of preparing students to participate in national CyberPatriot defense competitions. To date, over 100 middle and high school teams are registered on the Cyberhub website. The Cyberhub also promotes and provides links to free online CompTIA training in "IT Fundamentals."

[29] California Cyberhub, 2016, accessed June 11, 2018, https://ca-cyberhub.org/.

SECTION IV: SURVEY OF EDUCATIONAL PROVIDERS

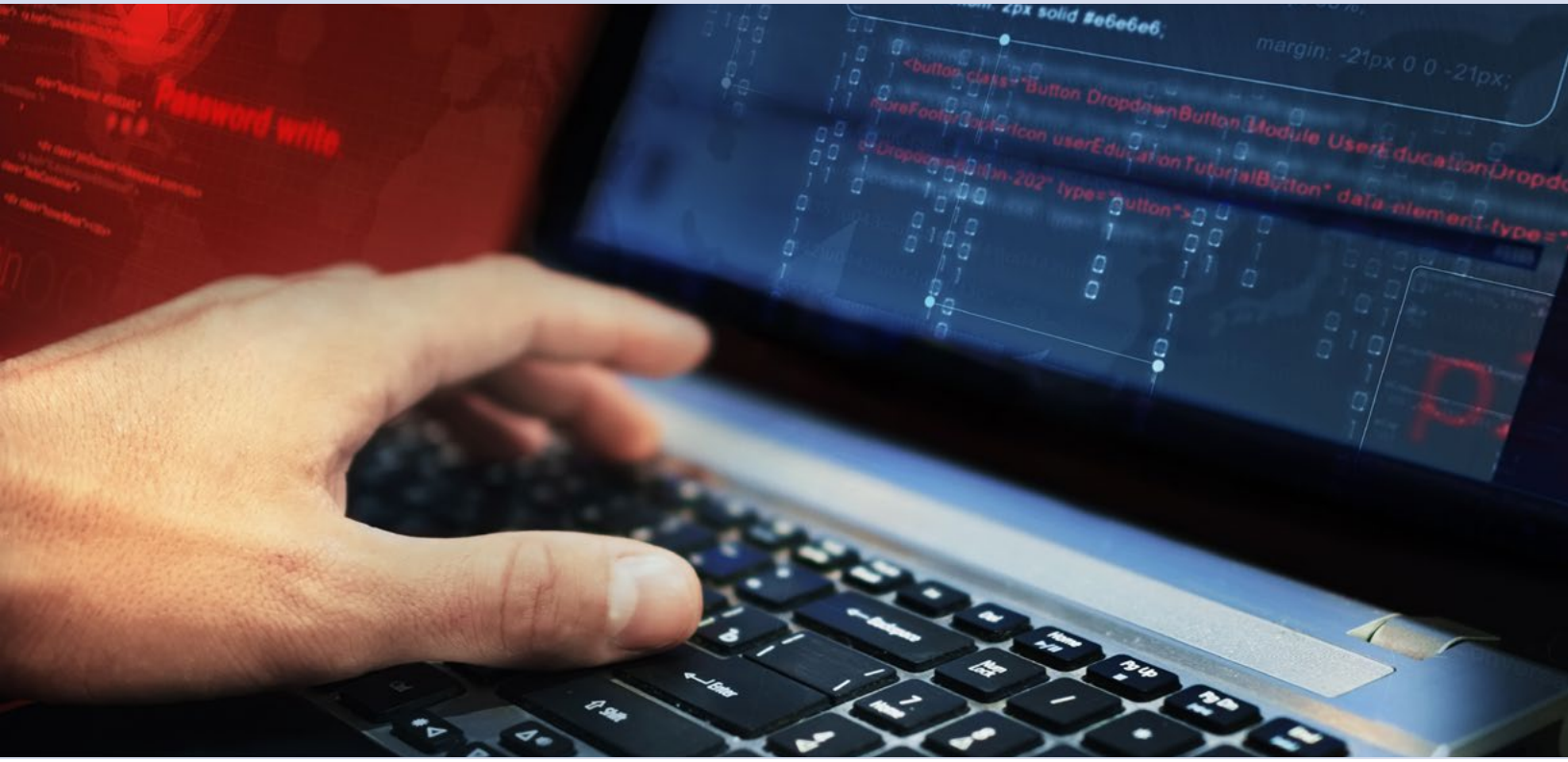
EDUCATIONAL PROVIDER CHARACTERISTICS

To glean additional information about cybersecurity programs offered by postsecondary institutions in California, a survey of postsecondary educational providers was conducted in spring 2018. Of the 242 institutions reporting to the U.S. Department of Education that they offer cybersecurity-related programs, 64 responded to the survey for an overall response rate of 26.4% (Exhibit 35). Seventy-five percent of responses were from community colleges, 24% were from four-year institutions and 1% was from a county office of education. Institutions with more focused cybersecurity programs were targeted for follow up, resulting in a higher response rate from that group. Survey feedback was received from 37.5% of programs characterized as "cybersecurity focused." Appendix K contains the survey questions sent to educational institutions.

