The University of Texas at Austin
Center for STEM Education

JULY· 2018
STEMCENTER.UTEXAS.EDU

Preparing Texas Students for the Cyber Economy

Recommendations of the Texas Computer Science Task Force

ABSTRACT

Texas has long been recognized as a leader in secondary education. In recent years, cities like Austin and San Antonio have emerged as industry hubs for computer science and cybersecurity. Despite this, however, Texas high schools have found themselves unable to offer courses in those subjects at a rate to match demand. The challenge is particularly acute in cybersecurity, a field whose importance to the US economy and prominence in the Texan job market warrants greater investment from the education sector.

This report examines these problems in detail. In particular, we find that there are very few options for students interested in cybersecurity education. Moreover, perverse incentive structures created by educational regulations force district administrators to make impossible choices between their fiscal and educational responsibilities. To address these and other problems, we propose a number of recommendations to the Texas State Board of Education and the Texas Education Agency.

This report was compiled between February and June 2018, and was produced with input from the 2018 Texas Computer Science Task Force, led by WeTeach_CS headquartered at the Center for STEM Education at the University of Texas at Austin College of Education.

ABOUT THE TASK FORCE

The 2018 Texas Computer Science Task Force was assembled to address the problem of computer science and cybersecurity education in Texas. Its members include educators, administrators, subject matter experts, and industry professionals. Member affiliations and titles are available at the end of this report.

ABOUT THE AUTHORS

Dr. Carol Fletcher is the Deputy Director of the Center for STEM Education at the University of Texas at Austin College of Education. She received her Ph.D. in Science Education from the University of Texas at Austin. Prior to that, she taught middle school science in Pflugerville, TX for six years. Dr. Fletcher continues her work with the Pflugerville school district, having served on the Board of Trustees since 2001, including five years as School Board President. She directs the WeTeach_CS project, one of the largest computer science teacher professional development programs in the nation.

Rohan Ramchand graduated from UT Austin with degrees in honors computer science, mathematics, and government. Prior to graduation, he worked at a number of prominent technology companies, and interned at the White House in Fall 2016. He also served as a student mentor and department ambassador for the UT Department of Computer Science. He works in San Francisco as a software engineer.

Suggested citation: Fletcher, C.L. & Romchand, R. (2018). *Preparing Texas Students for the Cyber Economy*. Austin, TX: The University of Texas at Austin. Retrieved from https://utexas.box.com/v/CS-Task-Force-Report-2018

Table of Contents

Introduction

TEXAS AND COMPUTER SCIENCE

The first Census survey of computer ownership was conducted in 1984, less than a decade after the first personal computer hit the market. The survey recorded that out of over 87 million households, just over eight percent owned a computer. The most recent survey of computer ownership was conducted in 2012. It revealed that in the three decades since the first survey, the percentage of homes with a computer increased almost tenfold, to nearly 80%[1]. Moreover, a poll conducted in February 2018 by the Pew Research Center found that 77% of all Americans, and 94% of all Americans aged 18-29, own a smartphone[2]. These numbers indicate that, simply put, we've come to depend on computers for everything we do.

As a result, jobs in computer science have become increasingly common and increasingly lucrative. There are close to 37,000 open jobs in computer science in Texas alone, the median salary for which is $91,000, almost double the statewide median salary. As it happens, Texas is extraordinarily well-positioned to fill these jobs. The University of Texas at Austin is one of the world's leading research institutions for computer science. Texas has among the highest levels of student enrollment in computer science courses at the high-school level, and is one of the leaders in enrollment among female and minority students. The certification process to become a teacher of computer science is robust, requiring a deep understanding of the subject matter. Most significantly, Texas is one of the only states that requires *every* high school in the state to offer a full complement of computer science courses.

Moreover, there is clear demand for computer science education at all levels. A recent Gallup poll found that more than nine in ten parents—around 91%—want computer science to be offered in school.[3] And, when those courses are offered, they tend to have the highest rates of student happiness among STEM courses[4]. Lawmakers, educators, and administrators at the local and state level have started to emphasize the importance of computer science at the high-school level as a vehicle for students to have access to those thousands of lucrative, open jobs in the field.

1 https://www.census.gov/data/tables/2012/demo/computer-internet/computer-use-2012.html

2 http://www.pewinternet.org/fact-sheet/mobile/

3 https://services.google.com/fh/files/misc/searching-for-computer-science_report.pdf

4 https://code.org/promote

CYBERSECURITY

A significant number of the open jobs in computing originate from one particularly important industry: cybersecurity. As computing has become more sophisticated, so too have the abilities of malicious agents looking to penetrate our networks and seize our private information. Data breaches of immense magnitude seem to take place on a routine basis, and they grow more and more effective each year. And, while many attacks target retailers like Target in the hopes of acquiring credit card data and other financial information, a large number of successful attacks have targeted government agencies like the Office of Personnel Management, financial institutions like Equifax, and even the core of our democratic process, elections.

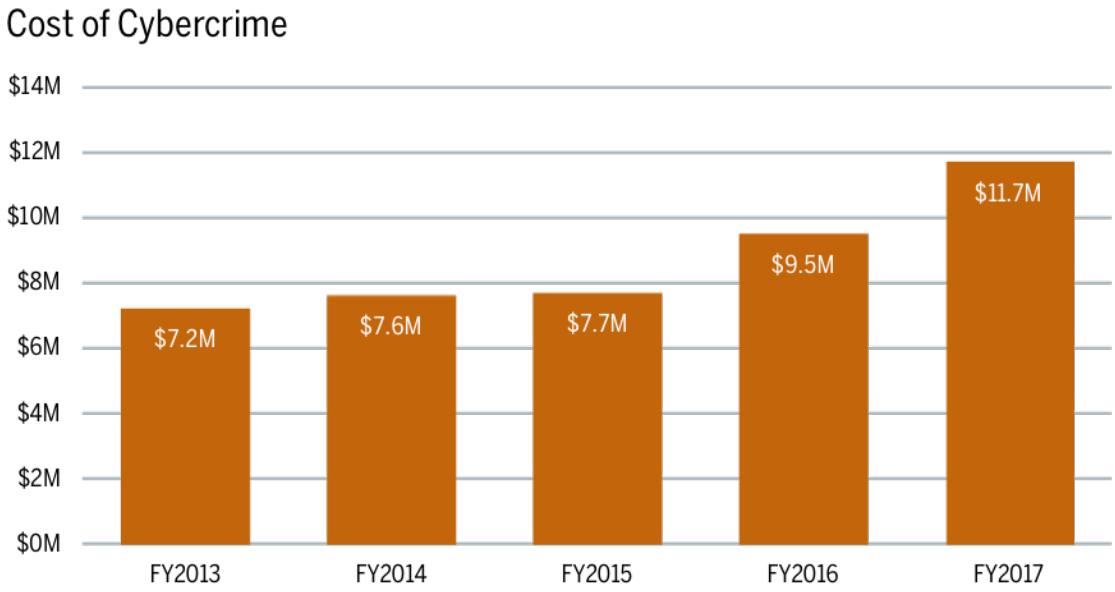


Figure 1: Cost of cybercrime over the last five years.[5]

The complacency leaders once exhibited in responding to these attacks is a thing of the past. CEOs and politicians are starting to demand better data security as cybersecurity has become an issue of national defense. As a result, tens of thousands of cybersecurity jobs are becoming available each year, from defensive network security experts to offensive penetration testers and bug bounty hunters. Unfortunately, though, these jobs often go unfilled, as they require an extensive knowledge of security—something most Americans, and even many computer scientists, lack.

