ISSN: 2473-4901
v9 n5955

Comprehensive Cybersecurity Programs: Case-Study Analysis of a Four-Year Cybersecurity Program at a Secondary Education Institution in Arizona

Paul Wagner
paulewagner@arizona.edu

Dalal Alharthi
dalharthi@arizona.edu

Department Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, Arizona 85747, USA

Abstract

Educating the next generation of cybersecurity professionals requires a shift into the K-12 space. Introducing cybersecurity at K-12 provides general cybersecurity literacy, career readiness, and early development of cybersecurity knowledge, skills, and abilities to become cybersecurity professionals. Cybersecurity education standards and guidelines traditionally focused on post-secondary education until 2021 when Cyber.org and TeachCyber released their K-12 Cybersecurity Learning Standards and the High School Cybersecurity Curriculum Guidelines respectively. Despite these initiatives, there is limited literature on the development of cybersecurity programs at secondary education institutions. Also, available resources to develop and support these programs differ from district to district and among states. To overcome these deficits, this paper presents a case study conducted at a comprehensive four-year cybersecurity program at a secondary education institution. The case study consisted of open-source research, document reviews, questionnaires, and interviews. The data collected were compiled into a program profile consisting of student enrollment; demographics; personnel; operational requirements; formal, informal, and non-formal learning activities; and pathway opportunities. The developed program profile provides a structure to analyze other programs internal or external to Arizona. The enhanced data set can provide the ability to compare programs to develop best practices for establishing cybersecurity education programs at secondary education institutions. This profile can allow schools considering the development of a program at their institutions to better understand the requirements and resources needed to establish the program. Additionally, the data collected provides a baseline to compare their district and school to understand the implications within the context of their environment.

Keywords: Cybersecurity Education, Workforce Development, K-12 Education, Program Evaluation, Educational Strategies

1. INTRODUCTION

Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. The most recent (ISC)2 Cybersecurity Workforce Study estimates a global cybersecurity workforce gap of over 3.4 million

(ISC2, 2022). CyberSeek estimates that there are over 750,000 cybersecurity job openings (CyberSeek, 2023). As cybersecurity threats continue to grow in sophistication, scope, and scale, the ability to secure the United States from these threats lies in the ability to develop cybersecurity professionals with the Knowledge, Skills, and Abilities (KSAs) to accomplish the tasks associated with cyber roles. The ability to supply qualified cybersecurity professionals is outpaced by the growing demand as previously outlined. Cybersecurity programs have been expanding at post-secondary institutions and are being introduced at secondary education institutions. This paper reviews a case study conducted on an established four-year comprehensive cybersecurity program at a secondary education institution in Arizona.

2. LITERATURE REVIEW

A Systematic Literature Review (SLR) technique was used to find relevant articles from 2010 to 2023. Selected articles provided relevant information for analysis and discussion, covering topics such as cybersecurity, standards, guidelines, education, K-12 education, legislation, dual enrollment, certifications, and safety. Given the limited research on K-12 cybersecurity education and its relevance to current workforce shortages, a comprehensive set of search criteria was employed. Full-text journal articles were analyzed to explore initiatives in K-12 cybersecurity education, training, and workforce development. Information from these articles was used to develop questionnaires, interview guides, and program profiles. Editorials, trade journals, and online resources were also consulted to gather current statistics, applications, and concerns in cybersecurity education and workforce development.

K-12 Education

At a fundamental level, cybersecurity education is, "providing students with an understanding of how connected electronic devices interact in a digital age, how to protect digital assets from vulnerabilities and the moral and ethical issues surrounding the uses of technology in our society." ("The State of Cybersecurity", 2020). K-12 education institutions have a key role in addressing the cybersecurity professional shortage in two primary ways. First, K-12 education provides the ability to raise awareness and interest in cybersecurity careers. Second, it provides a conduit for fundamental knowledge needed to pursue post-secondary education or career pathways in this field. However, nationally there is a lack of quality Science, Technology, Engineering, and Math (STEM) programs, which cybersecurity is part of; lack of accessibility by all students, specifically minority students and students from lower Socio-Economic Status (SES); and overall stagnant performance in STEM assessments (Burke, 2021). Additionally, 75% of recent high school graduates feel they are underprepared to make college and career decisions (Lucariello, 2022) and are underprepared to enter the workforce (Lim, 2019). Further, the results of a 2020 national survey on the state of cybersecurity education in K-12 schools identified the following:

- Most K-12 educators do not know a lot about cybersecurity education.
- Cybersecurity deserts associated with inequitable access to cybersecurity education persist.
- Most students know little or nothing about cybersecurity.
- Access to cybersecurity education is infrequent and uneven.
- Cybersecurity education is rarely a focus of extracurriculars despite student interest.
- Cyberbullying and Terrorism are the most frequent cybersecurity education topics in K-12 schools ("The State of Cybersecurity", 2020).

Standards

There are multiple standards organizations aligned with cybersecurity workforce and education. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181 (Petersen, 2021), the National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C) (NCAEC, N.D.), the Association for Computing Machinery's (ACM) curriculum guidelines for post-secondary degree programs in cybersecurity ("Curriculum Guidelines", 2017) and cybersecurity curricular guidance for associate-degree programs ("Cybersecurity Curricular Guidance", 2020) provide guidance on cybersecurity curriculum mainly focused on post-secondary education.

K-12 specific cybersecurity education standards and guidelines were not available until 2021 when the national K-12 Cybersecurity Learning Standards ("K-12 Cybersecurity Learning Standards", 2021) and the High School Cybersecurity Curriculum Guidelines (Dark, 2021) were released. The K-12 Cybersecurity Learning Standards identify key fundamentals of cybersecurity education including computing systems, digital citizenship, and security ("K-12

Cybersecurity Learning Standards", 2021). The Curriculum Guidelines identify eight "Big Ideas" which include ethics, establishing trust, ubiquitous connectivity, data security, system security, adversarial thinking, risk, and implications (Dark, 2021).

Curriculum

Similar to standards, there are multiple resources for cybersecurity education content developed for post-secondary. The National Cybersecurity Training and Education (NCyTE) ("Cybersecurity Curriculum," 2021), Centers of Academic Excellence in Cybersecurity Resource Directory (CARD) ("CARD," 2021), and Cybersecurity Labs and Resource Knowledgebase (CLARK) ("CLARK," 2021) provide various resources ranging from nanomodules (1 hour or less) to full courses (15 weeks) across a wide range of subjects.

Cyber.org and the RING (Regions Investing in the Next Generation) programs provide cybersecurity curricula specific to K-12. Cyber.org provides four cybersecurity-specific courses for K-12 education: Cyber Literacy (Grades 8 – 10), Cyber Literacy II (Grades 9 – 12), Cybersecurity Basics (Grades K – 8), and Cybersecurity (Grades 10 – 12) ("Cybersecurity," 2022).

RING is "an online high school cybersecurity course that offers interesting and engaging content specifically for students and schools without an existing cybersecurity program" that was officially launched in the summer of 2022 (Hairston, 2022). The program is divided into ten units consisting of an introduction, ethics, establishing trust, ubiquitous connectivity, data security, introduction to Python programming, system security, adversarial thinking, risk, and implications. RING is designed to be a fully developed year-long program for secondary education.

Despite the increasing amount of information on cybersecurity education, content, and curriculum, there is a lack of understanding of how cybersecurity education programs are developed, the resources needed to support these programs, and the formal, informal, and non-formal learning activities integrated into these programs.

3. RESEARCH METHODOLOGY

The purpose of this study was to identify the elements of a comprehensive high school cybersecurity program and develop a program profile containing the elements identified during research, document review, questionnaires, and interviews. The focus of the

Research Approach

This work utilized a case study approach. Yin (2003) defined a case study as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are evidence…and it relies on multiple sources." This research utilized multiple data collection techniques including reviewing relevant documents, conducting interviews, and compiling direct observations of the program.

Research Design

The five components related to case studies identified by Yin (2003) informed the research design and included the study's questions, study propositions, unit(s) of analysis, the logic linking the data to the propositions, and the criteria for interpreting findings.

Publicly accessible data was collected to establish the initial program profile. Questionnaires and interviews were conducted to identify additional elements missing from the initial program profile and provide context on how the program was established, identify the personnel and resources available, identify challenges and opportunities in establishing the program, and identify future growth and initiatives pursued by the programs.

The interviews followed a semi-structured approach where the interviewer and respondents engaged in a formal interview, the interviewer developed and used an interview guide, and although the interviewer followed the guide, topical trajectories which strayed from the interview guide were followed when appropriate.

Study propositions direct attention to something that should be examined in the scope of the study (Yin, 2003, p. 22). Based on the literature review about the current state of cybersecurity education institutions the following proposition was identified: Evaluating current cybersecurity programs at secondary education institutions can identify elements of a comprehensive cybersecurity education program.

The unit of analysis for a "case" study can be an individual, an event, or an entity. The unit of analysis for this case study was defined as the cybersecurity education program at Basha High School located in the Chandler Unified School District in Chandler, Arizona. Basha High School's cybersecurity program was selected since it is the most comprehensive and established program within Arizona. Stakeholders were identified as those having direct involvement in developing the program and those who had secondary input or taught within the program. All data collected were used to develop the program profile and used to address the proposition.

Finally, analogic inference was used to interpret the findings since statistical analysis would not be appropriate due to the limited number of interviews conducted. Analogic reasoning provides the ability to determine similarities and to make inferences from one situation to another (Calhoun, 2009). This method was appropriate considering that secondary education institutions share a similar architecture, follow state testing standards, and generally follow similar operational aspects.

4. ANALYSIS AND RESULTS

Researchers identified the salient elements informed by the literature review and interviews conducted during this study. The elements identified were enrollment; demographics; operations which included personnel and equipment; formal, non-formal, and informal learning activities; and pathways. The program profile provides insight into the cybersecurity program at the secondary education institution within Chandler Unified School District. The insight can identify personnel, resources, challenges, and opportunities for other schools interested in understanding the requirements to develop cybersecurity education programs at their institutions.

Basha High School's Cybersecurity Program

The entirety of Basha High School's program profile can be found in Appendix A. This section highlights some of the important data collected at this school. The program began in the 2019-2020 school year with 60 students. The 2022-2023 school year had 154 students. Figure 1 depicts the student enrollment breakdown. The cybersecurity program graduated one student in 2020, one student in 2021, two students in 2022, and 17 students in 2023 (Figure 2).

The operational aspects of the cybersecurity program consist of personnel, equipment, network, and facilities. The program is primarily supported by three Full Time Equivalent (FTE) teachers. The itemized initial equipment list for year one operations is in Appendix A. Initial startup costs were approximately $32,000. Additionally, the program required a separate network from the school district-provided network. The isolated network was installed in the cybersecurity classrooms and lab spaces to allow access to websites and resources to facilitate learning objectives that would be blocked on the district network. This isolation also required separate hardware due to restrictions on district-provided equipment. Finally, the program has four dedicated learning areas. There are three general-purpose classrooms and one Career and Technical Education (CTE) lab. The CTE lab has a larger footprint consisting of teaching space and a space for hands-on activities and equipment storage.

