CCBC Cybersecurity Institute

Trade Adjustment Assistance Community College and Career Training Grant Evaluation Final Report

The Community College of Baltimore County

Cybersecurity Institute

September 29, 2017

IMPAQ INTERNATIONAL LLC

SUBMITTED TO

The Community College of Baltimore County
Cybersecurity Institute

ATTENTION

Ron Hinkel, Director, Cybersecurity Institute
The Community College of Baltimore County
7201 Rossville Boulevard
Baltimore, MD 21237

SUBMITTED BY

IMPAQ International, LLC
10420 Little Patuxent Parkway
Suite 300
Columbia, MD 21044
(443) 256-5500
www.impaqint.com

PROJECT

The Community College of Baltimore County (CCBC) Cybersecurity Institute: Third-Party Evaluation Services for the Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant

TASK & DELIVERABLE

Task 3, Analysis and Reporting
Final Evaluation Report

AUTHORS

Nicholas Bill, M.P.P., IMPAQ International
Sandeep Shetty, Ph.D., IMPAQ International
Karen Armstrong, Ph.D., IMPAQ International
Andres Romualdo, M.A., IMPAQ International
Clancy Bertane, M.P.P., IMPAQ International

Table of Contents

Disclaimer

Executive Summary

I. CCBC Cybersecurity Institute TAACCCT Program Overview

In July 2013, the U.S. Department of Labor (DOL) awarded a $2.5 million Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant to the Community College of Baltimore County (CCBC). CCBC used this grant to expand the Cybersecurity Institute (CI) and enhance training in cybersecurity, information systems security, and network technology. The program's design and evidence-based strategies incorporate each of the six core TAACCCT elements[1] and address a critical need to align Maryland's education and training programs to meet the growing demand for skilled cybersecurity workers.[2]

Specific objectives of the program were to:

- Expand the CI's existing training capacity and increase enrollment among unemployed and underemployed individuals, dislocated workers, veterans, and TAA-eligible workers.
- Enhance online and technology-enabled learning by developing a virtual infrastructure and incorporating new training equipment.
- Create new accelerated stacked credentials programs to reduce the time required to earn industry certifications.
- Revise, update, and add industry-vetted curricula for degree or certification at the post-secondary level.
- Develop strategic partnerships for recruitment, training, and employment opportunities.

II. Evaluation Design Summary

As part of the TAACCCT funding requirements, grantees were required to engage a third-party independent evaluator to evaluate the grant initiative. In January 2014, CCBC awarded a contract to IMPAQ International, LLC (IMPAQ) to conduct an implementation study and

[1] The six core elements required of TAACCCT grantees are (1) evidence-based design, (2) stacked and latticed credentials, (3) transferability and articulation of credit, (4) advanced online and technology-enabled learning, (5) strategic alignment, and (6) alignment with previously funded TAACCCT projects.

[2] Alexander, Candy. "The Cybersecurity Skills Gap." *SC Magazine.* December 2014. Retrieved from http://www.scmagazine.com/the-cybersecurity-skills-gap/article/385079/. "Lack of Cybersecurity Skills Makes Firms a Hacker Target." National Cybersecurity Institute. August 2016. Retrieved from http://www.nationalcybersecurityinstitute.org/general-public-interests/lack-of-cybersecurity-skills-makes-firms-a-hacker-target/

outcomes analysis of the CI program. The objectives, data sources, and analysis methods for these two evaluation components are summarized below.

Implementation Study. The broad objectives were to gain an in-depth understanding of all program components; examine implementation fidelity throughout the project; and explore program successes, challenges, and lessons learned. General research topics included (1) program context, (2) program design, (3) program participation, (4) strategic partnerships, (5) program management and sustainability, (6) program implementation outcomes, and (7) promising practices and lessons learned. In the evaluation design stage, we worked closely with CCBC to finalize a program logic model by confirming the program's main inputs, activities, outputs, and anticipated outcomes. Using this logic model, we developed a list of detailed research questions within each topic area. To investigate these questions, we relied on information collected through site visits, key informant interviews, document review, focus groups, and participant-level datasets.

Outcomes Analysis. The objective of our outcomes analysis was to provide a detailed analysis of the socioeconomic characteristics and education and employment outcomes of program participants. Key research questions included:

- What were the participants' education outcomes, such as credits earned and credentials attained?
- What were the participants' employment and earnings outcomes following program completion? In what industries did participants find employment?
- Were any socioeconomic characteristics associated with differences in key outcomes, including program completion, educational achievements, and employment?
- How did observed participant outcomes compare to what was projected by CCBC, and what were the reasons for any differences?

The analysis relied on program participation data, educational achievement data, and administrative wage record data collected by CCBC. Although encouraged by DOL to use experimental or quasi-experimental methods to estimate CI program impacts, we were unable to do so because random assignment of participants was not feasible and because the projected sample size was insufficient to detect impacts unless the impacts were extremely large. Although our analysis cannot establish a causal link between participant outcomes and program participation, the results provide valuable information for assessing the program's possible impacts.

III. Implementation Study Findings

Despite a compressed schedule, CCBC was able to achieve its proposed program start-up milestones—including all facilities alterations and equipment procurement and installation—within the first year. CCBC then shifted its focus to other program activities such as participant

outreach and recruitment, curricula updates and enhancements, developing new stackable credentials programs, and cultivating strategic partnerships. Key observations of the program's achievements from our implementation study are summarized below.

- ***Increased training capacity.*** To address significant increases in enrollment, CCBC developed a virtual training infrastructure using Linux Virtualization equipment and VMWare workstations to create a virtual desktop interface for students. This enhancement provided students with unprecedented access to cybersecurity training across CCBC campuses and anywhere outside of the classroom.

- ***Advanced technology-enabled learning.*** CCBC enhanced cybersecurity-related curricula by incorporating new, advanced training equipment considered to represent the "gold standard" in the industry. This equipment enabled new hands-on learning exercises for students, including "attack-and-defend" scenarios, which provide valuable experience that students can then demonstrate to potential employers.

- ***Updates to existing curricula.*** CCBC used grant funding to make important changes to its existing information systems security and network technology program curricula. The changes included (1) systematically reviewing and updating curricula to maintain the "A" designation in Information Assurance/Cyber Defense from the Centers of Academic Excellence established by the National Security Agency (NSA) and (2) updating course material to stay current with changes in industry certification exams.[3] Incorporating the new training equipment also necessitated enhancements to existing curricula.

- ***New accelerated stackable credentials programs.*** CCBC responded to employer requests to reduce the time required for students and workers to obtain industry certifications by creating two accelerated stackable credentials programs: (1) the U.S. Department of Defense 8570 Stackable Certifications Program and (2) the Networking Certificate Program. Students can now complete blended certification courses (50 percent online) in just four weeks, rather than the standard 16-week semester. Although some employers wished that CCBC had gone further, the entirely new courses they wanted were not within the program scope.[4]

- ***Strategic partnerships.*** CCBC successfully engaged prior community college TAACCCT grantees[5] to gather information on lessons learned and strategies for developing the program and serving participants. Engagement with the public workforce system to coordinate outreach to target populations was lacking at first, but it later improved with support from the TAACCCT 4 Cyber Pathways Across Maryland outreach director. CCBC staff successfully engaged employers from the Baltimore-Washington

[3] Specifically, Cisco, A+, and Network+ certifications.

[4] CCBC did develop a new digital forensics course, not funded by TAACCCT, during the program's period of performance. The course was approved by the Maryland Higher Education Commission.

[5] Anne Arundel Community College (Round 1 TAACCCT) and Prince George's Community College (Round 2 TAACCCT).

area throughout the program to (1) identify job and internship opportunities for students, (2) facilitate guest lectures in class, and (3) organize tours of CCBC facilities for employers and tours of employer facilities for students. Some CCBC staff suggested that employers' most important contribution was to sponsor internships; however, internship opportunities were lacking. Instead, employer partnerships mostly involved employer representatives serving as guest lecturers.

IV. Outcomes Analysis Findings

Exhibit ES1 compares actual participant outcomes for four key measures to CCBC's projected goals. CCBC served a much higher number of participants than was initially targeted (202 served versus 130 projected), but fell short of the other three outcome targets.

Exhibit ES1. Summary of Observed Participant Outcomes Compared to Grant Goals

Key Outcome Category	Goal	Actual	Difference	Goal Met?
1. Participants served (program enrollment)	130	202	72	Yes
2. Program completers [a]	105	93	(12)	No
3. Total participants earning credentials [b]	105	93	(17)	No
4. Program completers employed [c]	50	16	(34)	No

[a] Defined as the number of participants earning a degree or completing coursework required to earn a CCBC certificate or degree. Most of these participants, though they completed enough hours to earn a certificate, were still enrolled at the end of the evaluation period; many were seeking a degree.
[b] Since program completion was defined as attaining or qualifying for a CCBC certificate or degree; therefore, the total participants earning credentials is the same as total completers.
[c] Does not include employment outcomes for incumbent workers, per DOL requirements.

Although CCBC fell short of meeting three outcome targets, the results are not necessarily reflective of the program's effectiveness. The observed outcomes may well be underestimated due to the following evaluation limitations and program characteristics:

- Most program participants were pursuing a two-year AAS degree. Many students who completed enough coursework to qualify for a certificate and were therefore counted, in accordance with DOL guidance, as program completers were still enrolled during the evaluation follow-up period. They may not seek employment until after earning a degree. Furthermore, part-time students are unlikely to complete the degree requirements within two years. In other TAACCCT programs that focus on shorter-term training, participants exit the program and start their job search in a much shorter time.

- The employment and earnings data used for the evaluation spans the fourth quarter of 2013 to the fourth quarter of 2016. Thus, employment outcomes for participants completing the program in 2017 are not captured in our analysis.

- Participants who obtained employment outside the state of Maryland or in the federal government were not covered by the employment and earnings data source.

- CCBC cannot count employment outcomes for incumbent workers, who comprised 56 percent of program participants (114 out of 202). DOL's definition of *incumbent worker* does not consider the type of industry or occupation in which the worker is employed. Given the intent of the program, workers in occupations totally unrelated to information systems security or network technology who obtain training-related employment after completing the program should arguably be considered to have experienced a successful employment outcome.

As noted earlier, the participant outcomes cannot be causally linked to the program given the lack of a comparison group design. Despite this limitation, the analysis provides an indication of the program's overall effectiveness.

V. Key Lessons Learned

- Achieving participant employment outcome goals requires more time for TAACCCT programs that focus on two-year college degree attainment rather than short-term, occupation-specific credentials. Both grant applicants and DOL should take this issue into consideration when proposing and reviewing participant employment projections during the grant application stage.

- The true impact of a TAACCCT program may be obscured or underestimated by the restriction on counting employment outcomes for incumbent workers—as defined by DOL. Not all incumbent workers will be employed in a field related to the training program at the time of enrollment. If these individuals obtain new employment in an occupation that is directly related to the training received, it should be considered a successful outcome given the intent of the program. To more rigorously assess employment outcomes, it would be helpful if grantees could collect more detailed information on the occupations held by incumbent workers before and after program participation.

- CCBC's new accelerated, stackable credentials programs that use hybrid, block-style training approaches are promising models for addressing the workforce needs of employers in the information technology and cybersecurity industries. These flexible models greatly improve access to community college training and significantly shorten the time required for individuals to obtain important—and often required—third-party industry certifications.

- Collaboration with industry experts to select and incorporate new training equipment allowed CCBC to provide students with valuable hands-on learning experiences that weren't previously available. These new opportunities are especially important for students because internship opportunities with industry employers—particularly those in the private sector—can be very difficult to find.

- Program start-up, especially for programs that involve substantial facility alterations and equipment purchases, is a time-consuming process that requires considerable staff resources. It can be difficult for grant staff to concentrate on outreach activities during this period if they have other roles and responsibilities. Therefore, to the extent feasible, grantees should consider including a full-time outreach director position in their staffing structure.

1. Introduction

In July 2013, the U.S. Department of Labor (DOL) awarded a $2.5 million Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant to the Community College of Baltimore County (CCBC). CCBC was a single applicant and received one of 14 state-designated grants from the third round of TAACCCT funding.[6] CCBC used the TAACCCT grant to expand and further develop the Cybersecurity Institute (CI), a comprehensive education and training program designed to train students, TAA-eligible workers, veterans, dislocated workers, and incumbent workers in current cybersecurity and information technology practices. The overarching goal of the grant was to increase and improve CCBC's capacity to attract and train individuals to fill a clearly identified gap in qualified professionals in the cybersecurity industry. Specific objectives of the program included the following:

- Expand the CI's existing training capacity and increase enrollment among unemployed and underemployed individuals, dislocated workers, veterans, and TAA-eligible workers.
- Enhance online and technology-enabled learning by developing a virtual infrastructure and incorporating new training equipment.
- Create new accelerated stacked credentials programs to reduce the time required to earn industry certifications.
- Revise, update, and add industry-vetted curricula for degree or certification at the post-secondary level.
- Develop strategic partnerships for recruitment, training, and employment opportunities.

As part of the TAACCCT funding requirements, grantees were required to engage a third-party independent evaluator to evaluate the grant initiative. In January 2014, CCBC awarded a contract to IMPAQ International, LLC (IMPAQ) to conduct an implementation study and outcomes analysis of the CI program. The objectives for each of these evaluation components are listed below. A detailed list of research questions for each component by topic area is included in the evaluation design report.

- ***Implementation study.*** This evaluation component examines seven research topics related to design and implementation of the program: (1) program context, (2) program design, (3) program participation, (4) partnerships, (5) program management and sustainability, (6) program implementation outcomes, and (7) promising practices and lessons learned. The data used to inform the implementation study include site visits, document reviews, participation data, and a focus group with program participants.

[6] TAACCCT Round 3: Funding Opportunity Number: SGA/DFA PY-12-10.

- ***Outcomes analysis.*** This analysis examines the socioeconomic characteristics and education and employment outcomes of CI program participants. The analysis relies on program participation data, educational achievement data, and administrative wage record data collected by CCBC.