As with computing as a whole, though, Texas is uniquely well-positioned in the field of cybersecurity. San Antonio is home to some of the world's leading security firms, including Digital Defense, Inc. and KGI. San Antonio also houses a significant number of governmental and military organizations focused on cybersecurity. Groups like the National Security Agency (NSA), the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISA), and the Defense Information Systems Agency (DISA) have headquarters or major offices in San Antonio. (The Air Force has a particularly large influence, as San Antonio is home to Lackland Air Force Base.)

These organizations are collectively responsible for 56,000 cybersecurity jobs in San Antonio alone[6]. What differentiates these jobs from positions in the information technology sector as a whole, however, is that many of them require no more than a high school diploma and a handful of industry-recognized certificates. More and more security companies are shifting towards a preference for on-the-job training, making the bar for entry achievable by qualified high-school graduates. Of course, many other positions require a bachelor's degree, but degree programs often require at least some exposure to computer science in high school for admission.

5 https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

6 http://www.sanantonioedf.com/industry-sectors/information-technology-cybersecurity/

Regardless of the path students wish to choose—to enter industry immediately after high school or to pursue post-secondary education in the information technology sphere—they must be given the chance to acquire, at the very least, a baseline level of education in the core principles of cybersecurity. At that point, students can make a choice to take a course aimed at preparing them for industry certification, or take a course aimed at giving them more subject matter expertise. A cybersecurity pathway, hewing to a curriculum familiar to and accepted by the academic and professional security communities, would create a common foundation for students who wish to pursue either path forward.

The next section discusses three important considerations: what Texas computer science education looks like as of now, what information a cybersecurity course should cover and how that information is currently presented, and what kinds of industry standards a motivated cybersecurity student could achieve in high school.

Background

THE EDUCATIONAL LANDSCAPE

Texas codifies curriculum standards in a series of documents called the Texas Essential Knowledge and Skills, or TEKS. Currently, 16 computer science courses are denoted Technology Applications (TA) courses in the Texas Administrative Code (TAC). Included in this list are a four-course standard pathway: Fundamentals of Computer Science, Computer Science I, Computer Science II, and Computer Science III. Both AP courses in computer science are included, along with two IB courses. The remainder of the TA courses include two independent study courses, as well as a number of subject-specific courses, such as Digital Forensics, Game Programming and Design, and Mobile Application Development.

A separate category of courses is listed under the Information Technology subheading of the Career and Technology Education (CTE) section in the TAC. While the Computer Programming I and II courses provide a very introductory exposure to actual computer science concepts, most other courses under the IT cluster would not be considered computer science and are related to "building linkages in IT occupations for entry level, technical, and professional careers related to the design, development, support, and management of hardware, software, multimedia, and systems integration services"[7]. These include courses such as Principles of Information Technology, Networking, and Computer Maintenance. Other courses like Digital Media and Web Technologies bear only a passing relation to computer science, and instead focus on applications of technology to other fields. (See Table 1 for a full list of CS courses available in Texas.)

There are two significant differentiators between courses offered under each heading: certification and funding. Texas requires that TA courses be taught by teachers certified either in Technology Applications or in Computer Science to teach computer science courses.[8] The CS certification process requires teachers to be equipped with a significant number of technical skills, and involves developing a proficiency with a topics such as software design and programming, loops and recursion, data structures, object-oriented programming, algorithms, Big-O notation, discrete math, digital forensics, robotics, and game and mobile app development.

1. Fundamentals of Computer Science	9. Digital Forensics
2. Computer Science I	10. Discrete Mathematics for Computer Science
3. Computer Science II	11. Game Programming and Design
4. Computer Science III	12. Mobile Application Development
5. AP Computer Science Principles	13. Computer Programming I*
6. AP Computer Science A	14. Computer Programming II*
7. IB Computer Science, Standard Level	15. Web Game Development
8. IB Computer Science, Higher Level	16. Robotics Programming and Design

Table 1: Texas Computer Science courses. ** course listed under CTE*

Although the certification process is time and effort intensive, the result is that Texas teachers who demonstrate mastery of these concepts through the TExES certification exam are well prepared to provide instruction in these areas to their students. On the other hand, the same requirement doesn't hold for the courses under the CTE heading. CTE courses can be taught by anyone with a business certification, which doesn't include a programming component. While some business certified teachers may have CS skills or a programming background, nothing about the actual certification process provides the same level of quality assurance for those who hire and supervise teachers or the parents of students enrolled in these courses.

7 http://ritter.tea.state.tx.us/rules/tac/chapter130/ch130k.html

8 The former is required for AP Computer Science Principles and Fundamentals of Computer Science; the latter is required for the bulk of the remaining courses.

Furthermore, CTE courses are funded differently than TA courses. Districts receive weighted funding on a per student basis for CTE course enrollment. No such additional funding exists for Tech Apps courses. In 2014, the first Texas Computer Science Task Force noted that a lack of funding for CS was a significant barrier to implementing CS courses in Texas high schools[9]. Because most high school CS courses are classified as TA, not CTE, school districts have no dedicated funding source to support the teacher professional development or instructional materials that are needed to develop CS course pathways.

In fact, schools actually have a disincentive to offer CS courses in Technology Applications as compared to CTE courses. Because districts receive weighted funding for students who complete CTE courses, schools are incentivized to offer those courses instead of computer science. This is particularly problematics for smaller schools, typically found in more rural districts, and charter schools, who can't offer as many program options as more comprehensive, large urban and suburban high schools and likely explains why rural schools are the least likely to offer CS courses. Since STEM programs such as Engineering, Biotechnology, and Health Sciences are part of CTE, it makes financial sense for small schools to limit their course options to those for which they will receive weighted funding.

This incentive structure puts district leaders in the position of balancing what is fiscally responsible against what is in the best interest of students. Moving every CS course under the CTE umbrella would solve that problem and ensure funding flows directly to districts who are actually enrolling students in CS courses. In addition, because CTE programs are also audited to ensure that the students enrolled in them are representative of the student body, this provides an additional incentive for districts to diversify their CS course enrollment. Even if CS courses were provided weighted funding or moved into CTE, however, it would be vitally important to maintain the quality assurance that a CS teacher certification guarantees to ensure that high school CS programs are staffed by qualified professionals in the field.