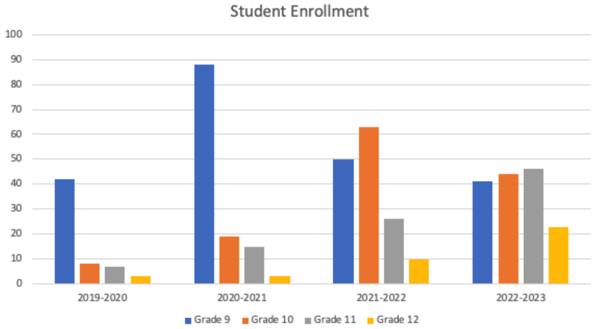


Figure 1: Basha High School Student Enrollment

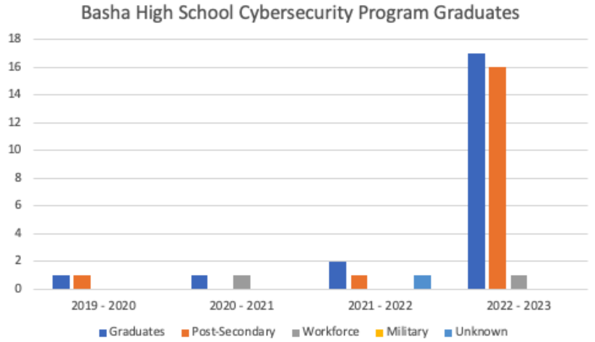


Figure 2: Basha High School Program Graduates

Basha High School's cybersecurity program's formal learning activities were modeled after the established pathway between Chandler Gilbert Community College (CGCC) and the University of Arizona (UA). Developing the program had an initial goal of providing a seamless pathway from the high school, through the community college, to the university. The courses within CGCC's cybersecurity program were analyzed to identify which courses would fit into Basha High School's cybersecurity program and articulation and pathways for students, meet dual-enrollment requirements, and align with existing Arizona CTE technical standards for network security identified as 11.1999.00. Ten courses were identified for inclusion into the program: Introduction to Computer Systems, Hardware and Software Configuration and Support (A), Hardware and

Software Configuration and Support (B), Introduction to LAN and Security Fundamentals (A), Introduction to LAN and Security Fundamentals (B), Linux OS, Advanced Linux, Information Security Fundamentals, Ethics in Information Technology, and Python. The descriptions for each course are outlined in the Basha High School cybersecurity program profile in Appendix A. Each of the ten courses allows dual enrollment.

Additionally, Basha High School is a Cisco Networking Academy (NetAcad). This provides access to curriculum and teaching resources, equipment and software, professional development opportunities, and help students access job opportunities (Cisco, 2023). Further, the program leverages content, assessments, and labs from Cisco, TestOut, and Cengage to meet formal learning objectives. The course alignments and costs of these materials are outlined in Appendix A. The program used RedHat Linux since program inception; however, due to changing requirements, the program will switch to Cisco curated content beginning in the 2023 – 2024 school year.

Non-formal learning activities include camps, certifications, internships, and externships. AZ Cyber Initiative and CyberPatriot are the cybersecurity-specific camps currently offered as part of Basha's cybersecurity program. AZ Cyber Initiative is a multifaceted program offering scholarships, mentorship, internships, and cybersecurity boot camps. Scholarships provide financial assistance for high school students pursuing degrees or professional certifications in cybersecurity-related fields or cybersecurity-related careers in the U.S. military. The mentorship program "connects high school students with qualified professionals to gain unique insights and important tools to help them find greater success ("AZ Cyber Mentorship", 2023)." Paid internship opportunities are provided to students who complete the associated boot camp which will be discussed next. These internship opportunities place students with companies and professionals to serve as cyber consultants for small businesses. Finally, AZ Cyber Initiative provides camps to high school students and teachers. Each boot camp is a weeklong course that provides students with knowledge, hands-on activities, career development, and career exploration. The teacher boot camp prepares teachers to integrate content into existing courses and develop cybersecurity courses or programs.

The CyberPatriot program provides multiple resources for middle and high school students. Basha High School began offering CyberPatriot camps in August of 2022. CyberPatriot offers a standard camp consisting of an introduction to CyberPatriot, an introduction to virtual machines, cyber ethics, Windows 10 and Ubuntu 18 Operating Systems. Additionally, an advanced camp offers cyber ethics, Windows 10 and Ubuntu 18 Operating Systems focusing on advanced skills and system administrator tasks and provides Cisco NetAcad access. Both camps offer a competition day to compete against other camps nationally.

A detailed discussion of the certifications integrated into Basha High School's cybersecurity program is outside the scope of this study. Program curriculum aligns with or introduces concepts for CompTIA's A+, ITF+, Linux+, Security+, TestOut's Security Pro, and Python Institute's Python Certified Entry-Level Program (PCEP) certifications. Certification allows high school students to be more employable and validate a foundational level of proficiency in several IT and cybersecurity work roles. For example, A+ aligns with Information Assurance Technical (IAT) I and Security+ aligns with Information Assurance Manager (IAM) I Department of Defense (DoD) approved baseline certifications ("DoD Approved 8570 Baseline Certifications," 2023).

Basha High School has partnered with several partners to provide students the opportunity to participate in internships and externships. The partnership with Open Source Integrators allows students to work with teams of open source Enterprise Resource Planning (ERP) professionals. The partnership with ElevateEdAZ provides externship opportunities focused on aligning education to workforce learning paths. This initiative prepares students for college and careers by partnering with education, business, and the community. The program specifically focuses on creating opportunities for high-wage, high-demand pathways which include Information Technology and Cybersecurity. This externship provides participants with a stipend upon completion of the program. The weeklong externship program consists of multiple sessions on technology-related topics, career pathways, required skills, and current events. Additionally, students participate in team-based projects and job preparation, and professional development sessions.

Informal learning activities include clubs, competitions, self-study and ad-hoc learning, conferences, and industry events. Basha High School's cybersecurity program integrates multiple informal learning activities for students. As part of their overall CTE program, The Future Business Leaders of America (FBLA) and Family, Career, and Community Leaders of America (FCCLA) prepare students to become community-minded business leaders. FCCLA is an example of a student club. Additionally, Basha High School's cybersecurity program offers students the opportunity to compete in the CyberPatriot competition and National Cyber League (NCL). CyberPatriot is typically held during the fall semester and NCL is held in the spring allowing students to compete throughout the school year. CyberPatriot competitions consist of a network security challenge and a Cisco networking challenge. Teams compete over six hours. Whereas CyberPatriot focuses on network defense, National Cyber League is a comprehensive competition including Open Source Intelligence (OSI), cryptography, password cracking, log analysis, network traffic analysis, forensics, web application exploitation, scanning, and enumeration and exploitation (NCL Categories, 2023). Additionally, the Basha cybersecurity program set up a tour of the PhoenixNAP Data Center providing insight into one aspect of the career field. Finally, self-study and ad-hoc learning and conferences are not coordinated through the program but advertised and encouraged. Teachers and students participated in CactusCon a Phoenix-based cybersecurity conference, Women in Cybersecurity (WiCyS), NICE K-12 Conference's student signing day, and Embry Riddle Aeronautical Engineering cyber day.

Pathways become part of a future-focused program. Preparing students for post-secondary education, trade schools and certification training, military service, or the workforce provide options and opportunities. As previously mentioned, the formal learning activities were designed with pathways in mind. Specifically, this is the partnership with CGCC and UA. These designed pathways do not limit student opportunities for other post-secondary opportunities. Alternatively, students can pursue certification and workforce opportunities through Advanced Business Learning (ABL). ABL is a state-licensed school providing concurrent, subsequent, or alternative learning paths to develop cybersecurity knowledge and skills and obtain industry certifications. ABL provides cybersecurity-related training aligned with DoD 8140 requirements, access to a cyber practice range, Risk Management Framework (RMF), and certification training for A+, Network+, Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP). Basha's cybersecurity program partners with the school's Junior Reserve Officer Training Corps (JROTC) program. JROTC provides exposure to military service. Additionally, the school offers the Armed Services Vocational Aptitude Battery (ASVAB) to students during the fall semester. This provides the opportunity for career exploration and provides an initial starting point for enlisting in military service. Finally, as an anecdotal example of direct-to-workforce pathway options, one of the first program cohort graduates was offered employment with Kelly Technologies.

Interview Results and Analysis

Interviews were conducted with the cybersecurity program director and two teachers involved in program development. Study participants completed the questionnaires and answered interview questions outlined in Appendix B to identify programmatic elements, motivations, challenges, and opportunities in program development. This section presents the results from interviews conducted at Basha High School.

The primary motivation for developing the cybersecurity program was a school district initiative sparked by an administrator attending a cybersecurity conference at the University of Arizona (UA). The district administrator was presented with the pathway from CGCC to UA and decided to develop a dual enrollment pathway to CGCC from Basha High School. Basha High School was selected due to the available land and planned development of the building which now houses the Institute of Cyber Operations and Networking (ICON). The program director previously taught cybersecurity courses at another high school and was identified and eventually hired to establish the program at Basha High School. When asked about personal motivation to develop the program, the director stated:

> "I attended a lot of conferences while preparing the course in cybersecurity. The cybersecurity community was welcoming, there wasn't competition among teachers and industry professionals, there was an obvious need for cybersecurity education, and I understood the importance. I took the opportunity to make the biggest difference to the biggest number of students. Cybersecurity offers something for everybody."

Cybersecurity standards, curricular guidelines, and frameworks did not exist when the Basha High School program was developed. The Technical Security Guidelines for Network Security 11.1999.00 CTE requirements were available; however, these were not used initially to develop the program. Despite this, the program must align to these standards which introduces some issues. Computer science, programming, and operating system courses are included in the program which adopts the Arizona Computer Science Standards from the Arizona Department of Education (ADE). Additionally, the program includes the ten dual enrollment courses outlined in the program profiles. The CTE and dual enrollment requirements create challenges as described by study participants:

> "State ADE Computer Science Standards require approval to bring in additional curriculum. Getting resources and approvals for the curriculum is an administrative burden. For example, I put in a request in July 2022 and still waiting on approval in April 2023."

> "Have to follow specific requirements which reduce flexibility and technology changes too fast to follow these timelines."

The operational elements include instructors, hiring challenges, equipment, networks, and facilities. Recruiting and retaining cybersecurity teachers is challenging. There may be teachers that are ineligible to be CTE-certified or dual enrollment certified in cybersecurity due to a lack of education or experience. Alternatively, industry professionals, people with the appropriate education without teaching experience, or individuals unwilling to teach due to the pay differential present additional challenges. Basha's program has had challenges with hiring and retention. For example, one teacher quit within 30 days. This individual was an industry professional with experience teaching post-secondary students but not secondary education. The individual did not feel the opportunity was a fit. A qualified teacher from the community college worked at the high school on an interim basis due to a lack of qualified teachers within the cybersecurity program to teach required courses. Another teacher left for industry opportunities with higher salary. Finally, a teacher was relieved of their duties for undisclosed reasons. This demonstrates rapid turnover over the four years of the program. Compounding this problem is that certifying teachers for CTE or dual enrollment can be lengthy. CTE certification requires classes on teaching, advisory board, and other requirements; state certification, and 140 hours of internship. This process typically takes six months. Alternatively, 5000 hours of industry experience can result in CTE credentialing. Each of these credentialing options represents a significant investment in time impeding the point-in-time need for teachers in the program. Dual enrollment certification is conducted by the community college and every community college has different certification requirements and processes. Specific comments from study participants included:

> "Recruitment and Retention are challenges. Potential teachers don't fit both molds of CTE and Dual Enrollment. May not be a fit for classroom requirements for secondary education and how to deal with "kids.""

