Fall 10-2023

Alumni Perceptions of Cybersecurity Employment Preparation Using the NICE Framework

Tobi West

Alumni Perceptions of Cybersecurity Employment Preparation Using the NICE Framework

A doctoral dissertation submitted to Dakota State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Cyber Defense

October 2023
by
Tobi West

Dissertation Committee:

Ashley Podhradsky, Ph.D.
Pam Rowland, Ph.D.
Kevin Streff, Ph.D.
Omar El-Gayar, Ph.D.

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Tobi West

Dissertation Title: Alumni Perceptions of Cybersecurity Employment Preparation Using the NICE Framework

---

Dissertation Chair/Co-Chair: DocuSigned by: Ashley Podhradsky 2FCFD585B9054E7... Date: 10/02/2023

Name: Ashley Podhradsky

Dissertation Chair/Co-Chair: _____ Date: _____

Name:

Committee member: DocuSigned by: Kevin Streff DFE9CC7B27D9456... Date: 10/02/2023

Name: Kevin Streff

Committee member: DocuSigned by: Pam Rowland F7D9F3DA4DD3452... Date: 10/02/2023

Name: Pam Rowland

Committee member: DocuSigned by: Omar El-Gayar BE671FC34D9845C... Date: 10/02/2023

Name: Omar El-Gayar

Acknowledgement

First, I would like to thank the late Dr. Wayne Pauli for all his contributions to the CAE in Cybersecurity Community and all that he did to make DSU a great place to learn. His presence is dearly missed. Next, my deepest appreciation goes to Dr. Ashley Podhradsky, my dissertation chair, for the unwavering support, guidance, and encouragement along the way. I am thankful for the invaluable input of my dissertation committee members Dr. Pam Rowland, Dr. Kevin Streff, Dr. Omar El-Gayar, and unofficial bonus member Dr. Davina Pruitt-Mentle. My committee's contributions were essential to the completion of this work.

This study was inspired by the wonderful work of Dr. John Sands, CSSIA Principal Investigator, and Corrinne Sande, NCyTE Principal Investigator. Special thanks to Dr. Yair Levy and Dr. Anne Kohnke for their continued encouragement. All have contributed significantly to the CAE in Cybersecurity Community and their national leadership has been an inspiration. I'd also like to thank Dr. Arica Kulm for forging the way and *soon-to-be Dr.* Katie Shuck for helping me stay connected to the Cyber Defense program. Your kindness, strength, and perseverance has been a beacon that kept me moving in the right direction towards the finish line.

Finally, I'm incredibly thankful to my sons, Ian and Ryan, for their love and support. To Brekky B-Rex for her puppy eyes and unconditional love that helped drain away the stress. A big thank you to the special person that shared every bit of knowledge and insight into this process each day, the entire way through. Your belief in me has been a wonderful motivation.

With deep appreciation,

Tobi West

Abstract

The cybersecurity workforce suffers from an ongoing talent shortage and a lack of information correlating cybersecurity education programs to alumni employment outcomes. This cross-sectional study evaluated the post-graduation employment outcomes of alumni who attended two-year colleges designated by the National Security Agency (NSA) as Centers of Academic Excellence in Cyber Defense (CAE-CD). Stakeholders of this project were identified as government agencies, the NSA, employers, faculty, students, and organizations that rely on cybersecurity talent to keep their systems secure from cyberattacks. This study used the explanatory sequential mixed methods approach to compare perceptions of the intended Program of Study work roles to alumni employment outcomes using the NICE Framework work roles.

This multi-phased, nested sample study included CAE-CD designated Points of Contact (POCs) at two-year colleges and their alumni. The first phase included a call for participation requesting POCs to provide academic program information via online survey and to contact their cybersecurity program alumni with a link to an online survey. The second phase of the study included an online survey requesting that the alumni provide data about their work experience, academic program information, industry-recognized certification achieved, and any co/extra-curricular participation.

Overall, the demographics of the alumni sample were more diverse than those of the U.S. cybersecurity workforce and the alumni noted that their two-year academic programs were important to the preparation for their current job. Of the alumni who reported they were currently employed, approximately 80% held technology-related positions. Recommendations are made for the use of the resulting knowledge by cybersecurity stakeholders to better understand the employment outcomes of two-year college alumni from CAE-CD cybersecurity programs.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Tobi West

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

Background

There is a persistent and critical need for cybersecurity workers as the worldwide workforce gap reached an estimated 3.4 million workers in 2022 according to the *(ISC)2 Cybersecurity Workforce Study* sponsored by the International Information System Security Certification Consortium (ISC)2 (2022). As the cybersecurity workforce shortage continues, noteworthy data breaches include the CAM4 network breach impacting 10.88 billion records in March 2020, the Yahoo! breach in 2017 impacting an estimated three billion records, and the breach of biometric data from Aadhaar in 2018 affecting over one billion people (Tarun, 2022; Tunggal, 2022). Cyberattacks are believed to have cost the world $6.9 trillion in 2021 alone (FBI News, 2022).

Critical infrastructure owned by private and public entities supports the health and wellbeing of United States (U.S.) citizens and provides goods and services to citizens of other countries as well (Kapellmann & Washburn, 2019). The networked systems of all critical infrastructure sectors can be affected by cyberattacks, including chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors and waste, transportation systems, and water and wastewater systems (AlDaajeha, et al., 2022; Ashley, et al., 2022; CISA, 2020). The effects of a cyberattack on critical infrastructure can be catastrophic and/or have immeasurable societal consequences, such as the ransomware attack on the Colonial Pipeline that took services down for nearly a week and caused vehicle fuel shortages in several states (Ashley, et al., 2022; Hamdan & Nsour, 2022; Llansó, 2018; Voas, Kshetri, & DeFranco, 2021).

The U.S. national defense budget request for fiscal year 2023 was $813.3 billion, a 4.1% increase over the prior year, and $11.2 billion of that was focused on cyberspace activities to ensure cyber resilience for the Joint Forces of the Department of Defense (Austin, 2022). The U.S. investment for national defense includes several major initiatives: zero trust architecture, support for the Defense Industrial Base cybersecurity, and growth of the cyber mission force teams. The risks to information technology (IT) systems containing sensitive and personal information continues to increase year after year, with reports from the U.S. Government and Accountability Office (GAO) showing that 15% of the security incidents on federal agencies were related to email and phishing attacks and 44% were due to improper usage (GAO, 2022). Together, these statistics demonstrate the ongoing need for cybersecurity education programs that prepare individuals for unfilled jobs in cybersecurity.

Developing talent to protect and defend critical infrastructure is vital to our nation's public health, physical safety, and economic security (Dawson & Thomson, 2018; Kapellmann & Washburn, 2019; Kim, Smith, Yang, & Kim, 2018). The expansion of education pathways has been implemented as one of the many strategies to increase the talent pipeline of people interested in working in the field of cybersecurity (Javidi & Sheybani, 2018; Kose, et al., 2018; Shen, Chiou, Mouza, & Rutherford, 2021; NCyTE, 2021). From two-year degrees and four-year degrees to graduate degrees, programs in higher education for cybersecurity can be found embedded in other disciplines such as engineering, computer science, law, or as standalone cybersecurity degrees (Parrish, 2018).

Despite concerted efforts to increase the supply of skilled cybersecurity professionals, the shortage has continued to grow over the past few years without significant shifts in the gaps in ethnicity and gender ((ISC)2, 2022; Parker, 2016). To tamp down the risk and shorten the

lifespan of computer security incidents resulting from cyberattacks, organizations should employ skilled cybersecurity teams to stop attacks, restore operations, and thwart future attacks (Sanders, 2022). Identifying the skills and competencies needed for cybersecurity work roles has been studied by many initiatives and supported by the U.S. federal government, including the National Initiative for Cybersecurity Education (NICE) which is one of the most well-documented (Dawson & Thomson, 2018).

In response to the need for more information about the alumni outcomes from the Center of Academic Excellence (CAE) program's two-year colleges from across the country, the Center for Systems Security and Information Assurance (CSSIA) and the National Cybersecurity Training and Education Center (NCyTE) conducted a study in 2018 that asked alumni to self-identify which of the NICE work roles they were employed in (Sands & Sande, Workforce Study: Community College Cybersecurity Alumni, 2019). The study included responses of 88 alumni from cybersecurity programs at 12 CAE-CD colleges that self-selected to participate in the study The results of the alumni outcomes study showed that the two-year colleges had prepared students for the workforce with recommendations for future tracking, development of occupation pathways, and to investigate associations between industry certification and NICE work roles (Sands & Sande, 2019).

As of 2022, there were 1,043 two-year colleges that awarded over one million degrees and certificates in the 2019-2020 academic year (American Association of Community Colleges, 2022). Two-year colleges offer the opportunity for post-secondary education to all populations with higher enrollment typically reported for historically under-represented, including ethnic-minority, lower-income, and female students (Howell, et al., 2022; Phillippe, 2022; Xu, Jaggars, Fletcher, & Fink, 2018). The American Association of Community Colleges (2019) reported that

the trend over the last few years shows an increase in students new to post-secondary education as first-generation attendees to college.

Pham, Greaney, & Abel (2020) note that employment outcomes research tends to focus on universities and that community college data is usually aggregated, which introduces limitations to its use. Two impactful omissions are the number of work hours and whether students became employed in the field in which they were trained (Pham, Greaney, & Abel, 2020). As a suggested alternative methodology, Pham, Greaney, & Abel (2020) recommend using surveys to gather self-reported alumni data about employment outcomes.

The 2018 study by CSSIA and NCyTE (2019) aimed to collect information about employment outcomes and industry certification completion from two-year college alumni using the work roles of the NICE Framework to find concentrations and gaps. The study provided otherwise missing information about CAE two-year college employment outcomes to cybersecurity stakeholders. Cybersecurity education programs have continued to emerge, and the demand for cybersecurity professionals has continued to increase with a growing supply shortfall. Therefore, a more current study is needed to provide cybersecurity stakeholders with new information about two-year college alumni outcomes.

In recent years, the primary organizations commonly referenced as providing national-level aggregated data about the cybersecurity workforce shortage are (ISC)2 and CyberSeek (NICE, 2022). (ISC)2 has conducted multiple annual studies to provide information about the current global cybersecurity workforce, the workforce talent gap, and trends of emerging interest such as gender and ethnicity gaps. (ISC)2 estimates that 4.7 million people worldwide worked in cybersecurity jobs in 2022, the highest they have ever reported ((ISC)2, 2022). CyberSeek (2022) is a partnership project between EMSI Burning Glass, CompTIA, and NICE, reporting

the U.S. workforce shortage as 769,736 cybersecurity job openings across the U.S. and over one million people employed in cybersecurity roles as of September 2022.

For over two decades, the U.S. federal government has recognized the cybersecurity talent shortage and continues to focus on programs that serve multiple age ranges and interests to educate and train the cybersecurity workforce of the future as indicated by the variety of sponsored activities (Baker, 2016; Erbschloe, 2017; Paulsen, McDuffie, Newhouse, & Toth, 2012; Pérez, et al., 2011). Government funding assists with student programs across the country; among the many initiatives, those familiar to higher education institutions are GenCyber, Scholarship for Service Cyber Corps (SFS), and STARTALK, which help adolescents and young adults build the skills and competencies needed to secure the computer networks of private and public organizations (Mountrouidou, et al., 2019; Sanders, 2022). Another significant cybersecurity initiative supported by the federal government is the Centers of Academic Excellence (CAE) which encompass the higher education institutions across the U.S. teaching cybersecurity that meets the rigorous criteria set forth by the CAE program. The following three sections will provide further background and introduction to the CAE program, two-year colleges, and the NICE Framework.

Background of the Centers of Academic Excellence Program

Initially aimed at addressing the workforce shortage of the intelligence community, the CAE program was launched in 1999 by the NSA with the title of Center of Academic Excellence in Information Assurance Education (CAE-IAE) (CAE in Cybersecurity Community, 2021). Under the broader CAE program, there are now multiple designations with special program requirements, including Cyber Defense (CAE-CD), Operations (CAE-O), and Research (CAE-R). As of this writing, there are 389 higher education institutions with one or more CAE

designation types, of which 350 institutions hold the CAE-CD designation (CAE in Cybersecurity Community, 2021). Of the 350 institutions, there were 145 two-year institutions holding the CAE-CD designation with the word college in their name.

Institutions of higher education demonstrate their ongoing commitment to the CAE program requirements through the application process, including several significant items. The CAE-CD application is evidence-based with documented proof required for each criterion. Table 1 below is an overview of the sections and criteria of the CAE-CD program application derived from the NCyTE document, CAE 2020 – Proposed Preparations Starting Guide (Levy, 2020).

Table 1. CAE Program Criteria Overview

IMPACT	CRITERIA
Institution	• Letter of institution commitment • Verification of regional accreditation • Faculty promotion/reappointment policy • Evidence of sound security posture
Program	• Curriculum assessment plans • At least three students over the last three years • An established cybersecurity center • Continuous improvement plan with process and regular schedule • Integration of cybersecurity curriculum into other academic programs • Articulation agreements and curriculum sharing
Curriculum	• Curriculum maps of the cybersecurity-related Program of Study • NICE Framework crosswalk alignment • Courses with hands-on assignments • Curriculum mapped to the knowledge units
Students	• Student participation in extracurricular activities • Professional development opportunities for students • Outreach to students, other institutions, and the CAE Community
Faculty	• Faculty qualifications • Faculty support of enrolled students • Program sustainability • Affirmation of the CAE core values and guiding principles • Professional development opportunities for faculty

Note: Information in this table was adapted from the CAE-CD Resources webpage of the National Cybersecurity Education & Training Center (NCyTE) website (NCyTE Center, 2023).

The Center of Academic Excellence (CAE) program is one of many initiatives instituted by U.S. federal government agencies to build early interest in cybersecurity education and careers. Capacity building and talent pipeline development programs such as GenCyber, STARTALK, and Scholarship for Service Cyber Corps, are regularly implemented by CAE institutions through dedicated funding to host the activities for a given period. Higher education institutions are designated as a CAE after their application is carefully peer reviewed to ensure that the institution meets the rigorous criteria for curriculum and program requirements as set forth by the CAE Program Office hosted at the NSA headquarters (Strickland, 2022).

Background of Two-Year Colleges

Two-year colleges, often known as community colleges or junior colleges, typically offer two-year associate degrees, short-term certificates, and career-oriented programs with open access to the community, or 100% acceptance, using federal and state funds to keep tuition costs low for in-state residents (Chen, 2022). According to Jassal (2021), some states have recently started to offer four-year bachelor's degrees at the two-year colleges due to state legislation changes. Public community colleges can be an academic stepping-stone between high school and university for traditional students and a mechanism for upskilling or reskilling for non-traditional students that do not intend to pursue a bachelor's degree or higher (Chen, 2022). Statistics show that as much as 8% of community college students are returning after having earned a bachelor's degree (American Association of Community Colleges, 2022).

Progressive two-year colleges offer dual enrollment courses to high school students, providing students with the opportunity to receive both high school and college credit simultaneously (Hooper & Harrington, 2022). Dual enrollment programs allow traditional students to enter college or university programs and finish sooner than their counterparts entering

without credit for prior dual enrollment (Rodriguez, Gao, Brooks, & Gutierrez-Aragon, 2021). Additionally, many colleges offer remedial support classes and specialized career courses that can be taken without a declared degree major which are not usually offered independently at the university campuses in most states (Chen, 2022).

Across the 50 states there are public two-year colleges and universities with different governance structures. For example, some states have a State Board of Education that oversees their two-year colleges separately from their four-year institutions without a coordinating entity over both sectors, including California, Georgia, Maine, New Hampshire, West Virginia, and Wisconsin (McGuinness, 2014). While others according to McGuiness (2014), such as Alaska, Georgia, Hawaii, and 14 other states have a board that governs both two-year and four-year institutions with some offering two-year degrees at the university institutions rather than a separate two-year institution. Arizona and Michigan are unique without a state-level board or authority over community colleges that are locally governed. In the U.S. as of 2021, there were 936 public two-year colleges, 35 tribal colleges, and 72 independent colleges (American Association of Community Colleges, 2022; Duffin, 2021).

Background of NICE Framework

In 2021, the current version of the NICE Framework was introduced in Special Publication 800-181, revision 1 of National Institute of Standards and Technology (NIST) (Petersen, Santos, Wetzel, Smith, & Witte, 2020). Unlike the first version released in 2013, the current version of the NICE Framework defines the Tasks, Knowledge, and Skills (TKS) as applied to cybersecurity work roles. Competencies are the building blocks made up of compilations of TKS statements from the NICE Framework to provide categories that can be

used by organizations for the hiring process. The NICE Framework Resource Center maintains the lists of Competencies and Work Roles as separate documents.

The NICE Framework was developed with input from multiple stakeholder perspectives, allowing subject matter experts in industry, government, and the public to influence the resulting document (NIST, 2021). Through revisions of the NICE Framework, NICE has published NISTIR 8355 to define competencies for assessment of learning for cybersecurity work in an evergreen document referred to as NICE Framework Competencies that will be routinely updated to continue to be valuable to the cybersecurity community (Wetzel, 2021). The public comment model of the NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, will now be followed for the NICE Framework which allows anyone from the public to submit comments through the online portal for a given period. Following is a conceptual model of the continuous improvement methodology used by NICE to ensure that the NICE Framework, Competencies, and Work Roles are up to date with feedback from federal, state, and local agencies of government, tribal territories, private industry, academia, international communities, and the public.

As part of the regular cycle of updates, NIST put out a call for comments for the NICE Framework work roles and categories on April 18, 2023, (NIST, 2023). The proposed update included a reduction from 52 work roles to 50 work roles with a change to many of the names. Also included in the proposed changes was a transition from seven to six categories. Figure 1 offers a visual representation of the continuous improvement methodology in which multiple stakeholder communities provide valuable input for the NICE Framework. The process provides for a global feedback cycle, with the inclusion of internal communities and the public.

Figure 1. NICE Framework Continuous Improvement Methodology

Note: Information in this figure was adapted from NIST Special Publication 800-181, Revision 1, revised November 2020 (NIST, 2021).

The vetting process to add items to the NICE Competencies list takes time due to the amount of input taken into consideration from such a broad variety of stakeholders. In the meantime, the work of cybersecurity professionals continues routinely with incident response teams hard at work in every industry sector, every government agency, and every sector of critical infrastructure (Doyle, 2021). Due to emerging threats and continuous changes in security, this presents a moving target that the NICE Framework attempts to keep up with through routine revisions and continuous stakeholder input (Knapp, Maurer, & Plachkinova, 2017; Parrish, 2018).

The NICE Framework, NICE Competencies, and NICE Work Roles are helpful to organizations that need to set up structures for their cybersecurity teams. These Framework resources can be used to define the TSKs and competencies an organization needs based on the types of threats it faces, the frequency of successful attacks, internal threats, and the volume and sensitivity of the information it maintains. The NICE Framework can be used to inventory

strengths and knowledge gaps of cybersecurity workforces, identify qualifications and training, improve job posting descriptions, develop career paths for the most relevant work roles, and provide a common language for recruitment and retention of cybersecurity workers (Rosencrance, 2019).

Competencies are learner focused, address employer needs, and are assessed at the competency level (Wetzel, 2021). Whereas, the Work Roles are work focused, define positions and responsibilities, and are task-level assessment as described by Wetzel (2021). The categories serve as high-level groupings for the work roles of the NICE Framework (Paulsen, McDuffie, Newhouse, & Toth, 2012). Table 2 shows the Work Roles grouped into Categories of the NICE Framework as of the 2023 proposed updates (NIST, 2023).

Table 2. NICE Framework Categories and Work Roles

CATEGORY	WORK ROLES
OVERSIGHT and GOVERNANCE (OG)	Authorizing Official Communications Security (COMSEC) Management Curriculum Development Executive Leadership Instruction Legal Advice Policy and Planning Privacy Compliance Product Support Program Management Project Management Security Control Assessment Systems Management Technology Portfolio Management Technology Program Auditing Workforce Management
DESIGN and DEVELOPMENT (DD)	Enterprise Architecture Research and Development Security Architecture Software Assessment Software Development System Testing and Evaluation Systems Development Systems Requirements Planning
IMPLEMENTATION and OPERATION (IO)	Data Analysis Database Administration Knowledge Management Network Management

CATEGORY	WORK ROLES
	System Administration Systems Analysis Technical Support
PROTECTION and DEFENSE (PD)	Cybercrime Investigation Cyberspace Defense Digital Forensics Incident Response Infrastructure Support Threat Analysis Vulnerability Analysis
INTELLIGENCE (IN)	All-Source Analysis All-Source Collection Management All-Source Collection Requirements Management Intelligence Planning Multi-Disciplined Language Analysis
CYBERSPACE EFFECTS (CE)	Cyber Operations Cyber Operations Planning Exploitation Analysis Mission Assessment Partner Integration Target Development Target Network Analysis

Note: Information in this table was adapted from the NIST website, Comments Requested on Proposed Updates to NICE Framework Work Role Categories and Work Roles, released April 18, 2023.

Problem Definition

In general, the types of studies conducted by (ISC)2, the National Student Clearinghouse, and the U.S. government provide aggregated data which is insufficient when evaluating curriculum and student preparedness for the workforce. CAE-CD two-year colleges offer academic programs to prepare students for cybersecurity work roles but do not always have the information about alumni employment outcomes. Administrative data collected by regional, state, and national organizations, such as the National Student Clearinghouse, is aggregated to include multiple academic programs and multiple disciplines without specificity to work roles.

Alumni employment outcomes often go untracked by the college. After graduating with a two-year degree, students may continue their education, attend training, pass industry

certification exams, and/or be employed in the workforce. These achievements are typically not recorded to this level of detail by the colleges at an individual or academic program level, so alumni employment outcomes are generally unknown or undocumented. Understanding the employment outcomes of alumni can aid CAE institutions in curriculum updates, the creation of program pathways, and the formation of partnerships with employers and 4-year institutions. A review of the literature shows two notable gaps, alumni employment outcome studies for two-year college cybersecurity programs and the relationship between academic pathways and NICE Framework work roles.

Without detailed alumni outcome data, faculty may rely more heavily on industry advisory board feedback and other industry trend influences. By obtaining more detailed information from alumni about the factors that affected their employment outcomes, faculty can update program offerings to help other students reach similar outcomes or find gaps in program offerings to help students prepare to obtain jobs with specific work roles. This way the alumni outcomes can have more of an impact on academic program updates, including curriculum, course content, and co/extra-curricular activities offered.

Objectives

The primary objective of the study is to identify the cybersecurity work roles that CAE-CD two-year college alumni are most frequently employed in and to correlate these to the work roles identified by the POCs of the CAE-CD. Additional statistical analysis techniques will be used to examine the relationships between program and career preparation, continued education after two-year college graduation, gender distribution ratios, and demographic variables.

Research Question

Through the gathering and analysis of perceptual data from POCs and alumni of CAE-CD programs and alumni employment outcomes, the study can provide knowledge to the CAE community. A survey will be used to collect data about the phenomenological circumstances to answer the proposed research questions. According to Creswell (2013), research questions are intended to "narrow and focus the purpose statement". A two-phased survey approach will be used to address the following research questions where quantitative and qualitative questions will be asked of the POC to identify programmatic details in the first phase and alumni will be asked qualitative questions to identify demographic and career-outcome related information in the second phase.

The primary research question and sub-questions proposed for this study were:

RQ1: Which cybersecurity work roles of the National Initiative for Cybersecurity Education (NICE) Framework are alumni of Centers of Academic Excellence in Cyber Defense (CAE-CD) two-year colleges employed in as compared to the work roles identified by their college?

RQ1.1: What proportion of the cybersecurity program alumni are not employed in any cybersecurity work roles?

RQ1.2: What proportion of the alumni pursued another degree within three years of graduation from a CAE-CD two-year college?

RQ1.3: How do the alumni gender and ethnicity demographics align with the gender and ethnicity demographics of the cybersecurity workforce of the United States?

Summary of the Intended Study

The purpose of this cross-sectional, mixed methods study was to examine cybersecurity program alumni employment outcomes to provide the CAE community with career outcome

data, identify work roles and gaps based on the NICE Framework, and understand the value of co/extra-curricular activities. CAE-CD POCs from two-year colleges were contacted via email with an invitation to participate in the study. POCs were asked to provide their contact information, Program of Study details, and their program's targeted work roles for later comparison to the alumni data. The POCs were asked to contact their program graduates to request that the alumni participate in the study. Each of the participating POCs were then provided with a link to send to their alumni which included an online survey questionnaire. The information has been stored in a secure manner to allow only authorized access for the intended purposes of this study.

Definition of Terms

Table 3 includes the defined terms and other acronyms used for purposes of this study. Some of the terms may be regularly used throughout the CAE community, in cybersecurity, and in higher education but may not be broadly recognized outside of those groups.

Table 3. Definition of Terms

TERM	DEFINITION
Two-Year College	An institution of higher education that offers two-year degrees, short-term certificates, and career-oriented programs. The associate degrees are approximately 60 units.
CAE-CD or Center of Academic Excellence in Cyber Defense	A special designation from the National Security Agency (NSA) given to higher education institutions that meet curriculum and program requirements.
Critical Infrastructure	There are 16 sectors considered vital to the United States: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors and waste, transportation systems, and water and wastewater systems.
Cyberattack	An attack carried out against networked systems or unauthorized attempts to access data with the intent to disrupt services, steal information, or ruin an organization's reputation.
Cybersecurity	The protection of networked systems and Internet-connected devices to ensure cyberattacks and breach attempts are unsuccessful.
Dark Web	An intentionally hidden portion of the Web that requires special browsers to access. Most known for online anonymity and websites that offer anonymous transactions for the purchase of illicit goods and services in exchange for cryptocurrency.

TERM	DEFINITION
Internet of Things	All mobile Internet-connected devices, including wearables, smart home devices, and medical devices.
KU or Knowledge Units	Concepts and skills defined by the CAE program as important for students to learn. CAE institutions map their curriculum to the knowledge units to meet curriculum requirements for the CAE program.
NICE Framework	A workforce planning reference tool that describes cybersecurity work roles based on the tasks, knowledge, and skills required to perform the functions of the related jobs. Reference for educators, hiring managers, and job seekers to aid in the greater understanding of the roles in the field of cybersecurity.
NICE Work Roles	Describes the tasks, knowledge, and skills needed to perform cybersecurity functions in the workplace.
POC or Point of Contact	The individual at a CAE institution that oversees the program to disseminate information and keep the program up to date.
PoS or Program of Study	An academic program, with curriculum culminating in the achievement of either a degree or certificate. May also be referred to as a student's degree major at higher education institutions.
Ransomware	Malware intended to lock up data and systems to demand a ransom, with payment often required in cryptocurrency.