ENROLLMENT OUTCOMES

These two distinctions have a significant effect on enrollment outcomes. Over the course of the 2014-15 school year, for example, 1,565 individuals completed a pre-service preparatory program to become math teachers—only 23 did so in computer science. Although a number of nonprofits and advocacy organizations have helped to dramatically improve these statistics in recent years, the absolute numbers are still fairly low. Some teachers in rural parts of the state might find themselves to be the only certified teacher in a two hundred mile radius.

This, combined with the incentives offered by weighted funding, doubly compels schools to focus on offering CTE courses over TA courses. Unless teachers can shoulder the burden of the certification process themselves, tech apps courses create additional costs for schools that CTE courses don't. As mentioned above, Texas requires every school to offer at least one course in computer science. Due in part to the excessive costs associated with doing so, many don't. Five years ago, only one in five schools offered a single computer science course.

Enrollment numbers are similarly dismal. There are more than 1.6 million high school students in the state of Texas. Around 49,000, or less than 3% of them, completed any computer science course. Fewer than one in 50 women in the state take a computer science course. The diversity problem in the computer science industry is mirrored in schools—26% of computer science students are female. Fewer than 9,000 high schoolers took either computer science AP exam in 2017. Around 2,400 of these students were female; 2,362 were Hispanic or of Latino origin; 327 were black; 23 were Native American. Fewer exams in computer science were taken than in any other STEM field. Essentially, given the diverse demographics of the state of Texas, the majority of students in this state are not being prepared for the high-wage, high-demand jobs that will drive the Texas economy and ensure our national security.

9 http://www.weteachcs.org/about-us/presentations-and-publications/

ADDRESSING THE PROBLEM

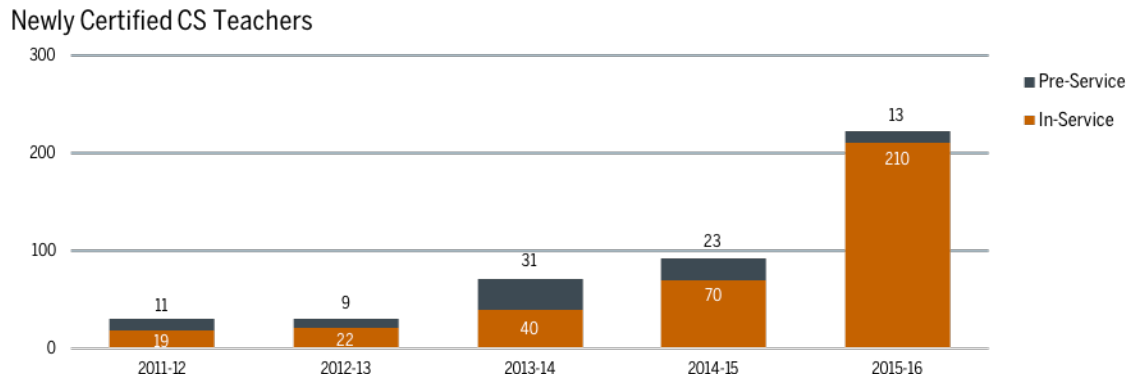
These disparities did not go unnoticed for long, and in October 2014, UT Austin's Center for STEM Education convened the first Texas Computer Science Task Force to define and address some of the challenges faced in building a robust K-12 CS pipeline in Texas. The output of that Task Force was a white paper, which outlined four key barriers along the path to a better educational landscape[10]. Those barriers, and the recommendations that the Task Force made to overcome them, are summarized in Table 2.

The first Task Force and its findings made an impact, and in 2015, the Center for STEM Education at UT Austin, through federal funding provided by TEA, founded WeTeach_CS, a project aimed at implementing these recommendations. The advocacy group CS4TX was also created to help educate stakeholders about the challenges faced in providing a comprehensive computer science education for K-12 students, as well as advocate for policy changes to improve and diversify student enrollment. The project identified five goals—increasing the number of certified CS teachers, increasing the percentage of high schools offering CS courses, increasing the number of enrolled computer science students, diversifying enrollment by expanding access to underrepresented or underserved groups, and expanding access to computer science at the K-8 level to create a pipeline to high school computer science.

Issue	Recommendation
Lack of trained and certified computer science teachers	Support professional development that prepares currently certified educators to teach high school computer science courses
No incentive for administrative investment in computer science	Move computer science courses out of Technology Applications and into Career and Technical Education
Low student and parent demand for computer science	Expand options for core computer science to include additional engaging, project-based courses like AP CS Principles
No system connecting high school courses to careers in industry	Develop a robust and scalable online system that connects high schools to careers and professionals in computer science fields

Table 2: 2014 Texas CS Task Force recommendations

Over the last few years, WeTeach_CS has aggressively tackled the first of these goals. The project now offers online and face-to-face certification programs for teachers looking to take the TExES teacher certification exam in computer science. Moreover, WeTeach_CS, with both state and philanthropic funding, provides a one-time stipend of $1,000 to any teacher who gets certified to teach computer science. The results speak for themselves. The year before WeTeach_CS was launched, a total of 71 teachers became certified to teach computer science. The next year, that number rose to 93; the year after, 223 teachers became certified for the first time. In total, over 400 new teachers



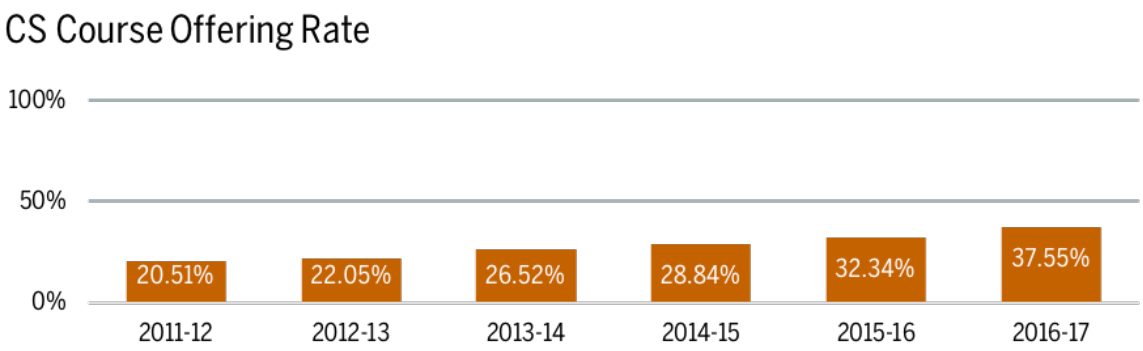
have benefited from the incentives and stipends offered by the program. (See Figure 2.)

10 https://www.slideshare.net/weteachcs/building-the-texas-computer-science-pipeline-strategic-recommendations-for-success

Figure 2: Teacher certification trends in Texas.

The exponential increase in teachers has had effects on both enrollment and course offering rates. The percentage of students who took at least one computer science course has more than doubled in the last five years, rising by 124%. Over the same time period, enrollment rates jumped among underrepresented minorities by 154% and among economically disadvantaged students by 156%. (Female enrollment rose by 104%, however, indicating a widening gender gap in enrollment.)

