Cyber Force Incubator Training

Tiffany Quynh Anh Dinh

Follow this and additional works at: https://louis.uah.edu/honors-capstones

Recommended Citation
Dinh, Tiffany Quynh Anh, "Cyber Force Incubator Training" (2020). Honors Capstone Projects and Theses. 311.
https://louis.uah.edu/honors-capstones/311

This Thesis is brought to you for free and open access by the Honors College at LOUIS. It has been accepted for inclusion in Honors Capstone Projects and Theses by an authorized administrator of LOUIS.
Cyber Force Incubator Training

by

Tiffany Quynh Anh Dinh

An Honors Capstone

submitted in partial fulfillment of the requirements

for the Honors Diploma

to

The Honors College

of

The University of Alabama in Huntsville

July 20th, 2020

Honors Capstone Director: Mrs. Sharon Johnson

Center for Cybersecurity Research and Education Deputy Director

Student (signature) 07/20/2020

Director (signature) 7-21-2020

Digitally signed by William Wilkerson
Date: 2020.07.22 11:31:50 -05'00'

Digitally signed by William Wilkerson
Date: 2020.07.22 11:32:04 -05'00'

Digitally signed by William Wilkerson
Date: 2020.07.22 11:31:50 -05'00'

Digitally signed by William Wilkerson
Date: 2020.07.22 11:32:04 -05'00'
Honors Thesis Copyright Permission

This form must be signed by the student and submitted as a bound part of the thesis.

In presenting this thesis in partial fulfillment of the requirements for Honors Diploma or Certificate from The University of Alabama in Huntsville, I agree that the Library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by my advisor or, in his/her absence, by the Chair of the Department, Director of the Program, or the Dean of the Honors College. It is also understood that due recognition shall be given to me and to The University of Alabama in Huntsville in any scholarly use which may be made of any material in this thesis.

_ Tiffany Dinh _

Student Name (printed)

[Signature]

Student Signature

07/20/2020

Date
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedication</td>
<td>2</td>
</tr>
<tr>
<td>Abstract</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Objectives</td>
<td>5</td>
</tr>
<tr>
<td>Platform Development and Choice</td>
<td>6</td>
</tr>
<tr>
<td>Workflow Design</td>
<td>7</td>
</tr>
<tr>
<td>Modules</td>
<td>7</td>
</tr>
<tr>
<td>Course Structure</td>
<td>8</td>
</tr>
<tr>
<td>Instructional Design</td>
<td>10</td>
</tr>
<tr>
<td>General Subject Matter</td>
<td>10</td>
</tr>
<tr>
<td>Hands-On Projects</td>
<td>10</td>
</tr>
<tr>
<td>Technical Certifications</td>
<td>11</td>
</tr>
<tr>
<td>Testing Design</td>
<td>12</td>
</tr>
<tr>
<td>Analysis</td>
<td>13</td>
</tr>
<tr>
<td>Determination of Success</td>
<td>13</td>
</tr>
<tr>
<td>High School Level of Education</td>
<td>15</td>
</tr>
<tr>
<td>Prior Exposure to Material</td>
<td>16</td>
</tr>
<tr>
<td>Parents with Graduate-Level Education</td>
<td>17</td>
</tr>
<tr>
<td>Recommendations &amp; Future</td>
<td>18</td>
</tr>
<tr>
<td>NICE Documentation</td>
<td>20</td>
</tr>
<tr>
<td>Summary</td>
<td>28</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>29</td>
</tr>
</tbody>
</table>
Dedication

To my family and friends.

You have always supported me and my wacky decisions every step of the way.

To the individuals who have always supported me at The University of Alabama in Huntsville Center for Cybersecurity Research and Education.

I cannot thank you enough for all the opportunities you have given me to succeed and pushing me to be the best I can be.
Abstract

Cyber Force Incubator Training is a standalone project for The University of Alabama in Huntsville Center for Cybersecurity Research and Education Cyber Force Incubator. The training was made in part through a National Security Agency grant known as the Acquire, Teach, Train, and Retain Adept Cyber Team. The purpose and objective of the curriculum is to expose students to cybersecurity, giving them a head start towards a future career in the field. The audience of the curriculum ranges from underserved rural high school students to military personnel with material covering everything from workplace etiquette to malware analysis. Within this paper, there is an examination of the effort of this curriculum, its performance in whether it met its objective to educate its students, and how it will be adapting based on the analysis of its performance and findings.
Introduction

The University of Alabama in Huntsville (UAH) Center for Cybersecurity Research and Education (CCRE) serves at one of the university’s premier research centers. As a component of its research, the center is involved in all aspects of cybersecurity to include identity management, supply chain security, intrusion detection, vulnerability analysis, medical device security, and digital forensics. CCRE is certified by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a Center of Academic Excellence in Cyber Defense Education (CAE/CDE) and a National Center of Academic Excellence in Cyber Defense Research (CAE-R) to fulfill national needs in cybersecurity.