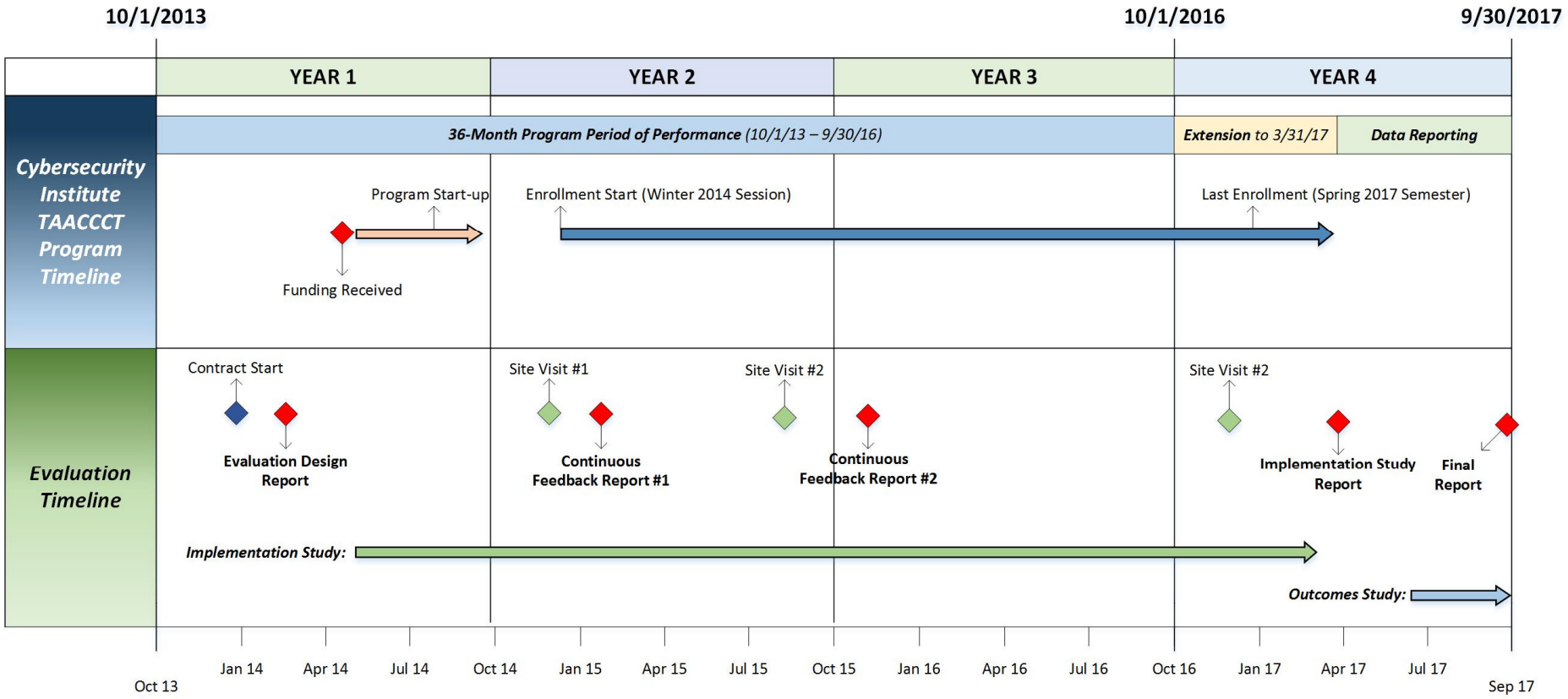
This final evaluation report provides summative implementation evaluation findings, covering the program's entire period of performance from October 2013 through March 2017. It also provides the final participant outcomes analysis results.[7] During the evaluation period (May 2014–September 2017), we submitted four reports to CCBC to document the evaluation activities and results: two continuous feedback reports, in February and December 2015; an interim evaluation report; and a final evaluation report. The continuous feedback reports provided formative feedback on the program's implementation at two points during the period of performance: at the conclusion of Year 1 and through August 2015, near the end of Year 2. The interim evaluation report was submitted in June 2017 after program activities ended. This report focused on the implementation study findings but also discussed preliminary participation and education outcomes.

Exhibit 1 provides an evaluation timeline that shows key evaluation activities and deliverables in relation to the TAACCCT program period of performance.

Chapter 2 of this report presents background on the cybersecurity industry, including a discussion of workforce development challenges and relevant labor market information. Chapter 3 provides an overview of the CI program, including a logic model that identifies the program inputs, outputs, activities, and anticipated outcomes. This chapter also presents a demographic profile of program participants. Chapter 4 presents our implementation study approach and findings, organized around key program activity areas. In Chapter 5, we describe the outcomes analysis methods, present final participant education and employment outcomes results, and discuss limitations of the analysis. Finally, in Chapter 6, we provide a high-level conclusion of our evaluation findings, highlighting program successes, challenges, and lessons learned.

[7] CCBC received a six-month program extension from the original end date of September 30, 2016.

Exhibit 1. Evaluation and Program Period of Performance Timeline



2. Cybersecurity Background and Labor Market Information

2.1 Background

Cybersecurity protects electronic data and information technology (IT) systems from unauthorized access or attacks that may cause damage to hardware, software, and critical information in an organization's operations and to any services the organization provides.

Globally, in 2014 a record 1 billion data records were compromised, affecting both public and private sectors.[8] Additionally, a 2015 PricewaterhouseCoopers report on the State of U.S. Cybercrime Survey found that 79 percent of U.S. executives, security experts, and other public and private sector respondents had detected a security incident in the past 12 months, up from 59 percent the year before.[9] At the federal level, a record 67,000 cyber intrusions were recorded in 2014; according to the director of National Intelligence to the Senate Armed Services Committee, this was a 67 percent increase from 2006.[10] In response to the increase in cyber break-ins, President Obama issued an executive order in April 2015 declaring that "the increasing prevalence and severity of malicious cyber-enabled activities … constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. I hereby declare a national emergency to deal with this threat."[11]

As the technology used for cyberattacks continues to grow and evolve, so does the need for new and advanced cybersecurity methods. To address cyber threats globally, both public and private sectors are expected to increase cybersecurity spending to $170 billion by 2020. This increase in spending is projected to grow the cybersecurity market at a compound annual rate of 9.8 percent from 2015 to 2020.[12] Within the U.S., the federal government continues to be the leading employer in the cybersecurity market; however, private sector organizations that

[8] "Releases Findings of 2014 Breach Level Index." Gemalto. February 2015. Retrieved from http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-2014-Breach-Level-Index.aspx

[9] "US Cybersecurity: Progress Stalled—Key Findings form the 2015 US State of Cybercrime Survey." PricewaterhouseCoopers. July 2015. Retrieved from http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

[10] "Cyber In-Security: Closing the Federal Talent Gap." Booz Allen Hamilton. April 2015. file:///C:/Users/nbill/Downloads/Cyber_In-Security_II__Closing_the_Federal_Talent_Gap-[2015.04.13]%20(1).pdf

[11] "Executive Order—'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities'." White House. April 2015. Retrieved from https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

[12] "Cyber Security Market by Solutions, Services, Security Type, Deployment Mode, Organization Size, Vertical and Region—Global Forecast 2021." Markets and Markets. July 2016. Retrieved from http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

manage large amounts of sensitive customer data, such as those in finance, health care, and retail trade, are quickly catching up.[13]

To keep up with the evolving cybersecurity threats, both public and private sector employers are demanding higher levels of education, skills, and experience from the cybersecurity workforce. According to a 2015 job report, 84 percent of cybersecurity job postings specify at least a bachelor's degree and 83 percent require at least three years of experience.[14] Many employers are also looking for candidates who have specific industry knowledge along with advanced cybersecurity certificates, such as Certified Information Systems Security Professional certification. This certificate requires holders to pass an exam and possess at least five years of information security experience.[15]

Given these unique skill requirements, it has been difficult for employers to find qualified cybersecurity personnel. Worldwide, there are an estimated 300,000 to 1 million vacant cybersecurity positions, roughly 200,000 of which are in the U.S.[16] Locally, the Maryland Department of Labor, Licensing, and Regulation expects the number of cybersecurity-related jobs to increase from 1,727 in 2012 to 10,316 by 2020.[17] This increase in demand is compounded by the large number of current federal workers who are expected to retire in the near future. At the same time, educational institutions are not producing enough graduates with the necessary skills or experience for even entry-level cybersecurity positions. For this reason, CCBC was awarded a TAACCCT grant to further develop, expand, and enhance its CI program and the certificate and degree programs it offers. CCBC's efforts through the grant were intended to address the critical workforce shortage and skills gap issues by improving the pipeline of cybersecurity specialists.

2.2 Labor Market Information

During the Great Recession, Maryland's growth rate in economic activity fell from 4.3 percent in 2007 to 2.6 percent in 2008. It hit a low of 1.8 percent in 2009, the official end date of the recession.[18] Since 2009, Maryland has been on a path of slow recovery, with over 3 percent compounded annual growth rate from 2009 through 2016. Although Maryland's economy has experienced good recovery and has created more jobs, the state still needs to catch up to reach

[13] "Job Market Intelligence: Cybersecurity Jobs, 2015." Burning Glass: Career in Focus. Retrieved from http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

[14] Ibid.

[15] "Certified Information Systems Security Professional." (ISC)². Retrieved from https://www.isc2.org/cissp-how-to-certify.aspx

[16] Alexander, Candy. "The Cybersecurity Skills Gap." *SC Magazine.* December 2014. Retrieved from http://www.scmagazine.com/the-cybersecurity-skills-gap/article/385079/. "Lack of Cybersecurity Skills Makes Firms a Hacker Target." National Cybersecurity Institute. August 2016. Retrieved from http://www.nationalcybersecurityinstitute.org/general-public-interests/lack-of-cybersecurity-skills-makes-firms-a-hacker-target/

[17] Maryland Department of Labor, Licensing, and Regulation, Department of Labor, Bureau of Labor Statistics, and ICF International. June 2013.

[18] Bureau of Economic Analysis retrieved from https://www.bea.gov/index.htm

pre-recession levels of employment. In 2016, the unemployment rate was 4.3 percent, which is a considerable recovery from 7.6 percent in 2010 but is still higher than the pre-recession levels of 3 to 4 percent. Growth in economic activity translates to increased opportunities and better economic well-being for residents. Economic activity and local labor market conditions in Maryland will largely determine the challenges and advantages CCBC graduates will face as they transition to employment or seek career growth in their current occupation. As the state's economy gathers more strength, CCBC graduates will be more and more likely to receive job offers and be employed.

According to the Maryland Department of Commerce, given the federal presence and strong university system in Maryland, industries such as IT, telecommunications, cybersecurity, aerospace, and defense will be the forces behind the state's future economic growth.[19] Information technology and health care are among the industries with increased demand for jobs. The need for jobs in information and technology security is growing fastest, as shown in Exhibit 2.[20] Jobs for information security experts are expected to grow by 41 percent by 2022.[21]

Exhibit 2. Projections for High-Growth Jobs in Maryland, 2012–2022

Occupational Title	2012	2022	Change	Growth Rate
Information security analysts	3,375	4,764	1,389	41%
Interpreters and translators	1,073	1,469	396	37%
Nursing instructors and teachers, postsecondary	800	1,080	280	35%
Diagnostic medical sonographers	1,214	1,611	397	33%
Meeting, convention, and event planners	2,152	2,834	682	32%
Market research analysts/marketing specialists	7,429	9,493	2,064	28%
Operations research analysts	2,850	3,577	727	26%

Source: MD Department of Labor, Licensing, and Regulation, https://www.dllr.state.md.us/lmi/iandoproj/wias.shtml

The rising demand for information security analysts demonstrates that CCBC has targeted an important field of study that offers promising job prospects for qualified individuals. However, most of the job openings require higher education levels than the certificates and associate degrees that CCBC is able to offer.

[19] Maryland Department of Commerce, http://commerce.maryland.gov/about/rankings-and-statistics

[20] Growth projections for all other occupations can be found at the Maryland Department of Labor, Licensing, and Regulation website, https://www.dllr.state.md.us/lmi/iandoproj/wias.shtml

[21] The Bureau of Labor Statistics estimates that about 88,880 positions nationwide fit the information security job profile, with an annual wage that ranges from $51,280 to $143,770. States other than Maryland that have high employment of graduates in information security are Virginia, California, Texas, New York, and Florida. Bureau of Labor Statistics, "Occupational Employment and Wages." May 2015. Retrieved from http://www.bls.gov/oes/current/oes151122.htm

A quick search on "cybersecurity" at the Maryland Workforce Exchange provides a snapshot of the availability of cybersecurity jobs around the state. In August 2016 and March 2017, approximately 500 openings were available for individuals with job expertise in information security or cybersecurity. The search found very few internships or junior-level positions in cybersecurity, the profile of interest for most CCBC CI graduates. The scan did indicate, however, that other IT-related positions, such as help desk support, network design technicians, and network administrators, were available.[22] Chapter 5 elaborates on job prospects, industry challenges, and student employability, discussing insights gleaned from key stakeholders during site visits.