> "It was a long process to get dual enrollment certification and to introduce new courses."

> "Money is a barrier. Teaching is a profession that doesn't yield the same results as industry."

> "Have to have a love for teaching and content expertise. You can write code and automate tasks that can do something repeatedly. Teaching is not like that, and every new year requires a teacher to do things manually over and over again."

The program profiles outline specific equipment, networks, and facilities available to the programs and teachers. All study participants stated that they had the necessary networks and facilities to meet learning objectives and support the program. For equipment, the Technical Standards provided information aligned with the networking aspects but didn't address cybersecurity holistically. The curriculum and courses dictated equipment requirements. Initial equipment requirements required research on setting up labs, furniture, and space. The school provides basic equipment for classroom instruction; however, the restrictions placed on the machines or their limited technical specifications hinder teaching certain content in the program. The following are study participant statements regarding networks and equipment:

> "District machines do not support cybersecurity education. Had to beg for computers and equipment to support CyberPatriot and other activities.

> Requested CPU kits for students to build computers associated with A+ / Hardware courses. Everyone has the same equipment for these courses to facilitate teaching and learning."

> "Convincing and justifying the need for equipment not on the pre-approved list was challenging."

> "Have donated equipment but don't have the infrastructure to support the equipment. Power to support networking equipment is an example. Would like to set up a cyber or networking range but don't have the equipment or infrastructure to support it."

> "District has certain restrictions which limit access to certain websites and software that can be loaded on machines. Impedes teaching certain material."

Formal learning activities were built based on the established pathway between CGCC and UA. Individual courses were developed to maintain dual enrollment requirements and the overall pathway. The course and course descriptions for these courses are outlined Appendix A. Additionally, Appendix A contains the specific non-formal and informal learning activities related to the cybersecurity programs. This section will address the perceived need to include non-formal and informal learning activities into the cybersecurity program. All study participants overwhelmingly agreed that non-formal and informal learning activities are critical to student learning and success. These opportunities provide alternate credentialing in the forms of certifications, experience from internships, and career exploration through externships and guest speakers. Additionally, competitions increase student engagement and understanding of the concepts covered in formal learning activities. Study participants provided the following responses specific to non-formal and informal learning activities:

> "Certification is a requirement of CTE. The program must align to a certification. Avenues with each class so that students can seek out opportunities after any year in the program. Show students the options they have within the curriculum. Stronger more comprehensive foundation."

> "Camps provide the opportunity to work with other kids to develop skills different than course requirements. Builds comradery. Being around like-minded people. Introduces career exploration."

> "Internships and Externships provide paid opportunities in high school. Working directly with the company. Students learned more about the requirements of the workplace. It is exciting and provides opportunities to gain industry experience. "Can't put a price tag on that experience.""

> "Competitions provide a fun learning environment. Drives students to succeed and work as a team. Students are engaged in the process. Competitions make learning great by sharing and reviewing the information from competitions."

> "CTFs, HackTheBox, and CyberPatriot activities keep student interest up. Helps keep students in the program."

> "Activities like these enhance student engagement and allows them to make sense of where to apply the things they are learning in formal learning activities. The real world application of concepts."

The program has the articulated pathway to CGCC and then UA. Although this pathway was a primary driver for program development, the program is designed to provide opportunities for students to enter the workforce, join the military, seek certification training, or attend post-secondary education. The program uses an access database to track students throughout the program. All students are required to complete a program-developed exit survey which asks for personal email addresses and plans post-graduation. Additionally, all students are required to fill out a survey for CTE completion. These surveys are given to students during classroom time to obtain maximum participation. The four-year program provides a solid foundation to pursue cybersecurity-specific and non-cybersecurity opportunities after graduation. Survey participants provided the following responses regarding pathways:

> "The four-year program provides a solid foundation. No matter where they are at in their senior year they have multiple opportunities to choose the pathway. Comprehensive enough to have choices. Cuts down on entry time into the field based on their experience."

ISSN: 2473-4901
v9 n5955

> "Hands-down prepares students with applicable information to succeed in fields outside cybersecurity-specific roles. Good employees with a foundation in technology and security. Provides different perspectives since people must interact with people in IT, Finance, and other business functions."

> "Good foundation for other STEM fields such as engineering, biomedical engineering, computer science, and other disciplines."

> "Industry engagement and building in activities into the program builds pathway opportunities for students. Provides tangible things to get students engaged in workforce opportunities."

> "Focus on analysis and problem solving skills that can be applied to other situations."

> "The comprehensive nature of the cybersecurity program can expose students to many different disciplines and if students lose interest in one area they can shift to another while still staying in STEM-related fields."

Participants' responses provided valuable insights for program profiles and identified additional recommendations, opportunities, and challenges. Table 1 provides a breakdown of those responses.

Recommendations	• Infuse yourself into industry by attending conferences and events to get ideas from others. • Be creative and solve problems. • Educate and work with people around you.
Opportunities	• Cybersecurity programs provide pathways to high paying / high opportunity jobs. • The country has a dire need for cybersecurity professionals. • These programs can make students better employees and citizens.
	• Increased student enrollment attracting different student demographics to the school and program.
Challenges	• Cybersecurity programs are a new concept for schools and the state. Can be challenging to get buy-in for time and resources. • Need to get administration at the school and district level engaged and bought into the idea. • Should cybersecurity courses be considered "weighted courses"? • CTE requirements to pass certain industry certifications can be challenging. • School counselor engagement and focus to determine what is best for student instead of forcing them into traditional paradigms. Cybersecurity courses didn't exist years ago. • Priorities within school: foreign language vs CS courses. • Teachers responsible for marketing their own programs without marketing experience or resources.

Table 1: Recommendations, Challenges, and Opportunities

5. FUTURE WORK

This study provides multiple opportunities for future research. The program profile provides a baseline to begin discussions with other school districts within Arizona and beyond. Additional program profiles could be developed at institutions across the country to develop a broader range of profiles. Additionally, interviews and focus groups could be conducted with different stakeholders to identify schools interested in developing cybersecurity education programs. Further, the scope of stakeholders could be expanded to include administrators, teachers, and staff involved in cybersecurity education or interested in supporting these programs.

6. CONCLUSIONS

Cybersecurity education and training initiatives continue to evolve in the United States. As K-12 institutions evaluate the potential introduction of cybersecurity content, curriculum, and programs, it is crucial to conduct a thorough assessment of the return on investment for pursuing these endeavors. This paper has presented a case study conducted on a four-year cybersecurity program at a secondary education institution in Arizona. The developed program profile provides a structure to analyze other programs internal or external to Arizona. By leveraging an enhanced data set, secondary schools considering the development of their own programs can gain a better understanding of the requirements and resources needed to establish successful initiatives. Additionally, the collected data can provide a baseline to compare their district and school to understand the implications within the context of their environment. Finally, the profiles identify existing opportunities for non-formal and informal cybersecurity learning activities to expose students to cybersecurity KSAs without building an entire program. This has far-reaching implications for the cybersecurity field and contributes to the broader student development within STEM disciplines.

7. REFERENCES

"AZ Cyber Initiative Mentorship Program," (2023). AZ Cyber Initiative. Retrieved June 3, 2023 from https://azcyber.org/mentorship-program/

Burke, A. and Rotermund, S. (2021). Elementary and Secondary STEM Education. National Science Foundation / National Science Board: Science and Engineering Indicators. https://ncses.nsf.gov/pubs/nsb20211/student-learning-in-mathematics-and-science.

"Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," (2017). CSEC. Association for Computing Machinery. Retrieved June 3, 2023 from https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

"Cyber Literacy," (2019). Cyber Literacy 1. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from https://cyber.instructure.com/courses/4.

"Cyber Literacy II," (2019). Cyber Literacy 1. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from https://cyber.instructure.com/courses/37.

"Cybersecurity," (2022). Cybersecurity. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from https://cyber.instructure.com/courses/100/pages/course-information.

"Cybersecurity Basics," (2022). Cybersecurity Basics. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from https://cyber.instructure.com/courses/227.

"Cybersecurity Curricular Guidance for Associate-Degree Programs," (2020). CCSEC. ACM Committee for Computing Education in Community Colleges. Retrieved Jun 3, 2023 from http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf.

"Cybersecurity Curriculum," (2021). NCyTE Center. https://www.ncyte.net/resources/cybersecurity-curriculum.

"Cyberseek Cybersecurity Supply/Demand Heat Map," (2023). CyberSeek. Retrieved June 3, 2023 from https://www.cyberseek.org/heatmap.html

Dark, M., Daugherty, J., Emry, M., Masey, D., and Peyrot, J. (2021). High School Cybersecurity Curriculum Guidelines & Glossary. Teach Cyber. https://teachcyber.org/wp-content/uploads/2021/04/High-School-Cybersecurity-Curriculum-Guidelines.pdf.

"DoD Approved 8570 Baseline Certifications," (2023). DoD Cyber Exchange. https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/.

Hairston, J and Sands, J. (2022). RING (Regions Investing in the Next Generation). CAE in Cybersecurity Community. https://caecommunity.org/initiative/k12-ring.

"(ISC)2 Cybersecurity Workforce Study," (2022). (ISC)2. Retrieved June 3, 2023 from https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.

Lim, V. (2019). Students don't feel their high schools prepare them for careers. Working Nation. https://workingnation.com/prepare-ri-provides-experiential-learning-students/.

Lucariello, K. (2022). National Survey Finds High School Graduates Not Prepared for College or Career Decisions. The Journal: Transferring Education Through Technology. https://thejournal.com/articles/2022/12/05/national-survey-finds-high-school-graduates-not-prepared-for-college-or-career-decisions.aspx.

"National Centers for Academic Excellence in Cybersecurity," (N.D.). National Security Agency / Central Security Service. Retrieved June 3, 2023 from https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.

Petersen, R., Santos, D., Smith, M., Wetzel, K., and Witte, G. (2020). NIST Special Publication 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework). National Institute for Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1.

"The State of Cybersecurity Education in K-12 Schools," (2020). EdWeek Research Center Cyber.org. Retrieved June 3, 2023 from https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf.

Yin, R. K. (2003). Case study research: Design and methods (3rd edition). Thousand Oaks, CA: Sage Publications.