The CCRE Cyber Force Incubator (CFI) is an experimental laboratory that provides students with rigorous internships while they earn degrees to prepare them for a cybersecurity career. During the internship, the students attend orientation, receive a set of job standards, and attend mock interviews. After assessing the research center’s customer training requests and internal needs, CCRE CFI saw a need to create a CFI curriculum and certificate for its student employees to ensure they have an understanding of concepts before entering the workforce. Additionally, the research center sought to fulfill its requirements in the NSA awarded grant known as the Acquire, Teach, Train, and Retain Adept Cyber Team (ATTRACT).

This curriculum is a result of the project developed by CCRE CFI Research Assistant Tiffany Dinh and her advisor CCRE Deputy Director Sharon Johnson to meet the needs of CFI customers and future awarded education-oriented grants.
Objectives

The proposed purpose of the CCRE CFI curriculum was to create a program that allowed participants to work through coursework asynchronously and obtain a certification after meeting specified requirements. Initially, the proposed trainee coursework consisted of only a few modules: orientation course, CompTIA Security+, CompTIA Network+ and risk management framework. However, as the development for the CFI Training progressed, the course turned into a more comprehensive curriculum. Now, as of the submission of this Honors Capstone Project, CFI Training coursework covers security clearances, the cybersecurity maturity model certification, three-dimensional modeling and computer-aided-design, microcomputers modifications and creation, military etiquette, military rank and civilian structure, and government pay structure. The curriculum developer, Tiffany Dinh, created further requirements for the CFI training to improve the project for future use and for her Honors Capstone Project. The requirements were as follows:

1. Analyze students’ progress through the CFI Training.
2. Using student analytics, determine improvements and additions to be made for the future development of the CFI Training.
Platform Development and Choice

CCRE required that the platform for its CFI Training to have a clean and intuitive interface, be flexible and scalable, contain a database for recording course data, assignment and grading features, and have built-in security. The project started in January of 2020. When the curriculum developer began producing the platform, the biggest problem was making sure everything was completed before the deadline, May 2020. Additionally, instructional materials had to be produced to accompany the curriculum. It soon became apparent that creating a learning platform to accommodate all of CCRE’s needs within such a short span of time was highly improbable. After researching other free and open-source learning management systems (LMSs) on the market, it was determined that it would be cheaper and require less work to use an existing LMS than building one from scratch.

Canvas Learning Management System was chosen as CCRE’s platform for its CFI Training because of its variety of tools to help an instructor design an engaging and interactive course. CCRE gained access to the LMS through UAH. Additionally, this LMS is used across hundreds of educational institutions and organizations, including other UAH departments. Taking these factors into consideration, it became apparent that Canvas was the perfect service for the CFI Training.
Workflow Design

On Canvas LMS, it was easy to create a course for CCRE and add any students not otherwise affiliated with UAH. CFI Training’s initial objective was to create a program where trainees would be introduced to CCRE and cybersecurity workforce fundamentals. Several factors influenced the development of this program, such as the scale at which the project would be implemented, the timing of when trainees would go through the course, and whether the course developer would be accessible during the course’s testing. As a result, it was decided that the course would be most effective if students could work at their own pace. The training was scalable, timing did not matter, and an active instructor was not necessary by deciding the course would be standalone.

The decision for the course to be autonomous and asynchronous for students allowed for a student to begin the course at any point during the year and work through the material at their own pace. There would be no need to worry about a teacher delegating assignments to students nor restrictions of when and how students could complete assignments. A benefit of this choice is that CCRE would not have to spend as much time and money actively managing the training. Additionally, this decision allowed the curriculum to teach students additional skills and information about industry etiquette and standards, resulting in the idea that the course could be used to teach audiences outside of ATTRACT.