Moreover, the fraction of schools offering CS courses has doubled in the last five years, from 21% to 39%. (See Figure 3.) This trend holds not just among schools in wealthy urban or suburban areas—rural schools have been among the fastest to adopt computer science into their curricula.



Students from economically disadvantaged or underrepresented backgrounds have more access to computer science education—at the high standards required by the state—than ever before.

Figure 3: Percent of high schools with at least one CS course.

CYBERSECURITY EDUCATION

How does cybersecurity fit into the educational landscape in Texas? Of the sixteen computer science courses currently offered, only one—Digital Forensics—has a focus on security. (A handful of other courses focus on security in particular environments; for example, the TEKS for Web Design mentions security as it pertains to online applications. In addition, a few of the research or independent study courses can optionally include a component on security.) The Digital Forensics course was based on a model promulgated by the International Society for Technology in Education (ISTE) and released in 2011.11 The TEKS itself are extraordinarily long for a course that can be offered for half-credit, comprising 49 separate knowledge requirements. (While other TEKS are longer, many are only available as a yearlong course.)

Moreover, it is far and away the least-taken course in computer science. In the 2016-17 school year, a little under 48,000 students enrolled in at least one computer science course. This amounts to about 3% of the Texas HS student population. Computer Science I had the highest enrollment—just shy of 16,000 students, or around one percent of the total student body, took the course. Digital Forensics, meanwhile, had a total of 53 enrollees—a staggeringly low 0.0035% of the Texas public high school population. This is, of course, in part because of the fact that few schools offer the course—of the nearly 2,400 high schools in Texas, only 9 offer Digital Forensics. (By comparison, 400 offer Computer Science I.)

Texas is not the only state in the nation to lack a robust cybersecurity course in high school, and as a result a number of programs have sprung up in recent years to fill the gap. Since as far back as 1998, the NSA, joined a few years later by the Department of Homeland Security, has provided funding for institutions of higher education to study and teach cybersecurity. These National Centers of Academic Excellence (CAE)12 can receive funding for, two- and four-year programs at both the

11 https://www.iste.org/standards/for-computer-science-educators

12 https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae

bachelor's and master's level, as well as funding for research into cybersecurity. (The Department of Computer Science at UT Austin has received research funding under this program.)

In 2014, another NSA program, the College of Cyber, launched a K-12 education outreach program called GenCyber. GenCyber started with eight student camps around the country during their pilot year, and in 2015, their official launch year, 43 camps were held. In 2018, the program has held or will hold 149 camps at 84 different institutions, divided between 95 student camps, 39 teacher camps, and 15 camps for both students and teachers. (One recipient of the NSA funding is the Center for STEM Education, which received a grant to host a WeTeach_Cybersecurity GenCyber summer camp for teachers in June 2018.)

The federal government has also set up non-military programs with the goal of expanding access to cybersecurity education. In 2009, the National Institute of Standards formed the National Initiative for Cybersecurity Education (NICE), with the goal of improving the cybersecurity education landscape. Among other things, NICE partners with academia and the private sector to help energize and promote a robust network for cybersecurity education, training, and workforce development.

On top of this, in 2016, the Obama Administration announced the first Cybersecurity National Action Plan (CNAP)13 which, among other things, forgave student loans for certain cybersecurity experts who joined the federal workforce, highlighted cybersecurity as a part of the Computer Science for All initiative, provided additional funding to the NSA's CAE program, and created a CyberCorps reserve program as part of the Scholarship for Service. In total, the CNAP called for a $19 billion investment in cybersecurity.

SUMMARY

While things are trending up, Texas still has a lot of work to do. Although the enrollment numbers have doubled in the last five years, the total fraction of students enrolled in a computer science course hovers around 3%—meaning that, despite the overwhelming need, very few students actually end up getting any kind of computer science education in high school. As enrollment numbers have increased, equity still continues to be a challenge, and enrollment among women is actually tracking downwards. Though young women represent just under half—49%—of the Texas high school population, they have gone from filling 29% to 26% of the seats in computer science courses over the past five years.

Many of these enrollment concerns are caused, directly or otherwise, by the structural problems outlined above. Consider, for example, weighted funding. Simply by allocating funding on the basis of enrollment to schools that offer computer science courses, a number of the problems discussed above could be solved. For one, schools would be incentivized by the promise of additional funding to get more students into computer science courses. That funding could then be used to cover the costs of certification and professional development for interested teachers, driving up teacher certification rates.

As more teachers become certified to offer computer science courses, more schools would be able to offer those courses, driving up offering rates. Moreover, the increase in demand would enable projects like WeTeach_CS to offer more certification courses to teachers from schools with a greater percentage of underprivileged and underserved students, ensuring that any increase in enrollment reflects a commensurate increase in enrollment among all students, not merely those from privileged backgrounds.

Finally, although Texas currently lacks a robust cybersecurity course, there are a plethora of resources and sources of funding available that will enable it to offer one in the short term. By taking advantage of the efforts undertaken by the public and private sector, Texas can address its own educational gap in cybersecurity, enabling students to pursue careers in what is turning out to be an extraordinarily lucrative field.

But what exactly should Texas offer? What kind of course will students benefit from the most, and what content should that course offer? Where will it fit into the complex mesh of regulation that defines the Texan system of high school education? And, more importantly, to what end will students pursue this course? All of these questions are addressed in the following sections.

13 https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Course Design

Recall from above that computer science courses are enumerated under two separate sections of the TAC. Most computer science courses offered under Tech Apps are taught by educators with robust credentials in computer science education, whereas courses offered under Career and Technology Education do not, in general, offer the same guarantee of teacher knowledge, but nevertheless result in more funding for school districts. What knowledge a teacher would need to have to teach a cybersecurity course, however, is dependent on the content of the course. This is discussed below.

CURRICULUM STANDARDS

A number of organizations have put forth curricula for courses in cybersecurity. These groups range from universities like the University of Rhode Island, which has made publicly available the curriculum for their introductory cybersecurity course, Cyber Security Fundamentals; to secondary school teachers like Nebraska high school teacher Derek Babb, who maintains his cybersecurity course materials on GitHub for public use; to education-focused nonprofits, like the Computer Science Teachers' Association, which maintains an annually-updated list of cybersecurity curriculum standards. These standards diverge slightly from each other in content and organization, but in general they hew to a common set of principles. (A sampling of such course standards is available in Appendix A.)

The gold standard of course materials, however, is CSEC 2017, an extensively detailed course curriculum created last year. The product of a joint initiative by the Association for Computing Machinery, the IEEE Computer Society, the Association for Information Systems Special Interest Group on Security, and the International Federation for Information Processing, the guidelines were compiled by an international group of computer science and cybersecurity experts. The curriculum covers six cross-cutting concepts, defined by the report as follows:

- **Confidentiality.** Rules that limit access to system data and information to authorized persons.
- **Integrity.** Assurance that the data and information are accurate and trustworthy.
- **Availability.** The data, information, and system are accessible.
- **Risk.** Potential for gain or loss.
- **Adversarial Thinking.** A thinking process that considers the potential actions of the opposing force working against the desired result.
- **Systems Thinking.** A thinking process that considers the interplay between social and technical constraints to enable assured operations.