Organization of this Paper

At the completion of this study, this research paper will be organized into five chapters. Following the introduction of concepts and terminology in Chapter 1 there is a review of the relevant literature regarding the cybersecurity workforce, the NICE Framework, cybersecurity education programs, and alumni outcomes studies in Chapter 2. An explanation of the mixed methods research methodology used in this study, and the steps taken to collect data from CAE-CD program POCs, and the program alumni is included in Chapter 3. After the POCs and alumni completed the surveys, an analysis of the data was conducted with results included in Chapter 4, followed by the recommendations, and concluding remarks in Chapter 5. The appendices contain the instruments of this study, such as the images of the online survey questionnaires used to collect data and the list of CAE-CD institutions extracted at the onset of this study.

Significance of this Study

Few studies focus on the employment outcomes in the field of cybersecurity for two-year college alumni and these cross-sectional studies become quickly outdated due to the constant expansion and dynamic changes of the cybersecurity workforce. The CAE-CD community

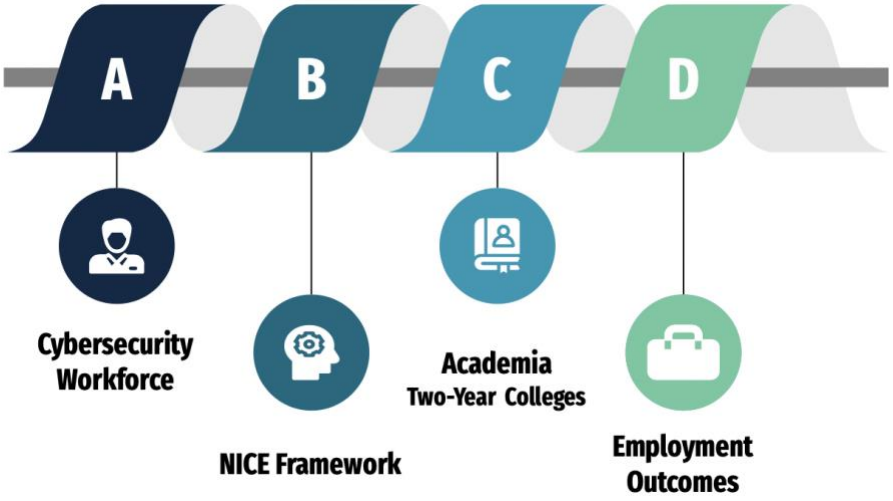
focuses significant effort to build interest in cybersecurity careers and to prepare students for cybersecurity jobs. Conducting this study could expand the body of knowledge about two-year college alumni outcomes in cybersecurity.

The results of this study can be used by the CAE-CD two-year colleges to focus on the most relevant work roles, evaluate significant work role gaps to identify additional specialized programs for curriculum development, integrate content that includes material for industry certifications that students have prepared for, consider extracurricular activities that alumni have identified as important, and the percentage of alumni that have furthered their education with other higher education institutions. Cybersecurity stakeholders will be able to leverage the results to inform their current and future support projects and decision making for workforce development, with emphasis on consideration for education requirements for entry-level positions.

Chapter 2. Literature Review

The present section includes a traditional literature review with an examination of the cybersecurity workforce shortage and diversity issues that the U.S. continues to face, the resources targeted to aid in closing the workforce gaps, academic pathways to supply the workforce, and alumni outcomes studies. The chapter will be organized into four groups: the cybersecurity workforce and global workforce studies by professional organizations, the NICE Framework, academic programs, and alumni employment outcomes. As noted by Creswell (1994), a visual representation of the literature review groupings can provide context to the sequence, a schematic for this section is shown in Figure 2 below.

Figure 2. Schematic of Literature Review



Cybersecurity Workforce

After 30 years of the World Wide Web, there are over 1.18 billion websites compared to just 130 websites available on the Web in 1993 (Huss, 2022; O'Malley & Rosenzweig, 1997). Early origins of computer security date back to the early 1970's before the public Internet was available (Chadd, 2020). The increase in Web traffic and proliferation of personal devices that make up the Internet of Things has led to organizations storing massive amounts of data that

must be protected from cybercriminals that stand to profit from the sale of stolen personal data on the Dark Web (Nazah, Huda, Abawajy, & Hassan, 2021). According to Kulm (2020), "a digital component can be found in nearly every crime committed today" which raises additional challenges for cybersecurity professionals. All the while, the cybersecurity workforce skills gap widens, leaving companies searching for talented, diverse individuals to defend their systems (Moses, 2022).

In a fireside chat at the NICE Symposium, then National Cyber Director, Chris Inglis shared the concept of 'all, many, and few' related to the need for cybersecurity education in which all people need to be secure as individuals and employees, many people work in roles that implicate cyber, and few work in roles dedicated to cybersecurity tasks (NICE Symposium, 2021). Through pathways initiatives, community colleges can provide cybersecurity education to many populations, including middle school, high school, adults, and the broader population. With extra-curricular activities and cybersecurity curriculum integrated into multiple disciplines, higher education can prepare the 'many' that are employed in roles working on projects that implicate cybersecurity such as logistic systems, supply chains, and vehicle manufacturing (NICE Symposium, 2021). CAE-CD programs likely tend to focus on the curricular programs that prepare the 'few' for cybersecurity careers and the 'many' and 'all' through extra-curricular and interdisciplinary projects.

The cybersecurity workforce is complex in that it encompasses many jobs at various levels within organizations, from technician to executive leadership, from short-term consultant to permanent employee, and everything in between (Dawson & Thomson, 2018). The demand for talented cybersecurity workers continues to grow as technology advances at a rapid pace and the sophistication of attackers continues to increase (McClurg, 2021; Ramezan, 2023). There is

global growth in the demand for a diverse cybersecurity workforce which continually outpaces the supply of graduates from cybersecurity and related academic programs ((ISC)2, 2022). Many entry-level jobs in cybersecurity also require prior cybersecurity-related work experience in addition to post-secondary specialized education (Carrese, Goss, Hermann, & Bartel, 2018; Marquardson & Elnoshokaty, 2020).

The surge in workforce demand has resulted in academic programs rooted in other disciplines and standalone cybersecurity programs as well (Cooper, et al., 2009; Parrish, 2018). There is a growing need for cybersecurity education pathways, including two-year colleges, as noted in The National Cyber Workforce and Education Summit's agenda which was held in July 2022 by CISA, Cybersecurity and Infrastructure Security Agency (Mitchell, 2022). The summit discussion intended to address issues using a 'call to action' approach according to Mitchell (2022), with emphasis on the workforce shortage, talent development through education, and diversity through previously untapped populations entering the workforce. Authors of The Cyber Vault (2018) document that there have been several Presidential Orders from the White House emphasizing the need to secure critical infrastructure, one of the first to focus on the cybersecurity workforce was Executive Order 13870 issued in 2019 (The White House, 2019).

These Presidential Orders have led to cybersecurity education related initiatives such as NICE and the CAE, plus many other organizations working independently to raise awareness and educate people on cybersecurity issues (AlDaajeha, et al., 2022). Parrish (2018) explained that the urgent need for cybersecurity education programs caused organic growth of cybersecurity embedded in existing disciplines but cybersecurity has now evolved to its own meta-discipline, like computer science in the 1960s. Despite the variety of education initiatives developed to increase the number of individuals prepared for the cybersecurity workforce,

government agencies often still require a bachelor's degree or higher for cybersecurity-related jobs and many industry employers have the same requirements (IBM Institute for Business Value, 2017; Marquardson & Elnoshokaty, 2020).

Cybersecurity professionals must have unique skillsets referred to as People, Process, and Technology by LeClair, Abraham, and Shih (2013) to understand the psychological motives of cyberattacks, build bridges within the organization to develop policies that secure the organization, and technical capabilities to configure, maintain, and integrate technology. The workforce includes employers from industry, government, and academia, all using different job titles and requirements that are not standardized, leading to complexity in communication between organizations and agencies. The NICE Framework was designed to bridge the gaps in communication by providing a common lexicon and taxonomy (Paulsen, McDuffie, Newhouse, & Toth, 2012). Due to the lack of common job terminology in industry and non-standardized education programs (Parrish, 2018; Paulsen, McDuffie, Newhouse, & Toth, 2012), the NICE Framework offers the best and most used widely used list of work roles as a basis for this research.

Multiple organizations have studied the continual shortage of individuals prepared to work in cybersecurity roles over the years, including the federal government and well-known professional organizations such as (ISC)2 and ISACA (Information Systems Audit and Control Association). Global workforce studies show that the shortage has only increased over the years with projections by the Center for Cyber Safety and Education in 2019 anticipating the shortage at 1.8 million for 2022 (Simpson, 2019) and the estimated shortfall reported in 2022 by (ISC)2 was nearly double the anticipated gap at 3.4 million cybersecurity workers ((ISC)2, 2022). Cybersecurity and the workforce shortage continue to be a global concern due to geopolitical

instability, the impact of emerging technology and threats, the lack of resources to quickly respond to regulatory changes, and the need for improved communication within organizations (Libicki, Senty, & Pollak, 2014; World Economic Forum, 2023). Additional challenges for the cybersecurity workforce include lack of ethnic diversity and low representation for women ((ISC)2, 2022; Parker, 2016; Simpson, 2019). Although the ratios for ethnicity and gender representation have shifted slightly over the years, the problem persists ((ISC)2, 2022). Up from 20% in 2019, women held 25% of the cybersecurity jobs globally, according to Cybersecurity Ventures (Morgan, 2022). The following sections cover the global and federal cybersecurity workforce studies conducted from 2004 to 2012, ISACA's State of Cybersecurity 2022, the workforce study completed by NCyTE and CSSIA for the National Science Foundation, and diversity gaps in the workforce.

Global cybersecurity workforce studies.

(ISC)2 Global Cybersecurity Workforce Studies.

This section covers the bi-annual and annual cybersecurity workforce studies conducted by the professional organization called International Information System Security Certification Consortium, known as (ISC)2 from 2004 to present which evaluate the state of the workforce with regard to number currently employed, the talent shortage, hiring manager decision making factors, and the future outlook ((ISC)2, 2022). Additional special reports by (ISC)2 have included regional reports and others focused on the gender imbalance and the need for diversity in the cybersecurity workforce. (ISC)2 is a non-profit organization that conducts workforce research and establishes international standards for the cybersecurity profession through internationally recognized training and certification exams. Their studies include participants from around the world employed in organizations of all sizes.

The 2004 white paper, (ISC)2 Information Security Global Workforce Study, included a survey of 5,371 participants from around the world employed in a variety of industry verticals and information security job functions (Carey, (ISC)2 Information Security Global Workforce Study, 2004). At that time, International Data Corporation (IDC) predicted that the cybersecurity workforce would reach 2.1 million professionals by 2008, up from the 1.15 million estimated employees in 2003. Certifications were important to 92% of the hiring managers surveyed when choosing a candidate. Of those surveyed, there was generally more experience in information technology with 13 years on average plus seven years of information security work experience. Education and experience were the primary deciding factors when hiring with certifications being a differentiator when multiple applicants had similar qualifications. Also, according to the 2004 report, the number of designated CAE institutions increased from just seven to 55, showing the commitment to increasing the availability of cybersecurity education.

When a similar study was conducted by IDC again in 2005, there were 4,305 respondents from organizations of various sizes employed in information security roles (Carey, 2005). One significant difference in responses from 2004 was that more security professionals expected the amount of security training to increase for the coming year and that the number of master's degree completers rose to 34% in 2005 as compared to 28% in the prior year. In addition to responding that certifications were an important factor in hiring decisions, respondents also reported that continuing education was a significant contributing factor to achieve the certification and demonstrate competency.

IDC's 2006 white paper emphasized the U.S. government perspective of the information security workforce with 4,016 responses (Carey, 2006). Survey respondents said that their time was focused on activities to meet regulatory compliance, research of new technologies, and

information systems certification and accreditation. Most averaged about 10 years of information security work experience. This was the first in the series of annual reports to call attention to the gender gap, identifying 17% women in federal defense, 21% women in federal non-defense, and 16% women in state and local government roles.

For the 2008 report, Frost and Sullivan were chartered to conduct the (ISC)2 global workforce study which was completed using an online survey in the fall of 2007 (Frost & Sullivan, 2008). There were significantly more responses in this study, with 7,548 information security professionals from over 100 countries around the world. Top information security concerns for the private sector included viruses and worms while government respondents identified cyber terrorism as their highest concern. The reported cybersecurity workforce of 2007 was estimated to be 1.66 million with anticipated growth to 2.7 million by 2012. The report highlighted that universities were continuing to develop specialized programs which may be causing information security professionals to feel pressure to achieve degrees in higher education related to the profession, with 47% worldwide having a bachelor's degree or equivalent.

In both 2009 and 2010, the studies focused on the perspective of federal Chief Information Security Officers (CISOs) and had relatively low response rates of 40 and 36 respondents respectively, due to the target group being surveyed (Government Futures, 2009), (Garcia Strategies, LLC, 2010). Data loss due to external threats was of highest concern, with internal threats and software vulnerabilities also being of concern for the CISOs.

A return to the global workforce study model in 2011 included 10,413 respondents from various sized organizations for the study conducted in 2010 (Frost & Sullivan, 2011). A worldwide estimate of 2.28 million information security professionals in 2010 with growth expected to hit 4.2 million by 2015. The skills gap was an urgent issue identified by study

participants. Application vulnerabilities emerged as a top threat and cloud computing emerged as the top skills training requested.

Frost & Sullivan reported in 2013 on the global study conducted for (ISC)2 in the fall of 2012, with 12,396 participants, the majority being (ISC)2 members (Frost & Sullivan, 2013). Top concerns remained the same in the 2013 report, application vulnerabilities and malware staying at the top of the list. Frost & Sullivan predicted that worldwide there would be 3.2 million people employed as information security professionals that year.

A report by the University of Phoenix (2014) on education-to-workforce skills gaps with a cybersecurity professionals roundtable, noted the requirements were becoming more standardized through the NICE Framework and the Department of Labor's (DOL) Cybersecurity Industry Competency Model. Roundtable stakeholders helped to identify major gaps, including "competency, professional experience, and education speed-to-market" (University of Phoenix, 2014). Curriculum and education program update recommendations from the roundtable group were to use labs and case studies, job shadowing and internships through employer partnerships, and student preparedness for employment. The report's conclusion provided final recommendations directed at education institutions, students, and employers to address each issue.

In 2015, Frost & Sullivan returned with the global cybersecurity workforce study reaching 13,930 cybersecurity professional respondents (Frost & Sullivan, 2015). Respondents were again from various sized organizations and multiple industry verticals. Again, application vulnerabilities and malware remained at the top of the list of high concerns for security. Notably, a high number of respondents reported job satisfaction and an average of 12.7 years security work experience. As far as respondent education levels, there was a downward trend for

bachelor's degrees at 44% and an upward trend for master's degrees at 43%. Additionally, a special report on Women in Cybersecurity was published in 2015, noting just 10% women employed in information security roles (Frost & Sullivan, 2015). The report provided differences in education level, work roles, and salaries for men and women.

The white papers and executive briefings commissioned for 2017 included another for Women in Cybersecurity, diversity, and another on the U.S. government perspective. The global report included responses from participants in over 170 countries and 19,641 information security professionals (Frost & Sullivan, 2017). There was no shift in the gender proportions, it was reported that there were 11% women employed worldwide in information security roles, with North America having the highest percentage at 14%. A larger proportion of women reported having experienced workplace discrimination, less representation in executive leadership roles, and the wage gap widened with women having lower salaries than men at all levels (Frost & Sullivan, 2017).

The report for 2018 had a name change to (ISC)2 Cybersecurity Workforce Study with a focus on the increasing skills shortage and the top job concerns of 1,452 cybersecurity professionals from 250 companies worldwide ((ISC)2, 2018). Globally there was a shortage estimate of 2.93 million cybersecurity professionals based on open positions. The top concern indicated that organizations were at extreme risk of cyberattack due to the lack of personnel with cybersecurity experience. A notable change in the gender proportion showed 24% women in information security positions worldwide which (ISC)2 report authors attributed to cybersecurity workforce assessments that have provided a broader view of demographics and gender gaps. Certifications were tracked as critical factors for advancing and maintaining career positions.

As of 2019, the Cybersecurity Workforce Study referenced the cybersecurity career path with emphasis on strategies for building strong cybersecurity teams as data breaches and ransomware concerns continued to increase ((ISC)2, 2019). The cybersecurity workforce was estimated to be 2.8 million globally with a shortage of 4.07 million. The lack of cybersecurity professionals continued to be a top concern with additional concerns for lack of standard terminology coming in as the second major concern for security professionals. This is the first report from (ISC)2 referencing a separate break out segment for associate degrees in the education levels. Respondents reported education in computer and information sciences, engineering, and business with the following levels 12% high school diploma, 11% associate degrees, 38% bachelor's degrees, 28% master's degrees, and 10% doctoral degrees.

During the first year of the global Covid-19 pandemic, the (ISC)2 Workforce Study was conducted in late spring with 3,790 participants ((ISC)2, 2020). Again, the report included estimates for the workforce and the shortage of cybersecurity professionals around the world. Many organizations worldwide transitioned to a remote work environment in a single day (30%) and 47% said they transitioned from a few days to a week. The report also considered the security preparedness of organizations for remote work, changes in security team communications, security incidents occurring after the transition, understanding of the implications by those in leadership roles, and security budget concerns. The workforce shortage saw its first decrease down to 3.12 million compared to the prior year's 4.07 million.

Over the last couple of years, cyber resilience has become the security posture for many organizations. The 2021 report included a global workforce estimate of 4.19 million and another decrease in the shortage down to 2.7 million ((ISC)2, 2021). Key findings in the report were related to the impact of the shortage on those that are working in the profession, which areas are

most lacking in talented individuals, and what the organizations are likely to do to retain and recruit talent as they move forward. Study participants were asked about job satisfaction, career pathways, education, compensation, top skills and attributes, and how best to diversify the cybersecurity workforce.

This year's report for 2022 considered the ongoing workforce gap as the highest concern with a shortage of 3.4 million worldwide ((ISC)2, 2022). Respondents from around the world totaled 11,779 from the estimated 4.65 million employed in cybersecurity roles. A vast majority stated that their organization was significantly short-handed in security professionals with not being able to find talent and attrition as the top two reasons. Many still reported high job satisfaction due to flexible work arrangements and high interest in the work of the profession. Younger respondents reported an interest in having their voices heard in the workplace and valued initiatives and efforts focused on diversity, equity, and inclusion (DEI).

Early versions of the (ISC)2 Workforce Study reports focused on security concerns of information security professionals, education levels, and certification attainment. Later versions focused on diversity in the workplace and career pathways leading to employment in the cybersecurity workforce to reduce the ongoing talent shortage. More recently, the reports have focused on global geo-political situations such as the Russian-Ukrainian war, implications of gender and age proportions, DEI efforts, and the impact of the workforce shortage on employees currently working in the field. For the most part, survey responses were gathered using online forms and those that mentioned the amount of time, stated that it took about 20 minutes for participants to complete the survey. There were also two small group roundtables with CISOs in 2009 and 2010 that referenced relatively small numbers below 50 participants. Table 4 shows the number of survey responses each year and the top concern identified in the report.

Table 4. (ISC)2 Workforce Study Response Rates Over the Years

REPORT YEAR	RESPONSES	TOP CONCERN
2004	5,371	Logical and physical security
2005	4,305	Spyware
2006	4,016	Hacking, identity theft, and cyber warfare
2008	7,548	Viruses and worm attacks; cyber terrorism
2011	10,413	Application vulnerabilities
2013	12,396	Application vulnerabilities
2015	13,930	Application vulnerabilities
2017	19,641	Data exfiltration/exposure
2019	3,237	Data breaches and ransomware
2020	3,790	Remote work and defending home systems
2021	4,753	Workforce shortage
2022	11,779	Emerging technologies; regulatory requirements

ISACA State of Cybersecurity 2022

Formerly known as Information Systems Audit and Control Association, ISACA is a professional association with international membership founded in 1969 (About Us, 2022). Membership is reported to cover 188 countries around the world with over 150,000 professionals in various roles of IT governance. ISACA's 2022 global update includes a study that was conducted in late 2021 using an online survey form where ISACA certification holders were asked to provide anonymous feedback on staffing issues, organizational cybersecurity budgets, the current threat landscape, and cybermaturity related to cyber-related risk factors (ISACA, 2022). The study covered multiple organization sizes and regions of the world with North America being the dominant response groups at 52%. For skills gaps, respondents reported that soft skills are one of the top concerns along with cloud-computing skills. Less organizations are requiring a bachelor's degree in the recruitment of new candidates compared to the study from the prior year. This is favorable to the two-year college efforts of the CAE program to establish associate degree programs that assist students with the education-to-career pathways in cybersecurity.

Federal Cybersecurity Workforce Studies

The federal government conducted a survey of close to 23,000 federal employees to better understand the cybersecurity workforce and future needs. Walker reported that the 2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) highlighted the age stratification in relation to impending retirement and the training needs of those surveyed (Molly, 2013). Also, according to Walker, the survey data accompanying the ITWAC Summary Report was provided in a Web-portal accessible to government agencies, allowing the opportunity for strategic planning of cybersecurity teams, including training to reduce skills gaps. In addition to age at the time of the survey, number of years to retirement, skills, and pay grades, the survey respondents noted their level of higher education degree achieved, types of degrees attained, and any related cybersecurity certifications.

Based on the NICE Framework, the IT Workforce Capability Assessment (ITWCA) was developed to gather federal workforce data. The ITWCA was used for assessment in 2003, 2004, and 2006 to assess the federal government's information technology workforce and the ITWCA was modified in 2011 to include cybersecurity competencies. The 2012 IT Workforce Assessment for Cybersecurity (ITWAC) study using the new ITWCA of 2011 included three objectives which are quoted below from the summary report (NICE, 2013).

- Identify federal employees with cybersecurity job responsibilities,
- Establish a baseline of current cybersecurity capabilities and proficiencies among the Federal workforce, and
- Understand the scope of the cybersecurity workforce pipeline.

In late 2012, survey responses from 22,956 federal employees were voluntarily collected using an online form using the Federal Competency Assessment Tool (FCAT) platform to provide their assessment of competencies in cybersecurity tasks. Participants provided a variety of

information related to time spent in the NICE Framework specialty areas, proficiency ratings, work experience, training needs, education, certification, and their demographics. The majority of study participants were over the age of 40, with the highest participant age range being 51-55, which was of particular concern because they were nearing retirement eligibility.

Estes, Kim, and Yang (2018) conducted an analysis of the alignment of cybersecurity job candidates and the NICE Framework to determine ways that the Framework could be useful as a workforce development tool. The article included a background on the Framework, a literature review of mapping methodologies for job functions, recruiting tools developed from mapping the knowledge, skills, and abilities for a work role, and the effects on the workforce development lifecycle. The conclusion indicated that the mapping could help to ensure that work roles are properly mapped out and to help organizations recognize the tasks belonging to work roles without inundating employees with too many tasks or requiring too many different skillsets. The mappings can also be used to select programs for training within the specialized work roles defined by the skillsets.

Two-Year College Workforce Study

Sands and Sande's (2019) examination of post-graduation career outcomes from some of the nation's top two-year colleges, "Workforce Study: Community College Cybersecurity Alumni. Where are they now?" was published under the partnership of the National Cybersecurity Training and Education Center (NCyTE) and the Center for Systems Security and Information Assurance (CSSIA). Sands (2021) stated that this study, conducted in 2018, was funded by the National Science Foundation to evaluate the trends in cybersecurity jobs filled by students that have graduated from CAE-CD designated two-year college as compared to the 52 work roles of the NICE Framework. The two primary criteria for colleges to participate in the

study, according to Sands (2021), were that the colleges had a cybersecurity program in place for at least five years and that they were a CAE.

The colleges included in the study self-selected and the lead faculty chose graduates that were known to be employed in cybersecurity work roles after graduation. Data were collected by student researchers that interviewed participants via remote meeting platforms and using a survey form for data input. Participants were asked how long they had been employed, if they believed that their education program prepared them for the job, which of the 52 NICE work roles their job tasks covered, and which industry-recognized certifications they had achieved.

From the 12 colleges, 88 students participated in the study, resulting in 213 work roles being indicated from the NICE Framework (Sands & Sande, 2019). The categories of the NICE Framework were then grouped by highest, middle, and lowest percentage of work roles tagged by participants. The industry certifications were ranked by the most frequently identified to least frequently identified by participants. Two-year colleges can use these higher percentage work role categories and certifications as a way to shape their programs to include education geared towards those most frequently identified by participants. The methods selected for this study were useful in obtaining results related to post-graduation employment outcomes for CAE two-year colleges.

Responses from the study indicated a high concentration of work roles in the Operate and Maintain category and the fewest responses in the Oversee and Governance category. This indicated a need for two-year college curriculum to prepare students for the Oversee and Governance, which includes work roles such as Information Systems Security Manager, Product Support Manager, and IT Program Auditor.

The majority of study respondents had completed the Associate of Applied Science at their college and 65% felt strongly that their programs prepared them for their current role in the cybersecurity workforce and 19% agreed that the programs well prepared them for these positions (Sands & Sande, 2019). Sands (2021) anticipated that the study results would be valuable to "change the perception of what community college students were capable of" to offset preconceived notions that community colleges only prepare students for two categories of the NICE Framework: *Protect and Defend* and *Operate and Maintain*. In the 2021 interview by Jim Rice, Sands also noted that most agencies and institutions are looking to hire Security Analysts that have already completed a bachelor's degree. The study by NCyTE and CSSIA provides strong evidence to indicate that CAE two-year colleges provide education that prepares students for a wider variety of cybersecurity work roles, including those that may typically require a bachelor's degree.

Due to delays caused by social distancing requirements of Covid-19, the Future Directions Summit initially scheduled for 2020 was held in 2022, featuring many cybersecurity research studies conducted in partnership with NSF, including the 2019 workforce study (Future Directions, 2022). In the open discussion session that followed the presentation by Dr. Sands, faculty from a variety of CAE institutions gather to share their thoughts on the study be conducted again with additional two-year college participants. The consensus of the dialogue was that another study would be useful to find out whether other CAE two-year colleges have prepared students for cybersecurity work roles aligned to the NICE Framework.

As seen with other workforce studies, there is a need to repeat the study with modifications to find current results based on new situations occurring with education and the workforce. The data collection instrument for Sand's and Sande's (2019) workforce study asked

alumni about any workforce training and mentorship that they may have participated in. The present study will frame the question slightly different to ask about participation in student clubs, competitions, and extracurricular activities. The CAE community and NICE affiliate program initiatives focus on building skills, interest, and awareness through extracurricular activities (Newhouse, 2018).