Modules

Implementing modules allowed for continuity with design and structure, specifically a linear progression. The CFI Training grouped similar material and learning objectives into modules. For example, information about military etiquette, military ranks, and civilian material
was organized under the DoD Etiquette and Structure module. To move from one module to the next, each student had to score at least 80% on the module’s assessment. Assessments varied by the category a module fell under and will be described later on. Modules allowed students to be self-sufficient with the course. Instructions on how to navigate through modules were provided through visual and informational cues.

**Course Structure**

A foreseeable issue was that students would get bored and lose motivation without an active instructor or interaction with other students. To keep trainees engaged with the course, defined objectives were created and communicated with trainees. Additionally, students had to complete modules according to a specific timeline. For example, the entire course had to be completed in eight weeks; the suggested schedule for completing the modules was given to students. Content in the course was split not only into modules but by a timeline.
**Figure**: Preview of the Full CFI Training Week 1 Module and Part of CFI Training Week 2 Module.
Instructional Design

Since CFI training aims to cover a wide variety of materials, all the concepts were grouped under three different categories: General Subject Matter, Hands-On Project, and Technical Certifications. The method by which instruction was given differed by category. For example, while one can learn math through a computer screen, riding a bike requires in-person training. With CFI training, some topics required access to a computer while others required access to circuits and tools. Under CFI Training’s three categories, the curriculum developer created instructional and assessment material differently.

General Subject Matter

General Subject Matter concepts were given to trainees to provide exposure or ensure a baseline-understanding that would be needed for working in an information technology position. Concepts defined as General Subject Matter were not weighed to need the same level of depth as the other two categories. As such, it did not make sense to provide any additional tasks beyond establishing a familiarity with some concepts. For example, trainees did not need to know everything about the security clearance process beyond the different levels, how to apply for one, and actions that would bar a person from receiving one. For topics categorized as General Subject Matter, instruction was given via Powerpoint presentations and videos. After trainees went through the material, they would take a quiz.

Hands-On Projects

While knowledge of concepts is important, it is also important that trainees have sufficient hands-on practice with the material they have learned. Thus, CFI training required students to develop their programming and computer-design skills through projects. Like
concepts related to General Subject Matter, instruction was delivered through Powerpoint presentations and videos. However, these videos and presentations had step-by-step walkthroughs of all objectives covered. Furthermore, assessments of concepts in this category not only assessed students’ knowledge of program interfaces; it also asked them to recreate projects. As a result, students were pushed to go beyond a theoretical understanding, ensuring that they understood how to apply the information they had learned.

**Technical Certifications**

CompTIA is a non-profit organization that specializes in issuing professionals information technology certifications. To work with the Department of Defense, many employers require certifications from CompTIA. Thus, CCRE wanted to include them in its course. CFI Training aimed to implement CompTIA certifications by providing students an understanding of the guidelines outlined by CompTIA certifications. Additionally, rather than reinvent already-well made and quality material on the market, the course developer used CompTIA-approved third-party material to provide instruction and assignments. This instruction would include videos over specific concepts covered by a CompTIA certification and testing over those concepts with questions often about a hypothetical real-world scenario or simulation.
Testing Design

As stated earlier, trainees were required to score a minimum of 80% on every assessment to pass the course. The score of an 80% was chosen because CCRE wanted to ensure students truly understood material they were being tested on. However, it was not expected that students would pass each assessment on their first attempt. So, students were given three attempts to obtain a passing score on each module. After each attempt, students’ assignments would be automatically graded. However, to help students improve on their subsequent attempts, they could view feedback as to why their original answer was incorrect. To prevent cheating, three tools were implemented: timing, lockdown browser, and question banks.

For timing, students had a time limit based on the following formula:

\[
\text{# of quiz questions} + 2 \text{ minutes} = \text{amount of time delegated for quiz}
\]

A time limit was imposed to prevent students from having the time to look up answers to questions on another technological device or utilize outside sources.

The lockdown browser feature on Canvas was implemented to prevent trainees from accessing anything on their personal devices besides the assessment. This would prevent trainees from looking up answers or using outside sources to answer a given question.