Appendix A: Basha High School Program Profile

Enrollment

Academic Year	Grade 9	Grade 10	Grade 11	Grade 12	Total	Graduates
2022 – 2023	41	44	46	23	154	17
2021 – 2022	50	63	26	10	149	2
2020 – 2021	88	19	15	3	125	1
2019 – 2020	42	8	7	3	60	1

2022 – 2023 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	41				41
10th	20	24			44
11th	11	5	26	4	46
12th	6	4	1	12	23
Total	78	33	27	16	154

** Year 3 Students are taking Year 3 and Year 4 courses.*

2021 – 2022 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	50				50
10th	25	38			63
11th	11	3	12		26
12th	6	3	1		10
Total	92	44	13		149

2020 – 2021 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	59	29			88
10th	18	1			19
11th	12	3			15
12th	2	1			3
Total	91	34			125

2019 – 2020 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	42				42
10th	8				8
11th	7				7
12th	3				3
Total	60				60

Demographics

	White	59.7%
	Hispanic / Latino	13.6%
	Asian or Asian / Pacific Islander	10.4%
	Black or African American	11%
	American Indian or Alaska Native	2%
	Other or Undeclared	3.3%
	Minority Enrollment	40.3%

Gender	Male	137
	Female	17
Student to Teacher Ratio		30:1

**Demographic Data represents the most recent data obtained for 2022 – 2023 school year*

Operations

Personnel

Teacher	Education Level	Certifications	Years of Experience		Courses Taught	Dual Enrollment Qualified
			Teaching	Industry		
Janet Hartkopf	MS Curriculum & Instruction - Technology	CTE Certified	11 Years	17 Years	Security Fundamentals Ethics in IT	Y
Sam Alexander	BS Biology AS Cisco Networking	CTE Certified MTA Java	25 years	N/A	Hardware and Software Configurations LAN & Security Fundamentals	Y
Jyoti Tamboli	MS Computer Applications	CTE Certified STEM Certified	3 Years	12 Years	CYB 120 - Introduction to Computer Systems CSC 305 – Java – Computer Science A CSC 125 – AP Computer Science Principles CYB 300 – Linux Administration (RHEL)	Y

Equipment

Equipment Type	Make	Model	Quantity	Cost
Computer Kit	Basha HS Equipment List		31	$25,000
Misc. Tools	Basha HS Lab Tool List		N/A	$2,346.97
Locking Storage	ULINE	H-6839	1	$1,300
Networking	Cisco	CCNA 200-301	4	$3,638.84
PCs & Monitors	"Chromebook" type laptop with ability to use PacketTracer			

Network

- Chandler Unified School District provided network access.
- Isolated network provided for cybersecurity classrooms and lab spaces.
  - Requires separate hardware and non-district issued machines.
  - Allows access websites, resources, and facilitates meeting the learning objectives of courses.

Facilities

- School has dedicated classroom space for cybersecurity program.

- Three general purpose classrooms and one Career and Technical Education (CTE) Lab.
    - CTE lab space provides larger footprint. Consists of teaching space and space for hands on activities and equipment storage.
        - Classrooms have webcams and in-classroom microphones (2) to support video-conferencing capabilities.

Formal Learning Activities

Course	Company	Cost
CYB 240A / CNT 140 – Intro to LAN & Security Fundamentals	Cisco	* Free Courseware
CYB 240B / CNT 150 – Intro to LAN & Security Fundamentals	Cisco	* Free Courseware
CYB 300A / CIS 126DL – Linux OS	Cisco	$30 per student lab fee
CYB 300B / CIS 238DL – Advanced Linux	Cisco	$30 per student lab fee
CYB 400A / CIS 110 – Information Security Fundamentals	TestOut	$2,900 per year (50 user license)
CYB 400B / CIS 111 – Ethics in Information Technology	Cengage	$4,620 for Print Student Edition + 6 years access to online platform MindTap x 40 (price includes shipping and processing)
CYB 130 / CIS 156 – Python	Cisco	* Free Courseware

* Must be member of Western Academy Support & Training Center – WATSC (~$500 per year)

- Reverse engineered from Chandler Gilbert Community College (CGCC) four year plan to ensure articulation and pathway for students.
- Aligns with Arizona Department of Education (DoE) CTE Network Security Technical Standards 11.1999.00.
- Completing fourth year of the program in School Year 2022 – 2023.
- Program used RedHat Linux content through 2022 – 2023 School Year. Will switch to Cisco content after 2022 – 2023 school year.

Course	Description	Syllabus	Dual Enrollment	Pre-Existing
CYB 120 / CIS 105 – Introduction to Computer Systems	Overview of computer technology, concepts, terminology, and the role of computers in business and society. Discussion of social and ethical issues related to computers. Use of word processing, spreadsheet, database, and presentation software. Includes uses of application software and the Internet for efficient and effective problem solving. Exploration of relevant emerging technologies.	Y	Y	N
CYB 230 A / BPC 170 – Hardware and Software Config & Support	This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.	Y	Y	N

CYB 230 B / BPC 270 – Hardware and Software Config & Support	This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.	Y	Y	N
CYB 240 A / CNT 140 – Intro to LAN & Security Fundamentals	This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.	Y	Y	N
CYB 240 B / CNT 150 – Intro to LAN & Security Fundamentals	This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.	Y	Y	N
CYB 300 A / CIS 126DL – Linux OS	Introduction to the Linux Operating system. Develop knowledge and skills required to install, configure, and troubleshoot a Linux-based workstation including basic network functions. Learn basic command line and Graphical User Interface (GUI) desktop environment utilities and applications. Fundamental abilities to achieve the entry-level industry certification covered.	Y	Y	N
CYB 300 B / CIS 238DL – Advanced Linux	Managing Linux Operating Systems including sophisticated manipulation of file structures, backup systems, printing processes, troubleshooting, user account management, hard disk maintenance and configuration, process monitoring and prioritizing, kernel customization, and system resource control. Preparation for industry certifications such as the CompTIA Linux+, the Red Hat Certified System Administrator (RHCSA), the Red Hat Certified Engineer (RHCE) and the Linux Professional Institute (LPIC-1).	Y	Y	N
CYB 400A / CIS 110 - Information Security Fundamentals	Fundamental concepts of information technology security. Topics include authentication methods, access control, cryptography, Public Key Infrastructure (PKI), network attack and defense methods, hardening of operating systems and network devices, securing remote access and wireless technologies, and securing infrastructures and	Y	Y	N

	topologies. Emphasis on hands-on labs in both the Windows and Linux environments. Builds on thorough understanding of TCP/IP and security concepts and Microsoft (MS) Windows and Linux Administration.			
CYB 400B / CIS 111 – Ethics in Information Technology	Ethical issues that arise as a result of increasing use of computers, and the responsibilities of those who work with computers, either as computer science professionals or end users. Critical inquiry and review of ethical challenges in information technology business, including professional and corporate responsibility, government regulation, fiduciary responsibilities of information, infringement of intellectual property, security risk assessment, Internet crime, identity theft, employee surveillance, privacy, compliance, social networking, and the ethics of IT corporations.	Y	Y	N
CYB 130 / CIS 156 - Python	Introduction to Python programming. Includes general concepts, program design, development, data types, operators, expressions, flow control, functions, classes, input, and output operations, debugging, structured programming, and object-oriented programming.	Y	Y	N

Non-Formal Learning Activities

Camps	• AZ Cyber Initiative • CyberPatriot
Certifications	• A+ • ITF+ • Linux+ • Security Pro • Security+ • Python PCEP
Internships	• Open Source Integrators
Externships	• ElevateEdAZ • Cybersecurity and Technology Externship

Informal Learning Activities

Clubs	• Future Business Leaders of America (FBLA)
Competitions	• National Cyber League • CyberPatriot
Self-Study / Ad-Hoc Learning	Students are provided a variety of resources for additional learning outside of the classroom. Examples include cyber.org range access, Professor Messer videos, YouTube videos, and other resources.
Conferences	• CactusCon • WiCYS • K12 NICE Conference – Student Signing Day • Embry Riddle Aeronautical Engineering Cyber Day
Industry Events	• PhoenixNap Tour

Pathways

Post-Secondary	• Chandler Gilbert Community College (CGCC) Cybersecurity AAS
Trade or Certification Program	• Advanced Business Learning (ABL)
Military	• Air Force JROTC
Workforce	• Kelly Technologies

Equipment, Hardware, and Software Requirements

Intro to Computer Systems

- MS Office Apps
- Internet access
- eBook curriculum

Hardware / Software Lab Setup

- Lab Tables w/integrated power
- Anti-Static Mat on the tables
- eBook curriculum
- Packet Tracer software

Computer Kit – the kit requirements will vary upon how you choose to allow students to connect for the purpose of downloading OS and various drivers (PacketTracer is now on the approved software list)

Component	Quantity
1. Motherboard – ATX (full size) a. LGA1200 – Intel	31
2. CPU w/heat sink & fan	31
3. Graphics Processing Card	31
4. RAM (8GB) - recommended by Cisco (2 X 4GB suggested) needed for VM practice in curriculum	31
5. Case (ATX)	31
6. Ethernet Card	31
7. PCI / PCIe	31
This storage setup will allow students to configure their machine and NOT have to reverse all their work for the next class. Each student would be assigned an SSD that would remain in the classroom and used for their work in the lab	
8. Storage a. Swappable SSD i. Bay (30) - ~$25/ea (CDW) ii. Trays (1 for each student) - ~$11/ea (CDW) b. SSD – 120GB (1 for each student) - ~$30/ea (CDW)	31 Bays 1/Tray per SSD 1 /per student

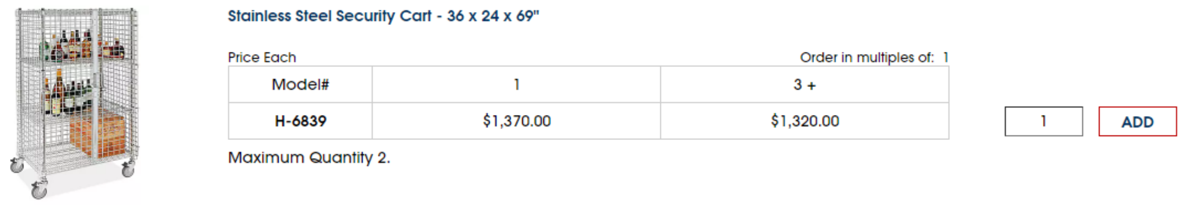
Cables

- Ethernet UTP bulk cable (CAT5e)
- Stranded UTP bulk cable (CAT5e)
- RJ45 connectors – Stranded and Solid Core
- RJ45 Network Cable Tester
- Crimpers
- Multimeter
- Networking scissors
- Cable stripper
- PC Power Supply Tester
- Anti-Static Duster
- Network Cable Tester

Tools

- 11-piece PC computer tool kit
- Anti-static wrist strap

Printer
Switch / Router
HDMI Monitors



Stainless Steel Security Cart - 36 x 24 x 69"