Ethnic and Gender Diversity in the Cybersecurity Workforce

In 2017, as more attention was paid to the shortfall of talent for the cybersecurity workforce, the lack of diversity and gender inequality was also broadly emphasized. From that perspective, it was noted that leveraging non-traditional students, veterans, and apprenticeships could be a way to increase the pool of talented individuals and offset these imbalances in ethnicity and gender (Gloster, 2022; IBM Institute for Business Value, 2017). There are perceived barriers, such as stereotypes and bias (Porter, 2020), that prevent women from choosing to work in cybersecurity roles (James, 2019; Peacock & Irons, 2017). A positive shift in the inequality could lead to improvements in the workforce and in business (Porter, 2020), as stated by Peacock and Irons (2017), a diverse workforce is known to be more productive.

Parker (2016) used a point-in-time comparison from 2006, to demonstrate that there has historically been fewer women in computer occupations such as information technology (IT) and cybersecurity, with women making up only 13% of the workforce at that time. Others have emphasized the salary disparity for women in STEM in their study finding that female faculty earned significantly less than their male counterparts in the Midwest (Liebl, et al., 2021). The two main barriers identified by women in one of the first known research studies of women in cybersecurity were lack of training opportunities and work environment (Bagchi-Sen, Rao, Upadhyaya, & Chai, 2010). The study referenced the male-dominated hacker culture of cybersecurity as playing a key factor in the lack of mentor-mentee opportunities for women and

"…concerns about safety and security for women working in computer laboratories alone at night and on weekends."

According to ISACA (2017), cybersecurity professionals have expressed concern about the gender imbalance in the workforce. Masters (2017) interviewed experts to share strategies to improve the issues with the lack of women in technology and cybersecurity roles. In October 2022, the Office of the National Cyber Director requested assistance from industry and government with the development of a diverse and inclusive cybersecurity workforce (Gloster, 2022). The shortage of cybersecurity professionals is viewed by the Deputy National Cyber Director, Technology and Ecosystem Security as an opportunity to close the gender gap and build ethnic diversity in the cybersecurity workforce (Gloster, 2022).

Modern cybersecurity workforce studies not only evaluate the ethnic and gender diversity of the workforce, these studies often include the demographic information of their study participants to consider whether the workforce diversity gaps are also reflected in the respondent pool. The workforce continues to face a lack of representation for women, with less than one-fourth of the workforce being female as compared to the overall workforce where women are more fairly represented at around 52% ((ISC)2, 2022; ISACA, 2022; Porter, 2020).

To better understand the lack of adequate representation of women and minorities in the field of cybersecurity, Shumba, et al. (2013), investigated the barriers, significant contributions by women in cybersecurity, participation level, cybersecurity initiatives, and best practices for broadening participation. The authors noted that working in cybersecurity is very different from working in the field of Computer Science, therefore research was needed to understand the lack of women and minority participation in cybersecurity. Some of the recommendations resulting from the informal survey by Shumba, et al. (2013) included, enhancing interest through inclusion

of women and minorities in public resource pages, inclusion of perspectives in online magazines, establishing a mentors' network, incentivizing conferences at the high school level, and encouraging terminology that is gender-neutral.

Drolet (2021) reported that Black and Hispanic people are underrepresented, and experience significant pay gaps as well, in computer occupations. These trends carry over into the cybersecurity workforce as noted in the previously mentioned global workforce studies. Adding to the challenges of developing a diverse cybersecurity workforce is the low volume of STEM degree graduates that are Black and Hispanic (Drolet, 2021). According to Nakama (2016), "the critical bridge" for women and minorities may be community college outreach because it reaches those that may not have otherwise had access to cybersecurity education (Dohm, 2015; Parker, 2016). Students state that the opportunity to explore community college courses in cybersecurity could play a key factor in choosing a career in cybersecurity (Nakama, 2016).

NICE Framework

The present section emphasizes the depth and breadth of the structure provided by the NICE Framework to improve stakeholder communications and define the careers in cybersecurity. For references in this section, multiple online searches were conducted for articles and materials related to cybersecurity workforce studies using the NICE Framework. Explanation of the use of the NICE Framework and studies using the NICE Framework work roles are discussed.

The NICE initiative spearheaded by NIST, has four complementary components: awareness, formal education, training and professional development, and workforce structure (Paulsen, McDuffie, Newhouse, & Toth, 2012). A major national level initiative, the NICE

Framework, first published in 2012, provides an authoritative perspective on the detailed aspects of the requirements for cybersecurity professionals after a three-year rigorous process (Shoemaker, Kohnke, & and Sigler, 2018). The functions of the profession are clearly defined in the NICE Framework, from tasks performed by individuals up through to initiatives for strategic planning at the organizational level (Shoemaker, Kohnke, & and Sigler, 2018). It also provides a clear taxonomy and lexicon for the field of cybersecurity that can be used by all stakeholders to define work roles and improve communications, including curriculum and training content (AlDaajeha, et al., 2022; McQuaid & Cervantes, 2019; Paulsen, McDuffie, Newhouse, & Toth, 2012).

Independent of the work roles, each of the categories of the NICE Framework are defined. Higher education institutions applying for the CAE-CD designation must select one or more these high-level grouping categories that their program curriculum is most closely aligned to. Table 5 below identifies the category definitions which indicate that most are specialized functions while some categories focus on technical support and others focus on leadership.

Table 5. Categories Defined within the NICE Framework.

CATEGORY	DEFINITION
OVERSIGHT and GOVERNANCE (OG)	Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.
DESIGN and DEVELOPMENT (DD)	Conducts research, conceptualizes, designs, and develops secure technology systems and networks.
IMPLEMENTATION and OPERATION (IO)	Provides the implementation, support, administration, and maintenance necessary to ensure effective and efficient technology system performance and security.
PROTECTION and DEFENSE (PD)	Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.
INTELLIGENCE (IN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for national intelligence.
CYBERSPACE EFFECTS (CE)	Plans, supports, and executes cybersecurity for cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

Note: Information in this table was adapted from the NICE Framework Resource Center on the NIST website, the Workforce Framework for Cybersecurity (NICE Framework) (NIST, 2021).

Each of the work roles is given context through its definition and categorization. Appendix A includes the title of each work role, the work role ID, and the statement that defines the work role. The work role IDs include abbreviations for the NICE Framework categories and specialty areas. The definitions help to clearly delineate the work performed under each work role.

CAE-CD institutions must develop programs with courses mapped to a minimum number of Knowledge Units (KU) as defined by the CAE Community and NSA Program Office (Dampier, 2015; Liu & Tu, 2020). The structure for a model KU includes mapping to at least one category of the NICE Framework (NCAE-C, 2020). Two-year colleges applying for the CAE-CD designation are required to map their program to at least 11 KUs; three foundational, five technical or non-technical core, and three optional KUs (Hudnall, 2019; Liu & Tu, 2020; Strickland, 2022). While there have been many changes to the CAE-CD application requirements over the years (Liu & Tu, 2020), the KU mapping requirement has remained.

In recent years more attempts have been made to develop standards for cybersecurity curriculum, including a joint task force on cybersecurity education made up of experts from Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers' IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The resulting model for cybersecurity curriculum guidelines is known as CSEC2017

(Burley, et al., 2017). The model provides knowledge units nested within a knowledge area. As an example of the coursework components within CSEC2017 guidance, the topics and learning outcomes associated with a given knowledge unit are mapped to the knowledge, skills, and tasks associated with a work role of the NICE Framework (Burley, et al., 2017).

A new course in *secure design* was introduced in 2018 based on the knowledge, skills, and tasks of the NICE Framework work roles (Sharevski, Trowbridge, & Westbrook, 2018). The authors noted that many cybersecurity issues arise from insecure use of technology and intentional misuse. Further, that an interdisciplinary approach which combines cybersecurity and user-centered design in the form of secure design could better prevent data breaches (Sharevski, Trowbridge, & Westbrook, 2018).

Ghosh and Francia (2021), have developed cybersecurity curriculum for the University of West Florida using scenario-based learning activities based on the knowledge, skills, and tasks outlined in the NICE Framework and the Office of Personnel Management Hiring Cybersecurity Workforce report. This innovative mapping also incorporated the authors' previous work with competency-based assessment development. Scenario-based learning provides an immersive context for the learner that would be like the real-world environment in which the skills would be applied (Ghosh & Francia, 2021). The authors focused on the development of learning objectives aligned to the work role tasks of the NICE Framework rather than the commonly used learning outcomes regularly associated with Bloom's taxonomy.

As previously indicated, the stakeholders of the NICE Framework are extensive, encompassing international communities that also have an interest in cybersecurity for their nation. University faculty from Finland's Jyväskylä University of Applied Sciences (JAMK) requested a research study be conducted on bachelor's degree alumni employment outcomes in

cybersecurity using the NICE Framework (Saharinen, Viinikanoja, & Huotari, 2022). The authors noted that the NICE Framework was intended to improve workforce development in education and training. Also developed in parallel by other countries were additional cybersecurity frameworks, curriculum guides, and workforce related publications, providing further evidence for the global need to establish cybersecurity focused education (Saharinen, Viinikanoja, & Huotari, 2022).

The 2022 JAMK study used social media to locate cybersecurity program alumni because most students had previously tagged their student profiles with the "do not contact" label (Viinikanoja, 2022). The Finnish study asked two questions of bachelor's degree alumni, the first was about place of employment and the second was the type of work performed based on the work roles of the NICE Framework. The intent of the study was to find out "Where are graduated students employed?" and "What kind of work responsibilities do the students have?" (Saharinen, Viinikanoja, & Huotari, 2022).

JAMK alumni responding to the survey were asked to rank the NICE work roles in first to fifth order, with the first being the work role that was most descriptive of the work they were currently performing (Viinikanoja, 2022). These 68 students were among the first in Finland to have 'cyber security' as the focus of their bachelor's degree. The JAMK researcher sought to determine where the 19 respondents were employed, including company size and industry sector (Saharinen, Viinikanoja, & Huotari, 2022; Viinikanoja, 2022). Referred to as the most important question of the study, the results showed that JAMK alumni indicated *Protect and Defend* and *Operate and Maintain* as the top two NICE categories most applicable to their work roles. *Cyber Defense Analyst* and *Network Operations Specialist* were the top two NICE work roles indicated by JAMK alumni as most closely related to their current work (Viinikanoja, 2022).

By providing information about employment outcomes and workforce needs, global and local workforce studies influence and impact the work being done to support workforce preparation. Elements of the NICE Framework have been used to develop and enhance curriculum as well as assess alumni employment outcomes. Leveraging the work roles defined within the NICE Framework, this study will examine how formal education, industry certification, and other professional development resources have shaped alumni employment outcomes.

Academic Programs and Career Preparation Resources

The CAE program initially began in 1999 with a small cadre of seven universities and, according to Carey (2004), grew to 55 within five years (CAE in Cybersecurity Community, 2021). By 2010, just a decade after its inception, there were 125 CAE designated institutions in 39 states, of which six were community colleges then labeled as CAE2Y (NSA, 2010). From 2016 to 2022, the number of designated institutions grew significantly from 196 to 350 (CAE in Cybersecurity Community, 2021; Eikenberry & Pfannenstein, 2016). The growth of the CAE community has been representative of the increased demand for career preparation as the cybersecurity workforce shortage continued to increase.

The cybersecurity workforce continues to evolve as new technologies and techniques emerge along with the growth in job demand, shifting some job roles to include additional specialized tasks (Moses, 2022). Cybersecurity education and training must also continually evolve to keep up with industry demand for employees with the knowledge and skills to perform specialized tasks (Knapp, Maurer, & Plachkinova, 2017; LeClair, Abraham, & Shih, 2013; Parrish, 2018). Employment outcome surveys provide educators with the information needed to make revisions that can prepare future students for current and emerging job roles.

The Special Interest Group on Computer Science Education (SIGCSE) of the Association for Computing Machinery (ACM) also placed an early investment in the security related context of computing. Shortly after the tragic events of September 11th, academia began to increase the awareness campaigns about integrating security content into computer classes in higher education (Boggs, 2002; Campbell, 2003; Mullins, et al., 2002). The Institute of Electrical and Electronics Engineers (IEEE) began working on cybersecurity education standards as well. The global cybersecurity workforce problem has been so prolific that a joint task force of ACM, IEEE, Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) have developed guidance for cybersecurity curriculum development, known as CSEC2017 to ensure that the fundamentals are consistently taught (Burley, et al., 2017).

The variety of curriculum development methods and interdisciplinary integration has led to the creation of both career preparatory and theory-based programs (Mouheb, Abbas, & Merabti, 2019). Higher education institutions can utilize industry advisory boards, local labor market information, and employer partnerships to further align their programs with industry needs (Knapp, Maurer, & Plachkinova, 2017). Due to this purposeful alignment with local job markets and funding for additional local initiatives, cybersecurity education programs can be distinctly different in their content and supporting resources for career preparation.

Undergraduate and postgraduate institutions have integrated cybersecurity into many technical and non-technical disciplines, as previously indicated (Alrabaee, Al-kfairy, & Barka, 2022). There is a recent emergence of cybersecurity as a stand-alone discipline as well (Burley, et al., 2017; Parrish, 2018). The complexity of the non-standardized curriculum development

over several decades, has led to the design of many frameworks and models to help institutions and practitioners learn to align content with the knowledge, skills, and tasks of cybersecurity work roles.

There is a recognized shortage of talent, commonly referred to by many organizations as the cybersecurity skills gap (Vogel, 2016). As Vogel (2016) indicates, increasing workforce capability requires many initiatives, both short-term and long-term. Short-term solutions include reskilling and upskilling to prepare IT professionals for cybersecurity roles through certificate and two-year degree programs. Long-term solutions include collaboration between academia, industry, and government on national initiatives, such as the endeavors of the CAE community and the NICE Framework.

As a mechanism to build early career interest before students leave high school, Career and Technical Education (CTE) programs develop pathways (Pelfrey & Peavy, 2019). The pathways movement has gained traction across the U.S. with emphasis on collaboration between secondary schools, colleges, and industry (Morrey, 2020). This includes dual enrollment programs at the secondary school level leading to completion of a college certificate at the same time as graduation from high school, known as stackable credentials (Morrey, 2020). Additional pathways projects include summer workshops for secondary school educators and students (e.g., GenCyber), industry certification, and professional experience (Morrey, 2020; Pelfrey & Peavy, 2019).

Additional education solutions include starting the cybersecurity education pathways at younger ages. To encourage young women and provide an anchor to cybersecurity, the CybHER initiative developed a program around the following themes: constant connection, knowledge and practice, inspiration, community, and supportive and engaged guardians (Rowland,

Podhradsky, & Plucker, 2018). Manson and Pike (2014) provide guidance on how students can achieve success in the cybersecurity workforce through time spent on curricular and extracurricular activities, similar to that of an athlete in training. This includes the integration of cybersecurity competitions into the education pathway as early as middle school to prepare for formal education beginning in college. The authors noted that some cybersecurity competitions were mapped to the knowledge, skills, and abilities of the NICE Framework (Manson & Pike, 2014).

With career preparation and employability in mind, some two-year colleges align their coursework with professional certification exams (Evans, Saflund, & Wijenaike, 2002; Knapp, Maurer, & Plachkinova, 2017; Ward, 2021). Amongst the qualifications, job postings include requirements for professional certification with some of the most favored being CompTIA Security+ and (ISC)2 CISSP (Marquardson & Elnoshokaty, 2020). Knapp, et al. (2017) noted that to remain competitive, governing organizations like CompTIA, EC-Council, (ISC)2, and Global Information Assurance Certification (GIAC) must keep their professional certification exams up to date with industry demand.

The Department of Defense provides lists of the approved baseline certifications for various government job codes (Department of Defense, 2020). A brief online search for the most popular cybersecurity professional certifications can produce over 30 lists with different sequences for the top five. Lists based on number of job postings can be helpful for learners looking to improve their resume with verification of knowledge and for higher education faculty seeking to update programs. Business News Daily offers such a list with corresponding number of job postings (Tittel, Lindros, & Kyle, 2023). According to Business News Daily (2023), the certifications ranked highest to lowest based on number of job board postings are Certified

Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Security+, Certified Ethical Hacker (CEH).

Curricular guidelines provide a good starting point to develop a formal education program that includes course content structured to help learners develop the knowledge, skills, and competencies for a given career path. From the CSEC2017 model, a newer model for two-year colleges has emerged, called Cyber2yr2020. This new model incorporates the knowledge units of the CAE and the NICE Framework (Tang, 2019). These guidelines and models are primarily focused on knowledge gained through classroom curriculum that prepares students for cybersecurity careers.

Alumni Employment Outcome Studies

According to authors of the *California Community Colleges Produce Positive Employment Outcomes* study, California has a unique economy and labor market and while most workforce studies rely on administrative data to determine degree impact on wage and career outcomes, there is value in local data collected through survey of two-year college graduates (Pham, Greaney, & Abel, 2020). The study by Pham, Greaney, & Abel emphasized completers of Career and Technical Education (CTE) programs which tend to focus on specific careers and work roles and the study excluded students that were still working on their two-year college education.

For the first round, an online survey form in Survey Monkey and email recruitment methods were used to reach participants. The second round of recruitment included a paper copy of the survey that was mailed to those that had not participated in the first round. And, finally, a telephone survey using Snap Surveys was used to reach potential participants in the third round

of the study. Wage outcomes from survey respondents was then compared to the administrative data collected annually for the California Community College Career Technical Education Employment Outcomes Survey (CTEOS) to determine that there are positive employment outcomes after the completion of CTE programs.

The alumni outcomes studies by Sands and Sande, and JAMK highlight the connection between formal education and career outcomes related to the NICE Framework. As indicated, administrative data is not enough due to its aggregated nature and lack of emphasis on specific career outcomes in the broad field of cybersecurity. This study will adopt many of the characteristics of these previous studies to gather alumni outcomes from CAE-CD colleges in the U.S.

Summary

The Department of Commerce (2018) declared cybercrime to be our nation's greatest threat in 2018. Risks of large-scale data breaches due to consumer preferences for online shopping and social media usage have spurred the cybersecurity workforce talent shortage. A call to action and increased awareness about cybersecurity careers referred to apprenticeships and the characteristics of individuals that may be well-suited to work in the profession. Despite the efforts set forth, the cybersecurity talent shortage persists, and many workforce studies have been conducted to better understand the challenges faced from year to year.

As found in this review of the literature, some researchers set out to validate administrative data, while many others have focused on the current skills, security concerns, threat landscape, and training needs to reduce skill gaps. The global and federal workforce studies included herein used online survey methods to reach thousands of cybersecurity professionals. The studies using the NICE Framework have helped to identify current workforce

coverage and skill gaps. Still, a deep understanding of the current and future needs of the cybersecurity workforce continues to be challenging to ascertain as technology rapidly evolves and threat actors continually become more sophisticated and organized in their efforts to conduct large scale attacks.

Although there are ongoing annual studies of the cybersecurity workforce, many focus on security trends and future workforce needs. This leaves at least two significant gaps in the literature available about 1) two-year college alumni from cybersecurity programs, and 2) two-year college career outcomes related to the NICE Framework work roles. Further study is necessary to evaluate the employment outcomes from higher education cybersecurity programs using the work roles of the NICE Framework.

Chapter 3. Research Methodology

The present chapter covers the research methodology, the research design, and the analysis methods used after data collection. The research onion model can be used as a way of defining research methodologies and their data collection and analysis techniques (Saunders, Lewis, & Thornhill, 2007). Saunders, et al. (2007) identify the research onion model, from outer layers to the center core, to include philosophies, approaches to theory development, strategies, choices of methodology, time horizons, and data collection techniques and procedures. Each of these research onion model layers will be discussed in this chapter.

In general, a research methodology defines a framework for the collection of data and how it will be analyzed and interpreted (Creswell J. W., 2013). Further, Creswell (2009) describes the plan for research design as "the intersection of philosophy, strategies of inquiry, and specific methods," which provides the framework for research studies. As compared to the research onion model which provides depth to research design, Creswell's definition generalizes the inclusion of approaches to theory development, strategies, time horizons, and data collection techniques and procedures. Saunders and Tosey (2013) suggest that using the outer layers of the research onion model helps researchers provide context and boundaries to designing research.

This national study focused on the collection and examination of data from CAE-CD two-year college faculty and alumni related to the NICE Framework work roles and other pertinent information, such as employment outcomes, industry certifications, and co/extra-curricular resources. The primary research question and sub-questions for this study were:
RQ1: Which cybersecurity work roles of the National Initiative for Cybersecurity Education (NICE) Framework are alumni of Centers of Academic Excellence in Cyber Defense (CAE-CD) two-year colleges employed in as compared to the work roles identified by their college?

RQ1.1: What proportion of the cybersecurity program alumni are not employed in any cybersecurity work roles?

RQ1.2: What proportion of the alumni pursued another degree within three years of graduation from a CAE-CD two-year college?

RQ1.3: How do the alumni gender and ethnicity demographics align with the gender and ethnicity demographics of the cybersecurity workforce of the United States?

This study was problem-oriented, taking the philosophic position of the pragmatic worldview to research design, focusing on the evaluation of work role clusters and gaps to evaluate a treatment implemented in response to a real-world problem, the cybersecurity workforce talent shortage. The pragmatic worldview allows for the use of survey methodology with mixed methods drawing on both quantitative and qualitative data (Creswell J. W., 2013; Rossman & Wilson, 1984) to elicit the information from alumni about their employment outcomes and from POCs about their academic programs. Focusing on solutions to problems, using approaches that work best to answer the research questions is the pragmatic philosophy to research design (Creswell J. W., 1994).

The purpose of this cross-sectional, mixed methods study was to examine cybersecurity program alumni employment outcomes to provide the CAE community with career outcome data, identify work roles and gaps based on the NICE Framework, and understand the value of co/extra-curricular activities. This information can be used to equip CAE-CD institutions with the information needed to validate the past and current institutional efforts and make determinations about program updates. The study used the survey methodology with purposive sampling to gather information relevant to the CAE community. The explanatory sequential

mixed methods approach was used to gather quantitative data from the POC participants, followed by gathering qualitative data from alumni participants, then to integrate the quantitative and qualitative data from the two participant groups (Ivankova, Creswell, & Stick, 2006). Although the CAE program is one among many solutions to aid in reducing the cybersecurity workforce shortage, the program has intended outcomes that can be evaluated using the taxonomies of the NICE Framework for comparison to the intended employment outcomes of alumni from these programs (Sands, 2021).

The following sections further describe the research methodology to be used; the design of the study, including the methods of data collection, analysis, interpretation, storage, and destruction; limitations; and a chapter summary. It also covers the anticipated types of infographic artifacts to be created resulting from the interpretation of the themes and patterns of the data (Creswell J. W., 2013). The data and infographics resulting from this research study can be used to further understand the phenomenological social context of the CAE program in relation to the alumni employment outcomes and their further pursuits in higher education and industry certification after program completion (Sands, 2021).

Research Methods

The survey research methodology was selected for this study as a guiding framework on assumptions and premises related to quality data collection via survey (Fowler, 2013). Three primary characteristics of surveys referenced by Fowler (2013) are the statistics resulting from the data contributed by the study population, analysis of collected data from the questions asked, and data from the sample population is considered representative of the larger target population. Developing a survey with unbiased, clearly written questions and reduced data collection errors will help to provide the best results to the research community (Fowler, 2013).

Systematic techniques of a research methodology provide the researcher with the tools to conduct the study, among other advantages (Igwenagu, 2016). According to Fowler (2013), in addition to a purposeful collection of statistical estimates, survey methodology has two goals: 1) reduction of error in the data collected via survey, and 2) measurement of the error. The explanatory sequential mixed methods approach was used in this study to allow for the collection of both quantitative and qualitative data; nominal, closed-ended questions with pre-populated answers, and open-ended questions to collect participant perceptions for later comparison. The advantages of the explanatory sequential mixed methods approach in two distinct phases, is to gather nominal data from the first group of participants to better understand the data gathered from the second group of participants (Creswell J. W., 2003).

The nested sampling approach used in this study was selected to ensure that only CAE-CD two-year alumni responded to the second phase survey. This also served to preserve the anonymity of alumni respondents allowing for privacy regarding disclosure of work task related information and academic experiences. Only the POC and their college maintained the alumni contact information. Other approaches, such as focus study groups or personal interviews were considered but would not have provided the level of privacy and multivariate individual response data that the online survey approach provided.

As mentioned in the literature review, the dynamics of the cybersecurity workforce are changing and the curriculum of higher education is evolving, therefore another workforce study was due for CAE-CD two-year college alumni employment outcomes. Building on the information gathered in the 2019 workforce study by Whatcom College (NCyTE) and Moraine Valley Community College (CSSIA) (Sands & Sande, 2019) that surveyed two-year college alumni about their work roles using the NICE Framework, the current study compared the POC's

perception of curriculum to the alumni work roles using the NICE Framework in the survey of students that graduated from CAE-CD two-year colleges. Data about work experience based on the cybersecurity work roles of the NICE Framework was collected via online survey from CAE two-year college alumni (NICE, 2022). Questions for the CAE-CD two-year college alumni included title of the program completed, post-graduation work experience, further academic studies, and how well the CAE-CD program prepared the alumni for their current work role.

Although intended to be similar, this study diverged from the 2019 by comparing POC and alumni work role responses rather than collecting only alumni work roles. The 2019 study collected data about alumni all work roles that they had experienced yet did not ask POCs which work roles they intended to prepare students for. This study also diverged from the 2019 study by using an online survey rather than conducting personal interviews. This study included additional questions about the co/extra-curricular activities that alumni had experienced while in the program. The current study used the latest version of the NICE Framework with six categories and 50 work roles made available in April 2023, while the 2019 study used a prior version with seven categories and 52 work roles.

Study Population

This study included two primary sources for data collection, 1) the CAE-CD POCs as representatives of the college programs and, 2) the alumni as individuals that are now graduated from the CAE-CD two-year colleges. This included POCs from two-year colleges designated as CAE-CD only, excluding CAE-R and CAE-CO because those designations have a different type of academic and career outcome focus. Acting as organizational representatives for the colleges, the CAE-CD POCs are commonly in faculty roles but may be employed in various roles, as faculty, academic deans, or other administrator roles.

There were 350 higher education institutions designated as CAE-CD, of which 145 had the word college in the name, as of July 22, 2022, (CAE in Cybersecurity Community, 2021). This study intended to collect contact information and reach out to all CAE-CD two-year colleges by email to collectively recruit approximately 200 total cybersecurity alumni to be surveyed. As points of reference, the previous study by Sands and Sande (2019) included 88 alumni participants from 12 CAE-CD two-year colleges while the previous study by JAMK included 19 alumni respondents. Considering the limited number of CAE-CD two-year colleges and program graduates, this nested purposive sampling strategy will be used as a technique for the selection of those that would provide the best information in qualitative research (Patton, 2014).