The curriculum itself is broken down into eight knowledge areas, each of which is focused on cybersecurity as applied to layers of the computing hierarchy (e.g., Data Security) and layers of the user hierarchy (e.g., Organizational Security). These knowledge areas are further broken down into knowledge units, topics, and learning outcomes.

The report itself is designed to serve as the basis for a collegiate cybersecurity program, spanning several years of courses at a post-secondary level. Nevertheless, while its recommendations can't be directly applied to the creation of a course at the introductory level, the concepts it covers and the knowledge areas it details are broad enough to be discussed over the course of a yearlong course in high school.

CYBERSECURITY CERTIFICATIONS

Before a student can enter the cybersecurity workforce, they must be certified as having expertise in the field. As the state of Texas builds a cybersecurity pathway in CTE, the courses selected for that pathway should be appropriate to prepare students who complete a four-year sequence to achieve one or more industry standards certifications, either directly out of high school or with minimal additional post-secondary coursework if possible.

One of the major employers in cybersecurity is the Department of Defense (DoD), which codifies certification requirements in DoD 8570[14]. Although the DoD is far from the only organization to hire cybersecurity talent, they are one of the major employers in the field in Texas, and as such their hiring requirements are worth a closer examination.

Of the fourteen positions discussed in DoD 8570, three require no prior experience. Each of these positions can be applied to with certifications from a variety of providers, but two certifications are more frequently received than the others:

- **CompTIA Security+.**[15] According to CompTIA, the Security+ certification is the most frequently taken course for DoD 8570 certification, and covers the fundamentals of network security. This certification is a requirement for the Level I and II Information Assurance Technician (IAT) and the Level I Information Assurance Manager (IAM) position. This certificate is achievable with a high-school background and some additional self-study, and is considered necessary (but is not formally required) to take the more advanced CompTIA Advanced Security Practitioner (CASP) certification[16].
- **Cisco Certified Network Associate-Security (CCNA).**[17] The CCNA is required for the Level I and II IAT positions, but unlike the Security+ certification would not qualify an applicant for the Level I IAM position. Unlike the more generic Security+ certification, the CCNA certification is specific to Cisco technologies, and may not be as broadly applicable.

(A full list of certifications recognized by DoD 8570 is available in Appendix B.)

Given the choice of orienting a course around one of these certifications, the Security+ is the more preferable option. Although both certifications are commonly taken, as noted above, the former is more generic, covering the general principles of information security. Moreover, the Security+ certification enables its recipients to apply directly for a managerial position, whereas the CCNA certification only applies to the technician position.

Obtaining either of these certifications would be a challenge for most high school students. An appropriate sequence of courses in high school, however, that focused on the competencies measured on the examination would provide high school graduates with a significant percentage of the training necessary to quickly pursue this certification after graduation.

14 https://iase.disa.mil/iawip/pages/iabaseline.aspx

15 https://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-401.pdf

16 The full requirements to take the CASP exam include the CySA+ and the PenTest+ certifications, along with the Security+ certification.

17 https://learningnetwork.cisco.com/community/certifications/ccna/ccna-exam/exam-topics

Implementation

TEXAS HOUSE BILL 3593

Recognizing the demand for qualified cybersecurity experts, the Texas Legislature passed House Bill 3593 in 2017. The bill revised sections of the Texas Administrative Code with the goal of improving cybersecurity education in Texas high schools. In particular, the bill proposed the creation of a five-course cybersecurity-focused pathway, which would prepare students for further study in security at the college level or for obtaining industry recognized certifications in cybersecurity. The bill quickly passed committee, was approved by the House and the Senate in short order, and was signed by the Governor a few months later.

The courses that form the pathway laid out in HB 3593 receive a number of important benefits. First, and most importantly, they will receive weighted funding. Moreover, the bill stipulates that "a teacher is entitled to a subsidy under this section if the teacher passes a certification examination related to cybersecurity." This stipend could provide the incentive needed for a teacher to master the concepts required to teach these courses. The relevant language of the bill is as follows (emphasis added):

> "In adopting rules under Subsection (c-1), the State Board of Education shall adopt or select **five technology applications courses on cybersecurity** to be included in a cybersecurity pathway for the science, technology, engineering, and mathematics endorsement. [...] "Career and technology education class" and "career and technology education program" include a **technology applications course on cybersecurity** adopted or selected by the State Board of Education under [the section above]."

In order for students to achieve the cybersecurity certifications that would enable them to pursue a job after high school, they would need to take more than just a single cybersecurity course, especially an introductory one. Those students who wished to pursue post-secondary education in cybersecurity would likely need to master a different set of competencies. The competencies needed for either path—industry or academia—do not differ significantly from each other, however. A single, carefully chosen pathway of courses would easily serve to address both sets of needs.

A PATHWAY TO CYBERSECURITY

In general, once they complete the pathway, students should achieve competency with three broad subject areas:

1. **Computer science.** While computer science and cybersecurity are often conflated, they are different fields or at minimum, different specialties in the same career. Nevertheless, a true cybersecurity expert—even one who would be able to achieve the Security+ certification—would benefit from some exposure to computer science while they study security.

   A number of existing courses can address this subject area, but four in particular strike the best balance of ease of implementation and relevance: Fundamentals of Computer Science, Computer Science I, AP Computer Science Principles, and AP Computer Science A. While students would likely only need one of these courses to develop a competency with computing, all four courses should be included as options in the pathway to provide school districts with the most flexibility of implementation.

2. **Security.** A background in computer science and networking is not sufficient to achieve the Security+ certification, and any student wishing to achieve the certification would need to study cybersecurity independently.

   As with networking, no existing course is both current enough and relevant enough to address this skill set well. Another innovative course—Principles of Cybersecurity—would fill that gap. The course, developed by Southwest ISD teacher and Associate Director of the CyberTexas Foundation, Michael Maldonado, is also currently classified as innovative, and should be promoted if adopted in the pathway.

3. **Networks.** One of the three major certifications required for most entry-level positions is the Network+ certification, which measures knowledge of system design at a network level. The security challenges are related, as noted by the CSEC 2017 standards, to those encountered in the study of individual device security, but are nonetheless different and require separate training.

   While a course in networking is currently included in TEKS, the material of the course has not been updated to account for changes in industry standards. On the other hand, Internetworking Technologies is far more recent and provides both an introduction to networking as well as some exposure to the fundamentals of routing and switching systems. The class is currently classified as an innovative course, but if included in the pathway should be classified as a standard course and included in TEKS.