[22] A quick search on indeed.com yielded more than 400 jobs for "network engineer" and more than 100 for "help desk support" in Maryland: https://www.indeed.com/jobs?q=network+engineer+or+help+desk+support&l=Maryland

3. Cybersecurity Institute Program Overview

The CI TAACCCT grant program is an innovative project designed to develop, enhance, and expand educational training for careers in cybersecurity. Its design and evidence-based strategies incorporate each of the six core TAACCCT elements[23] and address a critical need to align Maryland's education and training programs to meet the growing demand for skilled cybersecurity workers. The CI program's vision is to be "a national community college leader in cybersecurity education, curricula development, faculty training, and national collegiate cyber exercise design and delivery."[24]

3.1 Program Logic Model

Exhibit 3 presents the CI program logic model, which illustrates how the program's inputs, activities, and outputs were expected to lead to key outcomes. Chapter 4 discusses program components, implementation activities, the outcomes of those activities, and related challenges and successes. The program's inputs include funding, from both the TAACCCT grant and leveraged sources such as CCBC's operating budget; staff, both grant funded and non-grant funded; equipment; facilities and infrastructure alterations; strategic partnerships; and other service providers. Project activities include the following:

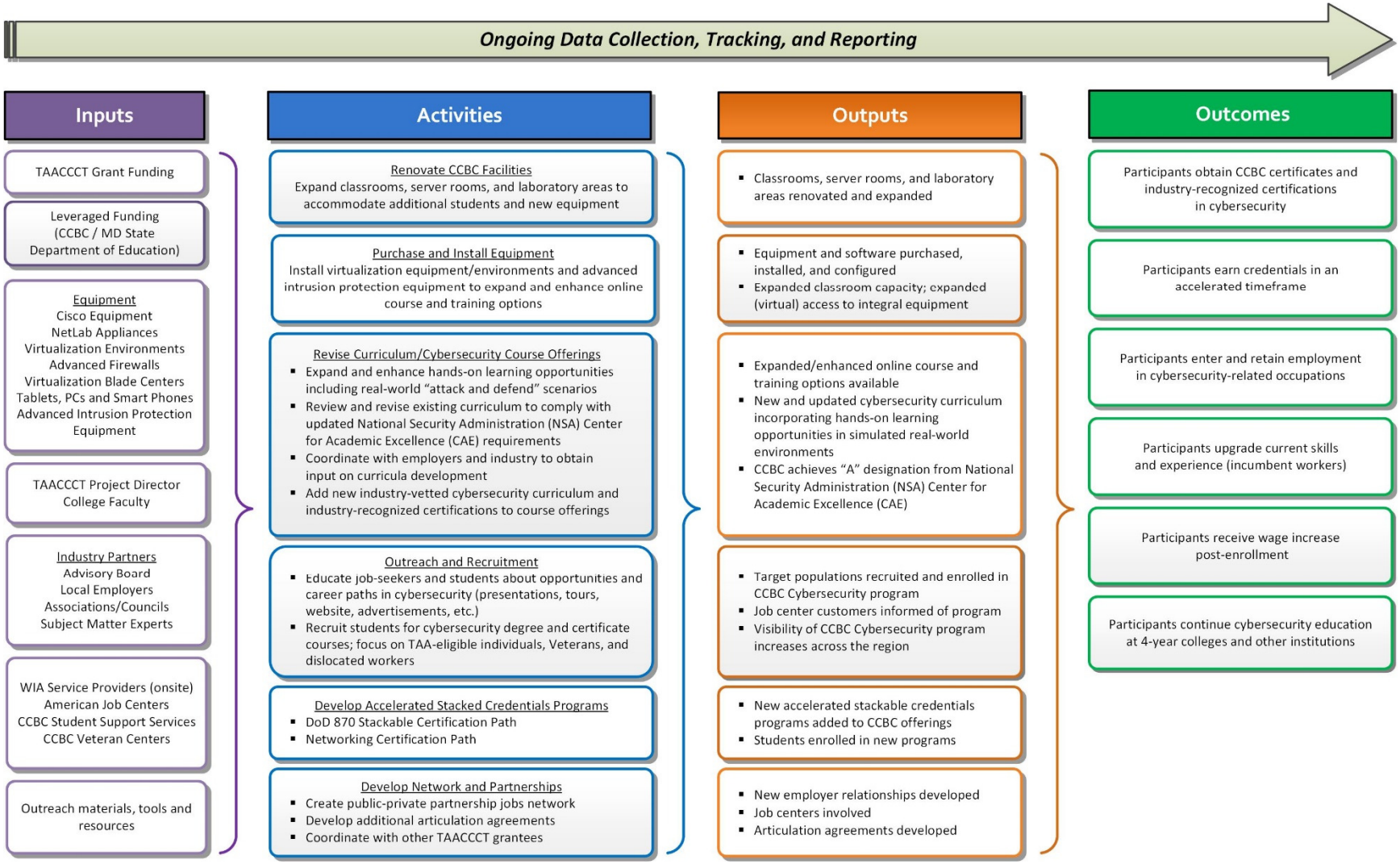
- Facilities alterations, virtual infrastructure development, and purchase and installation of state-of-the-art equipment and other technology to enhance training capabilities.
- Updating, revising, and adding new industry-vetted cybersecurity curricula to CCBC's course offerings.
- Creating new accelerated stackable credentials programs.
- Conducting outreach and recruitment to targeted populations.
- Developing strategic partnerships with employers, workforce organizations, educational institutions, and other key stakeholders.

These activities were designed to expand the capacity of the existing program to serve more students; provide more flexible access to training; offer additional credentials; accelerate time to credential attainment; and support students to obtain employment, upgrade current skills, increase wages, or be prepared to continue cybersecurity studies in a four-year institution.

[23] The six core elements required of TAACCCT grantees are (1) evidence-based design, (2) stacked and latticed credentials, (3) transferability and articulation of credit, (4) advanced online and technology-enabled learning, (5) strategic alignment, and (6) alignment with previously funded TAACCCT projects.

[24] CCBC School of Applied and Information Technology website: http://www.ccbcmd.edu/Programs-and-Courses/Schools-and-Academic-Departments/School-of-Applied-and-Information-Technology.aspx

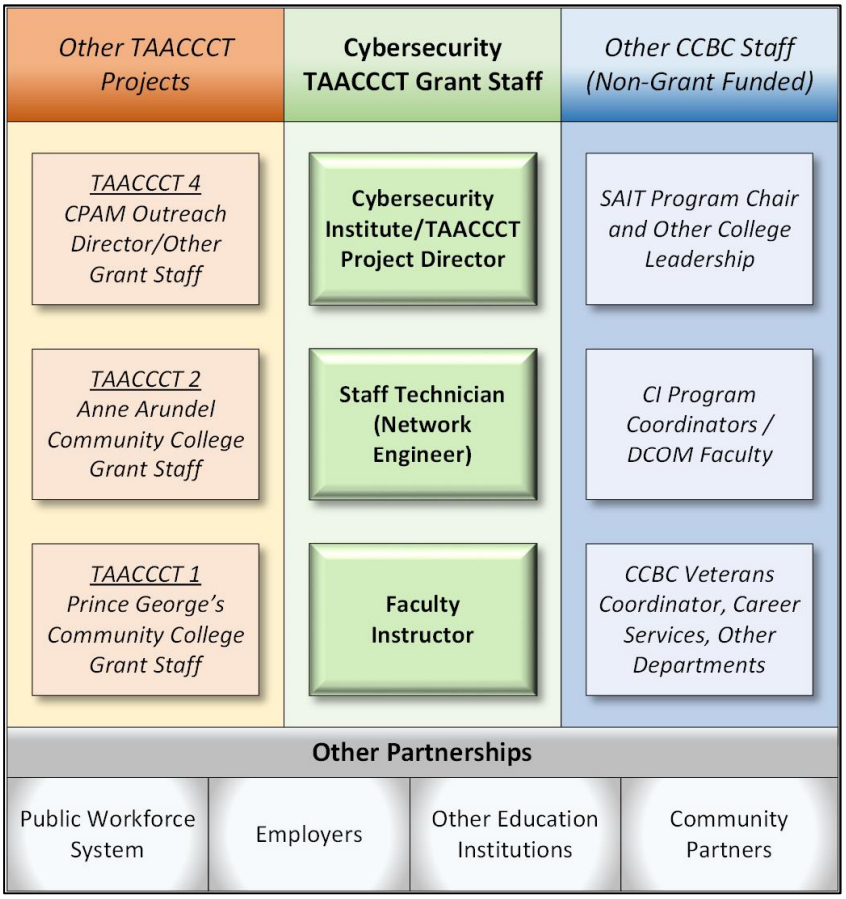
Exhibit 3. Program Logic Model



3.2 Organizational Structure

The cybersecurity TAACCCT grant team consisted of just three grant-funded positions: the TAACCCT project director, who was the director of the CI; a staff technician, who was a network engineer; and a faculty instructor. Development and implementation of the program, however, was a collaborative effort involving important contributions from other CCBC staff not funded by the grant—most notably the School of Applied Information Technology (SAIT) chair, college leaders, CI program coordinators, and faculty from CCBC's Data Communications (DCOM) department. Coordination with other TAACCT-funded projects and ongoing support from a variety of key partners were also important contributions to the program. Exhibit 4 depicts the grant's organizational structure.

Exhibit 4. Cybersecurity TAACCCT Organizational Structure



The TAACCCT project director was responsible for coordinating and managing the successful implementation all grant-related activities, including outreach and recruitment, purchasing new equipment, serving as the primary point of contact for grant partners, reporting to DOL on implementation progress and performance outcomes, and working with the third-party evaluator. The TAACCCT project director also served as the director of the CI and was responsible for overseeing a number of non-grant funded activities in the institute. A staff technician was hired

through the grant to facilitate development of the virtual infrastructure and to help purchase, install, and configure new equipment. A faculty instructor was also hired through the grant to work on curricula redesign and new accelerated stackable credentials programs.

Chapter 4 discusses the roles and contributions of other non-grant funded CCBC staff and key partners in the strategic partnerships section.

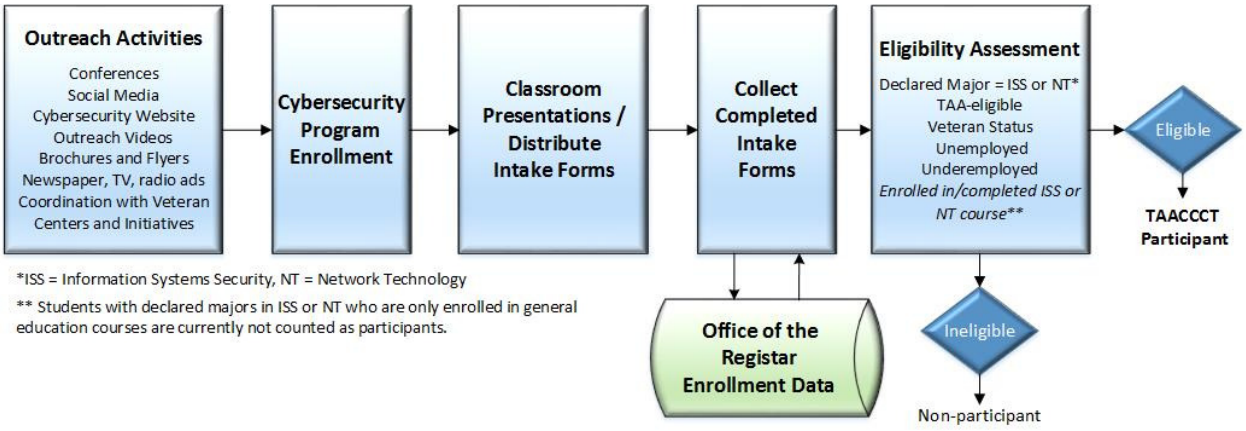
3.3 Program Participation

This section describes the process by which participants were enrolled into the program, presents the total number of unique participants served by the program from among target populations, and provides a demographic profile of all participants. Participant education and employment outcomes are discussed in Chapter 5, Outcomes Analysis.

3.3.1 Participant Intake Process

Exhibit 5 summarizes CCBC's process for participant recruitment, eligibility assessment, and program enrollment.

Exhibit 5. Program Participation Process



The process began with outreach and recruitment activities (described in Chapter 4). To generate awareness of and interest in CCBC's cybersecurity program offerings, grant staff, other CCBC staff, and key partners performed a wide variety of outreach activities. These outreach activities helped promote enrollment—for new students as well as students who had not yet declared a major.

At the beginning of each semester, the CI director and the School of Applied Information Technology chair visited each information systems security (ISS) and network technology (NT) classroom to deliver a presentation about the program and to distribute the TAACCCT participant intake forms (see Appendix A). This form was used to collect information on students' demographics (age, gender, race, veteran status, TAA eligibility, and disability status),

education and employment goals, and employment status. By signing the intake form, students agreed to release identifiable information for grant reporting and evaluation purposes.

The CI director collected the completed intake forms and submitted a request to the office of the registrar for data on all individuals enrolled at CCBC who had declared majors in ISS or NT. The CI director then compared the completed intake forms with these data to determine the initial pool of potential program participants. Next, the CI director reviewed the intake forms for students with declared majors in ISS or NT to assess their eligibility for the program. To be counted as participants, individual had to be one or more of the following: veteran, TAA-eligible, unemployed, or underemployed (that is, employed part-time).

3.3.2 Participants Served

TAACCCT participant enrollment began in January 2015 (spring semester) after the program startup activities were completed.[25] CCBC proposed to enroll 130 participants by the end of the grant. CCBC exceeded this goal by 72 participants. Exhibit 6 provides a breakdown of participants by program year.

Exhibit 6. Program Participation by Program Year

Category	Program Year				Total
	Year 1* (Oct. 2013–Sept. 2014)	**Year 2** (Oct. 2014–Sept. 2015)	**Year 3** (Oct. 2015–Sept. 2016)	**Year 4** (Oct. 2016–Sept. 2017)	
Unique Participants	**0**	**90**	**99**	**13**	**202**
TAA-eligible	*0*	*2*	*1*	*0*	*3*
Veteran	*0*	*12*	*5*	*4*	*21*
Full-time student	*0*	*68*	*69*	*4*	*141*
Part-time student	*0*	*22*	*30*	*9*	*61*
Incumbent worker	*0*	*46*	*57*	*11*	*114*

* Year 1 was dedicated to program startup activities. The TAACCCT Round 3 Solicitation for Grant Applications (SGA) required participant enrollment in education and training programs in March 2015.

As shown in Exhibit 6, there were only three TAA-eligible participants, which is not surprising given the decline in this population since the inception of TAACCCT.[26] About 10 percent of participants were veterans. Most students were enrolled full-time (70 percent), and more than half of all students, both full and part-time, were incumbent workers (56 percent).

[25] Program startup was completed in time for the fall semester (September) 2014, but CCBC did not start counting participants until the spring 2015 semester.

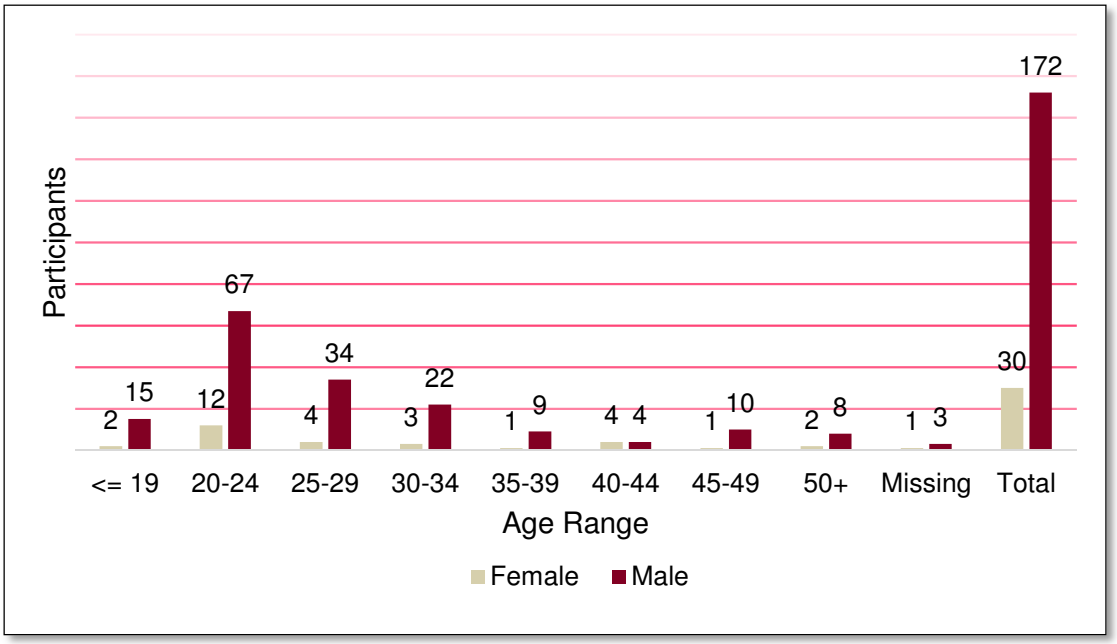
[26] The estimated numbers of workers covered by a certified TAACCT petition in Maryland: 79 in FY 2015, 282 in FY 2014, 402 in FY 2013. Table 29 of Trade Adjustment Assistances for Workers Program Fiscal Year 2013–15. Retrieved March 28, 2017, from https://www.doleta.gov/tradeact/docs/AnnualReport15.pdf

3.3.3 Participant Demographics

Age and Gender

As shown in Exhibit 7, 75 percent of participants (152) were 20 to 39 years of age; most were under age 25. Not surprisingly, the gender distribution is skewed toward males across age groups. Only 15 percent of the students were female. Women tend to be underrepresented in STEM-related occupations, including the cybersecurity field. According to the Bureau of Labor Statistics, women held only 21.8 percent of information security analyst jobs in 2016.[27] Compared with the percentage of women employed in the field, the percentage of female students enrolled in the program at CCBC was slightly lower.