Institutions applying for the designation of CAE-CD must have at least three graduates from the Program of Study prior to application submission. Additionally, a program must be in existence for at least three years in its current form to be validated for designation as a CAE-CD. Using the minimum possible CAE-CD program graduates, multiplying three alumni by the 145 CAE-CD two-year institutions with a confidence level of 95% and a five percent margin of error, the sample size of approximately 200 alumni was derived. The sample size recommended by Creswell (2018) for qualitative phenomenological studies is three to ten and the sample size for this study was well above that recommendation.

Baroudi and Orlikowski (1989), define three determinants of statistical power: significance criterion, precision of sample estimates, and effect size. A sample size of significance was defined by the minimum number of graduates that a CAE-CD institution must have to qualify for the designation. It is not feasible to establish a precise alumni sample size for this study due to the lack of public data on CAE-CD program graduates for each of the two-year

colleges. Additionally with the nested sampling approach there may be some two-year college POCs that participate in the first phase, yet they do not contact their alumni, or their alumni do not opt in to participate in the second phase. This can lead to a reduced effect size and reduced relationship between the phase one and phase two results for work roles and co/extra-curricular activities.

Although this sampling strategy could be likened to snowball sampling, it is different in that the nested samples are a sample (alumni) within a sample (POCs) (Patton, 2014). Differing from the snowball sampling method which continues to grow as more and more participants are accumulated from prior participants (Patton, 2014). In multi-phase sampling, the subset participant group is identified from the participants in the first phase, also known as a nested sampling process (Onwuegbuzie & Collins, 2007). According to Onwuegbuzie and Collins (2007), a nested sampling design is recommended to include a sample size of greater than or equal to three participants per subgroup. There is an established relationship between the nested sample groups, the alumni as a subset of the first phase of participants, which is the CAE-CD two-year colleges.

The participating POCs were asked to contact all students that have graduated within the last three years from their CAE-CD Program of Study to the exclusion of other degree and certificate programs that may be similar or closely related. This helped to ensure that only the alumni from the CAE-CD designated Programs of Study were contacted to be part of this study. It was anticipated that not all students that have graduated from the program would be interested in participating or that contact information may be outdated and not all former students would receive the request to participate in the study. This could lead to a small sample size thereby reducing the value of the study results. For these reasons, the contact list used by the POCs to

assist with recruitment could have included more than the CAE-CD application minimum of three.

From these recruitment efforts, survey responses were requested to be anonymously collected from one or more alumni at each of the participating CAE-CD two-year colleges. The goal was to include approximately 200 alumni that have previously completed a CAE-CD designated Program of Study. Therefore, the geographical distribution of the colleges and survey participants will depend on those that opt-in to respond to the survey.

Alumni of the two-year CAE-CD programs may be traditional students or non-traditional students, those that attend college immediately after graduating high school and those that may return to college after a gap, respectively. Non-traditional students are defined by a variety of factors, such as age range outside of the traditional 18-22, gender as compared to the majority in a career-based program, minority ethnicity as compared to the career-based program, and family responsibility status (NC Perkins Team, 2019-2020). This may include underrepresented groups, including women in technical programs, adult learners over age 22, some ethnic populations, and students caring for their children (Towson University, 2022).

Study Setting

The study took place at a distance with survey respondents participating from the location of their choice using an online survey form. Fowler (2013) notes that there are advantages to computer-based surveys over previously used methods of paper or telephone, including lower cost. The CAE community spans a large geographical region of higher education institutions in the 50 states of the U.S. and in Puerto Rico as a territory of the U.S. Most of the communications were electronic, including email and online survey forms, to allow for asynchronous responses without travel, thereby reducing costs.

Instrumentation and Procedures

The survey questions for this study were developed by adapting the questions from the instrument created for the 2019 study by Sands and Sande. The survey questions for the present study were grouped by type of questions and then the groups were sequenced by research question and sub-question. Optional questions about demographics were placed at the end of the survey.

A voluntary consent letter that outlined the purpose of the study was provided at the beginning of both the POC and alumni surveys. POCs were asked to provide personal information such as name and contact information because this would be needed to proceed to the second phase, the alumni survey. Questions about the POCs CAE-CD program and the work roles that they intend to prepare students were developed using the language of the CAE community and the NICE Framework categories and work roles last revised in April 2023. The work role options, and the program resource options were identical for the POC and alumni surveys.

Personal information such as name and location were excluded from the alumni survey to protect respondent anonymity. Questions about program completion and employment were frontloaded on the alumni survey to ensure that the respondent met the criteria to complete the remaining questions, thereby avoiding a sense of wasted time if they did not meet the criteria. Aligned with the primary research question and following the approach recommended by Fowler (2013) to begin with the most complex questions, the next segment included the most in-depth reading, asking alumni to identify five work roles from 50 options.

Following the work roles, alumni were asked to identify career preparation resources experienced in their academic programs. Alumni were then asked about industry certification, the importance of the program to their preparation, and how the program and resources helped

them to prepare for their current job. Finally, the alumni survey concluded with the optional questions related to demographics that used the choices for gender and ethnicity used in the Integrated Postsecondary Education Data System (IPEDS) of the National Center for Education Statistics.

Prior to sending out the survey to the intended respondents, a questionnaire should be validated by establishing face validity through expert review and making any necessary revisions (Creswell J. W., 2009; Elangovan & Sundaravel, 2021). The face validity of the survey instruments was established through review with three topic experts. A draft of the survey instruments was shared electronically with a POC from a CAE-CD two-year college, a Dean of Research and Institutional Effectiveness, and a Dean of Career Education from a CAE-CD. Minor revisions were then made to improve question clarity in the survey instrument. The results of the expert review determined the questions in each of the survey instruments were clear and aligned with the research questions of this study.

This study used a sequential two-phased survey method to first collect quantitative data about the work roles and program activities offered and qualitative for descriptive information about the college programs from POCs. The second phase was used to collect both quantitative and qualitative data from students about individual demographics, the program completed, and employment related details.

Information was collected in a sequential two-phased approach from CAE-CD POCs and CAE-CD program alumni using online surveys. In the first phase, the POCs were recruited to participate in the study and to contact alumni to participate in the second survey. Following is an explanation of the strategy used for gaining POC participation in the first phase.

Using the CAE list, the initial recruitment email to POCs was sent out by the researcher. Followed by email messages from the NSA Program Management Office (PMO) and the Chair of the CAE-CD Steering Committee to reach as many CAE POCs across the U.S. as possible, ensuring that the message was received from a known and trusted sender. The leads of the CAE regional hubs also sent out email to contact the CAE POCs by region. The CAE in Cybersecurity Community also added the call for participation to the weekly newsletter which reaches all POCs.

The call for participation email included a message requesting that interested POCs complete an online survey with programmatic information about their CAE Program of Study. Interested POCs were then provided with an email template to send to alumni which included a link to an online survey allowing interested alumni to provide responses electronically. As needed, follow up responses were made to POCs to confirm that alumni had been contacted. A second call for participation reminder was sent by the researcher after two weeks.

Phase two began with the participating CAE POCs sending an email to each of their CAE-CD program alumni which included a link to the online survey for alumni. Interested alumni were able to respond at any time of day as the survey was available online 24 hours a day, seven days a week. The survey remained open until there was an obvious drop in the response rate for both alumni and POC. The response rate was zero for three consecutive weeks and reminders to POCs resulted in no further interest.

At the end of the survey alumni were presented with the opportunity to submit their email address for a gift card drawing. There were five (5) $100 gift cards delivered electronically to the first five (5) names drawn at random after the first 100 alumni surveys were completed. This provided a possible reward for thoroughly completing the survey in a timely manner.

Independent of the survey form, alumni were asked to send an email if they were interested in being part of the gift card drawing to ensure that responses remained anonymous. From the list of those interested in the gift card drawing, names were collated by date and time of completion from oldest to newest, then each was assigned a numeric value, allowing for the selection of five random numbers for the drawing. Once the gift card winners were identified from the drawing, they were notified by email to redeem the electronic gift card valued at $100.

Data Analysis

The quantitative data collected in this study was analyzed using a deductive strategy, searching for themes and patterns to interpret social phenomena (Creswell J. W., 1994). The data was aggregated in multiple ways to be examined for themes and patterns. Statistical analysis techniques were applied to examine and correlate the quantitative and qualitative data collected in both phases one and two from the POCs and the alumni. Exploratory data analysis techniques were applied to find themes and patterns that provide key insights which may be useful to the CAE two-year college participants and to the CAE Community in general (Tyagi, 2021). Results have been reported using data visualization techniques and in basic tabular format (Miller, 2019).

Data analysis techniques included obtaining data, reviewing and verifying accuracy of the data, then coding, categorizing, and interpreting meanings (Creswell & Creswell, 2018). The qualitative data, or nonmetric data, was used to interpret and better understand the responses to the question of program preparation. As recommended by Hair, et al. (2019), the nonmetric data first underwent a data quality check, by reviewing for missing or inaccurate data in the free response fields and then checking for outliers. This included a first pass reading to understand the content, followed by a deeper analysis to find commonalities, and additional readings to generate specific findings (Creswell & Creswell, 2018; Vagle, 2018).

The nonmetric data for the alumni survey question about how the college's program and resources helped in preparation for the alumni's current employment position was analyzed following the emergent coding scheme in which it was first coded by connotation, then by topic, and categorized to find patterns in the open-ended content (Blair, 2015). Each short answer statement was coded by connotation which included identification of either a positive, negative, or neutral sentiment in the overall statement. Then the statements were coded by topic which included a review to determine topics as they emerged, then a return to the beginning to review again for any additional topics. The list of topics was then distributed into categories using the axial coding approach. The other open-ended short answer questions were also reviewed to separate the content for post-program continued education, professional credentials, and other preparatory resources that impacted employment outcomes.

Data Storage and Destruction

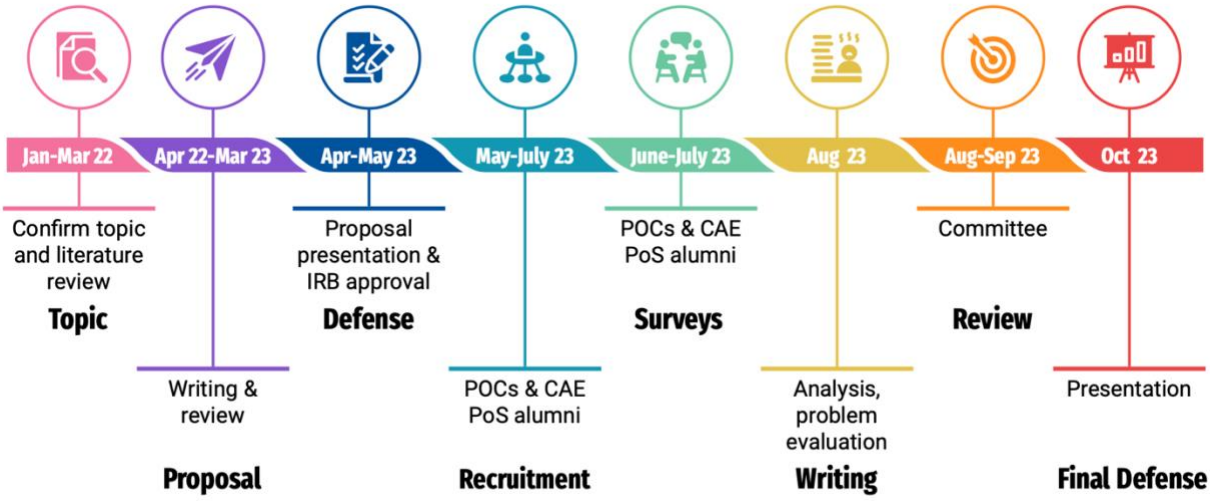
Data were collected in an online survey form and stored on the secure server hosted by Survey Monkey. Only the researcher had access to the data using Survey Monkey's secure authentication process (username and password login). Following guidelines in Code of Federal Regulations for 45 CFR 46, absent any other requirements, the raw data will be permanently deleted from the Survey Monkey account three years after the completion of the research (Department of Health and Human Services, 2022). Aggregated data has been securely stored on the researcher's password-protected and encrypted cloud-based drive and will be deleted three years after the completion of the research.

Timeline

The timeline shown in Figure 3 below is based on the projections of time periods needed to complete tasks towards the finalization of this study. It was anticipated that POCs will be

interested in participating and able to contact their program alumni soon after confirming participation. Additionally, many of the project milestones are dependent on the availability of others.

Figure 3. Research Study Timeline



Limitations

The primary limitations of the sequential multi-phased survey method selected for this study may have included selection bias and social-desirability bias or human error in the self-reported data. Due to the research design, there are two possibilities for selection bias 1) an individual recruiting specific CAE-CD institutions to participate, and 2) the first phase participants can be selective about the alumni contacted to participate in the second phase. Although these possibilities could have existed, should either of these situations have occurred, it would likely remain unknown.

Social-desirability bias can occur when a survey respondent "wants to 'look good' in the survey" (Rosenman, Tennekoon, & Hill, 2011). This can impact the way participants choose to answer survey questions, even if the survey data is collected anonymously online. The other possibilities of error can occur if survey questions are misinterpreted, questions are unclear, or

response options are vague (Dillman, Smyth, & Christian, 2014). To reduce these possibilities, the questions were developed to be concise and response options were appropriately worded.

Cross-sectional studies such as this are limited by the point-in-time in which the study is conducted, especially in relation to the phenomena being studied. Additional limitations may have included non-response issues related to outdated contact information, lack of interest in participating in an online survey, the timing of the recruitment message, and possible blocked email due to spam filters.

The nested sample approach also introduced potential limitations due to lack of time and relationships between POCs and their alumni. The only way to reach the alumni was through the POCs which relied on their time and relationship with the alumni. Additionally, some POCs expressed the lack of contact information to reach alumni and described that due to privacy concerns they were not allowed to have alumni contact information. In some cases, the email was sent by the college's institutional research team which may not be a well-known or trusted contact that alumni would respond to a survey from. A smaller than expected sample size could result from these limitations.

Summary

The survey research method and explanatory sequential mixed methods research approach were used for this study to collect data related to alumni employment outcomes from students that have completed CAE-CD programs using the NICE Framework as a tool for correlation. Survey research methods helped to reduce bias and provide objectivity in the design of the questions that were asked. Study participants in the sequential two-phased sampling design include CAE-CD Points of Contact and alumni that have graduated from CAE community colleges. The format of the study setting being primarily electronic communications allowed for

broad distribution across a nationwide geographic area and increased opportunity for participation based on the participant's available time to respond.

The research questions emphasized issues in the current cybersecurity workforce and the two surveys were designed to provide answers to the research questions. Correlation research and statistical analysis techniques were used to analyze the data collected. As study data has been collected and stored in an electronic format, a secure storage platform was used, and timely destruction has been established. This research project started in March of 2022 with topic approval and data collection was conducted May 2023 through July 2023. The scope and target participant availability may be limitations of the study, in addition to the time frame in which it was conducted.

Chapter 4. Results

The purpose of this cross-sectional, mixed methods study was to examine cybersecurity program alumni employment outcomes to provide the CAE community with career outcome data, identify work roles and gaps based on the NICE Framework, and understand the value of co/extra-curricular activities. A multi-phased approach was used to collect data from POCs and their alumni via online survey from May 2023 to July 2023. Of the 145 two-year college CAE-CD institutions, 39 self-selected to participate by completing the online survey. From the participating two-year colleges, 90 alumni survey responses were received from 17 colleges.

The initial data analysis included refinement of the data to exclude POC and alumni responses that did not meet the predefined criteria of the study. Responses that were incomplete or duplicate and those from four-year institutions were removed from the POC dataset because they did not meet the established study criteria. Responses from alumni that were incomplete or those that reported that they had not yet graduated were also removed from the alumni dataset.

Responses collected from the POCs included quantitative and qualitative data regarding their institution name, location, CAE program information, the NICE Framework categories and work roles that their curriculum intends to prepare students for, and the types of co/extra-curricular opportunities that their program provides for students. The POCs were also asked if any significant changes to the program had occurred within the last three years and were given the option to provide free-form comments.

Responses collected from the alumni included quantitative and qualitative data regarding their college's name, program name, prior academic achievements, employment information, the NICE Framework work roles they were tasked with at work, industry certifications achieved, and the types of co/extra-curricular opportunities that they participated in. The alumni were also

given the option to provide free-form comments in short answer form and demographic details in multiple choice form.

Based on the information collected from POCs and alumni, this research study intended to answer the following research questions:

RQ1: Which cybersecurity work roles of the National Initiative for Cybersecurity Education (NICE) Framework are alumni of Centers of Academic Excellence in Cyber Defense (CAE-CD) two-year colleges employed in as compared to the work roles identified by their college?

RQ1.1: What proportion of the cybersecurity program alumni are not employed in any cybersecurity work roles?

RQ1.2: What proportion of the alumni pursued another degree within three years of graduation from a CAE-CD two-year college?

RQ1.3: How do the alumni gender and ethnicity demographics align with the gender and ethnicity demographics of the cybersecurity workforce of the United States?

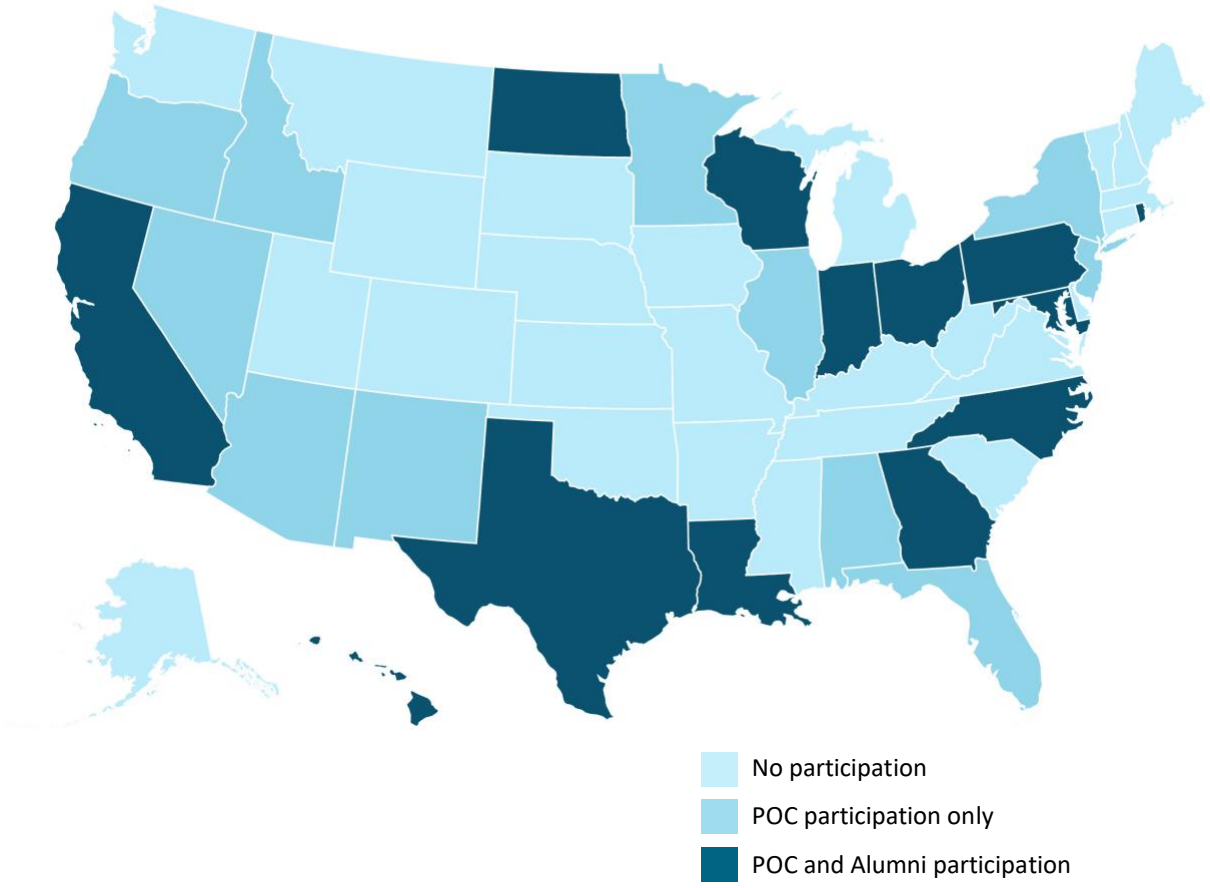
Findings

In this section, descriptive statistics serve to provide insights from the survey responses and answers to the research questions. The qualitative data were analyzed to identify recurring themes and patterns. Much of the data is grouped by state because the CAE in Cybersecurity Community commonly presents information this way to show representation for each state. The response rates by institution were too low to report individually while protecting the anonymity of the alumni participants.

Recruitment of the CAE-CD two-year colleges yielded approximately 27% (n_{1A}=39) from 24 states that completed the POC survey. The POCs did not share the number of alumni that were recruited from their college to complete the phase two (2) alumni survey. By design,

the alumni contact information was only known to the POC and/or their institutional research department. Alumni (n_2=90) responded from 13 different states. Below in Figure 4, participation by state is displayed in the heat map.

Figure 4. U.S. Map Indicating Point of Contact (POC) and Alumni Participation by State



Some states had zero participation for both the POC and alumni surveys. Some of the POCs indicated that although they completed the survey in the first phase, they were unable to send the second phase survey to their alumni, noting lack of alumni contact information and privacy policies as the primary reasons. The count of POC and alumni participants are listed by state in Table 6 below.

Table 6. Participant Count by State

STATE	POC COUNT (n_{1A}=39)	ALUMNI COUNT (n_2=90)
Alabama	1	0
Arizona	1	0
California	7	24
Florida	1	0
Georgia	2	6
Hawaii	2	19
Idaho	1	0
Illinois	2	0
Indiana	1	2
Louisiana	1	7
Maryland	2	1
Minnesota	1	0
North Carolina	3	4
North Dakota	1	11
Nevada	1	0
New Jersey	1	0
New Mexico	1	0
New York	1	0
Ohio	1	1
Oregon	1	0
Pennsylvania	1	9
Rhode Island	1	2
Texas	4	1
Wisconsin	1	3

Two-year colleges may offer degrees and/or certificates. Generally, a higher education institution can receive designation as a CAE-CD for one academic program, which can be either a degree or certificate. Of the alumni responses, 40 reported having received an Associate of Applied Science (AAS) degree, 28 reported having received an Associate of Science (AS) degree, and 22 were reportedly awarded a certificate. The AAS and AS degrees are typically 60 units, including general education coursework, while a certificate can have a broad range of nine units and higher. Completion of an AAS or AS degree can take two or more years depending on the number of units a student takes during each term. A certificate may be completed in one semester or take longer depending on the number of units required and the number of units a student takes during each semester.

Alumni reported an 88% employment rate in various careers with 70% overall reporting they were currently employed in a technology-related role. For 56% of the alumni, it had been two or more years since graduation and for 33% it had been only one year since graduation. Ten of the alumni had recently graduated within the prior two semesters. Grouped by award type, the figures for those employed in technology-related roles were 70% for the AAS alumni, 82% for the AS alumni, and 55% for the certificate completers. Table 7 below shows the percentages of alumni by state that were employed and in technology-related roles.

Table 7. Alumni Employment Figures by State

STATE	ALUMNI COUNT (n_2=90)	EMPLOYED PERCENTAGE	TECHNOLOGY-RELATED ROLE PERCENTAGE
California	24	83%	54%
Georgia	6	83%	67%
Hawaii	19	84%	84%
Indiana	2	100%	100%
Louisiana	7	71%	71%
Maryland	1	100%	0%
North Carolina	4	100%	50%
North Dakota	11	100%	82%
Ohio	1	100%	0%
Pennsylvania	9	89%	82%
Rhode Island	2	100%	50%
Texas	1	100%	0%
Wisconsin	3	100%	100%

The NICE Framework categories PROTECTION and DEFENSE (PD) and IMPLEMENTATION and OPERATION (IO) were highly ranked by POCs with each identified 15 and 14 times, respectively. OVERSIGHT and GOVERNANCE (OG) was identified one time and the remaining categories were identified zero times. This was well-aligned with the work roles selected by both populations.

Collectively, POCs tagged a total of 80 work roles while alumni tagged a total of 214 work roles. Within the top five work roles selected by both populations, the primary mismatch was that POCs indicated that their program content intended to prepare students for the

Vulnerability Analysis work role which is found within three of the four entry-level jobs for Cybersecurity Specialist, Incident and Intrusion Analyst, and IT Auditor, according to CyberSeek (2023). Alumni selected the Systems Management work role which does not appear in the entry-level jobs on CyberSeek as of 2023. This may be due to the level of experience required and some of the alumni had previously earned bachelor's degrees with possible prior work experience that helped to prepare for the Systems Management role. Additionally, it had been up to five years since graduation for some of the alumni, increasing their potential work experience as well. Table 8 below lists the top 5 work roles identified by the POCs and the alumni.

Table 8. Top 5 NICE Framework Work Roles Identified by POCs and Alumni

NICE FRAMEWORK WORK ROLE	POC RESPONSES (n_{1B}=17)	NICE FRAMEWORK WORK ROLE	ALUMNI RESPONSES (n_2=90)
System Administration IO-WRL-005	15	Technical Support IO-WRL-007	30
Network Management IO-WRL-004	10	System Administration IO-WRL-005	22
Technical Support IO-WRL-007	9	Network Management IO-WRL-004	11
Vulnerability Analysis PD-WRL-007	9	Systems Management OG-WRL-013	10
Incident Response PD-WRL-004	5	Incident Response PD-WRL-004	10

As required for the CAE designation, all POCs reported offering at least one co/extra-curricular activity to students in their programs. Most of the alumni, specifically 51, reported having taken part in at least one (1) or more co/extra-curricular activity while in their cybersecurity program. 39 alumni indicated that they did not participate in any co/extra-curricular activities while completing their cybersecurity programs. POCs reported offering other activities not listed on the survey instrument, including technical workshops, ePortfolio system, resume/interview workshops, cybersecurity awareness fair, virtual career fair, discounted exam

vouchers for industry certification, and job shadowing. Alumni reported participating in other activities not listed on the survey instrument, such as conference attendance and job shadowing. Table 9 below shows the co/extra-curricular opportunities available to students as indicated by POCs and utilized by alumni while they were students in their programs.