4. **Cybersecurity.** A new capstone course, **Cybersecurity I**, should be developed to bring all of these concepts together with hands-on experiences at a high level that equip students to address challenges similar to a cybersecurity professional. The course should be designed like a practicum and be motivated by the CSEC 2017 standards. It should cover topics such as:

- Systems Architecture and Design
- Risk Assessment
- Cloud Computing
- Identity and Access Management
- Mobile Security
- Cryptography
- Computer Architecture
- System Security on major operating systems, including Windows, macOS and Linux

5. **Specialized courses.** If students have additional space in their high school course schedule, other courses such as Computer Maintenance or Digital Forensics would also be appropriate to prepare them with the concepts they need to continue to pursue cybersecurity beyond high school. These courses would allow students who have an interest in specializing in areas such as hardware or computer security incident response to delve deeper in high school.

Summary and Recommendations

The availability and diversity of computer science course options in high school has exploded over the past 20 years. That progress could only have been achieved by a coalition of the willing: innovative educators, forward-thinking administrators, concerned parents, and of course, motivated students. But, while course options have increased, enrollment numbers are still at unacceptable levels. There is still much work to be done to ensure that every graduate has access to the kinds of high-paying, high-demand jobs that will drive the Texas economy forward.

After thoroughly reviewing the educational landscape; consulting educators, administrators, and subject matter experts; and carefully considering a number of different approaches, the Texas Computer Science Task Force has arrived at a list of recommendations for the Texas State Board of Education and the Texas Education Agency. These recommendations are divided into two categories. Recommendations I, II, and III pertain to the implementation of a cybersecurity pathway, as outlined by HB 3593. Recommendations IV, V, and VI call for further improvements to K-12 computing education policy and funding to support increased access to and enrollment in CS and cybersecurity course pathways by Texas students.

The report of the first Task Force, compiled in 2014, identified the roadblocks to creating a better educational system for computer science for the first time. The problems that report addressed were general and applied to the entire field of computer science. This report builds on those recommendations with an explicit focus on the field of cybersecurity. They are written for this moment, at a time when the implementation of HB 3593 can, if done right, lead to a dramatic and permanent increase of the availability, quality, and impact of computer science education in Texas high schools.

CREATE A CYBERSECURITY CAPSTONE

Recommendation I. The Texas State Board of Education should create a new capstone course, Cybersecurity I, for students seeking practical, hands-on experience in computer security.

As discussed above, while there currently exist courses that address the introductory aspects of cybersecurity (e.g., Principles of Cybersecurity), a capstone course that connects all the various competencies into one comprehensive, in-depth, year-long program of study is necessary to effectively prepare students for post-secondary careers. As such, it is the recommendation of this Task Force that the SBOE create a new capstone course—Cybersecurity I—with the intention of preparing students for more advanced study in cybersecurity. This course should give students the opportunity to develop and practice the skills and strategies that are deployed by cybersecurity professionals.

This course should be designed with the CSEC 2017 standards and the concepts it enumerates in mind. Moreover, the course should prepare students for the real world through practical exercises that build their competencies with different skill sets. The course should give students the ability to, at a minimum, be able to solve problems testing different competencies, such as cryptography, mobile security, and information assurance.

Students who complete this practicum as a capstone to the cybersecurity pathway should be able to sit for the CompTIA Security+ (or equivalent) certification exam with only a minimal level of self-study. As a capstone course, Cybersecurity I should allow teachers maximum flexibility in designing the course to their students' needs, but it should at the very least enable students to pursue the post-secondary track of their choice, be it further study or industry experience.

As outlined in Recommendations II and III, this course should be included in the cybersecurity pathway, and be classified under Career and Technical Education in the TAC. (It may, at some future point, be worth examining the certification SBOE requires for teachers of the course.)

DESIGNATE A CYBERSECURITY PATHWAY

Recommendation II. The Texas State Board of Education, pursuant to HB 3593, designate a list of courses, ending with Cybersecurity I, as part of a cybersecurity pathway.

HB 3593 empowers TSBoE to create a five-course pathway for students seeking to study cybersecurity. We recommend that the following courses be included in this pathway:

1. Fundamentals of Computer Science, Computer Science I, AP Computer Science Principles, and AP Computer Science A.
2. Principles of Cybersecurity
3. Internetworking Technologies.
4. Cybersecurity I.
5. Additional course options: Computer Maintenance, Digital Forensics, or any other computer science course. The current Web Communications course, if the TEKS were updated to include a study of web-based cyberwarfare, would be appropriate for this pathway as well.

As mentioned above, the second and third course on this list are both currently classified as innovative courses. It is the recommendation of this Task Force that, based on the standards for these courses related to cybersecurity and their ability to prepare students for industry certifications, they be reclassified as permanent courses and included in TEKS.

It is the belief of the Task Force that students who completed this pathway would, with some additional self-study, be prepared to sit for the CompTIA Security+ or equivalent certification exam. This, as noted above, would be sufficient to qualify them for one of the thousands of entry-level positions in cybersecurity in Texas.

MOVE COMPUTER SCIENCE TO CTE

Recommendation III. The Texas State Board of Education and the Texas Education Agency should move all computer science courses currently offered to Chapter 130 of the Texas Administrative Code and reclassify them under Career and Technical Education.

As outlined above, the current duality of computer science in Texas high schools—split as they are between Technology Applications and Career and Technical Education—presents a false choice to teachers and administrators between fiscal responsibility and student success. Schools are forced to cut the Gordian knot by offering CTE courses in lieu of the courses more relevant to computer science, even when they have teachers certified to the rigorous TA standard.

This situation is clearly untenable. By taking the step of moving every computer science course from TA to CTE, the SBOE would, as mentioned above, improve both offering and enrollment rates of computer science in Texas with one stroke. Moving all CS courses under the CTE umbrella would ensure funding flows directly to districts who are actually enrolling students in CS courses. In addition, because CTE programs are also audited to ensure that the students enrolled in them are representative of the student body, districts would be additionally incentivized to diversify their CS course enrollment.

The Center for STEM Education surveyed 40 CS teachers, industry experts, and other stakeholders in 2017 to determine specifically which courses fit the definition of computer science, as defined by the Computer Science Teachers Association, based on the content of their TEKS. Based on this feedback,

fourteen courses currently listed under Technology Applications (listed above in Table 1) fall under that classification, and should be considered as such for the purposes of this recommendation.

Moving CS courses from Technology Applications to CTE would also allow the state and local districts to draw down additional funding under the Perkins Act of 2006 that is not currently available to support computer science in Texas. A number of other states, including Missouri, Nevada, Georgia, North Carolina, Indiana, Utah, Rhode Island, Virginia, and Alabama, all classify CS as CTE courses, and thus are able to access Perkins funding to support teacher professional development and technology.

Moreover, moving all CS courses under the CTE umbrella would better connect students to the workforce and support alignment between CS courses and the rapidly changing technology landscape. Having CS under CTE in most districts would facilitate the connections to industry that are already the responsibility of the CTE coordinators in most districts. Currently, some districts manage computer science under Mathematics; others manage it under Technology; and still others manage it under CTE. As such, it is difficult for the state to provide consistent support for local districts. Aligning all CS courses under CTE could also facilitate and streamline the support that is desperately needed but currently unavailable from TEA.