Exhibit 7. Participant Profile: Age and Gender



Note: Four participants did not report age.

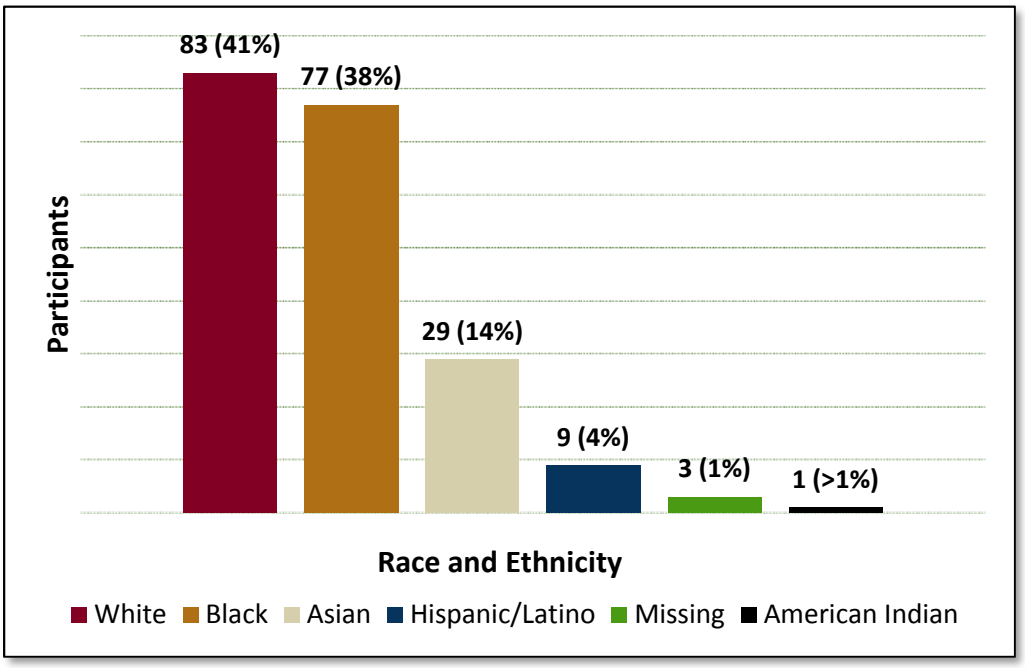
Race and Ethnicity

Racial diversity in the program was much higher than among information security analysts nationwide. According to Bureau of Labor Statistics data for 2016, only 9.2 percent of information security analyst jobs were held by African Americans, 8.9 percent by Hispanics, and 7.7 percent by Asians. The racial composition of the CCBC program is markedly different, perhaps because of the demographic diversity of the geographic region. As shown in Exhibit 8, of program participants who reported race, 41 percent were White, 38 percent were African

[27] Labor Force Statistics from the Current Population Survey, https://www.bls.gov/cps/cpsaat11.htm

American, 14 percent were Asian, 4 percent were Hispanic, and less than 1 percent were American Indian. Less than 1 percent of the students did not report their race.

Exhibit 8. Participant Profile: Race and Ethnicity



Employment Status at Enrollment

Fully 70 percent of students in the TAACCCT program were enrolled full-time. In addition, just over one-half (56 percent) of all students had some type of part-time employment. CI students who were employed full time were excluded from TAACCCT participation. Work status did seem to influence enrollment status. Employed students were less likely than unemployed students to be enrolled full time (64 percent vs. 76 percent). The majority (60 percent) of employed students were between the ages of 20 and 29.

4. Implementation Study

In this chapter, we present the summative results of our implementation study. We begin by describing the implementation study key research questions and our data collection and analysis approach. We then present our findings for each of the program's main components, with descriptions of the related activities and discussions of implementation outcomes, challenges, and successes.

4.1 Research Questions

Exhibit 9 lists the primary research topics and questions associated with the implementation study.

Exhibit 9. Implementation Study Research Questions

Program Context
▪ What is the status of the national and local labor market for cybersecurity professionals? ▪ What types of cybersecurity workforce development challenges exist? ▪ How did the CI program address regional labor market needs and workforce challenges?
Program Design
▪ What were the key components of the program and how were they developed and delivered? ▪ Were new programs, courses, and/or curricula created using grant funds? ▪ Were existing programs, courses, and/or curricula improved or expanded using grant funds? ▪ To what extent were online and technology-enabled strategies integrated into the CI program? ▪ What other types of training strategies were used by the program? ▪ What types of supportive services were provided to program participants?
Program Participation
▪ What were the eligibility criteria, and how were participants recruited and enrolled? ▪ How many participants from target populations were served by the program, and what were their demographic characteristics? ▪ Did recruitment efforts, strategies, and results differ across targeted populations? ▪ What challenges were faced in recruiting participants? What methods proved most successful? ▪ How satisfied were program participants with the program? What aspects of the program were participants dissatisfied with, if any?
Partnerships
▪ What contributions did each of the partners (non-grant funded CCBC staff, employers, the public workforce system, other TAACCCT grantees, community organizations, etc.) make in terms of: 1) program design, 2) curricula development, 3) recruitment, 4) training, 5) job placement, 6) program management, 7) leveraged resources, and 8) program sustainability? ▪ What factors contributed to partners' involvement or lack of involvement in the program? ▪ Which contributions from partners were most critical to the success of the CI program?
Program Management and Sustainability
▪ What institutional management practices led to successful implementation of the project? ▪ How were outcome data used to assess progress toward achieving outcomes?

▪ Did the grantee develop a formal plan for sustainability? Which program components will be sustained beyond the life of the grant, and how?
Program Implementation Outcomes
▪ Did the program meet its intended goals to (a) increase training capacity, (b) expand technological infrastructure, (c) update existing certification and degree programs in cybersecurity and information technology, (d) create new certifications, (e) train students and incumbent workers in current, state-of-the-art cybersecurity practices, and (f) create articulation agreements with other colleges and universities? ▪ Did the program achieve the "A" designation from the NSA Center of Academic Excellence? ▪ Did the program result in relevant, industry-recognized, stackable, portable certificates and credentials? ▪ In what respect was the program able to achieve its objectives and in what areas did it fall short?
Promising Practices and Lessons Learned
▪ What lessons can the field learn from the CI grant program's implementation? ▪ What promising practices were most important to the program's success? ▪ What challenges were faced during program implementation? How were they addressed?

4.2 Data Collection and Analysis

The implementation study findings presented in this report are based on qualitative data collected from key informant interviews, program documents, and a student focus group. We conducted three separate rounds of site visits to CCBC's Essex campus, in December 2014, August 2015, and February 2017.[28] Each site visit included semi-structured interviews with grant-funded program staff and other key CCBC staff not funded by the grant. The interviews focused on topics related to the program's implementation—staffing, facility alterations, equipment purchase and installation, cybersecurity curricula review and updates, outreach and recruitment activities, and program participation. In addition to the site visits, we interviewed key partners by phone, reviewed a variety of program documents[29] over the course of the evaluation, and held a focus group with CCBC students during the final site visit. Exhibit 10 provides a count of interviewees by type for each site visit round.[30]

[28] IMPAQ researchers also attended the CI program's ribbon-cutting ceremony on December 3, 2014.

[29] For example, the CI TAACCCT grant application (statement of work), budget narrative, database export of grant activities, quarterly progress reports, annual reports, online media, and other miscellaneous documents.

[30] Due to the relatively small number of interviewees, we have not identified all titles and organizations for purposes of anonymity.

Exhibit 10. List of Interviewees

Category	Count of Interviewees			
	Site Visit 1	Site Visit 2	Site Visit 3	Total
Grant staff (director, faculty, network engineer)	3	3	3	**9**
Other CCBC faculty/staff (non-grant funded)	3	6	6	**15**
Employers	2	0	2	**4**
Workforce system representative	0	0	1	**1**
CI students (focus group)	0	0	11	**11**
Totals	**8**	**9**	**23**	**40**

To examine the program's context and relevant labor market information, we used the following two data sources:

- ***Maryland Workforce Exchange labor market information.*** Maryland's labor market analysis website houses demographic information and economic data on unemployment, industry and occupation-specific employment (current and projected), and real-time job openings.

- ***Integrated Postsecondary Education Data System data***. This system is the core postsecondary education data collection program of the U.S. Department of Education National Center for Education Statistics. Information is collected annually from all providers of postsecondary education in fundamental areas such as enrollment, program completion and graduation rates, institutional costs, student financial aid, and human resources.

4.3 Implementation Study Findings

This section presents summative implementation study findings, which cover the entire program period of performance, from October 2013 through March 2017. We have organized our findings according to the following five program activity areas:

1. Expand training infrastructure and incorporate new equipment.

2. Create new accelerated stackable credentials programs.

3. Update, revise, and add industry-vetted cybersecurity curricula.

4. Conduct outreach and participant recruitment.

5. Develop strategic partnerships.

We begin each of the following sections by discussing the objective of the proposed activity—that is, the specific problem or need that the activity was intended to address. We then describe the implementation process and related outcomes over the course of the program. We conclude the discussion of each activity with a summary of key observations and any lessons learned. At the end of this chapter, we discuss the sustainability of these activities beyond the life of the grant.

4.3.1 Expand Training Infrastructure and Incorporate New Equipment

Activity Objectives

CCBC's School of Applied Information Technology has experienced significant increases in enrollment. As noted in the TAACCCT grant application, enrollment doubled from 400 in 2008 to approximately 800 in 2013, the year that CCBC received the grant funding.[31] This continuous increase in enrollment imposed a significant strain on CCBC's capacity to meet the demand for training. On occasion, qualified student applicants were turned away, and, in some instances (particularly at the Catonsville campus), classes were canceled because not enough full-time faculty or adjunct teachers were available to teach the courses. Furthermore, recruiting additional teachers (full-time or adjunct) to accommodate the increased enrollment was a significant challenge. Experienced individuals with expertise in the cybersecurity field can command much higher salaries working in the industry. CCBC knew it had to find an innovative approach to expanding its training capacity to meet the increasing demand and used the TAACCCT grant as the catalyst to do so.

At the same time, CCBC used the TAACCCT grant as an opportunity to purchase new equipment and technology to improve the quality of training and enhance student educational outcomes. Prior to the grant, the training relied primarily on textbook learning and classroom instruction. CCBC realized that the program needed to incorporate more hands-on learning opportunities to provide students with a better understanding of the types of technologies currently used to solve real-world problems in the ever-evolving cybersecurity environment.

Process and Outcomes

CCBC invested a significant portion of its grant funding to purchase state-of-the-art equipment to create a virtual infrastructure that greatly expanded access to cybersecurity training for students across CCBC's campuses.[32] CCBC purchased and installed Linux Virtualization equipment and VMWare workstations to create a virtual desktop interface for students.[33]

---

[31] Summer enrollment tripled over this period. There were approximately 1,000 students enrolled for the last summer program of the study period, summer 2017. [OR WHENEVER "CURRENTLY" MEANS]

[32] CCBC purchased most of the new equipment and network infrastructure and completed facility alterations to accommodate the new equipment in Year 1. The alterations included 4,832 square feet of additional space for the CI program. All building alterations were performed on the Essex campus; these alterations accounted for approximately 15 percent ($376,000) of the grant's total budget. To cover the full cost of the required facility alterations, CCBC contributed $214,503 in leveraged funds from its operating budget.

[33] The virtualization equipment is housed at CCBC's Catonsville campus.

Students could then work on the virtual system while in the classroom and could remotely access the servers while away from the classroom with any browser-capable computer. As described by CCBC faculty, this new virtualization equipment "allows students to work anytime, anywhere." Students could log in to the virtual desktops and access all the tools and software needed to complete the class exercises. CCBC also purchased video conferencing equipment to facilitate training across the CCBC campuses.

In addition to the virtualization equipment, CCBC purchased top-of-the-line advanced intrusion protection devices—including FireEye, AlienVault, and SAINTbox—to train students on the most current and cutting-edge cybersecurity equipment and practices. At the time of purchase, these brands were quickly growing in terms of market share, so CCBC wanted to incorporate this specific equipment into the training. This new equipment enabled CCBC to create realistic simulation environments for enhanced hands-on learning exercises, including attack-and-defend scenarios. FireEye, for instance, enables real-world cybersecurity threats to be entered into the system so faculty and students are aware of the types of threats that currently exist. CCBC faculty said that they appreciated the simulated training capabilities these systems provide because they allowed students to gain valuable experience without placing the college's network and equipment at real risk.

Other equipment purchases included advanced firewalls; virtualization blade centers (servers); and routers, switches, and cabling. CCBC purchased Mac Pro computers to supply video feeds to the student Network Operation Center and two classrooms. These classrooms are used for cyber competitions, and the CI director can control all the screens from an office. New Cisco devices were also added to provide students with additional hands-on network configuration experience.