A question bank was developed to prevent students from memorizing their previous answers. Each assessment had its own question bank with a varying amount of questions and answer choices. Questions were pulled at random with their answer choices in a randomized order. This would prevent students from completing the assessments together as they would have different questions.
Analysis

Determination of Success

To evaluate the success of the CFI Training, students took pre- and post-training examinations. Exam scores were used to determine whether a student’s level of cybersecurity and workforce understanding improved as well as their confidence in mastering this material. In these assessments, students were tested on the following: risk management framework, security clearances, cybersecurity natural model, computer-aided-design, DoD culture, military pay structure, network basics, and cybersecurity basics. In addition to inquiries on the aforementioned subject areas, trainees were also asked about their experience with various technologies and identifiers (e.g. access to computing and technology at home, parents’ highest level of education, extracurricular involvement, etc.). Not only did the curriculum developer track whether trainees improved in terms of score; they also sought to find the most successful type of student.

Once all participants finished the CFI Training, it was found that there was a 100% improvement from all students in terms of confidence and baseline score. On average, students scored a 46% on the pre-course examination and 70% on the post-course examination. When questioned again regarding their technical backgrounds, all individuals reported increased levels of familiarity with various technologies.
As seen in the scoring documentation, there are several outliers which skewed the calculated average score. Looking at the data, it is clear that the CFI Training was successful in teaching students; however, with fewer than 10 testees, the training still needs to undergo further assessment to accurately determine its effectiveness.

Additionally, while the training was determined successful through said methods, it is difficult to firmly declare so. This is because all testees worked at CCRE. To work at CCRE, it is assumed all employees have prior experience in cybersecurity. When examining the
characteristics of what led students to have higher success than others in the training, there were three defining characteristics:

1. **High School Level of Education**

The highest indicator of success of all three characteristics was a trainee’s level of education. 50% of the testing trainees were high school students. While it may seem counterintuitive that high school students were able to outperform every other level of education, the background of the high school trainees provide a clear explanation as to why. These students were hand selected from their high schools to work at CCRE because of their capacity for success in the field. A demonstration of these students' ability for success in cybersecurity was their heavy involvement in cybersecurity — whether that be through activities or coursework. The high schoolers were from the Huntsville City School (HCS) system which provides students access to their Cybersecurity Academy. All high school participants were involved in the HCS Cybersecurity Academy, taking information security classes similar to the instruction that comprised the CFI Training as well as CyberPatriot, a cybersecurity competition for middle school to high school students.

<table>
<thead>
<tr>
<th>Primary School</th>
<th>%</th>
<th>respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some High School but no diploma</td>
<td>50%</td>
<td>4 respondents</td>
</tr>
<tr>
<td>High School Diploma (or GED)</td>
<td>13%</td>
<td>1 respondents</td>
</tr>
<tr>
<td>Some College but no diploma</td>
<td>25%</td>
<td>2 respondents</td>
</tr>
<tr>
<td>Two-Year College Degree</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Four-Year College Degree</td>
<td>13%</td>
<td>1 respondents</td>
</tr>
<tr>
<td>Graduate-level Degree</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>None of the above</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>

**Figure:** Preview of the Pre-Course Examination Responses to “What is your highest level of schooling?”
When compared to the collegiate level individuals participating in the CFI Training, the high school students had a more cybersecurity focused education. Compared to underclassmen college computing-focused major students, who majority of the time are working on finishing their general education requirements and have not gotten started with their coursework, the high school students are far more experienced in the concepts the training sought the students to understand. With a background in cybersecurity, it is comprehensible as to why the high schoolers outperformed the college students. Additionally, these college trainees majored in computer science and information systems not anything cybersecurity focused like cybersecurity engineering.

2. **Prior Exposure to Material**

There is an expectation that students employed at CCRE have prior experience in cybersecurity. However, students come into the research center with varying degrees of experience. In the pre- and post- course examinations, students were asked about their background with a variety of different technologies, ranging from computer-aided-design to web development. Over 50% of students had prior exposure to inquired technologies and performed better on assessments than their peers. These trainees not only performed more successfully than their counterparts but also moved through the course at a faster pace with some moving through the eight-week course in less than half the time allotted. Having computing opportunities or previous experience self-learning allows students to pick up technical material more easily. For example, if a student lacked technical experience, they often struggled to pick up technical vocabulary.
Parents with Graduate-Level Degrees

As proved by the previous factors, a students’ background plays a large role in their success. Parents play an important figure in the lives of their children. Often, parents are cited as the primary influence on an individual's beliefs and perceptions of the world.

On average, parents with higher education hold a higher importance to the value of education. In the CFI Training course, 63% of trainees had parents with a graduate-level degree, and these students scored higher on assessments than those that did not. One explanation for this correlation between higher education and a trainee’s success is what
these parents have taught their children. Fruitful in their own education, there can be an assumption that parents will teach their children how to study and how to perform well in an academic environment. So, in terms of the CFI Training, the high performance of children results from the influence of their graduate educated parents.