Finally, by moving CS to CTE, the state achieves a long-term solution to the challenge of funding for teacher professional development. School districts who choose to offer computer science and/or cybersecurity courses will have the funding they need to support continued training for teachers both for initial certification and to keep them current on changing technology trends and tools. Continued investment in teacher growth is an absolute necessity given the rapidly changing nature of the field. This investment by the state should make it easier to then leverage philanthropic support for professional development and new teacher incentives for certification.

If this step were to be taken, however, it is the recommendation of the Task Force that the existing standard of teacher certification under Technology Applications be maintained under CTE. Troublingly, the CTE business certification exam, required to teach CTE courses, contains no actual measure of competency related to computer programming. The state would do a disservice to parents, administrators, and students if we did not ensure that teachers who are authorized to teach computer science have demonstrated mastery of the content needed to do so. Although this content is rigorous and challenging, projects like WeTeach_CS have demonstrated that, given the right training, support, and incentives, significant numbers of teachers are able to master the concepts that are measured on the TExES exam.

CREATE A PLAN FOR CYBERSECURITY

Recommendation IV. The Texas Education Agency should develop a long-range plan to monitor the implementation of the cybersecurity course pathway.

As certification requirements may change or evolve over time, a periodic review of all courses related to computer science, IT, and cybersecurity should be conducted to ensure they are up-to-date and cover the concepts that can lead to a Security+ or equivalent industry certification. An additional component of the long-range plan should ensure that the TEA leadership stays connected with and monitors federal agency efforts to develop high school cybersecurity courses. In particular, TEA should consider developing a Cybersecurity II course once enough students participate in the cybersecurity pathway, and enough teachers have been trained to warrant a more advanced course.

UPDATE COMPUTER SCIENCE TEKS

Recommendation V. The Texas State Board of Education should conduct a formal, thorough review of the TEKS for every computer science course, focusing on overlaps or oversights in course content.

Once every CS course is moved to CTE, the SBOE should conduct a review of Tech Apps and CTE courses to eliminate duplication and simplify the list of course options. There are a number of Tech Apps courses that have, over time, been replicated under CTE to receive better funding. For example, Computer Programming,

a CTE course, is replicated in large part by the far more rigorous Computer Science I, a TA course. Many schools offer Computer Programming because it receives weighted funding, even though they have a certified CS teacher with appropriate training who could teach Computer Science I. The SBOE may consider phasing out the Computer Programming course as enough teachers become certified to teach other CS courses.

UPDATE K-8 TECHNOLOGY APPLICATIONS TEKS

Recommendation VI. The Texas State Board of Education should update the current K-8 Technology Applications TEKS to include more emphasis on computational thinking and computer science rather than simply the use of technology.

Preparing students to consider a computing career must begin prior to high school. The current Technology Applications TEKS for K-8 courses need to be updated to better address the computational thinking practices and skills that are foundational to further study of computer science and also the personal digital security practices that every user of technology should employ and that form the basis for personal cybersecurity. The K-12 Computer Science Framework from the Computer Science Teachers Association provides a strong model for developing such standards.

The SBOE should also consider strategies for integrating computational thinking into the TEKS of other core academic courses to ensure the foundational problem-solving skills and thinking practices associated with computing fields are part of the broader educational experience of every student, regardless of the endorsement they choose in high school. This integration should be part of SBOE's regular TEKS review process.

Appendix A: Cybersecurity Curricula

In designing a new computer science course, a number of factors must be considered: what questions to answer and at what level to answer them. Fortunately, as computer science has become more and more vital to a secondary education, a number of curricula have been developed for public use. These are guidelines, and can help in considering what kinds of subjects to discuss and how to structure those discussions:

- The National Integrated Cyber Education Research Center (NICERC) provides curricula and course materials related to personal cybersecurity.
- Girls Go Cyberstart is a program sponsored by Governor Abbott's office designed to engage high school girls in cybersecurity.
- The University of Rhode Island has put together a curriculum for their CSF 102 course, Cyber Security Fundamentals.
- Derek Babb, a high school teacher in Nebraska, has open-sourced the curriculum for his cybersecurity course on GitHub. As a result, the curriculum is freely usable and editable.
- San Antonio College offers the Information Technology and Security Academy (ITSA) Level I certificate to their students.
- The CyberPatriot competition maintains a list of cybersecurity-focused modules online. The content of these units is informed by industry needs.
- The GenCyber program at the University of Tulsa maintains an extensive compendium of online resources, lesson materials, and capstone projects for high school cybersecurity courses.
- Hacker High School maintains an extensive list of course curricula and textbooks on their website.
- The Computer Science Teachers' Association curates a list of course standards, including a number of cybersecurity-focused requirements, updated annually.
- K-12 Computer Science maintains a similar list of course standards on their website.
- Project Lead the Way has created a cybersecurity course and maintains a curriculum and course resume online.
- CodeHS, an online platform that helps teachers offer computer science courses, offers an annual cybersecurity course, the curriculum for which is posted online.

In addition to these resources, a number of federal- and state-level standards have been created to define the scope and depth of the field:

- The National Institute for Science and Technology has developed the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which defines the key areas of cybersecurity and categorizes cybersecurity work into distinct specialty areas and work roles.
- The Virginia CTE Resource Center has developed a task list of fundamental competencies in cybersecurity. Of the 104 competencies on the list, 71 are focused on cybersecurity, while the remaining 33 apply to any CTE course.
- The Tennessee Department of Education has developed a number of IT-focused pathways offered to Tennessee high school students, and maintains an extensive list of certifications and online resources for course development.

Appendix B: DoD 8570 Certifications

The DoD 8570 matrix covers the certification requirements for four different jobs: Information Assurance Technician (IAT), Information Assurance Manager (IAM), Information Assurance Systems Architect and Engineer (IASAE), and Cybersecurity Service Provider (CSSP). The matrix is further broken down by job level. (DoD 8570.01-M[18] describes in detail the responsibilities and requirements of each of these roles.)

Each entry in the matrix contains a list of certifications from a number of different providers. (Applicants only need one, however.) In total, there are 27 certifications recognized by the DoD, provided by seven different certifying bodies:

PROVIDER	CERTIFICATIONS PROVIDED	JOBS AVAILABLE
Cisco	• CCNA Security • CCNP Security • SCYBER	• IAT L. I-II • IAT L. III • CSSP-A, CSSP-IR
CompTIA	• A+ CE • Security+ CE • CASP CE • Network+ CE • CySA+ CE	• IAT L. I • IAT L. II; IAM L. I • IAT L. III; IAM L. II; IASAE L. I-II • IAT L. I • IAT L. II; all CSSP except CSSP-SPM
EC-Council	• CEH	• all CSSP except CSSP-SPM
(ISC)2	• CISSP/Associate • CSSLP • CAP • SSAP • ISSEP • ISSMP • SSCP	• IAT L. III; IAM L. II-III; IASAE L. I-II • IASAE L. I-II • IAM L. I-II • IASAE L. III • IASAE L. III • CSSP-SPM • IAT L. I-II; CSSP-IS
ISACA	• CISM • CISA	• IAM L. II-III; CSSP-SPM • IAT L. III; CSSP-AU

18 http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf

PROVIDER	CERTIFICATIONS PROVIDED	JOBS AVAILABLE
GIAC	• GCIA • GCED • GCFA • GCIH • GICSP • GSEC • GSLC • GSNA	• CSSP-A • IAT L. III • CSSP-IR • CSSP-A, CSSP-IR • CSSP-A, CSSP-IS • IAT L. II • all IAM • CSSP-AU
Logical Operations	• CSP	• CSSP-A, CSSP-IR

Table 3: DoD 8570 certifications. The acronyms are expanded in the text of DoD 8570.