Key Observations and Lessons Learned

New equipment greatly enhanced the cybersecurity training and student learning outcomes. The new equipment CCBC purchased, including such intrusion protection devices as FireEye, AlienVault, and SAINTbox, represents the industry "gold standard." The equipment enabled students to apply what they had learned through attack-and-defend exercises in simulated environments designed to replicate real-word cybersecurity threats. Students used these systems to participate in and prepare for cyber competitions within CCBC and externally at various events. This type of experience is important for employers to see on résumés. As one interviewee noted:

> *The curricula changed from* saying *to actually* doing*. [Before the grant] they were talking about repairing a car, and now they have the car. Before TAACCCT [the students] couldn't do attack-and-defend scenarios—now they can.*

Furthermore, despite the ever-evolving nature of cybersecurity threats, the new equipment is highly sustainable. It will not become obsolete in the near future, because the equipment vendors push regular software updates to the devices.

The virtual infrastructure provided flexibility to meet students' needs. The implementation of new virtual environment technologies helped make access to the training flexible for students, so that CCBC did not have to rely solely on hiring additional faculty.

The equipment purchases and installation and the related facilities alterations were completed on schedule despite a challenging, compressed time frame. Because the first year of implementation focused primarily on facilities alterations, procurement and installation of equipment, and hiring grant personnel, a delay in the receipt of grant funding from DOL presented a challenge. Although the grant officially started in October 2013, CCBC did not receive the grant funds until May 2014. This delay reduced the time CCBC had to make the program operational for the first cohort of students to a five-month period (May to October 2014). Despite this challenge, CCBC met all milestones according to the project schedule. This success was attributable to effective planning and management and to the diligent efforts of the CI director and other grant and CCBC staff.

CCBC continues to integrate the new equipment into the curricula. Because of the extensive capabilities of the new equipment, faculty were still being trained at the end of the study period. They needed to become more familiar with all of the available features before the equipment could be fully integrated into the curricula. It is difficult for faculty to find the time for training, so integration is an ongoing process beyond the life of the grant.

4.3.2 Create New Accelerated Stackable Credentials Programs

Activity Objectives

As noted in CCBC's TAACCCT grant proposal, employers in local industry have been asking CCBC to reduce the amount of time required for students and incumbent workers to obtain industry-recognized certifications. In addition, under the 8570.1-M directive, also known as the Information Assurance Workforce Improvement Program, DoD passed a regulation requiring all federal information assurance personnel to be compliant with mandated IT and security certification standards within a certain time.[34] This directive created a pressing need for federal workers to obtain these certifications to maintain compliance and retain employment.

CCBC had certificate programs in place before the grant for A+, general networking, IT, Microsoft, Network+, Cisco, and Red Hat. The coursework in these programs prepared students to take third-party industry certifications from CompTIA, Cisco, EC-Council, and others, such as A+, Network+, Security+, Certified Ethical Hacker, Cisco Certified Network Associate, Certified Information Systems Security Professional, and the like. Students could take these programs individually or as a stacked and latticed certificate program while pursuing one of the degree programs. However, CCBC offered only full 16-week semester courses.

[34] The most common certifications included in the directive are A+, Network+, Security+, Certified Ethical Hacker, and Certified Information Systems Security Professional.

CCBC used its grant to reduce the time required for students to obtain certifications by redesigning the required course sequences into four-week training modules and creating a DoD 8570.1 stackable certificate path. The purpose of the stacked credentials program was to provide a pathway for students to obtain industry-recognized certifications in a shortened time frame to prepare them for employment in the cybersecurity industry. The accelerated programs focused on cybersecurity certifications in two key employment areas: (1) cybersecurity and network administration jobs and (2) cybersecurity jobs as outlined in DoD Directive 8570.

Process and Outcomes

CCBC began the process by establishing a stackable credentials workgroup to develop a strategic plan for creating the new accelerated stacked credentials programs using a block-style training model. The block-style model reduced the time required to complete each course to four weeks, rather than the standard 16-week semester. By spring 2016, the workgroup had fully developed plans for the design and implementation of both the accelerated networking certificate program (Exhibit 11) and the DoD 8570 program (Exhibit 12). The new, fully matured DoD 8570 program was offered in the spring 2017 semester, starting January 2017. Though fully developed, CCBC has not been able to offer the networking certificate program due to faculty resource constraints.

Exhibit 11. Accelerated Networking Certificate Program Curricula

Block	Course No.	Course Title	Length	Credits
Block I	DCOM 101	Intro to Networks	4 weeks	3 credits
Block II	DCOM 142	Intro to Linux/Unix	4 weeks	3 credits
Block III	DCOM 251	Network+	4 weeks	4 credits
Block IV	DCOM 258	Security+	4 weeks	3 credits
		Total	**16 weeks**	**13 credits**

Exhibit 12. Accelerated DoD 8570 Stackable Certifications Program Curricula

Block	Course No.	Course Title	Length	Credits
Block I	DCOM 251	Network+	4 weeks	4 credits
Block II	DCOM 258	Security+	4 weeks	3 credits
Block III	DCOM 214	Operating Systems Security	4 weeks	4 credits
Block IV	DCOM 215	Ethical Hacking and System Defense	4 weeks	4 credits
		Total	**16 weeks**	**15 credits**

Most courses in each program were offered as blended courses, 50 percent online and 50 percent in person. Because of the extensive amount of material covered in an aggressive timeline, CCBC wanted to ensure that students developed a proper in-person connection with the faculty. In addition, Cisco frowns on online courses, so the Cisco courses were offered only in person.

Key Observations and Lessons Learned

Initial enrollment in the DoD 8570 program was low but expected to grow. Only nine individuals enrolled in the first DoD 8570 program cohort. The participants were mostly incumbent workers with prior experience in the field who needed to gain the certifications or recertify. The low enrollment was expected, because the program was, intentionally, not promoted or even listed in the course catalog. Now that the initial pilot of the accelerated program has been completed, CCBC plans to advertise the program in the course catalog; enrollment should increase as a result.

The accelerated block-style training is an attractive option for employers. The cost of the programs are relatively low compared with the cost of similar programs at private training institutions; at only $180 per credit, the total cost is just $2,340 for the networking certificate program and $2,700 for the DoD 8570 program. Furthermore, the classes for the DoD 8570 program were offered in the evening; there were no day classes during the spring 2017 semester. CCBC also plans to offer evening classes for the networking certificate program when it is implemented. Evening classes are attractive to employers because their employees do not have to leave work to attend training.

The accelerated programs are not suitable for new students. Given the aggressive timeline and amount of material covered in these accelerated block-style training programs, CCBC respondents suggested that students should have some prior experience and knowledge to complete the programs successfully. Therefore, these new programs were geared toward incumbent workers and individuals seeking recertification.

Finding faculty to teach the programs is a significant challenge. The existing CCBC faculty are fully qualified and willing to teach the new accelerated courses. However, these faculty currently all have teaching overloads and college rules strictly prohibit them from taking on additional courses. CCBC has been working diligently to address this issue and was able to hire one new adjunct professor to help offset the faculty resource shortage. However, finding adjunct professors who are well-qualified, available, and willing to teach is also a major challenge that CCBC must contend with.

4.3.3 Update, Revise, and Add Industry-Vetted Cybersecurity Curricula

Activity Objectives

Other factors outside of accelerating credential pathways also motivated CCBC to review and revise the cybersecurity curricula. Curricula revisions were required due to the additional training capabilities introduced by new infrastructure technology and equipment purchased

through the grant. In addition, CCBC needed to review and update existing curricula to ensure continued compliance with the NSA Centers of Academic Excellence "A" designation in Information Assurance/Cyber Defense.

Process and Outcomes

The purchase of equipment created clear and specific motivation for the CI to update the curricula to incorporate the new technology. The CI director and faculty met regularly to standardize that incorporation by creating "step action documents". These documents described equipment capabilities, provided instructions on how to use the equipment, and outlined how the equipment could be used to train students. To supplement these documents, the grant team conducted train-the-trainer sessions to instruct faculty on training students in using the new equipment. The goal was to create curricula uniformity within the CI so all faculty members could teach the same course, in the same manner, at all CCBC locations. According to one CI faculty member, step action documents were designed to "make sure module components are standardized" in order to "ensure higher quality of education for the students."

CCBC was officially designated as a NSA Center of Academic Excellence in Information Systems Security Education in 2011, but the compliance requirements continuously evolve. Therefore, CCBC needed to review its curricula to ensure it was up to date with all of the new academic requirements outlined in the 2014 Centers of Academic Excellence in Information Assurance/Cyber Defense Knowledge Units document. The purpose of the academic requirement modifications outlined in that document was to "…better reflect the state to which the discipline of Information Assurance (IA) has evolved since the original publication of the training standards."

Starting in January 2014, the CI director and School of Applied Information Technology faculty met frequently to discuss the new curricula requirements, attended NSA Center of Academic Excellence webinars hosted by the National Cyberwatch Center, and mapped center topics to those covered in CCBC's course requirements to identify and address any gaps. CCBC subsequently completed its application and successfully achieved the "A" designation from NSA in November 2014.

In addition to the above activities, CCBC continuously reviewed curricula to ensure its relevance to employers and the evolving field of cybersecurity.[35] During the period of performance, CCBC constantly evaluated all course material for the need for updates using the instructional systems design methodology, which consists of the following five-phase process: (1) analysis, (2) design, (3) development, (4) implementation, and (5) evaluation. This process is continually repeated.

[35] CCBC completed several curriculum updates, such as Cisco updates, during Year 1 while waiting for the TAACCCT funds to be released.

Key Observations and Lessons Learned

Achieving the NSA Center of Academic Excellence "A" designation in Information Assurance/Cyber Defense was a major success. During the first program year, CCBC achieved the NSA "A" designation. This designation required extensive review of the academic requirements outlined in the 2014 Centers of Academic Excellence in Information Assurance/Cyber Defense Knowledge Units document, a comprehensive review of CCBC's curricula, and selected updates to ensure compliance.

Some stakeholders perceived that not enough curricula had been updated. A few stakeholders said that they had hoped the CI would not only update courses already being offered but introduce new classes as well. The development and addition of entirely new courses for the CI was not within the scope of the TAACCCT 3 grant. However, a new digital forensics AAS degree program was, in fact, developed by CCBC during the grant period. The CI director collaborated with (non-grant funded) CCBC faculty and TAACCCT 4 grant staff to develop this new course.[36] The curricula was presented to CCBC's board of directors and subsequently delivered to the Maryland Higher Education Commission, which approved it on May 17, 2017.[37] CCBC hopes to offer the new course in the fall 2017 semester. Furthermore, in addition to the curricula changes that occurred due to the "A" designation and the introduction of new equipment, CCBC made updates to Cisco, A+, and Network + course material to stay current with changes in industry certification exams.

Internships in cybersecurity positions presented unique challenges. Internships and other types of work-and-learn opportunities are invaluable for students in any field. In addition, DOL has made work-based training one of the important elements in a TAACCCT grant. Other CCBC departments at the time of this evaluation had a fairly strong internship program, which was supported by an office of supportive services serving all three CCBC campuses. However, because the CI did not require an internship for students to earn a degree or certificate, establishing internships for the CI was a low priority for the supportive services office. Any CI internships had to be arranged by CI faculty; this fact in itself was a barrier to success. However, the CI also found that employers were less than eager to take on cybersecurity students, because of the sensitive and important nature of the work. (More discussion on this issue is in the strategic partnership section below.) Furthermore, companies that serve federal agencies require employees to have security clearances—a cost that they are understandably unwilling to cover for temporary employees.

Cybersecurity competitions offer unique opportunities for hands-on learning. Given the number of barriers to cybersecurity internships, many of the stakeholders we interviewed suggested that a viable alternative was for CI students to enter competitions. Competitions give

[36] Round 3 TAACCCT grant funds were not allocated to fund the development of the digital forensics course; however, the CI director, whose position was fully funded by TAACCCT 3, was involved in all CI activities regardless of funding source. Several staff supported the course development, including staff funded by TAACCCT 4, non-grant funded faculty, and the CI director.

[37] See Appendix B: Digital Forensics Associate of Applied Science Degree Program: Maryland Higher Education Commission Approval Letter.

students an opportunity to work with team members on clearly defined tasks. These experiences simulate the type of work that employers would expect from a cybersecurity student. Seeing competitions on a résumé provides important signals to potential employers about the work experience and competencies of potential hires. One employer interviewee suggested that students should be required to participate in more competitions in place of internships.

It was evident from our interviews that CCBC faculty clearly understood the value of cybersecurity competitions for their students. The faculty said that they regularly informed students of upcoming events, encouraged them to apply, and helped them prepare. In March 2017, several CI students participated in the Maryland Community College Cyber Competition hosted by Montgomery College. At the time of IMPAQ's third site visit, several students were also preparing for a local competition to be hosted by the National Cyber League.

Focus on career pathways may have competed for time and energy needed to make significant curricula changes. One of the CI's main tasks within the grant was to create clear and accelerated pathways toward cybersecurity certificates and credentials. This focus may have pulled resources away from curricular changes in established courses.

4.3.4 Conduct Outreach and Participant Recruitment

Activity Objectives

For the TAACCCT grant, the targeted participant populations are TAA-eligible workers, veterans, dislocated workers, unemployed adults, underemployed workers, and employees from local industry looking to upgrade their skills. Therefore, CCBC made concerted efforts to conduct targeted outreach and recruitment to increase the enrollment levels among these target populations. Recruiting female students was also of particular interest, as women continue to be underrepresented in most STEM occupations, including cybersecurity. Although this effort was not supported by TAACCCT 3 grant funding, CCBC also emphasized outreach to high school students because pipeline development is paramount to developing a future talent supply to meet the growing demand for cybersecurity professionals in the workforce.

Process and Outcomes

During the period of performance, CCBC conducted a number of outreach and recruitment activities to generate awareness of and interest in the CI program. Selected examples of a few outreach and recruitment activities are listed below.

- CCBC conducted electronic and social media outreach by establishing a Twitter account (@CCBCCyberSec) and Facebook page and by posting an outreach video to the CI website.[38]

[38] See https://www.youtube.com/watch?v=XoNHgGM1Ufo&feature=youtu.be

- CCBC staff developed CI program brochures and distributed them at cybersecurity conferences across Maryland and at other local meetings and events.

- The CI director coordinated with on-campus coordinators to reach out to veterans through CCBC's veteran centers, school events, and veteran initiatives including the Boots to Suits program.

- The CI director provided Maryland's Department of Labor, Licensing, and Regulation Dislocated Worker Unit with CI program materials that could be disseminated to workforce system staff. The director also reached out to representatives from the local workforce investment board.

- Grant staff hosted several meetings and tours of the CI for key stakeholders, including state delegates, local employers, the Business Solutions Advisory Group, other Maryland community colleges, and a new veterans outreach coordinator.