Exhibit 35. Survey response rates by cybersecurity programming

	Number of Institutions with Programs*	Total Responses	Response Rate
Cybersecurity Focused	40	15	37.5%
Includes Cybersecurity	99	35	35.4%
Likely Includes Cybersecurity	233	63	27.0%
Unduplicated Overall Response Rate	**242**	**64**	**26.4%**

*There is duplication of institutions between cybersecurity program categories, as many institutions offer awards in multiple categories.



PROGRAM DEVELOPMENT

In utilizing the NICE Cybersecurity Framework, postsecondary institutions with cybersecurity-related programs were asked which of the seven NICE categories (interpreted here as program concentrations) were offered through their programs. Nearly two-thirds of respondents indicated they offered programs in "Operate and Maintain," while half have programs in "Protect and Defend" (Exhibit 36). Nearly half offer programs in "Investigate" and "Analyze," approximately one third in "Securely Provision," and one quarter offer programming in "Collect and Operate" and "Oversee and Govern."

Respondents also were asked whether they intended to develop programs in the NICE program concentration areas. Nearly half indicate they plan to develop programs in "Collect and Operate," which is the area where the fewest institutions report having programs in place. Conversely, one-fifth indicate they are considering developing programs in "Operate and Maintain," which is the concentration area with the highest proportion of respondents indicating they already have programs. Between a quarter and nearly a half of respondents indicated they do not have programs, and do not plan to develop programs, in the following concentration areas (listed in order of frequency of response): Oversee and Govern, Securely Provision, Collect and Operate, and Analyze.

Exhibit 36. Programmatic majors, concentrations, certificates or coursework/ training related to NICE Cybersecurity Workforce Framework

Program Concentration	Yes (program currently exists)	No (program does not exist; no plans to develop)	No, but we are considering developing one	Count
Securely Provision (includes: Risk Management; Software Development; Systems Architecture; Technology R&D; Systems Requirements Planning; Test and Evaluation; Systems Development)	31.2%	36.1%	32.8%	61
Operate and Maintain (includes: Data Administration; Knowledge Management; Customer Service and Technical Support; Network Services; Systems Administration; Systems Analyst)	63.9%	16.4%	19.7%	61
Oversee and Govern (includes: Legal Advice and Advocacy; Training, Education and Awareness; Cybersecurity Management; Strategic Planning and Policy; Executive Cyber Leadership; Program/Project Management and Acquisition)	24.6%	42.6%	32.8%	61
Protect and Defend (includes: Cyber Defense Analysis; Cyber Defense Infrastructure Support; Incident Response; Vulnerability Assessment and Management)	50.8%	13.1%	36.1%	61
Analyze (includes: Threat Analysis; Exploitation Analysis; All-Source Analysis; Targets; Language Analysis)	42.6%	24.6%	32.8%	61
Collect and Operate (includes: Collection Operations; Cyber Operational Planning; Cyber Operations)	26.2%	31.2%	42.6%	61
Investigate (includes: Cyber Investigation; Digital Forensics)	45.9%	14.8%	39.3%	61

PROGRAM DEVELOPMENT

Postsecondary institutions that indicated they were considering developing new cybersecurity programs were asked an open-ended question: What challenges are you facing as you consider adding/developing a new program or coursework/ training? The majority of responses fell into a few main categories: finding qualified instructors, curriculum development, budget, physical resources, and program marketing.

Here are a few illustrative quotes:

- Lack of qualified instructors. Lack of in-the-field-experienced instructors.
- Lack of space, talent and money.
- Funding for physical labs, funding for instructor training, program promotion.
- Small program minimally funded with limited time to complete curriculum development.
- Determining which coursework and training will result in a greater likelihood of our students finding employment.
- The lengthy curriculum approval process makes it difficult to respond quickly to industry and technology change.
- Marketing the program to the community to gain enrollment.