Table 9. Co/Extra-Curricular Activities Available and Utilized

ACTIVITY	POC RESPONSES (n_{1B}=17)	ALUMNI RESPONSES (n_2=90)
Apprenticeship	4 (24%)	5 (6%)
Capture-the-flag (CTF) competition	9 (53%)	23 (26%)
Cybersecurity competition(s)	14 (82%)	18 (20%)
Hands-on labs	16 (94%)	36 (40%)
Industry certification exam voucher	8 (47%)	19 (21%)
Industry speakers	17 (100%)	10 (11%)
Internship	4 (24%)	24 (27%)
Student club	14 (82%)	11 (12%)
Summer camp	4 (24%)	1 (1%)
Other (please specify)	5 (29%)	3 (3%)
No activities	0 (0%)	39 (43%)

Alumni survey responses indicated that 30 individuals held some form of industry-recognized certification. The range of certifications held by individuals was between 0 and 18. Ten (10) respondents held at least one certification. The other certifications included additional certifications from (ISC)2, AccessData, Check Point, Cisco, CompTIA, GIAC, ISACA, Microsoft, Palo Alto, and Saylor Academy. Table 10 below provides the count of certifications indicated by alumni.

Table 10. Industry-Recognized Certification Held by Two-Year College Alumni

CERTIFICATION	ALUMNI RESPONSES (n_2=90)
CompTIA Security+	18 (20%)
CompTIA A+	10 (11%)
CompTIA Network+	8 (9%)
CompTIA CySA+	6 (7%)
CompTIA PenTest+	5 (6%)
CompTIA Server+	4 (4%)
IT Infrastructure Library (ITIL)	4 (4%)
Cisco Certified Network Associate (CCNA)	4 (4%)
CompTIA CASP+	3 (3%)
Palo Alto Networks Certified Network Security Administrator (PCNSA)	3 (3%)
CompTIA Linux+	2 (2%)
(ISC)2 Certified Information Systems Security Professional (CISSP)	2 (2%)
(ISC)2 CISSP Information Systems Security Architecture Professional (ISSAP)	2 (2%)
(ISC)2 Systems Security Certified Practitioner (SSCP)	2 (2%)
(ISC)2 Certified in Cybersecurity Certification (CC)	2 (2%)
GIAC Certified Forensic Examiner (GCFE)	2 (2%)
GIAC Certified Incident Handler (GCIH)	2 (2%)
Other certifications	29 (32%)

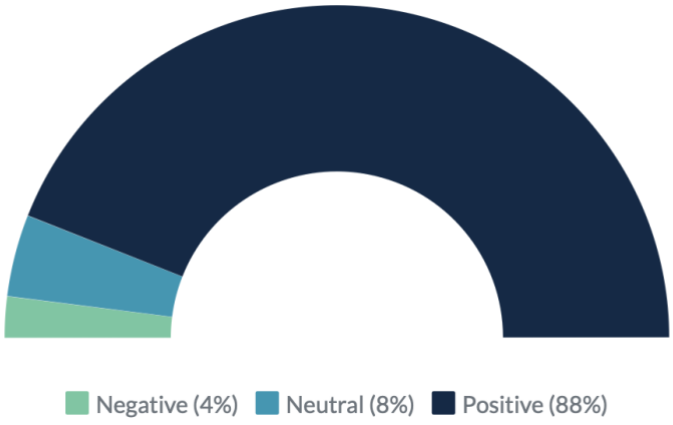
A Likert scale was used in the alumni survey to solicit opinions regarding the importance of their academic program in relation to their current job. To quantify the subjective opinions, the scale included choices of very important, important, neutral, unimportant, and very important. 54% rated the program as very important or important to their job, 38% indicated a neutral rating or did not respond to the question, and 9% rated their program as unimportant or very unimportant to their current work. The alumni survey included an open-ended comment section for respondents to share their thoughts on how the program prepared them for their current work role. 51 alumni (57%) included a comment with 45 providing positive feedback about the program, 4 neutral responses, and 2 responses with a negative tone.

An emergent coding scheme, or open coding, was used to develop the sentiment analysis from the qualitative open-ended comments. Blair (2015) explains that the codes are derived from the text without any preconceptions, or predefined labels, when the open coding approach is used. For this optional, open-ended alumni survey question, each of the 51 responses were

analyzed to determine themes and patterns. First, the comments were reviewed, and positive, neutral, and negative categories were applied, then on another review through the comments, the topics were assigned to each.

The positive topics that emerged most frequently indicated themes related to the program aiding in obtaining employment in a technology-related role, increasing technical skills, good program content, and faculty support. The neutral and negative topics that emerged emphasized scarcity of jobs and an overall feeling of being unprepared for the workforce. The topics were then aggregated to broader categories where the emergent themes were employment, skills gained, preparation provided by the academic program, and faculty support. Figure 5 below provides a chart of the sentiment analysis.

Figure 5. Sentiment Analysis



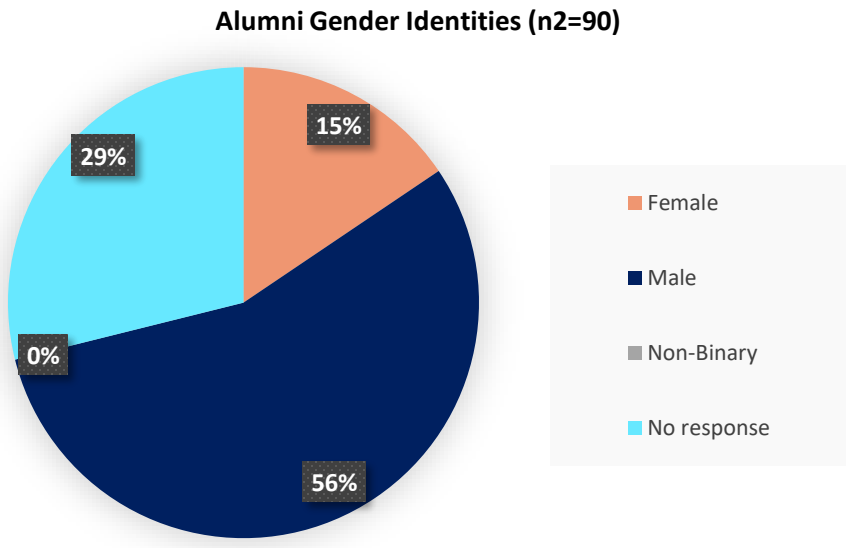
The topics that emerged were as follows, listed in order of frequency from most to least frequent: prepared, employment, technical skills, advanced skills, content, relationships, hands-on practice, critical thinking, unprepared, scarce jobs, credentials, encouragement, helped, advising, big picture, foundational knowledge, lack of security clearance, no change, organizational skills, and self-reflection. Employing the axial coding approach, the topics were

then distributed into categories that emerged from the topics, also listed in order of frequency from most to least frequent: employment, skills, program, faculty support, unemployed, personal growth, and credentials.

The remaining open-ended, short answer questions were also reviewed to separate the content for post-program continued education, professional credentials, and other preparatory resources that impacted employment outcomes. The pre-program education indicated by alumni respondents included associate degrees and bachelor's degrees. Post-program continued education indicated by alumni respondents included associate, bachelor's, and master's degrees. The certifications identified by alumni were separated by type and then by certification issuer to find frequency for comparison to previous studies.

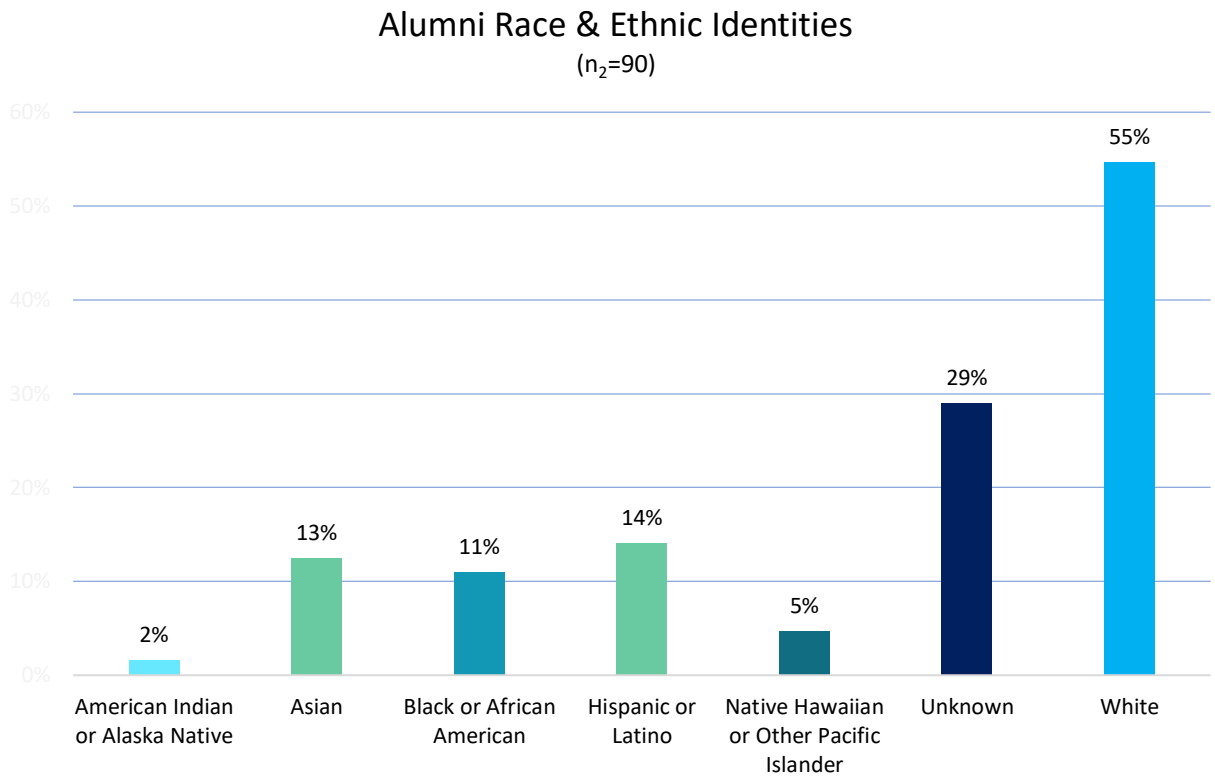
At the end of the survey, alumni were given the option to select their gender identity and/or their race/ethnic identity. Of the 63 total responses (70%) for gender identity, female was selected 14 times, male was selected 50 times, and non-binary had zero (0) responses. Figure 6 below is a pie chart of the percentages for gender identities reported by alumni.

Figure 6. Gender Identities



The racial and ethnic identities reported by alumni included one (1) American Indian or Alaska Native, eight (8) Asian, one (1) mixed Black and White, six (6) Black or African American, nine (9) Hispanic or Latino, three (3) Native Hawaiian or Other Pacific Islander, and 35 White. Figure 7 below is a chart of the alumni reported race and ethnic identity percentages.

Figure 7. Racial and Ethnic Identities



Summary

The survey results from the nested sample populations of CAE-CD POCs and alumni were analyzed. The findings of the study showed a participation rate of 39 POCs and 90 alumni from CAE-CD two-year colleges across the U.S. The results of the surveys were used to develop discussion and answer the research question and sub-questions. The POCs and alumni aligned on four of five NICE Framework work roles from those most frequently selected by both samples.

70% of the alumni were employed in technology-related roles, 37% indicated that they continued their education after completing their CAE-CD cybersecurity program, and the diversity gaps of the U.S. cybersecurity workforce were also reflected in the alumni sample.

Chapter 5. Discussion

This chapter includes a review of the findings as compared to the literature, as related to the research question and sub-questions, and recommendations to cybersecurity stakeholders on use of the results. Each of the following sections provides further contextualization to the literature and to the implications of the results of the study. Recommendations are provided to each of the cybersecurity stakeholder groups, including government agencies such as NSA and NICE, employers, faculty, and students.

Research Question Findings

This multi-phased research study included one overarching research question and three sub-questions. The research question and sub-questions were supported by a series of questions posed in the survey instruments. A frequency analysis was conducted to find the highest proportion of work roles identified by the POCs and the alumni. Further analysis was conducted to determine the number of alumni not employed in technology-related work roles.

RQ1: Which cybersecurity work roles of the National Initiative for Cybersecurity Education (NICE) Framework are alumni of Centers of Academic Excellence in Cyber Defense (CAE-CD) two-year colleges employed in as compared to the work roles identified by their college?

The results of the survey showed that POCs most frequently identified the following five work roles as those that their programs prepare students for: System Administration, Network Management, Technical Support, Vulnerability Analysis, Incident Response. Alumni reported employment in the following work roles with the highest frequency: Technical Support, System Administration, Network Management, Systems Management, Incident Response. The primary difference between the top five work roles for POCs and alumni were Vulnerability Analysis and Systems Management, respectively.

RQ1.1: What proportion of the cybersecurity program alumni are not employed in any cybersecurity work roles?

The findings showed that 88% of the alumni were currently employed, specifically 79 of 90. Nearly one third of the alumni were not working in positions that were technology-related roles; equivalent to 27 of 90 respondents, or 30%. Of the alumni that reported they were currently employed, approximately 80% held technology-related positions.

RQ1.2: What proportion of the alumni pursued another degree within three years of graduation from a CAE-CD two-year college?

From the 90 alumni respondents, approximately 41%, or 37 respondents, indicated that they pursued another degree after graduation and six (6) commented that they plan to do so in the future.

RQ1.3: How do the alumni gender and ethnicity demographics align with the gender and ethnicity demographics of the cybersecurity workforce of the United States?

Gender and ethnicity identifiers were optionally indicated by 71% of the respondents, or 64 of 90. Percentages for respondents indicating gender included 22% female and 78% male. The alumni responses for race and ethnicity identifiers in this study were as follows: American Indian or Alaska Native 2%, Asian 13%, Black and White mixed 2%, Black or African American 9%, Hispanic or Latino 14%, Native Hawaiian or Other Pacific Islander 5%, and White 55%.

Comparisons to Previous Research Studies

The 2022 global survey by ISC(2) reported that organizations with cybersecurity staff shortages planned to invest in training, certifications, and diversity initiatives ((ISC)2, 2022). The CAE-CD two-year colleges are also making similar investments regarding cybersecurity

programs. In comparison to the 96% of ISC(2) respondents with at least one industry certification, 33% of the alumni respondents for this study held at least one certification. 47% of the POCs reported offering industry certification vouchers to students, and only 21% of the alumni experienced such activities in their two-year college programs. Important qualifications for new hires include experience and practical skills, according to ISC(2) (2022). Alumni indicated that they felt positively that skills were gained in their two-year college programs.

Following are comparisons made between this study and the 2019 study by Sands and Sande related to work roles and industry certification. Both had similar alumni population sizes; this study had 90 alumni responses and the 2019 study had 88 responses. Only 20% of the alumni for this study indicated certification in CompTIA Security+ while 45% of those in the 2019 held the same certification. For the CompTIA Network+ certification, 9% of this study's alumni reported holding that certification and significantly more, 40% of the 2019 study alumni held the certification. The current study asked alumni to indicate the top five work roles they were performing in their current work functions while the 2019 study asked about all work roles ever performed in past and current work functions. The top category indicated by work role hits for this study was IMPLEMENTATION and OPERATION (75) and for the 2019 study it was Operate and Maintain (213).

Comparing this study to the Finnish JAMK university study from 2022, the top two categories identified in this study were IMPLEMENTATION and OPERATION (75) and OVERSIGHT and GOVERNANCE (48) while JAMK alumni identified Protect and Defend (29) and Operate and Maintain (24) as the top two categories. Using the 2023 NICE Framework crosswalk, the categories of IMPLEMENTATION and OPERATION and Operate and Maintain are very similar. The top two work roles were different between these two studies, this study's

two-year college alumni indicated Technical Support (30) and System Administration (22) and JAMK university alumni reported Cyber Defense Analyst (11) and Cyber Defense Incident Responder (11). According to ISACA's State of Cybersecurity report in 2022, less organizations require a bachelor's degree for cybersecurity jobs than in previous years which may lead to more alignment between university and two-year college employment outcomes in the future.

Each of these are cross-sectional studies took place at different points in time and with populations in different geographic locations. The comparisons of each of the previous research studies with this study demonstrated the variability of responses at different times. This furthers the recommendation for future research to conduct longitudinal research on the same population and a separate study to examine a comparison between CAE-CD university and two-year college alumni employment outcomes.

The primary research question investigated the relationship between the work roles POC prepared students for and the work roles that alumni were employed in. The POCs in this study identified PROTECTION and DEFENSE (PD) and IMPLEMENTATION and OPERATION (IO) as the top categories they prepare students for which aligns well with the top five work roles indicated by that population. Alumni identified work roles in the OVERSIGHT and GOVERNANCE (OG) category in the top five while POCs did not, which could mean that the POCs are potentially missing the opportunity to prepare students for work roles in that category.

Compared to the 2019 workforce study by Sands and Sande where the top two work roles identified by alumni were Network Operations Specialist and Systems Administrator, this study indicated that Technical Support and System Administration were the top two work roles. Less alumni in the current study had achieved any industry-recognized certification at 33% and just 20% had the CompTIA Security+ certification compared to the 2019 study in which 45% had the

CompTIA Security+ certification and others. Some students are not leveraging co/extra-curricular activities to prepare for work placement which may affect their ability to obtain work in technology-related roles. This is another opportunity for CAE-CD colleges to find ways to offer preparation for certification exams and no-cost or discounted vouchers to increase student employability upon graduation.

The first sub-question investigated alumni employment in cybersecurity work roles. Overall, alumni reported an employment rate of 88%, with only 70% reporting they were in technology-related positions. Compared to a report by Next Gen Personal Finance (2023), the percentage employed in their field of study for this group was higher than others where only 46% of college alumni reported that they are employed in their field of study. Considering the preparation for specific work roles by the CAE-CD two-year colleges and number of co/extra-curricular activities it would be fitting to conduct further studies to probe into possible reasons for the employment rates being less than 100% while industry demand is still very high.

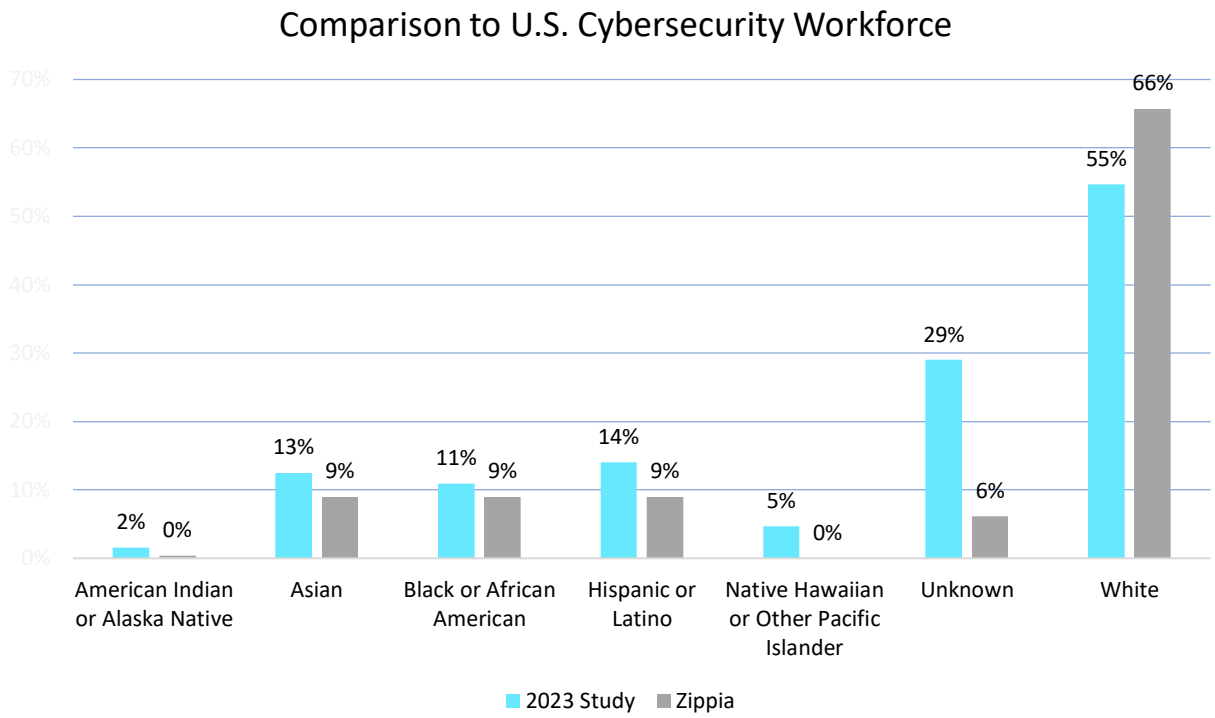
Students are entering CAE-CD college programs with credit from prior education, including bachelor's and master's degrees. POCs can examine how this can be leveraged to encourage student interests and develop education plans to aid in finding technology roles for students and alumni. Combining previous higher education achievements with industry-recognized certification and cybersecurity education can help increase employability.

The second sub-question investigated continued education after completion of a degree or certificate at the CAE-CD two-year college. Alumni are pursuing further education after completing CAE-CD programs at two-year institutions. Generalized transfer information typically offered may not assist cybersecurity students seeking more direct matriculation. Two-year colleges can assist with this by connecting students with transfer opportunities and

developing partnerships with four-year institutions as part of their academic pathways, making the transition to continued education more transparent to students. Making students aware of transfer opportunities in cybersecurity may also lead to increased employment opportunities.

The third sub-question investigated the alignment of alumni and national workforce demographics. Gender and ethnicity identifiers were optionally indicated by 71% of the respondents, or 64 of 90. Based on the Cybersecurity Ventures report (Morgan, 2022) which noted female representation is 24%, the alumni sample showed similar gender ratios to those found in the U.S. cybersecurity workforce, 22% of the alumni identified as female. The ethnic identifiers were different than the U.S. cybersecurity workforce based on responses to the (ISC)2 workforce study (2022) which showed a response rate of 87% White and 13% Non-White. Alumni responses for this study were more like those of the 2022 (ISC)2 report for cybersecurity workers under age 30 which was 50% White. According to Zippia (2023), racial and ethnic proportions of the U.S. cybersecurity workforce are 66% White, 6% unknown, and 28% ethnic diversity. Racial and ethnic identifier categories used for this study were adapted for comparison to Zippia, as shown in Figure 8 below.

Figure 8. Comparison of Racial and Ethnic Identities



The alumni population reflected more diversity than other U.S. cybersecurity workforce studies. Considering the additional student diversity often found at community colleges, the populations reached by cybersecurity programs could continue to produce alumni from diverse backgrounds which will enrich the workforce. As mentioned by the former National Cyber Director, two-year colleges should look to provide cybersecurity learning opportunities for 'all' individuals, the 'many' that will implicate cybersecurity through their job functions and focus on the 'few' that will work in cyber defense careers. The alumni expressed efforts towards continued education, achievement of industry-recognized certification, and demographics for gender and ethnic identities.

Recommendations

POCs and alumni engaged in this study to provide their feedback and enhance the cybersecurity community with knowledge about two-year college alumni employment outcomes and program experiences. The structure, methodology, and results of this study can be used by many in the cybersecurity community to learn more about employment outcomes from two-year college alumni. The CAE-CD designation criteria is structured to ensure that higher education programs can prepare students for the cybersecurity workforce. Stakeholders, including government agencies, the NSA, employers, faculty, students, and organizations that rely on cybersecurity talent to keep their systems secure from cyberattacks can gain valuable insights from the results of this study to aid in decision-making and program development. Table 11 below includes possible ways in which the results of this study can be used by different stakeholders.

Table 11. Stakeholder Group Usage of Study Insights

Stakeholder Group	Use of Study Insights
NSA and Government Agencies	• When evaluating work roles, pathway initiatives, and employment offerings for two-year college alumni
NICE	• To better inform the list of work roles that two-year college alumni are engaged with in the workplace
Employers	• To better understand the work roles that CAE-CD two-year colleges most often prepare students for and the types of industry certifications the alumni may have achieved
Faculty	• To evaluate academic programs • To recognize the need for additional student engagement with extra-curricular activities • To increase opportunities for industry-certification preparation and access to exam vouchers • To examine the work roles and other statistics from this study to evaluate curriculum and extra-curricular activities for gaps and to validate existing practices • To recognize the need for and value of continued alumni contact
Students	• To better understand the prominent work roles that two-year colleges most often prepare students for

POCs can establish procedures to continue contact with alumni that can enhance the learning environment with industry speakers and mentors. This may mean that POCs need to maintain personal contact information about alumni to keep in touch after their student status has expired. POCs can leverage student engagement data and alumni employment outcomes as considerations and influences as part of their annual program review/assessment and during program development. Faculty and POCs can benefit from maintaining contact with alumni to learn more about their experience in the workplace, their ongoing educational needs, and invite alumni back as industry speakers and mentors. These relationships can be invaluable to the program and to cultivating current students as they prepare for the cybersecurity workforce.

While labor market reports are critical elements used in curriculum development and program planning, alumni outcomes are equally valuable to understanding the types of career preparation that an academic program has provided to its students. Career education programs at two-year colleges can compare their local external labor market research reports with local alumni survey results on work roles to find gaps in existing curriculum. This type of comparison and gap analysis could provide additional opportunities for co/extra-curricular activities such as workshops and camps to augment formal curriculum with additional learning opportunities for students that help them prepare for the workforce. Local study results could be discussed with current students to help them understand the value of responding to the survey in the future as alumni of the program.

Students can benefit from an increase in the number of opportunities providing all cybersecurity students with some form of hands-on lab experience outside of the classroom to prepare for the workplace. The alumni that were not employed had less overall engagement with co/extra-curricular activities while in their cybersecurity program at the two-year colleges. POCs

can help students reach their career potential to become cybersecurity experts by emphasizing pathways activities and the 10,000 hours theory with encouragement to practice in the classroom and outside the classroom.

Chapter 6. Conclusion

Summary

This national level research study sought to provide more detailed information about perceptions of CAE-CD alumni on their academic preparation and employment outcomes compared to those of the POCs using the NICE Framework work roles. As previously noted, administrative data produced by higher education is usually aggregated leading to a lack of detailed information about two-year college alumni employment outcomes. The needs of the cybersecurity workforce continue to evolve, and higher education institutions can modify their programs by incorporating alumni employment outcomes to better prepare students for the workforce.

The work roles that alumni are filling with employers are closely aligned with those that POCs have set out to prepare students for, with one exception being the Vulnerability Analysis work role which was identified more frequently by alumni than POCs. A good proportion of alumni continued their education after completing their cybersecurity program. A moderate rate of employment in technology-related positions was indicated by the two-year college alumni from CAE-CD institutions. Although there was a high proportion of respondents from Hawaii in the alumni sample, that did not have a significant impact on the proportions of ethnicities identified by alumni as compared to the demographics of the U.S. cybersecurity workforce.