- CCBC published several newspaper articles and advertised the program on WBAL television and radio.

More recently, starting around June 2016, the CCBC cybersecurity program leveraged and benefited from additional outreach and recruitment resources made available through a $15 million TAACCCT Round 4 grant program—the Cyber Pathways Across Maryland—which will expand training for new cybersecurity professionals throughout Maryland. CCBC is one of 14 community colleges in Maryland that comprise the consortium. The consortium colleges are coming together with employer partners, including IBM, Raytheon, Lockheed Martin, Rockwell Collins, Booz Allen, MedStar, and a number of hospitals to develop training pathways for low-income workers with minimal prior education or experience in IT or cybersecurity.

Key Observations and Lessons Learned

Outreach to the veteran population and military community has been particularly strong. The CI director continues to work with veterans coordinators at each campus to promote the program. Furthermore, CCBC added a veteran outreach position in September 2015; this individual has a military background, is in the U.S. Army Reserve, and provides marketing materials and information about the program to the U.S. Army Reserve cyber unit. Veterans are promising candidates for the cybersecurity training and careers. Many already possess active security clearances, thus overcoming one significant employment barrier. The CI program also provides customized training to current military members. For example, CCBC developed Linux Red Hat certification training and provided it to U.S. Marine Corps members.

The lack of a full-time outreach coordinator position inhibited the volume of outreach activities. In retrospect, the CI director suggested that a full-time position dedicated to outreach, marketing, and recruitment activities was a missing component of the staffing structure. The director was heavily involved in all aspects of the program's implementation, so there was limited time to concentrate on outreach activities without compromising other core

components of the program. The CI director recommended that TAACCCT grantees be sure to fund a full-time outreach position.

In-class presentations were the most effective recruitment strategy. The most effective method of outreach, from the grant team's perspective, was visiting data communications classes to make presentations about the program and hand out intake forms. Disseminating brochures also generated phone calls from parents and students who wanted more information about the program. Conference attendance was helpful, but the costs involved in registering, setting up booths, and printing materials were high.

The free-tuition program for high school students was an effective recruiting tool. Although this effort was not funded by the TAACCCT 3 grant, the CI provides clear incentives for high school students to enroll. By completing up to 24 credits while still in high school, students can earn an AAS degree in as little as one year after graduating from high school.

4.3.5 Develop Strategic Partnerships

Activity Objectives

To ensure that the CI continued to provide relevant training to its students and to improve its outreach and job placement efforts, the grant aimed to help CCBC strengthen strategic partnerships with employers and with workforce and veteran agencies, develop additional articulation agreements with education institutions, and coordinate with other TAACCCT grantees.

Process and Outcomes

Partnerships with employers and with veteran and workforce agencies. Employers and industry representatives from the Baltimore-Washington area served on program advisory boards to review CCBC's NT and ISS curricula and to discuss workforce needs. Employers' input through these advisory boards was intended to ensure the ongoing relevance and quality of CCBC's cybersecurity training and education program offerings. Employers were also asked to assist with identifying real-world learning experiences and training opportunities for current students. Although some CCBC staff said that the most important way employers could contribute to student success was to sponsor internships, internship opportunities were lacking. Instead, employers partnered mostly by serving as guest lecturers.

The CI director coordinated with CCBC managers of veteran centers at each campus to promote the cybersecurity program to veterans. The CI director attended campus events that targeted veterans, such as Boots to Suits, which helps veterans transitioning to civilian life. The CI director and School of Applied Information Technology chair set up a booth at the Cyber Maryland conference in 2014, which was attended by many individuals still active in or transitioning out of the military. Finally, the CI director provided materials and information to the Veterans Integration to Academic Leadership staff; this program offers educational outreach and mental health services to eligible veterans at CCBC.

Program staff from CCBC went to American Job Centers and presented on the CI program. In these presentations, CI staff informed center staff about the CI program, the types of participants it was seeking, and the requirements and length of the program. To conduct additional outreach to the dislocated worker and TAA-eligible population, the CI director worked to set up meetings with representatives from Baltimore County's Department of Economic and Workforce Development to discuss collaboration. However, these meetings were significantly delayed due to a lack of response to the CI director's requests. These meetings did eventually take place with the support of a new outreach director hired for the TAACCCT 4 grant (described below).

Other TAACCCT projects. CCBC engaged with two previously funded TAACCCT grant programs: a TAACCCT 1 program developed by Anne Arundel Community College and a TAACCCT 2 program developed by Prince George's Community College. CCBC partnered with Anne Arundel to develop training programs to complement CCBC's offerings and to build on lessons learned. Prince George's helped CBCC by sharing strategies for providing enhanced services to veterans, including employment services.

CCBC is one of 14 Maryland colleges that comprise the TAACCCT 4 Cyber Pathways Across Maryland consortium. Participation in this new program is of particular importance to CI as the current TAACCCT 3 grant ends. To support this Round 4 TAACCCT grant, CCBC hired a full-time outreach director in June 2016. This individual's role directly benefits the CI because the outreach and recruitment efforts under the new TAACCCT program target the same population and the same training programs. According to our interview with the outreach director, he concentrates activities in four categories: (1) the public workforce system, (2) veterans organizations and representatives, (3) high schools, and (4) employers. The following are some examples of specific outreach activities within these categories.

- ***Outreach to the public workforce system.*** The outreach director attended, and continues to attend under TAACCCT 4, regular workforce centers management group meetings, which bring together directors of American Job Centers, to present information about CCBC's cybersecurity program, including the career pathways, associated training requirements, and occupational projections. In turn, the center managers should inform their frontline staff, who could then relay the program information to job center customers.

- ***Outreach to veterans organizations.*** The outreach director has developed numerous relationships with various veterans organizations, representatives, and advocates. Specific examples include the CCBC Director of Veterans Services, Maryland Department of Veterans Affairs, Maryland Department of Labor and Industry Veterans Service, Maryland Center for Veterans Education and Training, the South Baltimore Station (a residential program for homeless veterans), the Maryland Air National Guard, and the U.S. Coast Guard/Department of Homeland Security Asymmetric Resilient Cybersecurity Workgroup. The outreach director leverages these relationships to promote the cybersecurity program and careers in cybersecurity to veterans across MD and surrounding areas.

- ***Outreach to high schools.*** The outreach director, together with CI staff (particularly the program coordinator), make presentations at local public and private high schools to promote awareness of and interest in cybersecurity among youth. CCBC has a free-tuition program in which high school students can earn 16 credits in Cisco and eight credits in network technology while still in high school.

- ***Outreach to employers.*** The outreach director coordinates a number of activities to get employers involved with the program, such as hosting employer tours to showcase CCBC's facilities, recruiting employers to participate on the program's advisory board, and working with employers to develop internship and job opportunities for CCBC students.

Articulation agreements with other training institutions. Over 60 percent of CI students continue on to four-year universities. Therefore, CCBC continued to work with other education institutions to create cybersecurity articulation agreements and develop effective means of transferring credit toward an advanced degree. This task was particularly important to the CI, because most cybersecurity positions require at least a bachelor's degree. CCBC executed articulation agreements with American Public University online, Capitol Technology University, Towson University, Stevenson University, and the University of Maryland Baltimore County. When the study ended, CCBC was working to develop an agreement with the University of Maryland University College. CCBC also had representatives from Baltimore County Public Schools and Johns Hopkins University serving on its network technology advisory board.

Key Observations and Lessons Learned

Some employers identified a misalignment between their needs and CI program offerings and suggested that the "Cybersecurity Institute" branding was misleading. A few employers indicated that they would consider hiring only job candidates who were highly skilled in cybersecurity practices. One employer shared that he needed cybersecurity "superstars" to work for his company; no matter how good the training and equipment was, he would not consider a recent CI graduate for the type of work he needed. A few interviewees also suggested that the "Cybersecurity Institute" branding was misleading and could potentially set unrealistic expectations for both students and employers. One employer suggested that CCBC should stay focused on entry-level IT jobs that two-year degree students could obtain. In this way, he believed, the CI would be more successful at getting employers to support interns and eventually hire students.

One CCBC staff member acknowledged a general disconnect between some employers' expectations for the skill levels of job candidates and what CCBC is realistically able to provide in a 60-credit two-year AAS program. However, it was also apparent from our interviews and program observations that not all employers had these expectations or shared the sentiment that the program's branding was misleading. Evidence is provided by the fact that employers have hired graduates from the program for entry-level jobs in a cybersecurity career pathway. Several major employers—including NSA and Lockheed Martin—were, at the end of our study, actively working with CCBC to recruit interns.

Furthermore, our interviews clearly indicated that CCBC faculty did convey to students that a two-year degree prepares them for entry-level jobs in IT and not necessarily for jobs as cybersecurity analysts. However, faculty said that CCBC students are prepared to progress along a cybersecurity career pathway because the program's cybersecurity curricula incorporates cutting-edge equipment currently used in the industry.

Program offerings were not always aligned with workforce agency requirements. Although the CI program hoped to attract and serve displaced workers and other workforce agency clients, the Workforce Innovation and Opportunity Act requires applicants to go to providers on its eligible training provider list. CCBC was not on this list during the TAACCCT 3 period of performance. In addition, the length of training for agency clients needs to coincide with UI benefits receipt. Workforce agency representatives shared that they believed IT training is better suited for individuals with some experience and education. They saw the CI program as better suited for incumbent workers, training low-level employees who need certifications to advance in their current workplaces.

Other TAACCCT grants provide important support for success. Other TAACCCT grants made the CI more efficient in figuring out useful strategies for recruiting specific populations, particularly veterans. In addition, because CCBC is part of the Round 4 grant, the lessons learned in the Round 3 grant will be applied to the activities conducted in the new grant. For example, the CI director said that a program like this one needs to hire someone to be in charge of recruitment and outreach to employers. In response to this experience, the Round 4 grant has a designated staff member for whom recruitment and outreach are primary. That position will be able to support the CI beyond the end of the Round 3 grant period.

4.4 Sustainability

Perhaps one of the most important and successful aspects of this grant is the lasting impact and sustainability of program activities. Virtually all of the implementation activities funded by the grant will continue well beyond the life of the grant. For example, the large investment in virtual technology and training equipment will continue to provide flexible options for students to access training, enable greater opportunities for enhancing curricula and student experiences, and expand CCBC's capacity to train more students.

CCBC also decided to hire two of the grant-funded staff, the faculty member and the network engineer. The CI director position will be retained under the Cyber Pathways Across Maryland TAACCCT 4 grant. Therefore, the CI program and its students will continue to benefit from the experience and contributions from these staff members.

5. Outcomes Analysis

The outcomes analysis presented in this section examines the educational and employment outcomes of all participants in the CCBC TAACCCT program. Because the outcomes analysis design did not involve counterfactual analysis using a comparison group, it is not intended to establish a causal link between the program and participant outcomes. However, when combined with the implementation study findings presented in the previous section, the analysis provides valuable insights that result in a more comprehensive assessment of the program.

We analyzed participant education and employment findings across several participant categories:

1. All program participants, regardless of program completion or incumbent worker status
2. Program completers:
    - who were employed prior to enrollment (incumbent workers)
    - who obtained employment after enrollment but prior to program completion[39]
    - who obtained employment after program completion
    - who did not obtain employment after program completion

These participant categories are further defined in their respective sections of this chapter.

This chapter lists the key research questions in the original evaluation design and discusses our data collection and analysis strategies. It presents our findings for participant education outcomes and for employment outcomes separately and then compares these findings to the projected program goals. Finally, we discuss the limitations of the analysis.

5.1 Research Questions

The outcomes analysis was guided by the following research questions:

- What were the participants' educational achievements, including program completion, credentials earned, and enrollment in other programs?
- What were the participants' employment outcomes, including employment, employment by industry type, and earnings?

[39] These participants cannot be counted in the TAACCCT annual reporting outcome category "employed after program of study completion."

- What are the socioeconomic characteristics of participants across key outcome categories (program completion, education and employment outcomes)?
- What is the employment history of participants prior to program enrollment (employment status, earnings, industry, etc.)?
- What types of services did participants receive from the program (coursework, counseling and related services, industry focus of training, etc.)?
- Are differences in participant educational and employment outcomes associated with participant characteristics, employment history, and services received?

Although the research questions pertaining to participant support services and their effect on educational and employment outcomes were included in our initial evaluation design, we later excluded them from the outcomes analysis for two reasons. First and foremost, individual-level data on service utilization among participants were not available for the evaluation. Second, the TAACCCT grant funding was, by design, not used to provide support services exclusively for program participants. Services such as assessments, academic and career guidance, basic and soft skills training, job search and placement assistance, and so on were available both to program participants and to all other CCBC students through the same channels—for example, CCBC's career services department, academic advisors, and veterans coordinator and workforce agency representatives stationed on campus. Furthermore, there was only one participant reported as enrolling in further education after program completion, so we do not provide any detailed analysis or discussion regarding that research question.

Below, we describe the data collection and analysis methods we used to address the research questions listed above.

5.2 Data Collection and Analysis

We used two primary data sources for the outcomes analysis:

- ***TAACCCT participation and educational outcomes data.*** The CI director developed a custom tracking and reporting system for the TAACCCT grant. For each participant, the director entered data on demographics and employment status at the time of enrollment based on the completed TAACCCT intake form (see Appendix A). The director also collected educational outcome information from CCBC's office of the registrar on all CCBC students with a declared major in either ISS or NT. This outcome information included the number of course credits completed—both toward the major and for general education requirements—and credentials earned.

- ***Quarterly wage and industry data.*** In collaboration with Jacob France Institute (JFI)[40], CCBC provided data on quarterly wages and industry of employment for all program participants. These data served as the basis for the employment and earnings outcomes analysis. They enabled us to determine which participants were incumbent workers, meaning that they were employed when they enrolled, along with their earnings and their industry. The data also showed which individuals obtained employment after enrolling in or exiting from the program. The quarterly earnings data covered the fourth quarter (October through December) of 2013 through the fourth quarter of 2016.

Because the sample of participants was small (202), we conducted descriptive analyses of the observed participant educational and employment outcomes, including the distribution of participant socioeconomic characteristics. We did not use random assignment or a quasi-experimental comparison group design to explore program impacts on these outcomes. However, we conducted multivariate regression analysis to examine whether specific participant characteristics explained any variation in outcomes.

5.2.1 Descriptive Analysis

We conducted descriptive analyses of the following participant outcomes:

1. ***Participant characteristics.*** Using the demographic data received from CCBC, we examined the distribution of participant socioeconomic characteristics (gender, race, and age), including cross-tabulations of participant characteristics. These analyses present a detailed characterization of the types of individuals enrolled in the program.