CYBERSECURITY CERTIFICATIONS

Because industry certifications are often required for job preparation, the survey asked postsecondary institutions which certifications are included in their cybersecurity-related programs. The majority of respondents prepare students for CompTIA Security+ and Security+ industry certifications (Exhibit 37). Other frequently cited industry certifications include: Certified Ethical Hacker, CISCO Certified Network Associate Security, and Microsoft Certified System Administrator.

Exhibit 37. Industry certifications for which cybersecurity programs train students

Certification	Number Responding	Percent
CompTIA Security +	41	64.1%
Security +	33	51.6%
Certified Ethical Hacker (CEH)	27	42.2%
CISCO Certificated Network Associate Security (CCNA-S)	20	31.3%
Microsoft Certified System Administrator (MCSA)	15	23.4%
Other, please specify (Note: see table footnote)	14	21.9%
CompTIA Cybersecurity Analyst (CySA+)	10	15.6%
CompTIA PenTest+	10	15.6%
Certified Information Systems Security Professional (CISSP)	9	14.1%
Cisco CCNA Cyber Ops	9	14.1%
Palo Alto Networks Firewall	8	12.5%
CISCO Certified Network Professional Security (CCNP-S)	4	6.3%
CompTIA Network+	4	6.3%
CompTIA Advanced Security Practitioner (CASP)	3	4.7%
Certified Information Systems Auditor (CISA)	2	3.1%
EC-Council Certified Security Analyst (ECSA)	2	3.1%
Offensive Security Certified Professional (OSCP)	2	3.1%
Department of Defense Directive 8140 (Security Clearance)	1	1.6%
SANS/GIAC Certification	1	1.6%
Certified Information Security Manager (CISM)	1	1.6%
Certified in Risk and Information Systems Control (CRISC)	1	1.6%
GIAC Penetration Tester (GPEN)	1	1.6%
Jupiter Networks Certification Program (JNCP) Junos Security Certification	1	1.6%
Palo Alto Networks Endpoint	0	0.0%

Note: The following certifications were identified in the "other" category:

CompTIA IT Fundamentals
Server+
Computer Hacking Forensic Investigator (CHFI)
ccsp, aws
IACIS, A+, CPCT, CFOT, CCENT
Computer Hacking Forensic Investigator(C|HFI), Systems Security Certified Practitioner (SSCP)
Cyber Program still under development and will include Python Security + Forensics + CyberLaw
FTK Computer Forensics – Certification ACE
Certified Network Forensic Investigator

SOFT SKILLS

Cybersecurity employers often consider soft skills when conducting hiring. The survey asked postsecondary institutions which soft skills were emphasized in their cybersecurity coursework and training. The most frequently cited soft skills include: problem solving, ethics, troubleshooting, teamwork/collaboration, and communication skills (Exhibit 38).

Exhibit 38. Soft skills emphasized in cybersecurity coursework and training

Soft Skill	% (out of 64 surveys)	Number of Responses
Problem solving	73.4%	47
Ethics	65.6%	42
Troubleshooting	60.9%	39
Teamwork/collaboration	60.9%	39
Communication skills	57.8%	37
Writing	46.9%	30
Planning	39.1%	25
Self-starter	31.3%	20
Enthusiasm	31.3%	20
Building effective relationships	26.6%	17
Quick learner	25.0%	16
Quality assurance and control	23.4%	15
Total		**347**

Note: Respondents were requested to "mark all that apply."
Other soft skills noted by respondents in comment box:
Research
Hands on activities
Proactive development of domain language skills
Networking with industry professionals
Documentation
Critical thinking skills

EMPLOYER INVOLVEMENT

Career education (CE) programs at postsecondary institutions generally include some form of employer involvement, with the intent of better aligning curriculum with workforce needs. The survey asked postsecondary institutions in California with cybersecurity-related programming how they involve employers in their programs.

Exhibit 39 shows the responses, including "other" comments, which are included below the table. The most common roles of employers are: participation on advisory board(s), provision of information about the industry and jobs, internships for students, and guest lectures.

Exhibit 39. Employer involvement in cybersecurity programs

Involvement	% (out of 64 surveys)	Count
Employers participate on my advisory board(s)	65.6%	42
Employers provide information about the industry and jobs	51.6%	33
Employers provide internships for my students	46.9%	30
Employers act as guest lecturers	42.2%	27
Employers offer facilities tours	37.5%	24
Employers donate equipment to my program	23.4%	15
Total		**171**

Other, provided in comment box:
Provide phone consultations
Sponsor club activities; provide promotional giveaways; provide scholarships to conferences
Potential employers provide feedback on our curriculum. We are looking to formalize an advisory board just for cyber security curriculum.
Support, participate and fund cyber security competitions