Price Each

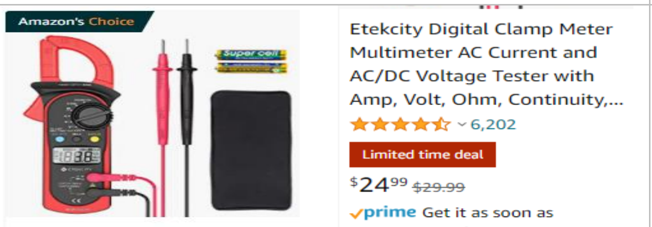
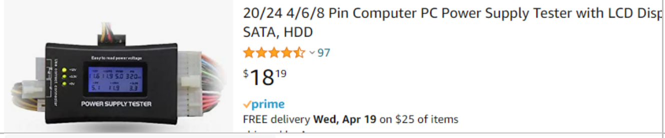
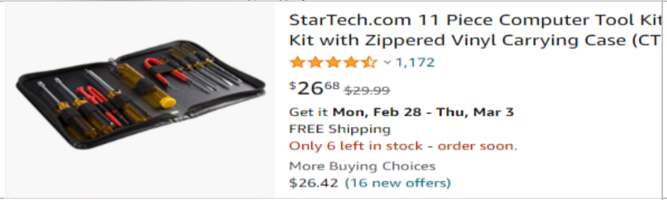
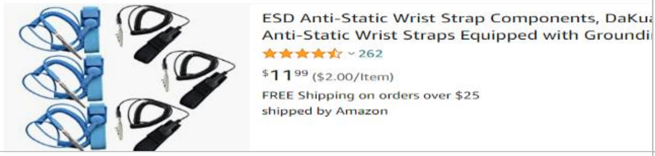
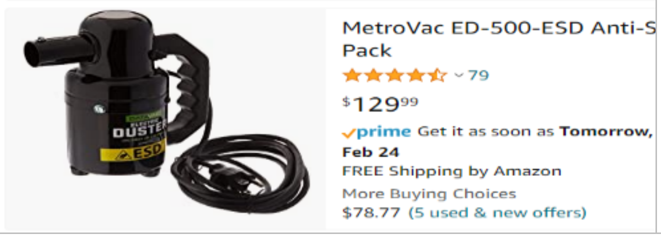
Order in multiples of: 1

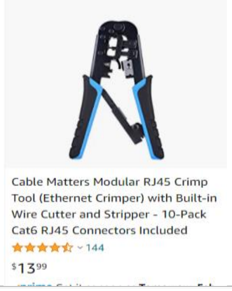
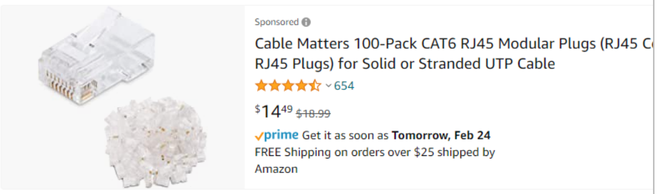
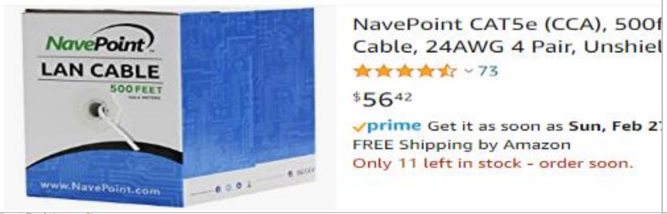
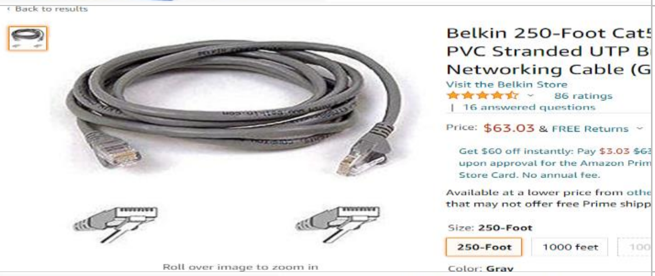
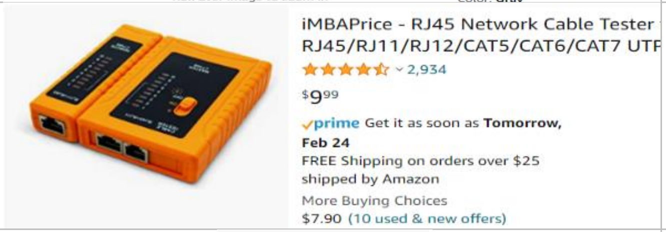
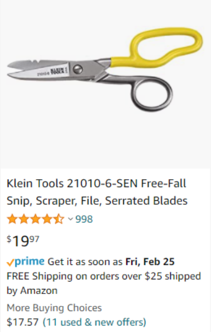
Model#	1	3 +
H-6839	$1,370.00	$1,320.00

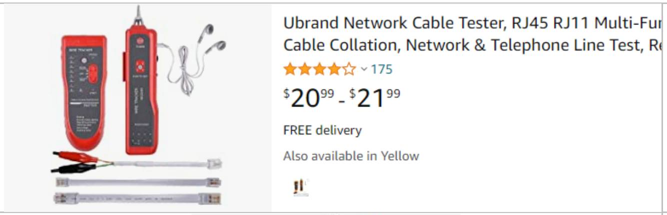
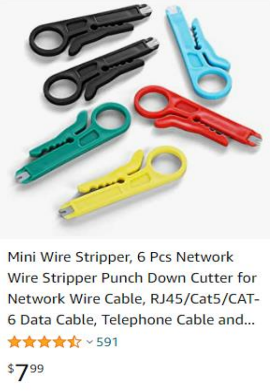
Maximum Quantity 2.

ULINE Search Results: Stainless Steel Mobile Security Cage

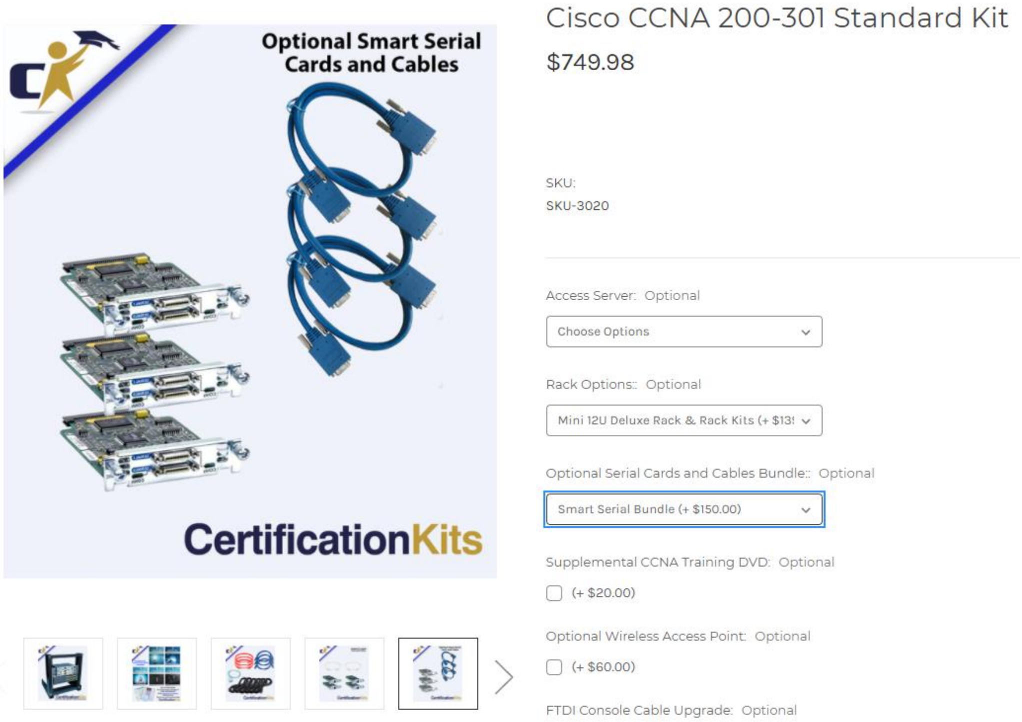
Basha High School Lab Tool Inventory

Item	Qty	Vendor	Picture	Total
Digital Multimeter, MSR-C600	2	Amazon	 Amazon's Choice Etekcity Digital Clamp Meter Multimeter AC Current and AC/DC Voltage Tester with Amp, Volt, Ohm, Continuity,... ★★★★☆ 6,202 Limited time deal $24.99 ~~$29.99~~ prime Get it as soon as	$49.98
PC Power Supply Tester	2	Amazon	 20/24 4/6/8 Pin Computer PC Power Supply Tester with LCD Disp SATA, HDD ★★★★☆ 97 $18.19 prime FREE delivery **Wed, Apr 19** on $25 of items	$36.38
11 Piece PC Computer Tool Kit	31	Amazon	 StarTech.com 11 Piece Computer Tool Kit Kit with Zippered Vinyl Carrying Case (CT ★★★★☆ 1,172 $26.68 ~~$29.99~~ Get it **Mon, Feb 28 - Thu, Mar 3** FREE Shipping Only 6 left in stock - order soon. More Buying Choices $26.42 (16 new offers)	$827.08
Anti-Static Wrist Strap	5	Amazon	 ESD Anti-Static Wrist Strap Components, DaKu Anti-Static Wrist Straps Equipped with Groundi ★★★★☆ 262 $11.99 ($2.00/Item) FREE Shipping on orders over $25 shipped by Amazon	$59.95
MetroVac Anti-Static Electric Duster	2	Amazon	 MetroVac ED-500-ESD Anti-S Pack ★★★★☆ 79 $129.99 prime Get it as soon as **Tomorrow, Feb 24** FREE Shipping by Amazon More Buying Choices $78.77 (5 used & new offers)	$259.98

Cable Crimpers RJ45 Crimp	30	Amazon	 Cable Matters Modular RJ45 Crimp Tool (Ethernet Crimper) with Built-in Wire Cutter and Stripper - 10-Pack Cat6 RJ45 Connectors Included 144 $1399	$419.70
RJ45 Connectors SHD CAT6 Solid/Stranded Core	10	Amazon	 Sponsored Cable Matters 100-Pack CAT6 RJ45 Modular Plugs (RJ45 C RJ45 Plugs) for Solid or Stranded UTP Cable 654 $1449 ~~$18.99~~ prime Get it as soon as **Tomorrow, Feb 24** FREE Shipping on orders over $25 shipped by Amazon	$144.90
NavePoint CAT5e, Solid Bulk Ethernet Cable UTP	1	Amazon	 NavePoint CAT5e (CCA), 500f Cable, 24AWG 4 Pair, Unshiel 73 $5642 prime Get it as soon as **Sun, Feb 2** FREE Shipping by Amazon Only 11 left in stock - order soon.	$56.42
Belkin 250 ft CAT5e Stranded UTP Bulk Networking Cable	1	Amazon	 Back to results Belkin 250-Foot Cat5 PVC Stranded UTP B Networking Cable (G Visit the Belkin Store 86 ratings 16 answered questions Price: $63.03 & FREE Returns Get $60 off instantly: Pay $3.03 $63 upon approval for the Amazon Prim Store Card. No annual fee. Available at a lower price from othe that may not offer free Prime shipp Size: **250-Foot** 250-Foot 1000 feet 100 Color: **Gray** Roll over image to zoom in	$63.03
RJ45 Network Cable Tester for LAN Phone/RJ45 WireTestTool	30	Amazon	 iMBAPrice - RJ45 Network Cable Tester RJ45/RJ11/RJ12/CAT5/CAT6/CAT7 UTP 2,934 $999 prime Get it as soon as **Tomorrow, Feb 24** FREE Shipping on orders over $25 shipped by Amazon More Buying Choices $7.90 (10 used & new offers)	$299.70
Networking Scissors	5	Amazon	 Klein Tools 21010-6-SEN Free-Fall Snip, Scraper, File, Serrated Blades 998 $1997 prime Get it as soon as **Fri, Feb 25** FREE Shipping on orders over $25 shipped by Amazon More Buying Choices $17.57 (11 used & new offers)	$99.85