2. ***Education outcomes.*** We used participant educational outcomes data received from CCBC to construct educational outcome measures following program enrollment. Outcomes available in the data included program enrollment, credits completed, CCBC certificate and degree attainment, and measures of time to program completion that was constructed by IMPAQ.

3. ***Employment outcomes.*** We used data on quarterly earnings and industry to explore the employment and earnings outcomes both of all participants, regardless of employment status at enrollment or program completion status, and of program completers only, regardless of employment status at enrollment. Due to the small sample size, we conducted cross-tabulations with participant characteristics only where feasible.

5.2.2 Multivariate Analysis

We used multivariate analysis to examine how differences in participant outcomes might be predicted by demographic characteristics and employment history, factors that are known to

[40] JFI is a leading source of high quality statistical information and research on employment, continued education and training opportunities to support research solutions for business, worker, and government investment decisions. (http://www.jacob-france-institute.org)

influence outcomes for training program participants. We used the following linear regression model:

$$Y\_i = \alpha + X_i \beta_1 + u_i$$

The dependent variable in this model (*Y*) is the outcome of interest. The control variable, X_i, includes a vector of participant socioeconomic characteristics; u_i is a mean zero disturbance term. The constant, α, captures the expected mean of the selected outcome, and the parameters vector, β_1, captures the extent of the relationship between participant socioeconomic characteristics and the outcome of interest. To test the significance of these relationships, we used simple t-tests to identify participant characteristics that have an important relationship with participant educational and labor market outcomes. The outcomes we analyzed using multivariate analysis were the *likelihood of program completion* and the *time to completion*.

5.3 Participant Education Outcomes

This section presents the education outcomes of program participants:

- ***Program completion.*** Completion means that participants either earned an AAS degree in ISS or NT or earned the CCBC certificate.

- ***Earned certificate***. Based on DOL guidance, CCBC was able to count participants as program completers if they completed the required coursework for a certificate, regardless of whether they actually applied for and obtained the certificate. Therefore, the "earned certificate" category includes both participants who actually obtained a certificate and those who qualified for a certificate. Our conversations with CCBC faculty revealed that many students in the program did not apply for the CCBC certificate. Although it is endorsed by CCBC, the certificate is not necessarily recognized in the industry or sought by employers. Also, based on our discussions with CCBC faculty, most CCBC students planned to earn an AAS degree, which is of much greater value to employers. Furthermore, students were more interested in earning industry-recognized third-party certifications.[41]

- ***Earned degree.*** Participants in this category earned an AAS degree in ISS or NT. The data did not indicate which subject.

[41] Students were interested in certificates from CompTIA, Cisco, EC-Council, and others, such as A+, Network+, Security+, Certified Ethical Hacker, Cisco Certified Network Associate, and Certified Information Systems Security Professional. Late into the grant period, CCBC became a certified Pearson-Vue testing center and began offering many of these certification exams on campus; however, certification outcome data were not being tracked for program participants.

5.3.1 Program Completion

As shown in Exhibit 13, there were 93 program completers out of 202 participants. Of these, 14 were females and 79 were males; most were younger than 30 years of age. Completion rates were highest among participants between the ages of 20 and 29, at 56 percent, and among participants age 50 or above (57 percent).

Exhibit 13. Program Completion by Age Group and Gender

Characteristic	Participants	Program Completers	Completion Rate
Gender			
Female	30	14	46%
Male	172	79	47%
Age at Enrollment			
<=19	36	11	31%
20–24	76	43	57%
25–29	29	16	55%
30–34	24	7	29%
35–39	8	2	25%
40–44	7	3	43%
45–49	13	6	46%
50+	7	4	57%
Missing	2	1	50%
Total	**202**	**93**	**46%**

CCBC has a diverse pool of students. As shown in Exhibit 14, the racial composition of participants who completed the certificate or degree requisites included 37 Whites and 37 African-Americans, the two predominant racial groups in the CCBC program. Among the 29 Asian participants, 12 completed the degree requirements.

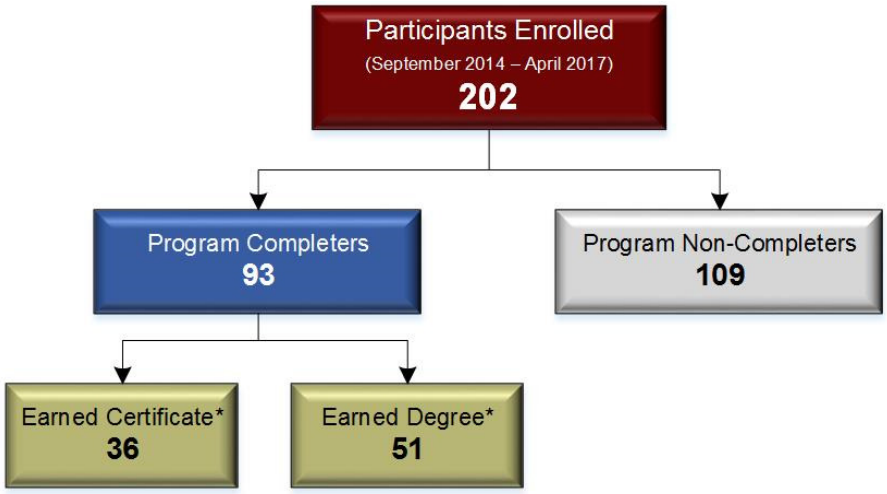
Exhibit 14. Program Completion by Race and Ethnicity

Race and Ethnicity	Participants	Program Completers	Completion Rate
White	83	37	45%
Black	77	37	48%
Asian	29	12	41%
American Indian	3	1	33%
Other/missing	10	6	60%
Hispanic	9	6	67%
Total [a]	**202**	**93**	**46%**

[a] Hispanic is not mutually exclusive to race, hence not included in the total.

Exhibit 15 provides an overview of participant educational outcomes. It shows the total number of participants enrolled, the number who completed the program, and the number of certificate versus degree earners.

Exhibit 15. Participant Educational Outcomes



* The total for Earned Certificate plus Earned Degree does not equal 93 because the data did not include certificate or degree information for six program completers.

5.3.2 Earned Certificate or Degree

Out of the 93 students completing the program, 36 completed the requirements to earn a CCBC certificate. As shown in Exhibit 15, 51 out of the 93 program completers earned a degree. The numbers of degree completers and certificate completers add up to 87, not to the total of 93 completers, because data for six students indicate only that they completed coursework but not whether they earned a certificate or a degree.

Exhibit 16 provides demographic information for program completers, presented separately by degree and certificate earners. Approximately 82 percent of degree earners and 92 percent of certificate earners were males. The dominant age group is 20 to 24 years, comprising 43 percent of degree completers and 47 percent of certificate completers. Both White and African-American participants were more likely to receive degrees (43 and 41 percent, respectively) than certificates. Of the degree earners, there were more participants (55 percent) employed at the time of enrollment (incumbent workers) than those who were unemployed (45 percent); 58 percent of the certificate earners were incumbent workers compared to 42 percent who were unemployed at the time of enrollment.

Exhibit 16. Demographic Profile of Program Completers, by Earned Degree and Earned Certificate

Demographics	Degree	Certificate
Total	**51 (25%)**	**36 (18%)**
Gender		
Female	9 (18%)	3 (8%)
Male	42 (82%)	33 (92%)
Age Range		
<=19	7 (14%)	4 (11%)
20–24	22 (43%)	17 (47%)
25–29	12 (24%)	3 (8%)
30–34	4 (8%)	3 (8%)
35–39	2 (4%)	-
40–44	-	2 (6%)
45–49	3 (6%)	3 (8%)
50+	1 (2%)	3 (8%)
Race		
White	22 (43%)	14 (39%)
Black	21 (41%)	13 (36%)
Asian	4 (8%)	7 (19%)
American Indian	1 (2%)	-
Other/missing	3 (6%)	2 (6%)
Employment Status at enrollment		
Incumbent workers	28 (55%)	21 (58%)
Unemployed	23 (45%)	15 (42%)

Note: For six program completers, the data do not indicate whether they completed a degree or a certificate.

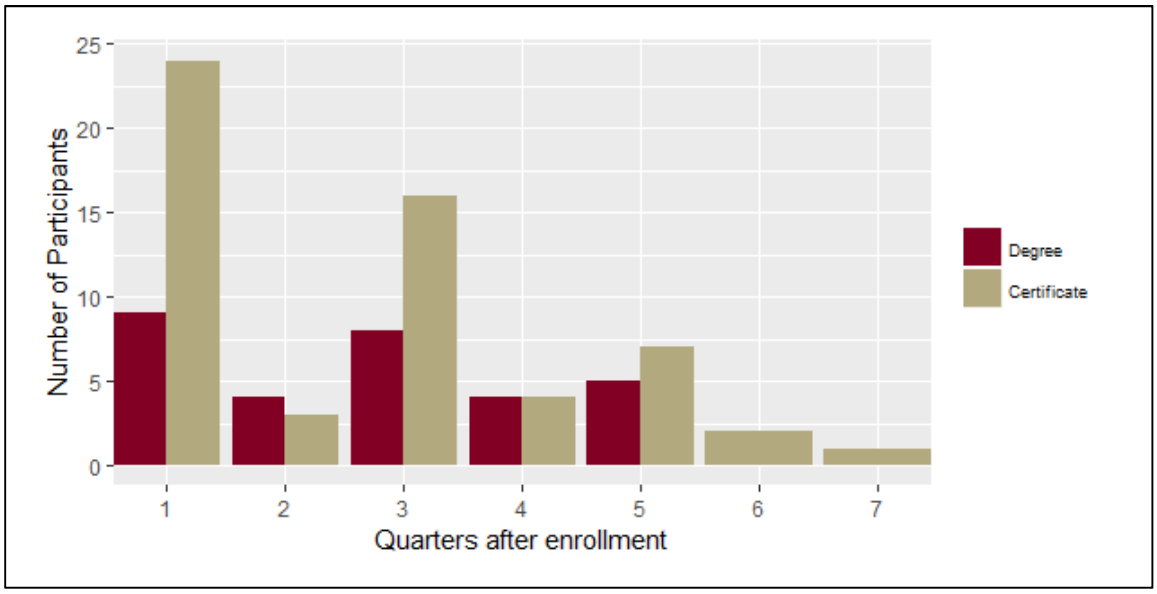
Multivariate regression analysis also showed that participants who had relatively higher number of accumulated credits in the first observed semester in the data were 2.5 percent more likely to earn a degree or certificate.

5.3.3 Time to Completion

The time students took to complete a certificate or a degree varied. The time to completion is defined as the difference between the date of enrollment and the date of program completion, measured in three-month quarters. A quarter is roughly equivalent to one semester.

Exhibit 17 shows the distribution of the time to completion in quarters for those who obtained certificates and degrees.

Exhibit 17. Time to Degree or Certificate Completion



The analysis of time to completion of a degree or certificate does not control for the number of credits accumulated at the time of program enrollment or for full-time or part-time enrollment status, both of which can strongly affect the outcome.

Among those who earned a CCBC certificate, 42 percent (24) participants completed their coursework in one semester (one quarter). As shown in Exhibit 17, some participants took longer to obtain the necessary credits to qualify for a CCBC certificate.

Among degree completers, participants took anywhere from one to five quarters to complete a degree. About 40 percent (13) of the degree completers took one or two quarters to complete, 27 percent (8) took three quarters, and the rest to more than three quarters. Given the small sample size of completers, the distribution of duration is only for descriptive purposes. Moreover, in our multivariate analysis we did not find any statistically significant association of participant characteristics on time to completion.

5.4 Participant Employment Outcomes

This section discusses the employment and earnings data on CCBC participants provided by JFI and outlines the industries in which participants were employed. The quarterly earnings data covered the fourth quarter of 2013 through the fourth quarter of 2016. Finally, we focus on students who were unemployed at time of enrollment and who subsequently gained employment.

5.4.1 Employment

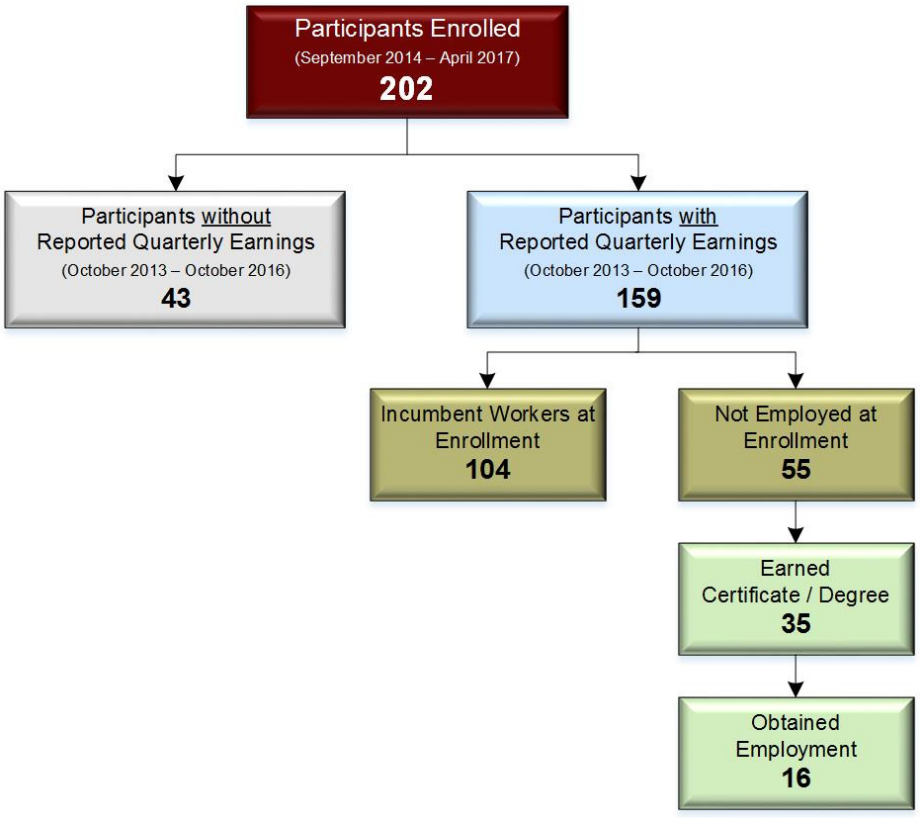
Quarterly earnings data were reported for 159 of the 202 program participants. Since the earnings data covered the period from the fourth quarter of 2013 until the fourth quarter of 2016,

most participants who were employed at any time during this period were captured in the data set. The 43 participants with no earnings data may have been unemployed, or they may not have been covered for some other reason. The JFI data set does not include people who are self-employed, employed in a state other than Maryland, or employed by the federal government. Lack of clear information on these 43 individuals means we cannot include them in the analysis.