Naturally, the research scope introduces limitations on any given study. The sample size also influences the applicability of the data resulting from the study. POC interest and participation in this research study was strong yet did not produce the alumni sample size expected. The relatively small alumni sample population provided valuable information about their accomplishments, including employment outcomes, co/extra-curricular experiences,

industry-recognized certifications, and continued education. Several limitations related to the nested sampling approach, difficulty reaching alumni, population size, lack of complete coverage across all states, and the impact of point-in-time data will be discussed in this chapter.

Limitations and Recommendations for Future Research

Although the nested sample approach was necessary to reach only the intended CAE-CD two-year college alumni, some of the colleges and POCs did not maintain current contact information which may have caused the alumni sample to be smaller than its potential given a different approach. The time between graduation from the two-college and completion of the survey was between zero and five years. Many states were not represented in the study due to lack of participation. Less than half of the two-year colleges that participated received corresponding alumni responses. Collectively, these issues caused limitations to the overall results for the study.

Some of the POCs that were interested yet unable to participate in the study expressed a lack of alumni contact information and shared that they did not have continued relationships with alumni after graduation. The POCs could have benefitted from such a connection because most of the alumni surveyed were employed in technology-related roles which could have led to further industry contacts and awareness of student needs. The faculty researchers for the JAMK study indicated that they used alumni feedback to help with further curriculum and program development by surveying alumni about what they would have liked to have had included in the program. The lack of continued communication after graduation appears to be a missed opportunity for the POCs and two-year colleges to gather valuable information from alumni.

The online survey method reached a broad group across the country and allowed for asynchronous response in a short timeframe aligned with the intent of the study. This method has

been successfully used by (ISC)2 and other global studies as well to reach tens of thousands working in cybersecurity. It is possible that more qualitative data could have been obtained from the POCs and alumni had they been interviewed instead. Additionally, a focus group of POCs could aid in further understanding of the contact information needed for the alumni surveys.

Cross-sectional studies such as this offer point-in-time data collection which can limit the generalizability of the results. This also introduces limitations on the opportunity to gather insight into the changes over the length of the alumni career pathways to understand the most influential impacts. Although limited, the results of this study can serve as a foundation to guide future research.

Future research study opportunities exist which can align with this study or examine other higher education populations in a similar manner using the NICE Framework. Additional research studies of this type are necessary to offset the cross-sectional nature and provide long-term value through comparison to future results. Similar to the (ISC)2 annual reports on the cybersecurity workforce, a longitudinal study that surveys an alumni population repeatedly at given intervals could be valuable to provide guidance on the career patterns and pathways of two-year college alumni. Additionally, using a verbal interview rather than a survey form could provide the opportunity to obtain additional qualitative data for the study and for respondents to ask clarifying questions.

Future research should also include soliciting alumni feedback to rank the factors that most contributed to their ability to obtain a job in cybersecurity, especially with emphasis on alumni that have played in cybersecurity competitions. Work roles identified by alumni could also be compared to the co/extra-curricular resources utilized by students during their time in the academic program to determine which provide the most preparation for specific work roles.

Another opportunity for further research could be to compare the work roles and competencies most frequently identified by alumni of four-year and two-year cybersecurity programs.

Concluding Remarks

As technology continues to advance and the sophistication of cyber adversaries continues to increase, the need for advancement in the cybersecurity workforce is ever more warranted. Cybersecurity stakeholders can use the results of this study towards education and workforce development for all, many, and few, which collectively and individually have an impact on U.S. national cyber defense. While recent trends show the landscape of the cybersecurity workforce improving with respect to gender and ethnic diversity, and two-year college programs should continue to raise awareness to influence non-traditional and historically underrepresented populations to pursue cybersecurity education and careers.

When alumni work in technology-related roles, the relationships with POCs can potentially be a key to establishing additional industry partnerships for the college and returning to encourage other students in their cybersecurity studies. The potential value of alumni relationships appears not to be utilized to its fullest extent by higher education institutions. Maintaining relationships with alumni can be a beneficial way for faculty and POCs to gain insights into which factors positively impacted career opportunities for students completing their programs.

References

(ISC)2. (2018). *(ISC)2 Cybersecurity Workforce Study: Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4DEA45372594D98EAA419E6815ED7C10AA21FEB3

(ISC)2. (2019). *(ISC)2 Cybersecurity Workforce Study: Strategies for Building and Growing Strong Cybersecurity Teams.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

(ISC)2. (2020). *(ISC)2 Cybersecurity Workforce Study: Cybersecurity Professionals Stand Up to a Pandemic.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

(ISC)2. (2021). *(ISC)2 Cybersecurity Workforce Study, 2021: A Resilient Cybersecurity Profession Charts the Path Forward.* International Information Systems Security Certification Consortium.

(ISC)2. (2021). *International Information System Security Certification Consortium.* Retrieved from (ISC)2 Cybersecurity Workforce Study: A Resilient Cybersecurity Profession Charts the Path Forward: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx?la=en&hash=9776A8010A72AEC5C879976FAC4FB2B493906F39

(ISC)2. (2022). *(ISC)² Cybersecurity Research*. Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/Research#

(ISC)2. (2022). *(ISC)2 Cybersecurity Workforce Study: A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

AlDaajeha, S., Saleousa, H., Alrabaeea, S., Barkaa, E., Breitingerb, F., & Chooc, a. K.-K. (2022, May 18). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 11*.

Alrabaee, S., Al-kfairy, M., & Barka, E. (2022). Efforts and Suggestions for Improving Cybersecurity Education. *IEEE Global Engineering Education Conference (EDUCON)*, 1161-1168.

American Association of Community Colleges. (2019). *Community college enrollment crisis? Historical Trends in Community College Enrollment.* American Association of Community Colleges.

American Association of Community Colleges. (2022). *Fast Facts.* Retrieved from American Association of Community Colleges: https://www.aacc.nche.edu/research-trends/fast-facts/?_gl=1*1hiw5il*_ga*MTYzNTE5MDQwLjE2NzM3MzExMTA.*_up*MQ..

Ashley, T. D., Kwon, R., Gourisetti, S. N., Katsis, C., Bonebrake, C. A., & Boyd, a. P. (2022, October 31). Gamification of Cybersecurity for Workforce Development in Critical Infrastructure. *IEEE Access, 10*.

Austin, L. J. (2022, March 28). *The Department of Defense Releases the President's Fiscal Year 2023 Defense Budget.* Statement, U.S. Department of Defense, Washington DC. Retrieved from https://www.defense.gov/News/Releases/Release/Article/2980014/the-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg/

Bagchi-Sen, S., Rao, H., Upadhyaya, S., & Chai, a. S. (2010, January/February). Women in Cybersecurity: A Study of Career Advancement. *IT Professional, 12*(1), pp. 24-31.

Baker, M. (2016). *Striving for Effective Cyber Workforce Development.* White Paper, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA.

Baroudi, J., & Orlikowski, W. (1989, March). The Problem of Statistical Power in MIS Research. *MIS Quarterly, 13*(1), 87-106.

Blair, E. (2015). A reflexive exploration of two qualitative data coding techniques. *Journal of Methods and Measurement in the Social Sciences, 6*(1), 14-29.

Boggs, G. R. (2002). *Protecting Information The Role of Community Colleges in Cybersecurity Education.* Community College Press. Washington, D.C.: American Association of Community Colleges.

Burley, D. L., Bishop, M., Buck, S., Ekstrom, J. J., Futcher, L., Gibson, D., . . . Parrish, A. (2017). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.* Joint Task Force on Cybersecurity Education. Association for Computing Machinery (ACM).

CAE in Cybersecurity Community. (2021). *What is a CAE in Cybersecurity?* Retrieved from CAE Community: https://www.caecommunity.org/about-us/what-cae-cybersecurity

Campbell, R. D. (2003, June 1). Community College Corner: Cybersecurity. *Special Interest Group on Computer Science Education (SIGSCE), 35*(2), 24-26.

Carey, A. (2004, October). *(ISC)2 Information Security Global Workforce Study.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2004.ashx?la=en&hash=5BCFAB95359C8DB3FC008FE1EF8088E883BD2F7D

Carey, A. (2005, December). *2005 Global Information Security Workforce Study.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2005.ashx?la=en&hash=30910C0FE313F85D8D83CCF924C835E5A00B9895

Carey, A. (2006, December). *2006 Global Information Security Workforce Study: A Special U.S. Government Perspective.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2006-US-Gov.ashx?la=en&hash=A6AB39C51384B0B8E046ABE59FDC90BC300ADD69

Carrese, J., Goss, M., Hermann, A., & Bartel, T. (2018). *Cybersecurity: Labor Market Analysis and Statewide Survey Results.* Centers of Excellence for Labor Market Research, Economic and Workforce Development Program, California Community Colleges. California Advanced Supply Chain Analysis & Diversification Effort (CASCADE).

CC Daily Staff. (2017, October 24). *Workforce concerns in cybersecurity*. (American Association of Community Colleges) Retrieved from Community College Daily: American Association of Community Colleges: https://www.ccdaily.com/2017/10/workforce-concerns-cybersecurity/

Chadd, K. (2020, November 24). *The history of cybersecurity*. Retrieved from Avast Software: https://blog.avast.com/history-of-cybersecurity-avast#

Chen, G. (2022, September 7). *What is a Community College?* Retrieved from Community College Review: https://www.communitycollegereview.com/blog/what-is-a-community-college

CISA. (2020, October 21). *Critical Infrastructure Sectors*. Retrieved from Cyberssecurity & Infrastructure Security Agency: https://www.cisa.gov/critical-infrastructure-sectors

Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., . . . Brynielsson, J. (2009, December). An Exploration of the Current State of Information Assurance Education. *ACM Inroads - SIGCSE Bulletin (Special Interest Group Computer Science Education), 41*(4), 109-125.

Creswell, J. W. (1994). *Research Design: Qualitative and Quantitative Approaches* (Vol. 1st edition). Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches* (Vol. 2nd edition). Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Vol. 3rd edition). Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Vol. 5). SAGE Publications.

Creswell, J., & Creswell, J. (2018). *Research Design: Qualitative, Quantative, and Mixed Methods Approaches* (Vol. 5th). SAGE Publications.

CyberSeek. (2021). *Hack the Gap, About CyberSeek, Methodology*. Retrieved from CyberSeek: https://www.cyberseek.org/index.html#aboutit

CyberSeek. (2022). (Burning Glass, CompTIA, and National Initiative of Cybersecurity Education) Retrieved from CyberSeek: https://www.cyberseek.org

CyberSeek. (2023, April). *Cybersecurity Career Pathway*. Retrieved from CyberSeek: https://www.cyberseek.org/pathway.html

Dampier, D. (2015). Building a Successful Cyber-security Program.

Dawson, J., & Thomson, R. (2018, June). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology, 9*.

Department of Commerce. (2018, November 2). *Addressing the Cybersecurity Workforce and Skills Gap*. Retrieved from Newstex: The Commerce Blog.

Department of Defense. (2020). *DoD Approved 8570 Baseline Certifications*. Retrieved from DoD Cyber Exchange Public: https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

Department of Health and Human Services. (2022). *Code of Federal Regulations: Title 45*. Retrieved from National Archives: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-46

Dillman, D., Smyth, J., & Christian, L. (2014). *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method* (Vol. 4th edition). Wiley.

Dohm, L. (2015, January 27). Community College Cyber Summit (3CS) Addresses the Need for Cybersecurity Education ASAP.

Doyle, K. (2021, September 2). *Incident responder careers: What's it like to work in incident response?* Retrieved from INFOSEC Institute: https://resources.infosecinstitute.com/topic/incident-responder-careers-whats-it-like-to-work-in-incident-response/

Drolet, M. (2021). *Diversity in cybersecurity: Barriers and opportunities for women and minorities.* CSO (Online). Framingham: Foundry.

Duffin, E. (2021, November 15). *Community colleges in the United States - Statistics & Facts*. Retrieved from Statista: https://www.statista.com/topics/3468/community-colleges-in-the-united-states/

Eikenberry, H., & Pfannenstein, L. (2016, March). Centers of Academic Excellence in Cyber Security (CAE-C). *3RD CYBER SECURITY WORKSHOP PROCEEDINGS. Cyber T&E Workforce Development Track.* Arlinton, VA: The International Test and Evaluation Association.

Elangovan, N., & Sundaravel, E. (2021). Method of preparing a document for survey instrument validation by experts. *National Library of Medicine, 8*.

EMSI Burning Glass. (2022). *Interactive Map*. (EMSI Burning Glass; CompTIA; NICE) Retrieved from CyberSeek: https://www.cyberseek.org/heatmap.html

Erbschloe, M. (2017). *Threat Level Red: Cybersecurity Research Programs of the U.S. Government* (Vol. 1st edition). CRC Press.

Estes, A. C., Kim, D. J., & Yang, T. A. (2018). Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates. *Frontiers in Education: Computer Science and Computer Engineering*, 58-64.

Evans, N., Saflund, P., & Wijenaike, M. (2002, June 26-29). IT Security Specialist— Integrating Academic Credentials with Professional Certifications. *Protecting Information: The Role of Community Colleges in Cybersecurity Education*, pp. 73-87.

FBI News. (2022, March 22). *FBI Releases the Internet Crime Complaint Center 2021 Internet Crime Report.* Retrieved from FBI National Press Office: https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report

Fowler, F. J. (2013). *Survey Research Methods (Applied Social Research Methods Book 1)* (Vol. 5th edition). SAGE Publications, Inc.

Frost & Sullivan. (2008). *The 2008 (ISC)2 Global Information Security Workforce Study.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2008.ashx?la=en&hash=C761C8AFE26899C88B34EF1A7BA860FFE35D6250

Frost & Sullivan. (2011). *The 2011 (ISC)2 Global Information Security Workforce Study.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2011.ashx?la=en&hash=0AAA6A6BD401CE13E650E99E6C7369F56366B1B2

Frost & Sullivan. (2013). *The 2013 (ISC)2 Global Information Security Workforce Study.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2013.ashx?la=en&hash=61704642B20BFF3D352B6C53D0F5818D2DA74FAE

Frost & Sullivan. (2015). *The 2015 (ISC)2 Global Information Security Workforce Study.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-2015.ashx?la=en&hash=6D7686173046E0AD6DF6DD9671E96035140A1C24

Frost & Sullivan. (2015). *Women in Security: Wisely Positioned for the Future of InfoSec.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/GISWS-Women-In-Security-Study-2015.ashx?la=en&hash=AFFB0803389B7FEFF3931E3B06CE81CC37D2413C

Frost & Sullivan. (2017). *2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/h/-/media/Files/Research/GISWS-Report-N-America-.ashx

Frost & Sullivan. (2017). *The 2017 Global Information Security Workforce Study: Women in Cybersecurity.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/ISC2-Women-in-Cybersecurity-2017.ashx?la=en&hash=FA78E4BDA2F858A0D3CFAC75AF9E789369A0BC8D

FTC. (2022). *New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021*. For Release, Federal Trade Commission.

Furnell, S. (2021). The Cybersecurity Workforce and Skills. *Computers & Security*.

Future Directions. (2022, June 26-28). *Future Directions: 2022 Summit*. Retrieved from NCyTE Center: https://www.ncyte.net/about-ncyte/future-directions-2022-summit

GAO. (2022). *Cybersecurity: An overview of cyber challenges facing the nation, and actions needed to address them*. (U.S. Government Accountability Office) Retrieved from U.S. Government Accountability Office: https://www.gao.gov/cybersecurity

Garcia Strategies, LLC. (2010). *The 2010 State of Cybersecurity from the Federal CISO's Perspective.* Retrieved from https://www.isc2.org/-/media/Files/Research/GISWS-Archive/CISO-Survey-Report-2010.ashx?la=en&hash=EC6FAFD675F6DFA400F07F78A204448E8473EFFE

George Washington University. (2018, March). *Presidential Orders*. Retrieved from National Security Archive: https://nsarchive.gwu.edu/news/cyber-vault/2018-11-07/presidential-orders

Ghosh, T., & Francia, G. (2021, September 23). Assessing Competencies Using Scenario-Based Learning in Cybersecurity. *Journal of Cybersecurity and Privacy, 1*, 539–552.

Gloster, C. S. (2022, October 3). *Office of the National Cyber Director Requests Your Insight and Expertise on Cyber Workforce, Training, and Education*. Retrieved from The White House: https://www.whitehouse.gov/oncd/briefing-room/2022/10/03/office-of-the-national-cyber-director-requests-your-insight-and-expertise-on-cyber-workforce-training-and-education/

Government Futures. (2009, April). *The 2009 State of Cybersecurity from the Federal CISO's Perspective.* Retrieved from https://www.isc2.org/-/media/Files/Research/GISWS-Archive/CISO-Survey-Report-2009.ashx?la=en&hash=784DA7A5C045DA938AA526D8D752405088F20745.

Hair, J. F., Babin, B. J., Anderson, R. E., & Black, W. C. (2019). *Multivariate Data Analysis* (Vol. 8th edition).

Hamdan, B., & Nsour, a. R. (2022). Curriculum Development for Teaching Cybersecurity of Industrial Control Systems & Critical Infrastructure. *Intermountain Engineering, Technology and Computing (IETC)*.

Hooper, K. M., & Harrington, C. (2022). Equity Gaps in Dual Enrollment. *Journal on Transforming Professional Practice, 7*(3).

Howell, J., Hurwitz, M., Ma, J., Pender, M., Perfetto, G., & Wyatt, a. J. (2022). *College Enrollment and Retention in the Era of Covid: Fall 2021 Update on Continued Pandemic Impacts.* College Board.

Hudnall, M. (2019, March). Educational and Workforce Cybersecurity Frameworks: Comparing, Contrasting, and Mapping. *Computer, 52*(3), pp. 18-28.

Huss, N. (2022, April 7). *How Many Websites Are There in the World?* Retrieved from Siteefy: https://siteefy.com/how-many-websites-are-there/

IBM Institute for Business Value. (2017, October 25). Workforce Concerns in Cybersecurity. *Community College Daily*.

Igwenagu, C. (2016). *Fundamentals of research methodology and data collection.* Enugu State University of Science and Technology.

IMS Global Case Network Labs. (2019-2020). *NICE Framework - Work Roles*. Retrieved from IMS Global Learning Consortium: https://labs.casenetwork.imsglobal.org/cftree/item/4165

ISACA. (2017, February 13). *Survey: Cyber Security Skills Gap Leaves 1 in 4 Organizations Exposed for Six Months or Longer*. Retrieved from ISACA Press Releases: https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2017/survey-cyber-security-skills-gap-leaves-1-in-4-organizations-exposed-for-six-months-or-longer

ISACA. (2022). *About Us*. Retrieved from ISACA: https://www.isaca.org/why-isaca/about-us

ISACA. (2022). *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations.* ISACA.

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice. *Field Methods, 18*(1), pp. 3–20.

James, S. L. (2019, September). The Underrepresentation of Females in the United States Cybersecurity Workforce: A Multiple-Case Study. *ProQuest*.

Jassal, P. (2021, October 28). *Can You Get a Bachelor's Degree at a Community College?* Retrieved from Unmudl: Skills-to-Jobs Marketplace: https://unmudl.com/blog/bachelors-degrees-community-colleges

Javidi, G., & Sheybani, a. E. (2018). K-12 Cybersecurity Education, Research, and Outreach. *IEEE*.

Kapellmann, D., & Washburn, a. R. (2019). Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure. *11th International Conference on Cyber Conflict: Silent Battle (CyCon).* Institute of Electrical and Electronics Engineers (IEEE).

Kim, K., Smith, J., Yang, T. A., & Kim, D. J. (2018, June 5-7). An Exploratory Analysis on Cybersecurity Ecosystem Utilizing the NICE Framework. *National Cyber Summit Research Track*, 1-7.

Knapp, K. J., Maurer, C., & Plachkinova, a. M. (2017, December 12). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education (JISE), 28*(2), 101-114.

Kose, Y., Ozer, M., Bastug, M., Varlioglu, S., Basibuyuk, O., & Ponnakanti, H. P. (2018). Developing Cybersecurity Workforce: Introducing CyberSec Labs for Industry Standard Cybersecurity Training. *International Conference on Computational Science and Computational Intelligence (CSCI)*.

Kulm, A. (2020). *A Framework for Identifying Host-based Artifacts in Dark Web Investigations.* Dissertation, Dakota State University, Madison, SD.

LeClair, J., Abraham, S., & Shih, a. L. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. *Information Security Curriculum Development Conference* (pp. 71–78). Kennesaw, GA: Association for Computing Machinery (ACM).

Levy, Y. (2020). *CAE-CD Resources: Proposed Preparations Starting Guide* . Retrieved from National Cybersecurity Training & Education Center (NCyTE): https://www.ncyte.net/home/showpublisheddocument/26/637896704208330000

Libicki, M. C., Senty, D., & Pollak, J. (2014). *Hackers Wanted: An Examination of the Cybersecurity Labor Market.* Santa Monica, CA: RAND Corporation.

Liebl, A., Rowland, P., Kiesow, A., Podhradsky, A., Redlin, M., Gaiani, M., . . . and Emery, M. (2021). Salaries in Higher Education Systems: A System-wide Perspective on Career Advancement and Gender Equity. *ADVANCE Journal*.

Liu, F., & Tu, M. (2020, August). An analysis framework of portable and measurable higher education for future cybersecurity workforce development. *Journal of Education and Learning (EduLearn), 14*(3), p. 322~330.

Llansó, T. H. (2018). *A Capability-Centric Approach to Cyber Risk Assessment and Mitigation.* Madison, SD: Dakota State University.

Manson, D., & Pike, R. (2014, March). The case for depth in cybersecurity education. *ACM Inroads, 5*(1), 47–52.

Marquardson, J., & Elnoshokaty, A. (2020, February). Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs. *Information Systems Education Journal (ISEDJ), 18*(1), 20-28.

Masters, G. (2017, July-August). A Diversified Workforce. *SC Magazine*, pp. 28-31.

McClurg, J. (2021, September). Emerging Technology, Evolving Threats — Part II: The Asymmetry Effect. *Security Magazine*.

McGuinness, A. (2014). *Community College Systems Across the 50 States.* Background Information for the Nevada Legislative Committee to Conduct an Interim Study Concerning Community Colleges, National Center for Higher Education Management Systems.

McQuaid, P., & Cervantes, S. (2019, September). How to Achieve a Seasoned Cybersecurity Workforce. *Software Quality Professional, 21*(4), pp. 4-10.

Miller, K. (2019, September 17). *17 Data Visualization Techniques All Professionals Should Know*. Retrieved from Harvard Business School Online: https://online.hbs.edu/blog/post/data-visualization-techniques

Mitchell, C. (2022, July 19). *Office of National Cyber Director hosts cyber workforce summit with CISA, other senior officials*. Retrieved from Inside Cybersecurity: https://www.proquest.com/trade-journals/office-national-cyber-director-hosts-workforce/docview/2691763739/se-2

Molly, B. W. (2013, April 4). Federal cybersecurity workforce study highlights age, training needs. *Fierce Government IT*, pp. https://www.proquest.com/trade-journals/federal-cybersecurity-workforce-study-highlights/docview/1466236481/se-2.

Morgan, S. (2022). *Women in Cybersecurity 2022 Report.* Cybersecurity Ventures.

Morrey, C. P. (2020, October 2-3). Pathway Mapping for an Educational Program. *2020 Intermountain Engineering, Technology and Computing (IETC)*, 1-5.

Moses, C. (2022, December 2). *How to develop the global cybersecurity workforce and build a security-first mindset*. (A. W. Services, Producer) Retrieved from World Economic Forum: https://www.weforum.org/agenda/2022/12/how-to-develop-the-global-cybersecurity-workforce-and-build-a-security-first-mindset/

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity Curriculum Design: A Survey. In *Transactions on Edutainment XV.* SpringerLink.

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M., Bhatia, S., Gagne, G., . . . Yuen, T. (2019). *Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education.* ITiCSE: Innovation and Technology in Computer Science Education. Aberdeen, Scotland, UK: Association for Computing Machinery (ACM).

Mullins, P., Wolfe, J., Fry, M., Wynters, E., Calhoun, W., Montante, R., & Oblitey, a. W. (2002). Panel on Integrating Security Concepts into Existing Computer Courses. *Special Interest Group on Computer Science Education (SIGCSE)* (pp. 365-366). Covington, Kentucky: Association of Computing Machinery (ACM).

Nakama, D. (2016). Community Colleges' Outreach Role in Cybersecurity. *National Cybersecurity Institute Journal, 3*(2), 35-40.

Nazah, S., Huda, S., Abawajy, J. H., & Hassan, M. M. (2021). An Unsupervised Model for Identifying and Characterizing Dark Web Forums. *IEEE Access, 9*, 112871-112892.

NC Perkins Team. (2019-2020). *Postsecondary Perkins Data Portal - Indicator Definiton*. Retrieved from North Carolina Perkins: https://www.ncperkins.org/data/indicator_definition.php?i=5P1

NCAE-C. (2020). 2020 CAE Cyber Defense (CAE-CD) Knowledge Units. *National Centers of Academic Excellence in Cybersecurity*.

NCyTE. (2021, June). *Local Academic and Economic Impacts of the CAE-CD Designation: A Case Study of Whatcom Community College and Jackson State Community College.* Retrieved from National Cybersecurity Training & Education Center: https://www.ncyte.net/about-ncyte/future-directions-2022-summit

NCyTE Center. (2023). *CAE-CD Resources*. Retrieved from NCyTE Center: https://www.ncyte.net/institutions/centers-of-academic-excellence/cae-cd-resources

Newhouse, B. (2018, Fall). *NICE 2018 Fall eNewsletter*. (National Institute of Standards and Technology (NIST)) Retrieved from National Initiative for Cybersecurity Education (NICE): https://www.nist.gov/itl/applied-cybersecurity/nice/nice-2018-fall-enewsletter#Featured%20Article

Next Gen Personal Finance. (2023, January 22). *Question of the Day: What percentage of college graduates work in their field of study?* Retrieved from NGPF: https://www.ngpf.org/blog/question-of-the-day/qod-what-percent-of-college-graduates-end-up-working-in-the-field-of-their-major/

NICE. (2013). *IT Workforce Assessment for Cybersecurity (ITWAC).* Washington, D.C.: U.S. Department of Homeland Security and CIO Council.