Network Cable Tester	1	Amazon	 Ubrand Network Cable Tester, RJ45 RJ11 Multi-Fu Cable Collation, Network & Telephone Line Test, R ★★★★☆ 175 $20.99 - $21.99 FREE delivery Also available in Yellow	$22
Mini Wire Stripper	1	Amazon	 Mini Wire Stripper, 6 Pcs Network Wire Stripper Punch Down Cutter for Network Wire Cable, RJ45/Cat5/CAT-6 Data Cable, Telephone Cable and... ★★★★½ 591 $7.99	$8
Total Cost				$2,346.97

Cisco CCN 200-301 Standard Kit



Cisco CCNA 200-301 Standard Kit

$749.98

SKU:
SKU-3020

Access Server: Optional
Choose Options

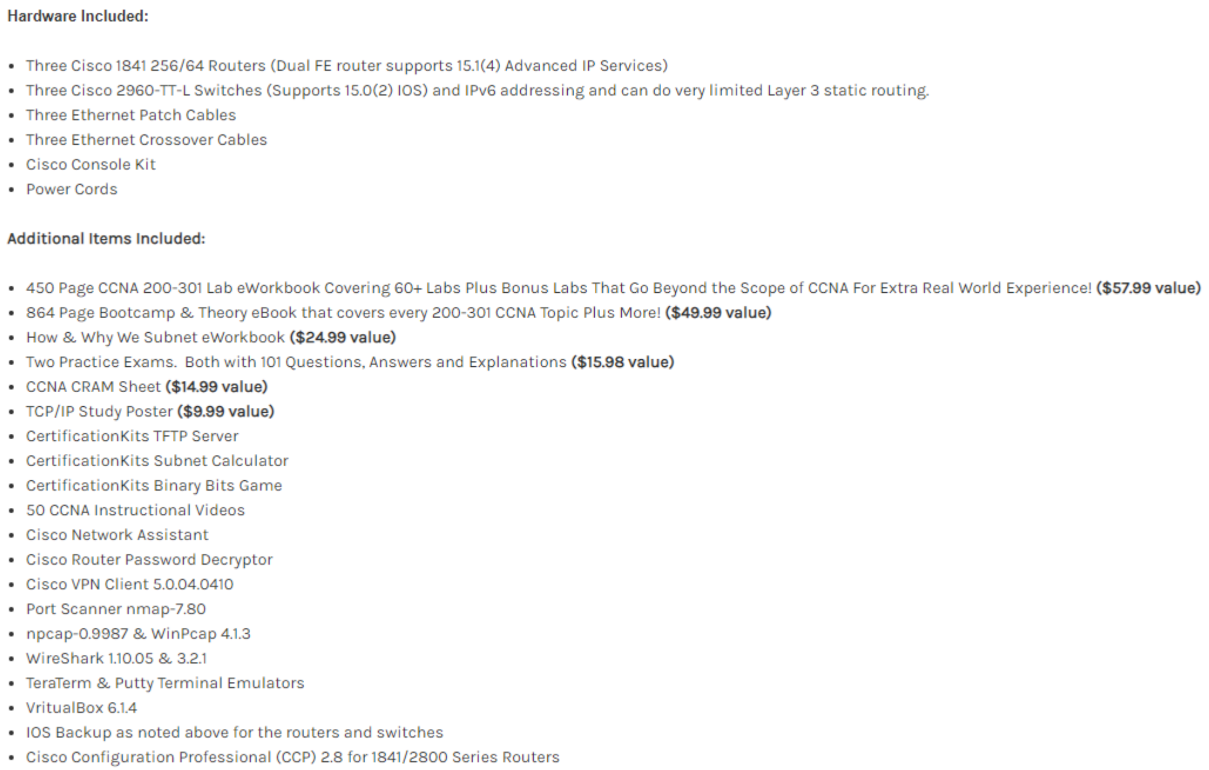
Rack Options:: Optional
Mini 12U Deluxe Rack & Rack Kits (+ $13!

Optional Serial Cards and Cables Bundle:: Optional
Smart Serial Bundle (+ $150.00)

Supplemental CCNA Training DVD: Optional
□ (+ $20.00)

Optional Wireless Access Point: Optional
□ (+ $60.00)

FTDI Console Cable Upgrade: Optional

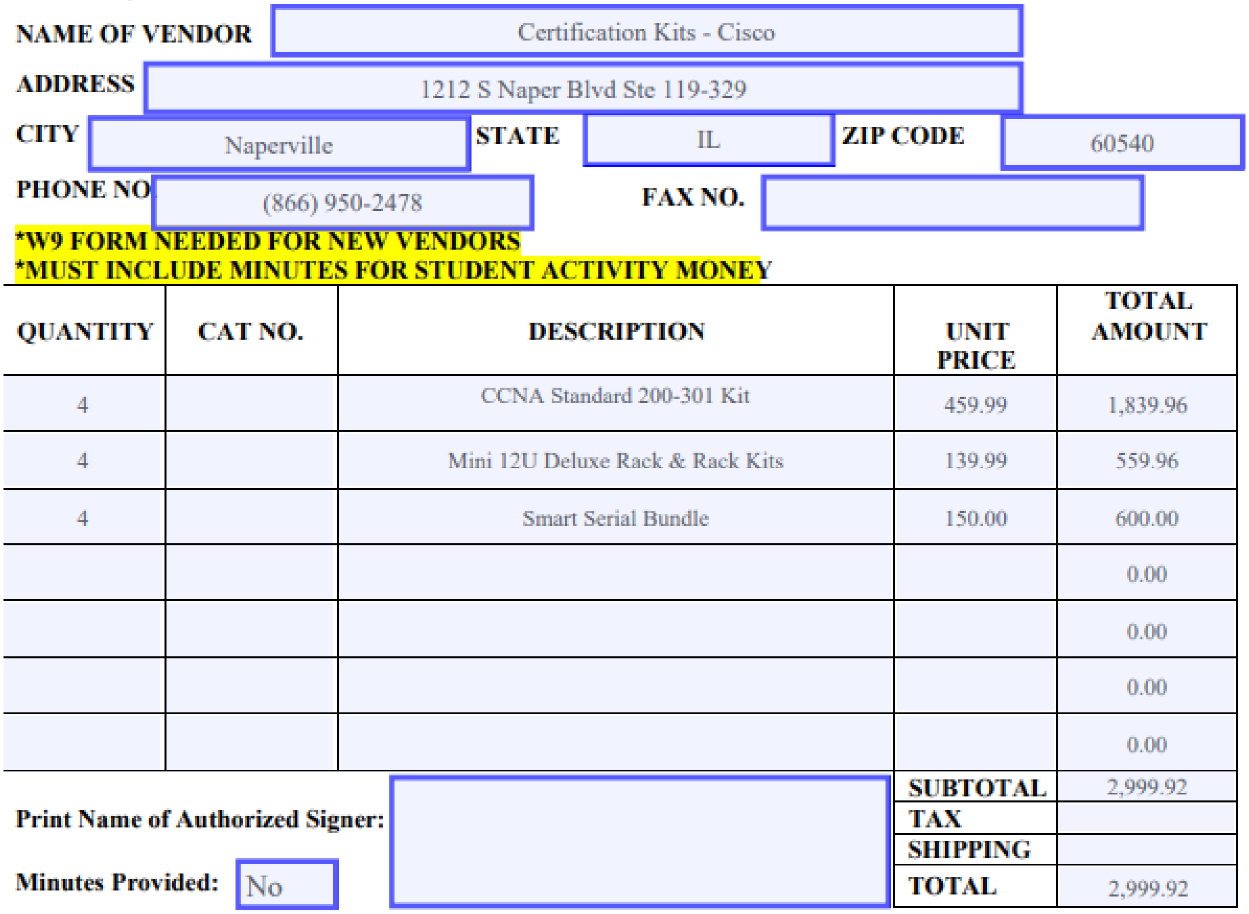


Hardware Included:

- Three Cisco 1841 256/64 Routers (Dual FE router supports 15.1(4) Advanced IP Services)
- Three Cisco 2960-TT-L Switches (Supports 15.0(2) IOS) and IPv6 addressing and can do very limited Layer 3 static routing.
- Three Ethernet Patch Cables
- Three Ethernet Crossover Cables
- Cisco Console Kit
- Power Cords

Additional Items Included:

- 450 Page CCNA 200-301 Lab eWorkbook Covering 60+ Labs Plus Bonus Labs That Go Beyond the Scope of CCNA For Extra Real World Experience! **($57.99 value)**
- 864 Page Bootcamp & Theory eBook that covers every 200-301 CCNA Topic Plus More! **($49.99 value)**
- How & Why We Subnet eWorkbook **($24.99 value)**
- Two Practice Exams. Both with 101 Questions, Answers and Explanations **($15.98 value)**
- CCNA CRAM Sheet **($14.99 value)**
- TCP/IP Study Poster **($9.99 value)**
- CertificationKits TFTP Server
- CertificationKits Subnet Calculator
- CertificationKits Binary Bits Game
- 50 CCNA Instructional Videos
- Cisco Network Assistant
- Cisco Router Password Decryptor
- Cisco VPN Client 5.0.04.0410
- Port Scanner nmap-7.80
- npcap-0.9987 & WinPcap 4.1.3
- WireShark 1.10.05 & 3.2.1
- TeraTerm & Putty Terminal Emulators
- VritualBox 6.1.4
- IOS Backup as noted above for the routers and switches
- Cisco Configuration Professional (CCP) 2.8 for 1841/2800 Series Routers