Using only data on those individuals with available earnings information, we can separate those who were employed on enrollment from those who were not. Then we can discuss employment outcomes for program completers who were not incumbent workers at the time of enrollment.

Exhibit 18 summarizes the information above. Of the total of 202 participants, 159 had earnings information. Of those, 104 had earnings during the quarter in which they enrolled in the CCBC program, so they are counted as incumbent workers on enrollment.[42] The other 55 did not have earnings and are presumed to have been unemployed. Of those 55, 16 both completed the program and obtained employment.

Exhibit 18. Employment Outcomes of Participants



[42] CCBC intake form data show that 114 participants reported that they were employed at the time of enrollment. This discrepancy may have to do with participants' interpretation of the question on the intake form, or participants' employment status at the time of signing the form may have been different from their status on the enrollment start date. We used the administrative data from JFI for employment-related information.

5.4.2 Industry of Employment

Using the six-digit North American Industry Classification System (NAICS) codes[43] from the wage records data, we found that program participants with earnings information were employed across a variety of industries. For ease of presentation, we collapsed the six-digit industry codes to two digits to obtain broader industry categories.

Exhibit 19 shows the distribution of employment among the two-digit industry codes for participants who were shown in the data to have been employed at the time of enrollment and those who were employed during the last available quarter of earnings data, October through December 2016.[44] At enrollment, most employed participants were in the accommodation and food services and retail trade industries, followed by health care and social assistance. Only two students were employed in the information industry. Between the time of enrollment and the final quarter of earnings data, the change in distribution of industries is marginal. Although the number of participants with employment increased, only slight changes in industry types appeared in the final quarter. Industries such as finance and insurance and wholesale trade, which were not observed at the quarter of enrollment, were recorded in the last quarter of earnings data. The percentage of participants in retail trade and in accommodation and food services did not change, and there was no increase of employment in the information industry.

Exhibit 19. Industry of Employment

NAICS Code	Industry	Quarter of Enrollment	Final Quarter (Oct.–Dec. 2016)
44–45	Retail trade	35 (34%)	41 (33%)
72	Accommodation and food services	22 (21%)	26 (21%)
62	Health care and social assistance	9 (9%)	8 (6%)
56	Administrative and waste services	8 (8%)	7 (6%)
61	Educational services	7 (7%)	5 (4%)
48–49	Transportation and warehousing	7 (7%)	13 (10%)
81	Other services, except public administration	6 (6%)	4 (3%)
54	Professional and technical services	0	8 (6%)
51	Information	2 (2%)	1 (1%)
31–33	Manufacturing	2 (2%)	4 (3%)
71	Arts, entertainment, and recreation	1 (1%)	1 (1%)
23	Construction	1 (1%)	1 (1%)
54	Finance and insurance	0	3 (2%)
42	Wholesale trade	0	2 (2%)
92	Public administration	1 (1%)	0

[43] https://www.census.gov/eos/www/naics/

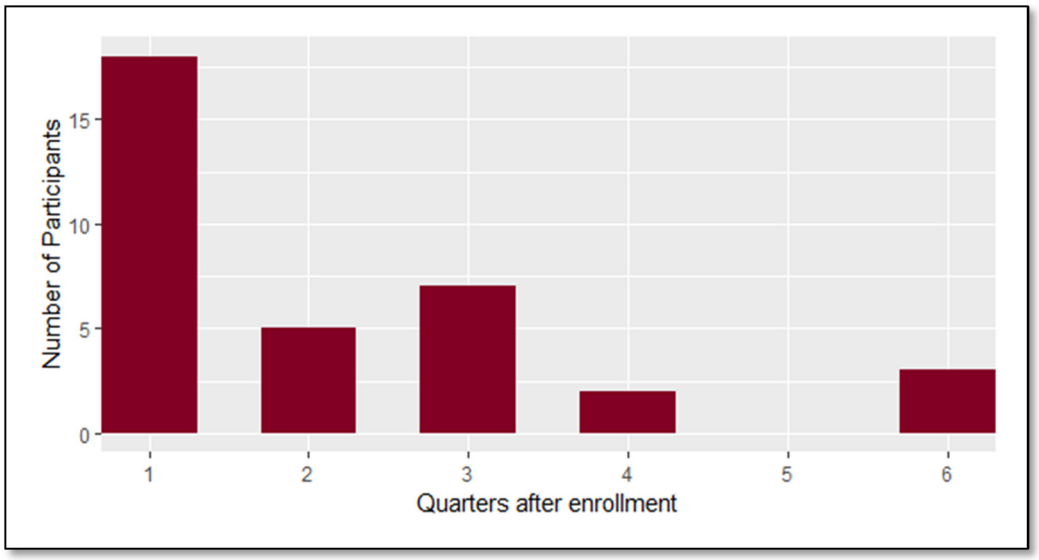
[44] Some participants had more than one industry reported. In these cases, we used the industry with highest earnings for that participant.

Based only on the NAICS industry information, it is difficult to conclude whether participants were working in occupations related to information systems security or network technology. The need for professionals in network security, cybersecurity, and other IT-related work cuts across industries. Without information on occupation titles, we do not have sufficient information to conclude whether participants were working in jobs related to their training under the CCBC program.

5.4.3 Participants Who Obtained Employment

Of the 55 participants who were shown in the wage data to have been unemployed at the time of enrollment, 35 obtained employment in the quarters subsequent to enrollment. Eighteen were employed one quarter after enrolling in the program, and five more were employed two quarters after enrollment. Exhibit 20 shows when participants obtained employment after enrollment.

Exhibit 20. Students Obtaining Employment After Enrollment



Of the 35 participants who gained employment after enrollment, 16 earned a degree or certificate. For DOL reporting purposes, TAACCCT grantees may count employment outcomes only for unemployed participants who have completed the program.[45] There were 55 participants who were unemployed at the time of enrollment. **Therefore, the 16 program completers gaining employment translates to a program employment rate of 30 percent.**

Exhibit 21 summarizes the education and labor market outcomes described above.

[45] Department of Labor, Form ETA-9160, Total Number Employed After Program of Study Completion, https://www.doleta.gov/taaccct/pdf/taaccct_round2_annua2_report.pdf

Exhibit 21. Summary of Participant Education and Labor Outcomes

Outcomes	September 2015 – April 2017
Students Enrolled	**202 (100%)**
Program Completers	93 (46%)
Educational Outcomes	
Earned Certificate	58 (29%)
Earned Degree	30 (15%)
Labor Market Outcomes*	
Unemployed at program enrollment	55 (27%)
Obtained employment during program	35 (17%)
Obtained employment and completed program	16 (8%)
Participant employment rate (%)	**30%**

* Derived from quarterly earnings data from October 2013 through December 2016.

5.5 Summary of Participant Outcomes Compared to Program Goals

Exhibit 22 compares actual program outcomes to the projected goals from the grant application. The program served a much higher number of students than was initially targeted (202 served versus 130 projected). The program enrolled a diverse group of students across age, race, gender, and labor force characteristics.

Program completion and education and employment outcomes fell short of projections, primarily because of the length of the training program, the limited evaluation follow-up period, and the broad definition of *incumbent worker.* (See the limitations section for discussion.) Therefore, the program's outcomes are likely to be underestimated.

Exhibit 22. Participant Outcomes Compared to Goals

Key Outcome Category	Goal	Actual	Difference	Goal Met?
Participants served (program enrollment)	130	202	72	Yes
Program completers [a]	105	93	(12)	No
Total participants earning credentials [b]	105	93	(17)	No
Program completers employed [c]	50	16	(34)	No

[a] Defined as the number of participants earning a degree or completing coursework required to earn a CCBC certificate or degree. Most of these participants, though they completed enough hours to earn a certificate, were still enrolled at the end of the evaluation period; many were seeking a degree.
[b] Since program completion was defined as attaining or qualifying for a CCBC certificate or degree; therefore, the total participants earning credentials is the same as total completers.
[c] Does not include employment outcomes for incumbent workers, per DOL requirements.

5.6 Limitations of Outcomes Analysis

CCBC enrolled a much higher number of students than was projected in its grant application. After the initial efforts to build training capacity and technological infrastructure were completed, the program focused on outreach and recruitment and so was able to enroll a large number of students.

The rates at which participants completed the program and gained employment must be considered within the context of the CI program's characteristics. CCBC's TAACCCT program was unique among TAACCCT programs in that the training was intended to lead to a two-year AAS degree. In other TAACCCT programs that focus on shorter-term training, participants exit the program in much less than two years and are expected to obtain employment shortly thereafter. Although CCBC could count participants who completed sufficient coursework to qualify for a CCBC certificate as completers, almost all of these students remained enrolled as they continued to work toward an AAS degree. They would not exit the program until they earned the degree. Furthermore, many students—especially those enrolled part-time—would not complete the degree program within two years. These individuals also remained enrolled and were not likely to gain new employment during the evaluation period. In addition, from our focus group discussions, an estimated 60 percent of program completers were expected to continue their education and work toward a bachelor's degree.

These challenges mean that the analysis does not capture the education and labor market outcomes of students who enrolled in the last two or three semesters of the program period. In addition, the administrative source for earnings data has limited coverage on industries and is unable to account for employment and earnings outcomes of students who are self-employed, employed outside of Maryland, or employed by the federal government. Moreover, the earnings information spans the period from October 2013 to December 2016. Program completers who gained employment in 2017 are not captured in the data, though the period of performance extended to September 2017. Thus, the results likely underestimate the actual educational and labor market outcomes of participants.

As noted earlier, the participant outcomes cannot be causally linked to the program because there was no comparison group. The program's sample size was too small to support a randomized control study, and there were no programs similar enough to this special cybersecurity program to support a quasi-experimental study. Despite this limitation, the analysis provides an indication of the program's effectiveness.

Another limitation relates to DOL's definition of an incumbent worker, which does not consider the type of industry or occupation in which the worker is employed and does not distinguish between part-time and full-time employment. Many CCBC students were employed part-time at enrollment and were therefore classed as incumbent workers. However, they may not have been employed in industries or occupations that are relevant to cybersecurity. For example, an individual employed part-time in the retail industry at the time of enrollment would be counted as an incumbent worker. These employed students were seeking new careers in the field of cybersecurity and planned to change occupations after graduation. Given the intent of the

program, these individuals arguably should not have been counted as incumbent workers because they were not working in the industry targeted by the program at the time of enrollment. At the time of our study, 104 of the 202 participants (51 percent) were incumbent workers based on DOL's definition. Even if these individuals successfully entered into new careers related to cybersecurity, they would not be counted as successful employment outcomes.

Appendix A: TAACCCT Participant Intake Form

CCBC The Community College of Baltimore County

Release of Information Statement – TAACCCT Grant

About this information collection: Community College of Baltimore County is requesting the information below to evaluate the overall effectiveness of training programs supported by grant funds. While the information is voluntary, please complete as much of the form as possible. All data supplied will be treated in a confidential manner and all reports will be based on combined data for project participants and will not include any personally- identifiable information. The data will not impact your ability to participate in programs and courses at CCBC.

Name:

Are you over 18 years of age? ☐ Yes ☐ No
Gender: ☐ Male ☐ Female
Ethnicity: Are you Hispanic/Latino? ☐ Yes ☐ No

Race: (Please check all that apply)
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☐ White

Eligible Veteran Status:
- ☐ Yes, Less Than 180 Days
- ☐ Yes, Eligible Veteran
- ☐ No

Educational Goal (you may check more than one)
- ☐ To get a job
- ☐ To get a better job
- ☐ To excel in my current job
- ☐ Personal Enrichment

Date of Birth:

Student ID:

Employer: _____

Start Date: ____/____/____

Employment Status:
- ☐ Employed Full Time
- ☐ Employed Part Time
- ☐ Employed, but received termination Notice or military separation
- ☐ Not Employed or Not in Military
- ☐ TAA (Trade Adjustment Assistance) Eligible

Employment Focus
- ☐ Currently Employed in Computer/Networking field
- ☐ Currently Employed in Cyber Security Field

Disability
- ☐ Yes
- ☐ No

Social Security Number:

Email:

I certify that I have reviewed this form and that the information given is true to best of my knowledge. I give permission for the Community College of Baltimore County to release the information above and applicable enrollment data as required by the U.S. Department of Labor for the TAACCCT grant reporting specifications. I agree to participate in follow-up surveys or additional requests for information, and I understand that any information I provide in support of the project evaluation will be kept strictly confidential and used only for reporting related to project outcomes.

_____ _____
Signature Date

This workforce product was funded by a grant awarded by the U. S. Department of Labor's Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The U.S. Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability, or ownership. It is the policy of The Community College of Baltimore County to provide equal educational and employment opportunities and not illegally discriminate on the basis of gender, race national origin, creed, age, marital status or disability in its educational programs, activities or its employment and personnel policies.

Appendix B: Digital Forensics Associate of Applied Science Degree Program – MHEC Approval Letter

MHEC
Creating a state of achievement

May 17, 2017

Dr. Mark McColloch
Vice President of Instruction
Community College of Baltimore County
7201 Rossville Boulevard
Baltimore, MD 21237

Dear Dr. McColloch:

The Maryland Higher Education Commission has reviewed a request from the Community College of Baltimore County to offer an Associate of Applied Science (A.A.S.) in Digital Forensics.

I am pleased to inform you that the program proposal is approved. This decision is based on an analysis of the program proposal in conjunction with the law and regulations governing academic program approval, in the particular Code of Maryland Regulations (COMAR) 13B.02.03. As required by COMAR, the Commission circulated the proposal to the Maryland higher education community for comment and objection. The program meets COMAR's requirements and demonstrates potential for success, an essential factor in making this decision.

For the purposes of providing enrollment and degree data to the Commission, please use the following HEGIS and CIP codes:

Program Title	Award Level	HEGIS	CIP
Digital Forensics	A.A.S	5505-00	43.0116

Should the Community College of Baltimore County desire to make a substantial modification to the program in the future, review by the Commission will be necessary. I wish you continued success.

Sincerely,

Dr. James D. Fielder
Secretary

JDF:MK:vb

C: Ms. Jody Kallis, Legislative Director, MACC

Maryland Higher Education Commission
6 N. Liberty Street • 10th Floor • Baltimore, MD 21201
T 410.767.3300 • 800.974.0203 • F 410.332.0270 • TTY for the Deaf 800.735.2258 www.mhec.maryland.gov