NICE. (2022, July 6). *Cybersecurity Workforce Demand.* Retrieved from NIST: https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf

NICE Symposium. (2021, November 16). *Fireside Chat with Chris Inglis, Kiersten E. Todt, and JJ Green*. Retrieved from https://www.youtube.com/watch?v=E0BMqHesdjY

NIST. (2021, September 23). *NICE Framework Resource Center*. Retrieved 2022, from National Institute of Standards and Technology: https://www.nist.gov/system/files/documents/2021/12/15/NFupdateprocess_summary14dec2021_clean.pdf

NIST. (2022). *NICE Framework Resource Center*. (NIST National Institute of Standards and Technology) Retrieved from Applied Cybersecurity Division /National Initiative for Cybersecurity Education (NICE): https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

NIST. (2023, April 18). *Comments Requested on Proposed Updates to NICE Framework Work Role Categories and Work Roles*. Retrieved from National Institute of Standards and Technology: https://www.nist.gov/news-events/news/2023/04/comments-requested-proposed-updates-nice-framework-work-role-categories-and

NIST CSRC. (2021, December). *NISTIR 8355 (Draft); NICE Framework Competencies: Assessing Learners for Cybersecurity Work (2nd Draft)*. (NIST National Institute of Standards and Technology) Retrieved from NIST Computer Security Resource Center: https://csrc.nist.gov/publications/detail/nistir/8355/draft

NSA. (2010). *CAE Fact Sheet 2010.* Retrieved from National Security Agency: https://www.nsa.gov/portals/75/documents/news-features/press-room/press-releases/2010/cae_fact_sheet_2010.pdf

O'Malley, M., & Rosenzweig, R. (1997). Brave New World or Blind Alley? American History on the World Wide Web. *The Journal of American history, 84*(1), 132-155.

Onwuegbuzie, A., & Collins, K. (2007, June). A Typology of Mixed Methods Sampling Designs in Social Science Research. *The Qualitative Report, 12*(2).

Parker, C. (2016). Cybersecurity Gender Inequality: The Role and Effort of the Community College. *National Cybersecurity Institute Journal, 3*(2).

Parrish, A. I. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. *23rd Annual Conference on Innovation and Technology in Computer Science Education.* Larnaca, Cyprus: Association for Computing Machinery.

Patton, M. (2014). *Qualitative research & evaluation methods: Integrating theory and practice* (Vol. 4th). SAGE Publications.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, a. P. (2012). NICE: Creating a Cybersecurity Workforce and Aware Public. *IEEE Computer and Reliability Societies*, 76-79.

Peacock, D., & Irons, A. (2017, May 22). Gender Inequality in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression. *International Journal of Gender, Science, and Technology, 9*(1), 5-44.

Pelfrey, A., & Peavy, P. (2019, September). Prototyping, Piloting & Program Implementation: Starting a Cybersecurity Pathway. *Techniques, 94*(4), 29-33.

Pérez, L., Cooper, S., Hawthorne, E., Wetzel, S., Brynielsson, J., Gökce, A., . . . Upadhyaya, S. (2011). Information Assurance Education in Two- and Four-Year Institutions. *Innovation and Technology in Computer Science Education (ITiCSE)* (pp. 39-53). Darmstadt, Germany: Association For Computing Machinery (ACM).

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181, Revision 1.* National Institute of Standards and Technology.

Pham, M., Greaney, K. C., & Abel, L. (2020). California Community Colleges Produce Positive Employment Outcomes. *Community College Journal of Research and Practice, 44*(1), 52-60.

Phillippe, K. (2022). *DataPoints: Enrollment by race/ethnicity.* American Association of Community Colleges.

Porter, J. (2020, December). Career Satisfaction of Women Information Assurance Programs Graduates: An Exploratory Qualitative Study. Capella University.

Ramezan, C. (2023). Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field. *Journal of Information System Education, 1*(34), 94-105.

Rodriguez, O., Gao, N., Brooks, B., & Gutierrez-Aragon, a. G. (2021). *Dual Enrollment in California: Promoting Equitable Student Access and Success.* Public Policy Institute of California.

Rosencrance, L. (2019, June). *Definition: NICE Framework*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/NICE-Framework

Rosenman, R., Tennekoon, V., & Hill, L. (2011). Measuring bias in self-reported data. *Int J Behav Healthc Res*, *2*(4), pp. 320-332.

Rossman, G. B., & Wilson, B. L. (1984). *Numbers and Words: Combining Quantitative and Qualitative Methods in a Single Large-Scale Study.* Research for Better Schools, inc., Annual Meeting of the American Educational Research Association (68th, New Orleans, LA, April 23-27, 1984). Washington, DC: National Institute of Education (ED).

Rowland, P., Podhradsky, A., & Plucker, S. (2018, January). CybHER: A Method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. *Hawaii International Conference on System Sciences, 51*, 3727-3735.

Saharinen, K., Viinikanoja, J., & Huotari, J. (2022). Researching Graduated Cyber Security Students: Reflecting Employment and Job Responsibilities Through NICE Framework. *The 21st European Conference on Cyber Warfare and Security*, *21*, pp. 247-255. Finland.

Sanders, R. (2022). The War for Cyber Talent: Can the US Win It? In R. Sanders, *The Great Power Competition* (Vol. 3). Springer.

Sands, J. (2021). *Topic 1: Workforce Study: Community College Cybersecurity Alumni, Where Are They Now?* (J. Rice, Director, & J. Rice, Performer) YouTube, U.S. Retrieved from YouTube: https://www.youtube.com/watch?v=yVM9SAAnja0

Sands, J., & Sande, C. (2019). *Workforce Study: Community College Cybersecurity Alumni.* Retrieved from https://www.ncyte.net/images/downloads/2019-workforce-study/2019-workforce-study.pdf

Saunders, M., & Tosey, P. (2013, Winter). The Layers of Research Design. *Rapport*, 58-59.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students* (Vol. 8). Upper Saddle River, NJ: Pearson Education.

Sharevski, F., Trowbridge, A., & Westbrook, J. (2018, March 10). Novel Approach for Cybersecurity Workforce Development: A Course in Secure Design. *2018 IEEE Integrated STEM Education Conference (ISEC)*, 175-180.

Shen, C. C., Chiou, Y.-M., Mouza, C., & Rutherford, a. T. (2021). Work-in-Progress—Design and Evaluation of Mixed Reality Programs for Cybersecurity Education. *7th International Conference of the Immersive Learning Research Network (iLRN)*.

Shoemaker, D., Kohnke, A., & and Sigler, K. (2018). *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0).* Boca Raton, FL: CRC Press.

Shumba, R., Taylor, C., Acholonu, G., Ferguson-Boucher, K., Franklin, G., Bace, R., . . . Hall, L. (2013). Cybersecurity, Women and Minorities: Findings and Recommendations from a Preliminary Investigation. *ITiCSE: Innovation and Technology in Computer Science Education* (pp. 1-13). New York, NY: Association for Computing Machinery.

Simpson, J. (2019, May). Urgent Need for Cybersecurity Professionals Grows. *Signal*, pp. 30-32.

Strickland, F. L. (2022, July). Going Beyond Considering the Use of Competency-based Education for Designing a Cybersecurity Curriculum. *Cybersecurity Pedagogy & Practice Journal*, *1*(1), pp. ISSN: 2832-1006.

Tang, C. (2019, June). Cyber2yr2020: ACM Guidelines for Associate-Degree Cybersecurity Programs. *ACM Inroads, 10*(2), pp. 8-11.

Tarun, R. (2022). Addressing the Skills and Diversity Gap. In R. Tarun, *Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders* (pp. 59-68). Wiley.

The White House. (2019, May). America's Cybersecurity Workforce. *A Presidential Document by the Executive Office of the President*. Washington, D.C., United States.

Tittel, E., Lindros, K., & Kyle, M. (2023, Feb 21). *Best InfoSec and Cybersecurity Certifications of 2023*. Retrieved from Business News Daily: https://www.businessnewsdaily.com/10708-information-security-certifications.html

Towson University. (2022). *Cultural Identity Resources: Non-Traditional Students*. Retrieved from Towson University Counseling Center: https://www.towson.edu/counseling/culturalidentity/nontraditional.html

Tunggal, A. T. (2022, June 26). *The 65 Biggest Data Breaches (Updated for January 2022)*. Retrieved from UpGuard: https://www.upguard.com/blog/biggest-data-breaches

Tyagi, N. (2021, January 18). *7 Types of Statistical Analysis: Definition and Explanation*. Retrieved from Analytics Steps: https://www.analyticssteps.com/blogs/7-types-statistical-analysis-definition-explanation

University of Phoenix. (2014). *Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals.* Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/Files/Research/GISWS-Archive/Workforce-Competencies-Report-Phoenix-2014.ashx?la=en&hash=3C2118A053B3CAA398D00EE870B4E9FC0956D009

Vagle, M. (2018). *Crafting Phenomenological Research.* Routledge.

Viinikanoja, J. (2022, January). Employment information of former students with cybersecurity specialization reviewed utilizing NICE Framework.

Voas, J., Kshetri, N., & DeFranco, J. F. (2021, Sept.-Oct.). Scarcity and Global Insecurity: The Semiconductor Shortage. *IT Professional, 23*(5), 78-82.

Vogel, R. (2016). Closing the Cybersecurity Skills Gap. *Salus Journal, 4*(2), 32-46.

Ward, P. (2021, June). Development of a Small Cybersecurity Program at a Community College. *Information Systems Education Journal (ISEDJ), 19*(3), 4-10.

Wetzel, K. (2021). *NICE Framework Competencies: Assessing Learners for Cybersecurity Work (2nd Draft).* National Institute of Standards and Technology, NIST. Retrieved from National Institute of Standards and Technology.

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023.*

Xu, D., Jaggars, S. S., Fletcher, J., & Fink, a. J. (2018). Are Community College Transfer Students "a Good Bet" for 4-Year Admissions? Comparing Academic and Labor-Market Outcomes Between Transfer and Native 4-Year College Students. *The Journal of Higher Education, 89*(4), 478-502.

Appendix A: Work Roles Defined within the NICE Framework

	Work Role	ID	Definition
OVERSIGHT AND GOVERNANCE (OG)	Authorizing Official	OG-WRL-001	Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation.
	Communications Security (COMSEC) Management	OG-WRL-002	Responsible for managing the Communications Security (COMSEC) resources of an organization.
	Curriculum Development	OG-WRL-003	Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques based on instructional needs and requirements.
	Executive Leadership	OG-WRL-004	Responsible for establishing vision and direction for an organization's cybersecurity resources and operations. Possesses authority to make and execute decisions that impact an organization broadly.
	Instruction	OG-WRL-005	Responsible for developing and conducting cybersecurity awareness, training, or education.
	Legal Advice	OG-WRL-006	Responsible for providing cybersecurity-related legal advice and recommendations.
	Policy and Planning	OG-WRL-007	Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
	Privacy Compliance	OG-WRL-008	Responsible for developing and overseeing an organization's privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs.
	Product Support	OG-WRL-009	Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components.
	Program Management	OG-WRL-010	Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment with agency or organizational priorities.
	Project Management	OG-WRL-011	Responsible for overseeing and directly managing cybersecurity projects. Tracks and communicates project status and demonstrates project value to the organization. Ensures cybersecurity is built into projects to protect the organization's critical infrastructure and assets, reduce risk, and meet organizational goals.
	Security Control Assessment	OG-WRL-012	Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.
	Systems Management	OG-WRL-013	Responsible for managing the cybersecurity of a program, organization, system, or enclave.
	Technology Portfolio Management	OG-WRL-014	Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities.
	Technology Program Auditing	OG-WRL-015	Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards.

	Workforce Management	OG-WRL-016	Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, education, and hiring processes. Makes adjustments in response to or in anticipation of changes to cybersecurity-related policy, technology, and staffing needs and requirements.
DESIGN AND DEVELOPMENT (DD)	Enterprise Architecture	DD-WRL-001	Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures.
	Research and Development	DD-WRL-002	Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecurity. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Security Architecture	DD-WRL-003	Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.
	Software Assessment	DD-WRL-004	Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable results.
	Software Development	DD-WRL-005	Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs.
	System Testing and Evaluation	DD-WRL-006	Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings.
	Systems Development	DD-WRL-007	Responsible for designing, developing, testing, and evaluating system security throughout the systems development life cycle.
	Systems Requirements Planning	DD-WRL-008	Responsible for consulting with customers to evaluate and translate functional requirements and integrating security policies into technical solutions.
IMPLEMENTATION AND OPERATION (IO)	Data Analysis	IO-WRL-001	Responsible for analyzing data from multiple disparate sources to provide security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
	Database Administration	IO-WRL-002	Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.
	Knowledge Management	IO-WRL-003	Responsible for managing and administering processes and tools to identify, document, and access an organization's intellectual capital.
	Network Management	IO-WRL-004	Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments.
	System Administration	IO-WRL-005	Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation.
	Systems Analysis	IO-WRL-006	Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares,

			performs, and manages the security aspects of implementing and operating a system.
	Technical Support	IO-WRL-007	Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes.
PROTECTION AND DEFENSE (PD)	Cybercrime Investigation	PD-WRL-001	Responsible for conducting detailed investigations of cyberspace-based crimes to establish documentary or physical evidence, including digital media and logs associated with intrusion incidents. Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
	Cyberspace Defense	PD-WRL-002	Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.
	Digital Forensics	PD-WRL-003	Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation.
	Incident Response	PD-WRL-004	Responsible for investigating, analyzing, and responding to network cybersecurity incidents.
	Infrastructure Support	PD-WRL-005	Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity.
	Threat Analysis	PD-WRL-006	Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat/warning assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.
	Vulnerability Analysis	PD-WRL-007	Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.
INTELLIGENCE (IN)	All-Source Analysis	IN-WRL-001	Responsible for analyzing data and information from one or multiple sources to conduct preparation of the environment, responding to requests for information, and submitting intelligence collection and production requirements in support of intelligence planning and operations.
	All-Source Collection Management	IN-WRL-002	Responsible for identifying collection authorities and environment; incorporating priority information requirements into intelligence collection management; determining capabilities of available intelligence collection assets and identifying new capabilities; constructing and disseminating intelligence collection plans; and monitoring execution of intelligence collection tasks to ensure effective execution of collection plans.
	All-Source Collection Requirements Management	IN-WRL-003	Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of intelligence collection requirements. Evaluates performance of intelligence collection assets and operations.
	Intelligence Planning	IN-WRL-004	Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

	Multi-Disciplined Language Analysis	IN-WRL-005	Responsible for processing, analyzing, and disseminating intelligence information derived from language, voice, and graphic material. Creates and maintains language-specific databases and working aids and provide subject-matter expertise in foreign language-intensive or interdisciplinary projects.
CYBERSPACE EFFECTS (CE)	Cyber Operations	CE-WRL-001	Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conducts collection, processing, and geolocation of systems to exploit, locate, and track targets. Performs network navigation and tactical forensic analysis and executes on-net operations when directed.
	Cyber Operations Planning	CE-WRL-002	Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integration during the execution of cyber actions.
	Exploitation Analysis	CE-WRL-003	Responsible for identifying access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
	Mission Assessment	CE-WRL-004	Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; and determining whether systems perform as expected.
	Partner Integration	CE-WRL-005	Responsible for developing assessment plans and performance measures; determining whether systems performed as expected; and conducting strategic and operational mission effectiveness assessments.
	Target Development	CE-WRL-006	Responsible for performing target system analysis and building and maintaining electronic target folders to include inputs from environment preparation and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations and presents candidate targets for vetting and validation.
	Target Network Analysis	CE-WRL-007	Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; and developing techniques to gain target information. Determines how targets communicate, move, operate, and live based on knowledge of target technologies, digital networks, and applications.

Note: Information in this table was adapted from the NICE Framework Resource Center on the NIST website, the Workforce Framework for Cybersecurity (NICE Framework) (NIST, 2023).

Appendix B: CAE-CD Colleges

List of CAE-CD designated institutions with college in the name as of July 27, 2022. Includes the years of their CAE designation, the state, and CAE region that the college is located in.

Institution Name	CAE Type	CAE-CD Years	State	Region
Alamance Community College	CAE-CD	2020 - 2025	North Carolina	Southeast
Anne Arundel Community College	CAE-CD	2021 - 2028	Maryland	Northeast
Arapahoe Community College	CAE-CD	2019 - 2024	Colorado	Northwest
Augusta Technical College	CAE-CD	2018 - 2023	Georgia	Southeast
Bismarck State College	CAE-CD	2019 - 2024	North Dakota	Southeast
Blue Ridge Community and Technical College	CAE-CD	2016 - 2027	West Virginia	Northeast
Bluegrass Community and Technical College	CAE-CD	2019 - 2024	Kentucky	Southeast
Bossier Parish Community College	CAE-CD	2014 - 2027	Louisiana	Southwest
Brookdale Community College	CAE-CD	2019 - 2024	New Jersey	Northeast
Butler Community College	CAE-CD	2019 - 2024	Kansas	Midwest
Calhoun Community College	CAE-CD	2018 - 2023	Alabama	Southeast
Cecil College	CAE-CD	2019 - 2024	Maryland	Northeast
Central New Mexico Community College	CAE-CD	2017 - 2022	New Mexico	Southwest
Central Piedmont Community College	CAE-CD	2021 - 2026	North Carolina	Southeast
Century College	CAE-CD	2019 - 2024	Minnesota	Midwest
Champlain College	CAE-CD	2017 - 2022	Vermont	Northeast
Chemeketa Community College	CAE-CD	2020 - 2025	Oregon	Northwest
Chippewa Valley Technical College	CAE-CD	2022 - 2027	Wisconsin	Midwest
City College of San Francisco	CAE-CD	2019 - 2024	California	Southwest
Clark State Community College	CAE-CD	2017 - 2022	Ohio	Midwest
Coastline Community College	CAE-CD	2019 - 2024	California	Southwest
College of DuPage	CAE-CD	2017 - 2027	Illinois	Midwest
College of Eastern Idaho	CAE-CD	2021 - 2026	Idaho	Northwest
College of Southern Maryland	CAE-CD	2014 - 2020	Maryland	Northeast
College of Southern Nevada	CAE-CD	2018 - 2023	Nevada	Southwest
Collin College	CAE-CD	2022 - 2027	Texas	Southwest
Columbia Basin College	CAE-CD	2017 - 2022	Washington	Northwest
Columbus State Community College	CAE-CD	2019 - 2024	Ohio	Midwest
Community College of Rhode Island	CAE-CD	2018 - 2023	Rhode Island	Northeast

Institution Name	CAE Type	CAE-CD Years	State	Region
Cosumnes River College	CAE-CD	2021 - 2026	California	Southwest
County College of Morris	CAE-CD	2017 - 2022	New Jersey	Northeast
Cypress College	CAE-CD	2018 - 2023	California	Southwest
Danville Community College	CAE-CD	2017 - 2022	Virginia	Northeast
Delta College	CAE-CD	2019 - 2024	Michigan	Midwest
Eastern Florida State College	CAE-CD	2022 - 2027	Florida	Southeast
Edmonds College	CAE-CD	2017 - 2022	Washington	Northwest
El Paso Community College	CAE-CD	2018 - 2023	Texas	Southwest
Estrella Mountain Community College	CAE-CD	2019 - 2024	Arizona	Southwest
Excelsior College	CAE-CD	2019 - 2024	New York	Northeast
Fayetteville Technical Community College	CAE-CD	2018 - 2023	North Carolina	Southeast
Florida State College at Jacksonville	CAE-CD	2018 - 2023	Florida	Southeast
Forsyth Technical Community College	CAE-CD	2019 - 2024	North Carolina	Southeast
Fullerton College	CAE-CD	2022 - 2027	California	Southwest
Gaston College	CAE-CD	2022 - 2027	North Carolina	Southeast
Germanna Community College	CAE-CD	2019 - 2024	Virginia	Northeast
Glendale Community College	CAE-CD	2019 - 2024	Arizona	Southwest
Grand Rapids Community College	CAE-CD	2018 - 2023	Michigan	Midwest
Great Falls College Montana State University	CAE-CD	2019 - 2024	Montana	Northwest
Green River College	CAE-CD	2018 - 2023	Washington	Northwest
Guilford Technical Community College	CAE-CD	2022 - 2027	North Carolina	Southeast
Gwinnett Technical College	CAE-CD	2020 - 2025	Georgia	Southeast
Hagerstown Community College	CAE-CD	2021 - 2026	Maryland	Northeast
Harford Community College	CAE-CD	2021 - 2026	Maryland	Northeast
Henry Ford College	CAE-CD	2017 - 2022	Michigan	Midwest
Highline College	CAE-CD	2021 - 2026	Washington	Northwest
Hill College	CAE-CD	2019 - 2024	Texas	Southwest
Honolulu Community College	CAE-CD	2014 - 2021	Hawaii	Southwest
Hood College	CAE-CD	2022 - 2027	Maryland	Northeast
Houston Community College	CAE-CD	2017 - 2022	Texas	Southwest
Howard Community College	CAE-CD	2014 - 2020	Maryland	Northeast
Hudson County Community College	CAE-CD	2022 - 2027	New Jersey	Northeast
Indian River State College	CAE-CD	2018 - 2023	Florida	Southeast

Institution Name	CAE Type	CAE-CD Years	State	Region
Ivy Tech Community College	CAE-CD	2017 - 2022	Indiana	Midwest
Jackson State Community College	CAE-CD	2017 - 2022	Tennessee	Southeast
John A Logan College	CAE-CD	2016 - 2027	Illinois	Midwest
Johnson County Community College	CAE-CD	2019 - 2024	Kansas	Midwest
Lake Superior College	CAE-CD	2017 - 2022	Minnesota	Midwest
Lakeland Community College	CAE-CD	2022 - 2027	Ohio	Midwest
Lansing Community College	CAE-CD	2019 - 2024	Michigan	Midwest
Laredo College	CAE-CD	2018 - 2023	Texas	Southwest
Laurel Ridge Community College	CAE-CD	2016 - 2027	Virginia	Northeast
Leeward Community College	CAE-CD	2018 - 2023	Hawaii	Southwest
Lehigh Carbon Community College	CAE-CD	2018 - 2023	Pennsylvania	Northeast
Lemoyne-Owen College	CAE-CD	2019 - 2024	Tennessee	Southeast
Lincoln Land Community College	CAE-CD	2018 - 2023	Illinois	Midwest
Long Beach City College	CAE-CD	2018 - 2023	California	Southwest
Macomb Community College	CAE-CD	2019 - 2024	Michigan	Midwest
Madison College	CAE-CD	2019 - 2024	Wisconsin	Midwest
McLennan Community College	CAE-CD	2019 - 2024	Texas	Southwest
Mercy College	CAE-CD	2021 - 2026	New York	Northeast
Metropolitan Community College	CAE-CD	2018 - 2023	Nebraska	Midwest
Metropolitan Community College - Kansas City	CAE-CD	2018 - 2023	Missouri	Midwest
Miami Dade College	CAE-CD	2022 - 2027	Florida	Southeast
Missoula College	CAE-CD	2017 - 2022	Montana	Northwest
Mohawk Valley Community College	CAE-CD	2016 - 2028	New York	Northeast
Montgomery College	CAE-CD	2022 - 2027	Maryland	Northeast
Montreat College	CAE-CD	2017 - 2022	North Carolina	Southeast
Moraine Valley Community College	CAE-CD	2021 - 2028	Illinois	Midwest
Mount Aloysius College	CAE-CD	2022 - 2027	Pennsylvania	Northeast
Mountain Empire Community College	CAE-CD	2020 - 2025	Virginia	Northeast
Mt. Hood Community College	CAE-CD	2019 - 2024	Oregon	Northwest
New River Community College	CAE-CD	2022 - 2027	Virginia	Northeast
North Idaho College	CAE-CD	2017 - 2022	Idaho	Northwest
Northampton Community College	CAE-CD	2021 - 2026	Pennsylvania	Northeast
Northeast Community College	CAE-CD	2018 - 2023	Nebraska	Midwest

Institution Name	CAE Type	CAE-CD Years	State	Region
Northern Virginia Community College	CAE-CD	2021 - 2028	Virginia	Northeast
Ohlone College	CAE-CD	2019 - 2024	California	Southwest
Oklahoma City Community College	CAE-CD	2016 - 2027	Oklahoma	Southwest
Owensboro Community and Technical College	CAE-CD	2019 - 2024	Kentucky	Southeast
Pennsylvania Highlands Community College	CAE-CD	2018 - 2023	Pennsylvania	Northeast
Pikes Peak Community College	CAE-CD	2018 - 2023	Colorado	Northwest
Pitt Community College	CAE-CD	2020 - 2025	North Carolina	Southeast
Pittsburgh Technical College	CAE-CD	2020 - 2025	Pennsylvania	Northeast
Portland Community College	CAE-CD	2018 - 2023	Oregon	Northwest
Prince George's Community College	CAE-CD	2014 - 2021	Maryland	Northeast
Pueblo Community College	CAE-CD	2017 - 2022	Colorado	Northwest
Red Rocks Community College	CAE-CD	2017 - 2022	Colorado	Northwest
Roane State Community College	CAE-CD	2020 - 2025	Tennessee	Southeast
Rock Valley College	CAE-CD	2019 - 2024	Illinois	Midwest
Rockland Community College	CAE-CD	2017 - 2022	New York	Northeast
Rose State College	CAE-CD	2014 - 2027	Oklahoma	Southwest
Rowan College at Burlington County	CAE-CD	2022 - 2027	New Jersey	Northeast
Saint Vincent College	CAE-CD	2020 - 2025	Pennsylvania	Northeast
Sampson Community College	CAE-CD	2019 - 2024	North Carolina	Southeast
San Antonio College	CAE-CD	2021 - 2028	Texas	Southwest
Sierra College	CAE-CD	2019 - 2024	California	Southwest
Sinclair Community College	CAE-CD	2012 - 2027	Ohio	Midwest
Snead State Community College	CAE-CD	2017 - 2022	Alabama	Southeast
South Texas College	CAE-CD	2017 - 2022	Texas	Southwest
Southern Maine Community College	CAE-CD	2019 - 2024	Maine	Northeast
Southwest Virginia Community College	CAE-CD	2019 - 2024	Virginia	Northeast
Spokane Falls Community College	CAE-CD	2019 - 2024	Washington	Northwest
St. Louis Community College	CAE-CD	2017 - 2022	Missouri	Midwest
St. Petersburg College	CAE-CD	2019 - 2024	Florida	Southeast
St. Philip's College	CAE-CD	2014 - 2027	Texas	Southwest
Talladega College	CAE-CD	2022 - 2027	Alabama	Southeast
Terra State Community College	CAE-CD	2017 - 2022	Ohio	Midwest
Texas State Technical College Harlingen	CAE-CD	2018 - 2023	Texas	Southwest

Institution Name	CAE Type	CAE-CD Years	State	Region
The College of Westchester	CAE-CD	2022 - 2027	New York	Northeast
The Community College of Baltimore County	CAE-CD	2011 - 2027	Maryland	Northeast
Thomas Nelson Community College	CAE-CD	2017 - 2022	Virginia	Northeast
Tidewater Community College	CAE-CD	2016 - 2021	Virginia	Northeast
Trident Technical College	CAE-CD	2019 - 2024	South Carolina	Southeast
University of Hawaii Maui College	CAE-CD	2019 - 2024	Hawaii	Southwest
Valencia College	CAE-CD	2018 - 2023	Florida	Southeast
Valley Forge Military College	CAE-CD	2017 - 2022	Pennsylvania	Northeast
Virginia Western Community College	CAE-CD	2019 - 2024	Virginia	Northeast
Volunteer State Community College	CAE-CD	2022 - 2027	Tennessee	Southeast
Wake Technical Community College	CAE-CD	2020 - 2025	North Carolina	Southeast
Wallace State Community College	CAE-CD	2022 - 2027	Alabama	Southeast
Walsh College	CAE-CD	2016 - 2027	Michigan	Midwest
Washtenaw Community College	CAE-CD	2020 - 2025	Michigan	Midwest
Waukesha County Technical College	CAE-CD	2017 - 2027	Wisconsin	Midwest
Westchester Community College	CAE-CD	2019 - 2024	New York	Northeast
Whatcom Community College	CAE-CD	2021 - 2028	Washington	Northwest

Appendix C: Participating CAE-CD Colleges

List of CAE-CD two-year colleges that self-selected to participate in this study.