NAME OF VENDOR Certification Kits - Cisco

ADDRESS 1212 S Naper Blvd Ste 119-329

CITY Naperville **STATE** IL **ZIP CODE** 60540

PHONE NO (866) 950-2478 **FAX NO.**

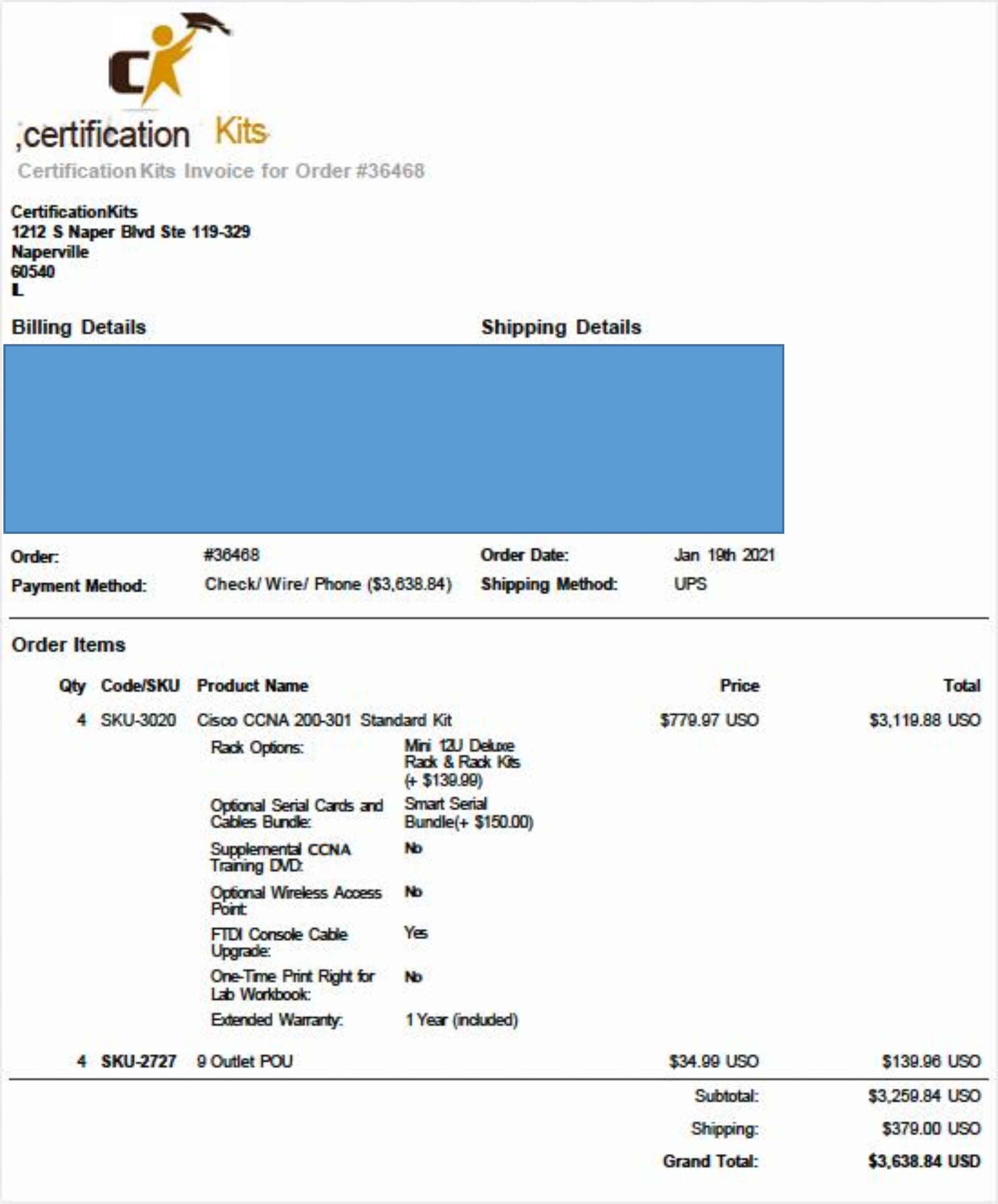
***W9 FORM NEEDED FOR NEW VENDORS**
***MUST INCLUDE MINUTES FOR STUDENT ACTIVITY MONEY**

QUANTITY	CAT NO.	DESCRIPTION	UNIT PRICE	TOTAL AMOUNT
4		CCNA Standard 200-301 Kit	459.99	1,839.96
4		Mini 12U Deluxe Rack & Rack Kits	139.99	559.96
4		Smart Serial Bundle	150.00	600.00
				0.00
				0.00
				0.00
				0.00
			SUBTOTAL	2,999.92
			TAX	
			SHIPPING	
			TOTAL	2,999.92

Print Name of Authorized Signer:

Minutes Provided: No

https://shop.certificationkits.com/cisco-ccna-200-301-standard-kit/



,certification Kits

Certification Kits Invoice for Order #36468

**CertificationKits
1212 S Naper Blvd Ste 119-329
Naperville
60540
L**

Billing Details **Shipping Details**

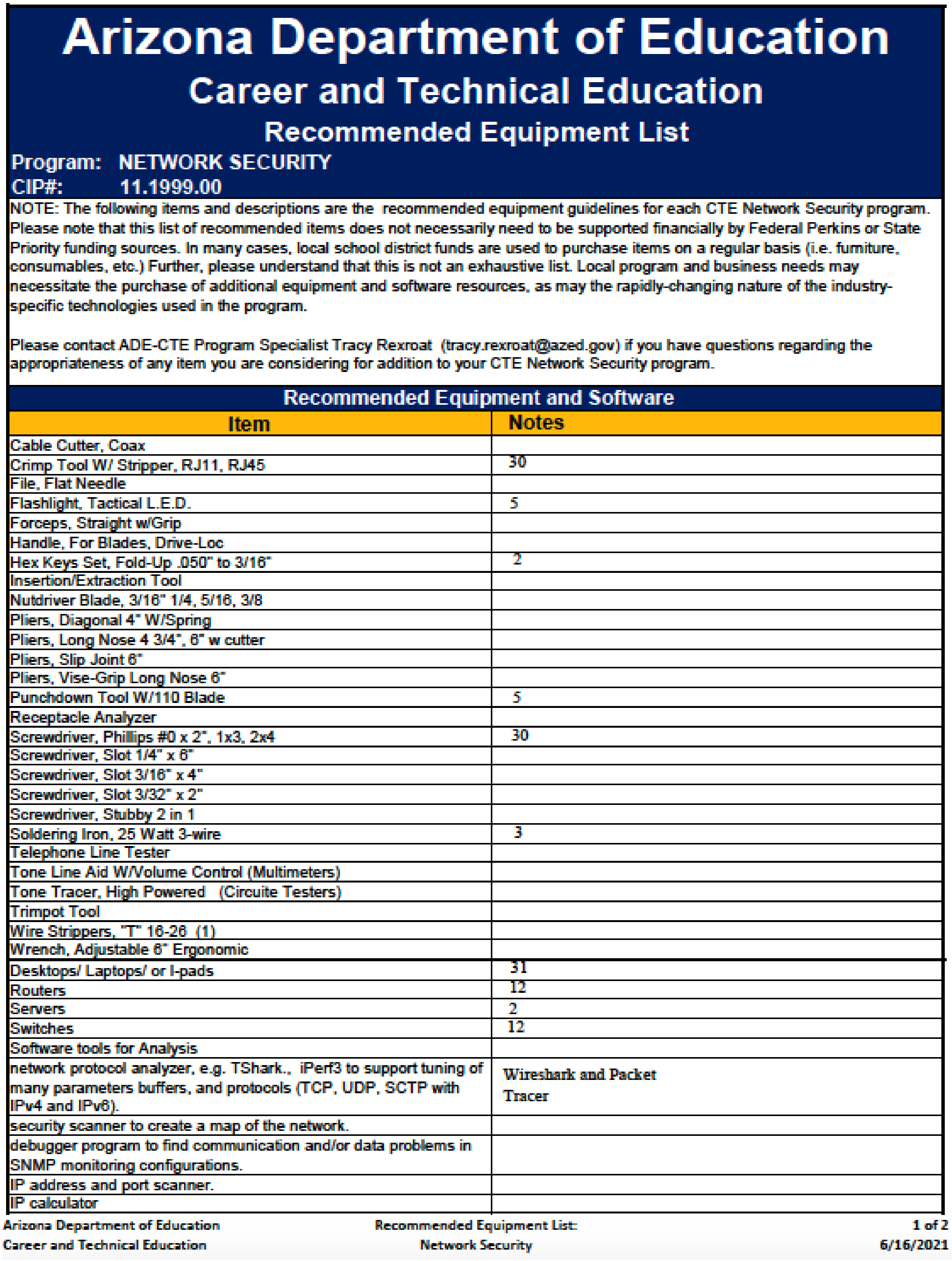
[redacted]

Order:	#36468	**Order Date:**	Jan 19th 2021
Payment Method:	Check/ Wire/ Phone ($3,638.84)	**Shipping Method:**	UPS

Order Items

Qty	Code/SKU	Product Name		Price	Total
4	SKU-3020	Cisco CCNA 200-301 Standard Kit		$779.97 USO	$3,119.88 USO
		Rack Options:	Mini 12U Deluxe Rack & Rack Kits (+ $139.99)		
		Optional Serial Cards and Cables Bundle:	Smart Serial Bundle(+ $150.00)		
		Supplemental CCNA Training DVD:	No		
		Optional Wireless Access Point:	No		
		FTDI Console Cable Upgrade:	Yes		
		One-Time Print Right for Lab Workbook:	No		
		Extended Warranty:	1 Year (included)		
4	**SKU-2727**	9 Outlet POU		$34.99 USO	$139.96 USO
				Subtotal:	$3,259.84 USO
				Shipping:	$379.00 USO
				Grand Total:	**$3,638.84 USD**

Arizona Department of Education CTE Recommended Equipment List



Arizona Department of Education

Career and Technical Education

Recommended Equipment List

Program: NETWORK SECURITY
CIP#: 11.1999.00

NOTE: The following items and descriptions are the recommended equipment guidelines for each CTE Network Security program. Please note that this list of recommended items does not necessarily need to be supported financially by Federal Perkins or State Priority funding sources. In many cases, local school district funds are used to purchase items on a regular basis (i.e. furniture, consumables, etc.) Further, please understand that this is not an exhaustive list. Local program and business needs may necessitate the purchase of additional equipment and software resources, as may the rapidly-changing nature of the industry-specific technologies used in the program.

Please contact ADE-CTE Program Specialist Tracy Rexroat (tracy.rexroat@azed.gov) if you have questions regarding the appropriateness of any item you are considering for addition to your CTE Network Security program.