Task Force Membership

Dr. Carol Fletcher -Chair
Deputy Director, Center for STEM Education
The University of Texas at Austin

Brittany Barnes
Security Software Engineer
IBM Corporation

Dr. Amie Berg
Career and Technical Education Teacher
Magnolia Independent School District

Jennifer Bergland
Government Relations
texas Computer Education Association

Joonyee Chuah
Education and Outreach Program Coordinator
Texas Advanced Computing Center

Camille Clay
Senior Director, College and Career Transition Programs
Leander Independent School District

Edward Doan
Customer Engineer
Google for Education

Tommy Gober
Curriculum Development Specialist
National Integrated Cyber Education Research Center

Lizzette Gonzalez Reynolds
Vice President of Policy
Excel in Ed

Rohan Ramchand
Software Engineer

Ann Graham
Cyber Day Program Manager
IBM Corporation

Frederick Hall
Cyber Security Expert
United States Airforce

Kim Hughes
Director, UTeach Institute
The University of Texas at Austin

Kathryn Ives
Coordinator of Instructional Technology
Pflugerville Independent School District

Deborah Kariuki
Computer Science Teacher
Pflugerville Independent School District

Dr. Herb Krasner
Senior Lecturer, Electrical and Computer Engineering
The University of Texas at Austin

Dr. Craig Levy
Secondary Math Specialist
Austin Independent School District

Dr. Calvin Lin
Professor of Computer Science
The University of Texas at Austin

Michael Maldonado
Cybersecurity Teacher
Southwest Independent School Distirct

Ryan Monaghan
Computer Science Teacher
Richardson High School

Kevin Nolten
Director of Academic Outreach
National Integrated Cyber Education Research Center

John Owen
Computer Science PD Specialist,
Center for STEM Education
The University of Texas at Austin

Robin Painovich
Executive Director
Career and Technology Association of Texas

Julie Petrus
Counselor
San Marcos Independent School District

Aaron Schmidlkofer
Clinical Teacher of Computer Science
Richardson Independent School District

Hal Speed
Founder
CS4TX

Ryan Torbey
Computer Science Education Consultant
Coding4TX

Henry Vo
Computer Science Teacher
Richardson Independent School District

Joules Webb
Associate Director, Pre-Engineering Program
The University of Texas at San Antonio

Amy Werst
Assistant Director for Outreach and Strategic
Planning, Center for STEM Education
The University of Texas at Austin

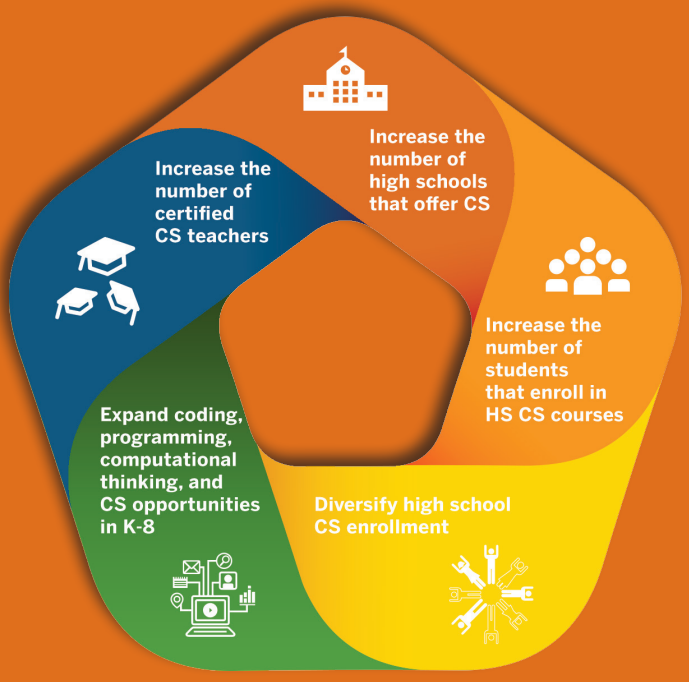
Sylvia Wood
Computer Science Teacher
Leander Independent School District

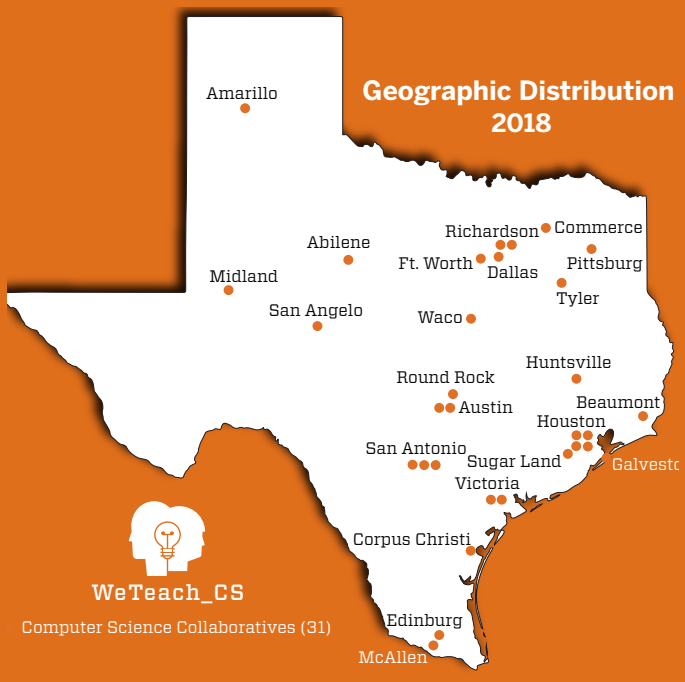
What is WeTeach_CS?

Since 2014, WeTeach_CS has built teacher, district, and state-wide capacity in K-12 computing education. By substantially increasing the number of certified CS teachers, WeTeach_CS has contributed to significant improvement in the number of high schools offering CS, the number of students completing CS courses, and the diversity of students completing CS courses.

STATEWIDE NETWORK

On December 15, 2017, The University of Texas at Austin announced that WeTeach_CS had received a $5 million grant from the Texas Education Agency (TEA) to provide professional development to computer science teachers around the state and to help increase the number of certified CS teachers in Texas. Thirty-one WeTeach_CS Collaboratives were funded for 2018.





TEXAS

The University of Texas at Austin