Institution Name	State	Region
Alamance Community College	NC	Southeast
Anne Arundel Community College	MD	Northeast
Augusta Technical College	GA	Southeast
Bismarck State College	ND	Southeast
Bossier Parish Community College	LA	Southwest
Chemeketa Community College	OR	Northwest
Clark State College	IL	Midwest
Coastline College	CA	Southwest
College of Southern Nevada	NV	Southwest
College of Western Idaho	ID	Northwest
Collin college	TX	Southwest
Community College of Rhode Island	RI	Northeast
County College of Morris	NJ	Northeast
Cypress College	CA	Southwest
Eastern New Mexico University-Ruidoso Branch Community College	NM	Southwest
Fayetteville Technical Community College	NC	Southeast
Fullerton College	CA	Southwest
Glendale Community College	AZ	Southwest
Guilford Technical Community College	NC	Southeast
Gwinnett Technical College	GA	Southeast
Hill College	TX	Southwest
Ivy Tech Community College	IN	Midwest
Kapiʻolani Community College	HI	Southwest
Laredo College	TX	Southwest
Leeward CC	HI	Southwest
Long Beach City College	CA	Southwest
Miami Dade College	FL	Southeast
Moraine Valley Community College	IL	Midwest
Northampton Community College	PA	Northeast
Northwood Technical College	WI	Midwest
Ohlone College	CA	Southwest
Prince George's Community College	MD	Northeast
Riverside City College	CA	Southwest
Rockland Community College	NY	Northeast
San Antonio College	TX	Southwest
Sierra College	CA	Southwest
Sinclair Community College	OH	Midwest
Snead State Community College	AL	Southeast
St. Cloud Technical & Community College	MN	Midwest

Appendix D: CAE-CD Program Data Collection Form

Research Study Participation

My name is Tobi West. I am a doctoral candidate in the Computer and Cyber Sciences Department at Dakota State University. I am conducting a research study as part of the requirements of my degree in Cyber Defense and I would like to invite you to participate. Results of the study will be shared with the CAE Community to aid in program development.

The goal of this phase of the study is to gather perceptions of cybersecurity employment outcomes. If you choose to participate, you will be asked to complete a survey about your cybersecurity program. In particular, you will be asked questions about your college's Center of Academic Excellence in Cyber Defense (CAE-CD) Program of Study (PoS), the work roles of the NICE Framework aligned to your program, and the supporting resources made available to students in your program.

After completing the online survey, you will be asked to contact alumni of your CAE-CD PoS that graduated between fall 2019 and spring 2022. The email you send to your alumni will include a survey to ask them about their current work role and the alignment to the NICE Framework work roles.

Participation is confidential and voluntary. You may refuse or discontinue participation at any time without penalty or loss of benefits to which you may otherwise be entitled. The results of the study may be published or presented at professional meetings, but your identity will not be revealed. If interested, your college may choose to be named in the study. Study information will be kept in a secure location.

I am happy to answer any questions you have about the study. You may contact me at the e-mail address below.

The survey is expected to take between 10-12 minutes. If you would like to participate, please complete the survey. When you are done with the survey, please contact me at the email listed below to discuss additional steps.

Thank you for your consideration.

With kind regards,

Tobi West

Tobi West, CISSP
Doctoral Candidate
Dakota State University
tobi.west@trojans.dsu.edu

If you have any questions about the rights of research subjects or research-related injury, please contact the DSU IRB office by email at IRB@dsu.edu or by phone at 605-256-5100.

* 1. Do you consent to voluntarily participate in this study?

- ◯ Yes, I consent to participate in this study.
- ◯ No, I do not wish to participate in this study.

CAE-CD Point of Contact

* 2. Your first and last name

* 3. Your email address

4. Your phone number

* 5. CAE-CD institution name

* 6. CAE-CD institution location (city & state)

* 7. CAE-CD Program of Study title
(e.g., AS in Cybersecurity, AAS in Information Security, Certificate of Achievement in Computer Science)

* 8. CAE-CD Program of Study catalog description

* 9. Cyber Center webpage (URL)

* 10. Which of the NICE Framework categories is your CAE-CD Program of Study aligned with? (select all that apply)

- [ ] **DESIGN and DEVELOPMENT** (DD)
  Conducts research, conceptualizes, designs, and develops secure technology systems and networks.
- [ ] **IMPLEMENTATION and OPERATION** (IO)
  Provides the implementation, support, administration, and maintenance necessary to ensure effective and efficient technology system performance and security.
- [ ] **OVERSIGHT and GOVERNANCE** (OG)
  Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.
- [ ] **PROTECTION and DEFENSE** (PD)
  Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.
- [ ] **INTELLIGENCE** (IN)
  Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for national intelligence.
- [ ] **CYBERSPACE EFFECTS** (CE)
  Plans, supports, and executes cybersecurity for cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

* 11. Choose the work role(s) that are most closely associated with your institution's CAE-CD Program of Study. (up to 5)

- [ ] **Authorizing Official** OG-WRL-001
  Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation.
- [ ] **Communications Security (COMSEC) Management** OG-WRL-002
  Responsible for managing the Communications Security (COMSEC) resources of an organization.
- [ ] **Curriculum Development** OG-WRL-003
  Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques based on instructional needs and requirements.
- [ ] **Executive Leadership** OG-WRL-004
  Responsible for establishing vision and direction for an organization's cybersecurity resources and operations. Possesses authority to make and execute decisions that impact an organization broadly.
- [ ] **Instruction** OG-WRL-005
  Responsible for developing and conducting cybersecurity awareness, training, or education.
- [ ] **Legal Advice** OG-WRL-006
  Responsible for providing cybersecurity-related legal advice and recommendations.
- [ ] **Policy and Planning** OG-WRL-007
  Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
- [ ] **Privacy Compliance** OG-WRL-008
  Responsible for developing and overseeing an organization's privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs.
- [ ] **Product Support** OG-WRL-009
  Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components.
- [ ] **Program Management** OG-WRL-010
  Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment with agency or organizational priorities.

- [ ] **Project Management** OG-WRL-011
  Responsible for overseeing and directly managing cybersecurity projects. Tracks and communicates project status and demonstrates project value to the organization. Ensures cybersecurity is built into projects to protect the organization's critical infrastructure and assets, reduce risk, and meet organizational goals.

- [ ] **Security Control Assessment** OG-WRL-012
  Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.

- [ ] **Systems Management** OG-WRL-013
  Responsible for managing the cybersecurity of a program, organization, system, or enclave.

- [ ] **Technology Portfolio Management** OG-WRL-014
  Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities.

- [ ] **Technology Program Auditing** OG-WRL-015
  Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards.

- [ ] **Workforce Management** OG-WRL-016
  Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, education, and hiring processes. Makes adjustments in response to or in anticipation of changes to cybersecurity-related policy, technology, and staffing needs and requirements.

- [ ] **Enterprise Architecture** DD-WRL-001
  Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures.

- [ ] **Research and Development** DD-WRL-002
  Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecurity. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

- [ ] **Security Architecture** DD-WRL-003
  Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.

- [ ] **Software Assessment** DD-WRL-004
  Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable results.

- [ ] **Software Development** DD-WRL-005
  Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs.

- [ ] **System Testing and Evaluation** DD-WRL-006
  Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings.

- [ ] **Systems Development** DD-WRL-007
  Responsible for designing, developing, testing, and evaluating system security throughout the systems development life cycle.

- [ ] **Systems Requirements Planning** DD-WRL-008
  Responsible for consulting with customers to evaluate and translate functional requirements and integrating security policies into technical solutions.

- [ ] **Data Analysis** IO-WRL-001
  Responsible for analyzing data from multiple disparate sources to provide security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.

- [ ] **Database Administration** IO-WRL-002
  Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.

- [ ] **Knowledge Management** IO-WRL-003
  Responsible for managing and administering processes and tools to identify, document, and access an organization's intellectual capital.

- [ ] **Network Management** IO-WRL-004
  Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments.

- [ ] **System Administration** IO-WRL-005
  Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation.

- [ ] **Systems Analysis** IO-WRL-006
  Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages the security aspects of implementing and operating a system.

- [ ] **Technical Support** IO-WRL-007
  Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes.

- [ ] **Cybercrime Investigation** PD-WRL-001
  Responsible for conducting detailed investigations of cyberspace-based crimes to establish documentary or physical evidence, including digital media and logs associated with intrusion incidents. Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

- [ ] **Cyberspace Defense** PD-WRL-002
  Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.

- [ ] **Digital Forensics** PD-WRL-003
  Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation.

- [ ] **Incident Response** PD-WRL-004
  Responsible for investigating, analyzing, and responding to network cybersecurity incidents.

- [ ] **Infrastructure Support** PD-WRL-005
  Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity.

- [ ] **Threat Analysis** PD-WRL-006
  Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat/warning assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.

- [ ] **Vulnerability Analysis** PD-WRL-007
  Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.

- [ ] **All-Source Analysis** IN-WRL-001
  Responsible for analyzing data and information from one or multiple sources to conduct preparation of the environment, responding to requests for information, and submitting intelligence collection and production requirements in support of intelligence planning and operations.

- [ ] **All-Source Collection Management** IN-WRL-002
  Responsible for identifying collection authorities and environment; incorporating priority information requirements into intelligence collection management; determining capabilities of available intelligence collection assets and identifying new capabilities; constructing and disseminating intelligence collection plans; and monitoring execution of intelligence collection tasks to ensure effective execution of collection plans.

Appendix E: CAE-CD Alumni Data Collection Form

Research Study Participation

Hello,

My name is Tobi West. I am a doctoral candidate in the Computer and Cyber Sciences Department at Dakota State University. I am conducting a research study as part of the requirements of my degree in Cyber Defense and I would like to invite you to participate. Results of the study will be shared with community colleges across the country to increase awareness about the outcomes and benefits of cybersecurity education.

The goal of this phase of the study is to gather alumni perceptions of cybersecurity employment outcomes. If you choose to participate, you will be asked to complete a survey about the cybersecurity program you attended. In particular, you will be asked questions about your employment and the supporting resources made available to you while in college.

Participation is confidential and voluntary. You may refuse or discontinue participation at any time without penalty or loss of benefits to which you may otherwise be entitled. Study information will be kept in a secure location. The results of the study may be published or presented at professional meetings, but your identity will not be revealed. Your college may choose to be named in the study, but your participation will be kept confidential.

I am happy to answer any questions you have about the study. You may contact me at the e-mail address below.

The survey is expected to take between 12-14 minutes. Thank you for your consideration. If you would like to participate, please complete the survey.

With kind regards,

Tobi West

Tobi West, CISSP
Doctoral Candidate
Dakota State University
tobi.west@trojans.dsu.edu

If you have any questions about the rights of research subjects or research-related injury, please contact the DSU IRB office by email at IRB@dsu.edu or by phone at 605-256-5100.

* 1. Do you consent to voluntarily participate in this study?

- ◯ Yes, I consent to participate in this study.
- ◯ No, I do not wish to participate in this study.

College Information

These questions refer back to the two-year college that contacted you to participate in this study.

* 2. Have you completed a certificate at Kapi‘olani Community College?

- ◯ Yes
- ◯ No
- ◯ Other (please specify)
- ◯ None of the above

* 3. Title of this certificate
(e.g., Certificate of Achievement in Information Security and Assurance (CO-ISA), AAS in Information Security, Certificate of Achievement in Computer Science)

4. Term in which this certificate was completed

- ◯ 2022 Fall
- ◯ 2022 Spring
- ◯ 2021 Fall
- ◯ 2021 Spring
- ◯ 2020 Fall
- ◯ 2020 Spring
- ◯ 2019 Fall
- ◯ 2019 Spring
- ◯ Other (please specify)

5. Were you awarded any degree(s) prior to completing this associate degree or certificate?

- ◯ Yes
- ◯ No
- ◯ Prefer not to say
- ◯ Other (please specify)

6. List any degree(s) completed prior to this certificate, if applicable.

Employment

7. Are you currently employed?

- ◯ Yes
- ◯ No
- ◯ Prefer not to answer
- ◯ Other (please specify)

Cybersecurity Employment

8. Title of your employment position

9. Company/Organization name

10. Are you currently working in a role that includes tasks related to technology (e.g., cybersecurity, information technology, software development, threat intelligence, etc.)?

- ◯ Yes
- ◯ No
- ◯ Prefer not to answer
- ◯ Other (please specify)

Work Roles and College Preparation

Review the following work roles from NICE Framework call for comments published on April 18, 2023. Then complete the remaining questions about your college experience.

* 11. Considering your current tasks at work, choose the work role(s) that are most closely associated. (up to 5)

- ☐ **Authorizing Official** OG-WRL-001
  Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation.
- ☐ **Communications Security (COMSEC) Management** OG-WRL-002
  Responsible for managing the Communications Security (COMSEC) resources of an organization.
- ☐ **Curriculum Development** OG-WRL-003
  Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques based on instructional needs and requirements.
- ☐ **Executive Leadership** OG-WRL-004
  Responsible for establishing vision and direction for an organization's cybersecurity resources and operations. Possesses authority to make and execute decisions that impact an organization broadly.
- ☐ **Instruction** OG-WRL-005
  Responsible for developing and conducting cybersecurity awareness, training, or education.
- ☐ **Legal Advice** OG-WRL-006
  Responsible for providing cybersecurity-related legal advice and recommendations.
- ☐ **Policy and Planning** OG-WRL-007
  Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
- ☐ **Privacy Compliance** OG-WRL-008
  Responsible for developing and overseeing an organization’s privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs.
- ☐ **Product Support** OG-WRL-009
  Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components.
- ☐ **Program Management** OG-WRL-010
  Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment with agency or organizational priorities.
- ☐ **Project Management** OG-WRL-011
  Responsible for overseeing and directly managing cybersecurity projects. Tracks and communicates project status and demonstrates project value to the organization. Ensures cybersecurity is built into projects to protect the organization’s critical infrastructure and assets, reduce risk, and meet organizational goals.
- ☐ **Security Control Assessment** OG-WRL-012
  Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.

- [ ] **Systems Management** OG-WRL-013
  Responsible for managing the cybersecurity of a program, organization, system, or enclave.

- [ ] **Technology Portfolio Management** OG-WRL-014
  Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities.

- [ ] **Technology Program Auditing** OG-WRL-015
  Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards.

- [ ] **Workforce Management** OG-WRL-016
  Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, education, and hiring processes. Makes adjustments in response to or in anticipation of changes to cybersecurity-related policy, technology, and staffing needs and requirements.

- [ ] **Enterprise Architecture** DD-WRL-001
  Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures.

- [ ] **Research and Development** DD-WRL-002
  Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecurity. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

- [ ] **Security Architecture** DD-WRL-003
  Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.

- [ ] **Software Assessment** DD-WRL-004
  Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable results.

- [ ] **Software Development** DD-WRL-005
  Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs.

- [ ] **System Testing and Evaluation** DD-WRL-006
  Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings.

- [ ] **Systems Development** DD-WRL-007
  Responsible for designing, developing, testing, and evaluating system security throughout the systems development life cycle.

- [ ] **Systems Requirements Planning** DD-WRL-008
  Responsible for consulting with customers to evaluate and translate functional requirements and integrating security policies into technical solutions.

- [ ] **Data Analysis** IO-WRL-001
  Responsible for analyzing data from multiple disparate sources to provide security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.

- [ ] **Database Administration** IO-WRL-002
  Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.

- [ ] **Knowledge Management** IO-WRL-003
  Responsible for managing and administering processes and tools to identify, document, and access an organization's intellectual capital.

- [ ] **Network Management** IO-WRL-004
  Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments.

- [ ] **System Administration** IO-WRL-005
  Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation.

- [ ] **Systems Analysis** IO-WRL-006
  Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages the security aspects of implementing and operating a system.

- [ ] **Technical Support** IO-WRL-007
  Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes.

- [ ] **Cybercrime Investigation** PD-WRL-001
  Responsible for conducting detailed investigations of cyberspace-based crimes to establish documentary or physical evidence, including digital media and logs associated with intrusion incidents. Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

- [ ] **Cyberspace Defense** PD-WRL-002
  Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.

- [ ] **Digital Forensics** PD-WRL-003
  Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation.

- [ ] **Incident Response** PD-WRL-004
  Responsible for investigating, analyzing, and responding to network cybersecurity incidents.

- [ ] **Infrastructure Support** PD-WRL-005
  Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity.

- [ ] **Threat Analysis** PD-WRL-006
  Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat/warning assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.

- [ ] **Vulnerability Analysis** PD-WRL-007
  Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.

- [ ] **All-Source Analysis** IN-WRL-001
  Responsible for analyzing data and information from one or multiple sources to conduct preparation of the environment, responding to requests for information, and submitting intelligence collection and production requirements in support of intelligence planning and operations.

- [ ] **All-Source Collection Management** IN-WRL-002
  Responsible for identifying collection authorities and environment; incorporating priority information requirements into intelligence collection management; determining capabilities of available intelligence collection assets and identifying new capabilities; constructing and disseminating intelligence collection plans; and monitoring execution of intelligence collection tasks to ensure effective execution of collection plans.

- [ ] **All-Source Collection Requirements Management** IN-WRL-003
  Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of intelligence collection requirements. Evaluates performance of intelligence collection assets and operations.

- [ ] **Intelligence Planning** IN-WRL-004
  Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

- [ ] **Multi-Disciplined Language Analysis** IN-WRL-005
  Responsible for processing, analyzing, and disseminating intelligence information derived from language, voice, and graphic material. Creates and maintains language-specific databases and working aids and provide subject-matter expertise in foreign language-intensive or interdisciplinary projects.

- [ ] **Cyber Operations** CE-WRL-001
  Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conducts collection, processing, and geolocation of systems to exploit, locate, and track targets. Performs network navigation and tactical forensic analysis and executes on-net operations when directed.

- [ ] **Cyber Operations Planning** CE-WRL-002
  Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integration during the execution of cyber actions.

- [ ] **Exploitation Analysis** CE-WRL-003
  Responsible for identifying access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

- [ ] **Mission Assessment** CE-WRL-004
  Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; and determining whether systems perform as expected.

- [ ] **Partner Integration** CE-WRL-005
  Responsible for developing assessment plans and performance measures; determining whether systems performed as expected; and conducting strategic and operational mission effectiveness assessments.

- [ ] **Target Development** CE-WRL-006
  Responsible for performing target system analysis and building and maintaining electronic target folders to include inputs from environment preparation and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

- [ ] **Target Network Analysis** CE-WRL-007
  Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; and developing techniques to gain target information. Determines how targets communicate, move, operate, and live based on knowledge of target technologies, digital networks, and applications.

* 12. Please select any extra-curricular and/or co-curricular career preparation resources that you participated in while pursuing this certificate.
(select all that apply)

- [ ] Apprenticeship
- [ ] Capture the flag (CTF) competition
- [ ] Cybersecurity competition(s)
- [ ] Hands-on labs
- [ ] Industry certification exam voucher
- [ ] Other (please specify)
- [ ] Industry speakers
- [ ] Internship
- [ ] Student Club
- [ ] Summer camp
- [ ] None of the above

13. List any industry certification received since beginning this cybersecurity program.

14. Rate how important this cybersecurity program was to your preparation for your current work role.

Very Unimportant	Unimportant	Neutral	Important	Very Important
★	★	★	★	★

15. Describe how the college's program and resources helped you prepare for your current employment position.

* 16. After completing this certificate, have you continued your education in another program?

- ◯ Yes
- ◯ No
- ◯ Other (please specify)

17. Additional Comment

Demographics (optional)

This section is optional. Demographic information is being collected to compare the results of this study to the demographics of the national cybersecurity workforce.

18. Gender identity

- [ ] Female
- [ ] Male
- [ ] Non-Binary
- [ ] Prefer not to answer
- [ ] Other (please specify)

19. Race/Ethnic identity

- ( ) American Indian or Alaska Native
- ( ) Asian
- ( ) Black or African American
- ( ) Hispanic or Latino
- ( ) Native Hawaiian or Other Pacific Islander
- ( ) White
- ( ) Prefer not to answer
- ( ) Other (please specify)

Appendix F: Work Roles Selected by POCs and Alumni

	Work Role	ID	POC (n_1=39)	Alumni (n_2=90)
OVERSIGHT AND GOVERNANCE (OG)	Authorizing Official	OG-WRL-001	0	9
	Communications Security (COMSEC) Management	OG-WRL-002	1	3
	Curriculum Development	OG-WRL-003	4	2
	Executive Leadership	OG-WRL-004	0	1
	Instruction	OG-WRL-005	9	2
	Legal Advice	OG-WRL-006	0	0
	Policy and Planning	OG-WRL-007	0	3
	Privacy Compliance	OG-WRL-008	0	2
	Product Support	OG-WRL-009	0	2
	Program Management	OG-WRL-010	2	3
	Project Management	OG-WRL-011	0	5
	Security Control Assessment	OG-WRL-012	1	2
	Systems Management	OG-WRL-013	5	10
	Technology Portfolio Management	OG-WRL-014	0	1
	Technology Program Auditing	OG-WRL-015	0	4
	Workforce Management	OG-WRL-016	1	0
DESIGN AND DEVELOPMENT (DD)	Enterprise Architecture	DD-WRL-001	1	5
	Research and Development	DD-WRL-002	0	3
	Security Architecture	DD-WRL-003	3	6
	Software Assessment	DD-WRL-004	2	9
	Software Development	DD-WRL-005	1	1
	System Testing and Evaluation	DD-WRL-006	3	7
	Systems Development	DD-WRL-007	3	1
	Systems Requirements Planning	DD-WRL-008	0	2
IMPLEMENTATION AND OPERATION (IO)	Data Analysis	IO-WRL-001	1	2
	Database Administration	IO-WRL-002	0	4
	Knowledge Management	IO-WRL-003	0	4
	Network Management	IO-WRL-004	25	11
	System Administration	IO-WRL-005	30	22
	Systems Analysis	IO-WRL-006	6	4
	Technical Support	IO-WRL-007	22	30
PROTECTION AND DEFENSE (PD)	Cybercrime Investigation	PD-WRL-001	2	2
	Cyberspace Defense	PD-WRL-002	4	7
	Digital Forensics	PD-WRL-003	5	6
	Incident Response	PD-WRL-004	11	10
	Infrastructure Support	PD-WRL-005	9	6
	Threat Analysis	PD-WRL-006	3	6
	Vulnerability Analysis	PD-WRL-007	11	6

	Work Role	ID	POC (n_1=39)	Alumni (n_2=90)
INTELLIGENCE (IN)	All-Source Analysis	IN-WRL-001	0	4
	All-Source Collection Management	IN-WRL-002	0	1
	All-Source Collection Requirements Management	IN-WRL-003	0	1
	Intelligence Planning	IN-WRL-004	0	0
	Multi-Disciplined Language Analysis	IN-WRL-005	0	0
CYBERSPACE EFFECTS (CE)	Cyber Operations	CE-WRL-001	4	1
	Cyber Operations Planning	CE-WRL-002	0	2
	Exploitation Analysis	CE-WRL-003	1	1
	Mission Assessment	CE-WRL-004	0	0
	Partner Integration	CE-WRL-005	1	0
	Target Development	CE-WRL-006	0	0
	Target Network Analysis	CE-WRL-007	1	1

Appendix G: Industry-Recognized Certification of Alumni

Organization and Certification Title	Alumni Response (n_2=90)
CompTIA	
CompTIA Security+	18
CompTIA A+	10
CompTIA Network+	8
CompTIA CySA+	6
CompTIA PenTest+	5
CompTIA Server+	4
CompTIA CASP+	3
CompTIA Linux+	2
CompTIA Project+	1
International Information System Security Certification Consortium	
(ISC)2 Certified Information Systems Security Professional (CISSP)	2
(ISC)2 CISSP Information Systems Security Architecture Professional (ISSAP)	2
(ISC)2 Systems Security Certified Practitioner (SSCP)	2
(ISC)2 Certified in Cybersecurity Certification (CC)	2
(ISC)2 Certified Cloud Security Professional (CCSP)	1
Cisco	
Cisco Certified Network Associate (CCNA)	4
Cisco Certified Network Professional (CCNP) Security	1
Cisco Certified CyberOps Associate	1
Global Information Assurance Certification	
GIAC Certified Forensic Examiner (GCFE)	2
GIAC Certified Incident Handler (GCIH)	2
GIAC Foundational Cybersecurity Technologies (GFACT)	1
GIAC Security Essentials (GSEC)	1

Organization and Certification Title	Alumni Response (n_2=90)
Information Systems Audit and Control Association	
ISACA Certified Data Privacy Solutions Engineer™ (CDPSE®)	1
ISACA Certified in Governance of Enterprise IT (CGEIT)	1
ISACA Certified in Risk and Information Systems Control® (CRISC®)	1
ISACA Certified Information Security Manager (CISM)	1
ISACA Certified Information Systems Auditor (CISA)	1
ISACA COBIT Design and Implementation	1
ISACA COBIT Foundations	1
Microsoft	
Microsoft Azure Fundamentals	1
Microsoft 365 Fundamentals	1
Microsoft Security Compliance and Identity Fundamentals	1
Palo Alto Networks	
Palo Alto Networks Certified Network Security Administrator (PCNSA)	3
Palo Alto Networks Certified Network Security Engineer (PCNSE)	1
Palo Alto Networks Certified Security Automation Engineer (PCSAE)	1
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)	1
Additional Certifications	
AccessData Certified Examiner	1
Check Point Certified Security Administrator (CCSA)	1
Help Desk Institute (HDI) Support Center Certification	1
IBM QRadar SIEM SOC Analyst	1
Offensive Security Certified Professional (OSCP)	1
Project Management Institute Project Management Professional (PMP)®	1
Saylor Academy CS120: Bitcoin for Developers	1
Saylor Academy PRDV151: Bitcoin for Everybody	1
Scrum Alliance Certified ScrumMaster (CSM)	1