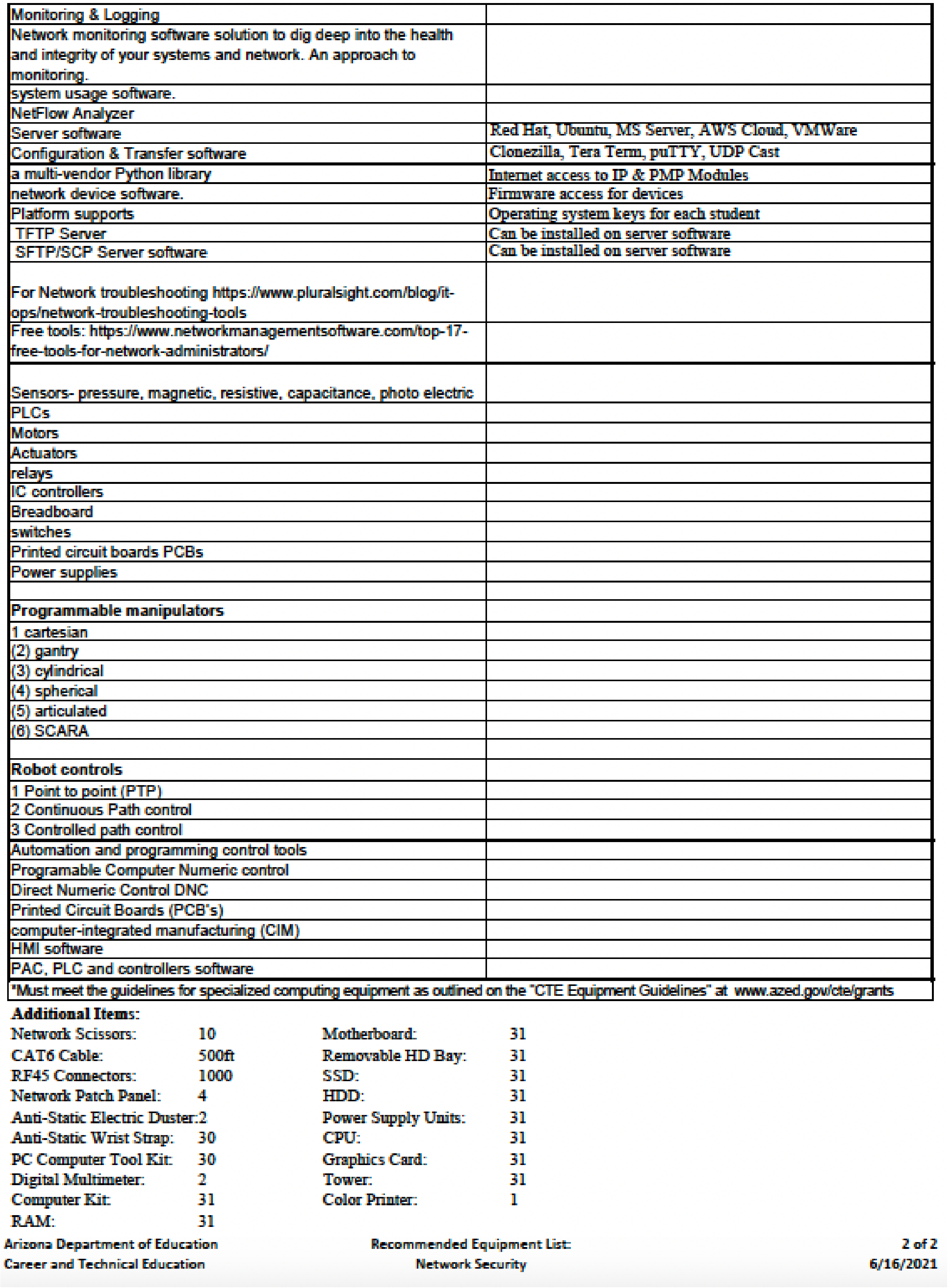
Recommended Equipment and Software

Item	Notes
Cable Cutter, Coax	
Crimp Tool W/ Stripper, RJ11, RJ45	30
File, Flat Needle	
Flashlight, Tactical L.E.D.	5
Forceps, Straight w/Grip	
Handle, For Blades, Drive-Loc	
Hex Keys Set, Fold-Up .050" to 3/16"	2
Insertion/Extraction Tool	
Nutdriver Blade, 3/16" 1/4, 5/16, 3/8	
Pliers, Diagonal 4" W/Spring	
Pliers, Long Nose 4 3/4", 6" w cutter	
Pliers, Slip Joint 6"	
Pliers, Vise-Grip Long Nose 6"	
Punchdown Tool W/110 Blade	5
Receptacle Analyzer	
Screwdriver, Phillips #0 x 2", 1x3, 2x4	30
Screwdriver, Slot 1/4" x 6"	
Screwdriver, Slot 3/16" x 4"	
Screwdriver, Slot 3/32" x 2"	
Screwdriver, Stubby 2 in 1	
Soldering Iron, 25 Watt 3-wire	3
Telephone Line Tester	
Tone Line Aid W/Volume Control (Multimeters)	
Tone Tracer, High Powered (Circuite Testers)	
Trimpot Tool	
Wire Strippers, "T" 16-26 (1)	
Wrench, Adjustable 6" Ergonomic	
Desktops/ Laptops/ or I-pads	31
Routers	12
Servers	2
Switches	12
Software tools for Analysis	
network protocol analyzer, e.g. TShark., iPerf3 to support tuning of many parameters buffers, and protocols (TCP, UDP, SCTP with IPv4 and IPv6).	Wireshark and Packet Tracer
security scanner to create a map of the network.	
debugger program to find communication and/or data problems in SNMP monitoring configurations.	
IP address and port scanner.	
IP calculator	

Arizona Department of Education
Career and Technical Education

Recommended Equipment List:
Network Security

1 of 2
6/16/2021



Monitoring & Logging	
Network monitoring software solution to dig deep into the health and integrity of your systems and network. An approach to monitoring.	
system usage software.	
NetFlow Analyzer	
Server software	Red Hat, Ubuntu, MS Server, AWS Cloud, VMWare
Configuration & Transfer software	Clonezilla, Tera Term, puTTY, UDP Cast
a multi-vendor Python library	Internet access to IP & PMP Modules
network device software.	Firmware access for devices
Platform supports	Operating system keys for each student
TFTP Server	Can be installed on server software
SFTP/SCP Server software	Can be installed on server software
For Network troubleshooting https://www.pluralsight.com/blog/it-ops/network-troubleshooting-tools	
Free tools: https://www.networkmanagementsoftware.com/top-17-free-tools-for-network-administrators/	
Sensors- pressure, magnetic, resistive, capacitance, photo electric	
PLCs	
Motors	
Actuators	
relays	
IC controllers	
Breadboard	
switches	
Printed circuit boards PCBs	
Power supplies	
Programmable manipulators	
1 cartesian	
(2) gantry	
(3) cylindrical	
(4) spherical	
(5) articulated	
(6) SCARA	
Robot controls	
1 Point to point (PTP)	
2 Continuous Path control	
3 Controlled path control	
Automation and programming control tools	
Programable Computer Numeric control	
Direct Numeric Control DNC	
Printed Circuit Boards (PCB's)	
computer-integrated manufacturing (CIM)	
HMI software	
PAC, PLC and controllers software	
"Must meet the guidelines for specialized computing equipment as outlined on the "CTE Equipment Guidelines" at www.azed.gov/cte/grants	

Additional Items:

Network Scissors:	10	Motherboard:	31
CAT6 Cable:	500ft	Removable HD Bay:	31
RF45 Connectors:	1000	SSD:	31
Network Patch Panel:	4	HDD:	31
Anti-Static Electric Duster:	2	Power Supply Units:	31
Anti-Static Wrist Strap:	30	CPU:	31
PC Computer Tool Kit:	30	Graphics Card:	31
Digital Multimeter:	2	Tower:	31
Computer Kit:	31	Color Printer:	1
RAM:	31		

Arizona Department of Education
Career and Technical Education

Recommended Equipment List:
Network Security

2 of 2
6/16/2021

ISSN: 2473-4901
v9 n5955

Appendix B: Questionnaire and Interview Guide

Interviewee Questionnaire

1. What is your current role or job title?
2. If applicable, what academic degrees do you hold?
3. If applicable, what industry certifications do you hold?
4. How many years of experience do you have in secondary education?
5. What courses have you taught at the secondary education level and how many years have you taught each course?
6. If applicable, how many years of experience do you have in industry work related to cybersecurity, information technology, computer science, or related field?
7. What was your role in developing the cybersecurity education program at your institution?
8. If there is anyone else that you believe had input into the program and can provide insight into program development and operations, please provide them with my contact information and have them contact me.

Program Profile Questionnaire Questions

1. Describe the operational elements of the cybersecurity education program.
   a. Instructors (Education, Certifications, Years of Experience (Teaching / Industry), Courses Taught, Dual Enrollment Qualified (If so, What Courses).

Teacher	Education Level	Certifications	Years of Experience		Courses Taught	Dual Enrollment Qualified
			Teaching	Industry		

   b. Equipment (Type, Make, Model, Number, Cost)

Equipment Type	Make	Model	Quantity	Cost

2. Describe the formal learning activities. Formal learning is the type of learning that is intentional, organized, and structured. Formal learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program.
   a. What courses are included in the cybersecurity program?
   b. What are the course descriptions for courses within the cybersecurity program?
   c. Can you provide the syllabi for the courses within the cybersecurity program?
   d. Is the course dual enrollment?
   e. Did the course exist before the development of the cybersecurity program?

Course	Description	Syllabus	Dual Enrollment	Pre-Existing

Interview Questions

1. What was the motivation for starting a cybersecurity education program at your institution?
2. Describe how the cybersecurity education program was developed at your institution.
   a. What standards, guidelines, or frameworks were used to develop the program?
   b. How were the courses selected for inclusion in the cybersecurity program at your institution?
3. Describe the operational elements of the cybersecurity education program.
   a. Instructors
      i. How are qualified teachers identified or hired to teach cybersecurity courses?
      ii. If applicable, describe the challenges in finding qualified instructors for cybersecurity courses.
   b. Equipment
      i. How was the equipment listed identified or determined to be needed to support the selected courses?
      ii. If applicable, describe the challenges in procuring the equipment necessary to support the selected courses.
   c. Networks
      i. Describe the networks that students use for their cybersecurity curriculum and assignments.
      ii. If applicable, describe the challenges in operating on those networks.
   d. Facilities
      i. What facilities are used by students in the cybersecurity program?
      ii. Are these facilities utilized by students outside the cybersecurity program and if so by what programs?
      iii. Describe the process for acquiring these facilities.
      iv. If applicable, describe the challenges in obtaining these facilities to support the selected courses.
4. Describe the formal learning activities. Formal learning is the type of learning that is intentional, organized, and structured. Formal learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program.
   a. Why were these courses selected for inclusion in the program?
5. Describe the non-formal learning activities. Non-formal learning is a type of learning that may or may not be intentional or arranged by an institution, but is usually organized in some way, even if it loosely organized. There is no form of credits granted in non-formal learning situations. Examples of non-formal learning activities include camps, certifications, internships, and apprenticeships.
   a. Based on the provided definition and examples, what non-formal learning activities are incorporated in the cybersecurity program?
   b. How do these activities support the cybersecurity program and cybersecurity students?
6. Describe the informal learning activities. Informal learning is a type of learning that is never organized. Rather than being guided by a rigid curriculum, it is often thought of as experiential and spontaneous. Examples of informal learning activities include clubs, competitions, self-study / ad-hoc learning, conferences, and industry events.

   a. Based on the provided definition and examples, what non-formal learning activities are incorporated in the cybersecurity program?

   b. How do these activities support the cybersecurity program and cybersecurity students?

7. Describe the pathways for students. Students have four primary options after graduating from secondary education: go directly into the workforce, join the military, enter a trade or certification program, or attend post-secondary education.

   a. How does the cybersecurity program prepare students for the various pathways outlined above?

   b. How does the program track students upon graduation from the cybersecurity program?