<table>
<thead>
<tr>
<th>Primary School</th>
<th>0 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some High School but no diploma</td>
<td>1 respondents</td>
</tr>
<tr>
<td>High School Diploma (or GED)</td>
<td>0 %</td>
</tr>
<tr>
<td>Some College but no diploma</td>
<td>0 %</td>
</tr>
<tr>
<td>Two-Year College Degree</td>
<td>0 %</td>
</tr>
<tr>
<td>Four-Year College Degree</td>
<td>2 respondents</td>
</tr>
<tr>
<td>Graduate-Level Degree</td>
<td>5 respondents</td>
</tr>
<tr>
<td>None of the above</td>
<td>0 %</td>
</tr>
</tbody>
</table>

**Figure:** Preview of the Pre-Course Examination Responses to “What is the highest level of schooling that either parent (or primary guardian) has completed?”

**Recommendations & Future**

In the post-course examination, students also provided feedback on training improvements. Analysis of the feedback revealed a resounding request for more visual aids and study material. For example, the Security Basics and Network Basics modules, which comprised the majority of the coursework, consisted mainly of video instruction, making it difficult for non-auditory learners to comprehend. Students were expected to complete both modules composed of over twenty hours of course material within a span of two weeks. Thus, the training often drained students if they did not pace themselves. One of the biggest difficulties CCRE had with the training were issues concerning COVID-19. While the training provided hands-on
projects for students to do in-person, COVID-19 prevented many of those activities from being used and tested. In the future, CCRE hopes to support different types of learning to ensure all trainees can succeed.

English proficiency was a significant blind spot that was missed in the creation of the CFI training that arose during its testing. Amongst the testees, there was an individual whose second language was English. The student had a substantial amount of trouble understanding the information in the course, especially the new technical jargon. To address this issue, the testee was given more time to complete assignments and unlimited attempts for some assessments. As CCRE continues to improve the CFI Training, more work will be needed to help ESL students master the material.

With the success of this CFI Training, CCRE is looking to add more modules to the training and develop this training into a two-year program. Depending on funding and grants awarded, the CFI Training may expand into a course recognized by the industry, covering high-level technical material that meets the needs of the DoD.
To begin the process of getting CFI Training recognized by industry and government, the coursework has been matched to the NICE Cybersecurity Workforce Framework. The NICE Cybersecurity Workforce Framework is an industry level recognized resource used to help current and future members of the cybersecurity workforce gain and demonstrate their skills and knowledge.
<table>
<thead>
<tr>
<th>Security</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>A001:</td>
<td>Knowledge of computer networking concepts and protocols, and network security methodologies.</td>
</tr>
<tr>
<td>A002:</td>
<td>Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).</td>
</tr>
<tr>
<td>A003:</td>
<td>Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.</td>
</tr>
<tr>
<td>A004:</td>
<td>Knowledge of cybersecurity and privacy principles.</td>
</tr>
<tr>
<td>A005:</td>
<td>Knowledge of cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td>A006:</td>
<td>Knowledge of specific operational impacts of cybersecurity lapses.</td>
</tr>
<tr>
<td>A007:</td>
<td>Knowledge of concepts and practices of processing digital forensics data.</td>
</tr>
<tr>
<td>A009:</td>
<td>Knowledge of computer networking concepts and protocols, and network security methodologies.</td>
</tr>
<tr>
<td>A010:</td>
<td>Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).</td>
</tr>
<tr>
<td>A011:</td>
<td>Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.</td>
</tr>
<tr>
<td>A012:</td>
<td>Knowledge of cybersecurity and privacy principles.</td>
</tr>
<tr>
<td>A013:</td>
<td>Knowledge of cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td>A014:</td>
<td>Knowledge of specific operational impacts of cybersecurity lapses.</td>
</tr>
<tr>
<td>A015:</td>
<td>Knowledge of cyber defense and vulnerability assessment tools and their capabilities.</td>
</tr>
<tr>
<td>A016:</td>
<td>Knowledge of cybersecurity and privacy principles and manage risks related to the use, processing, storage, and transmission of information or data.</td>
</tr>
<tr>
<td>A017:</td>
<td>Knowledge of vulnerability information notification sources (e.g., alerts, advisories, errata, and bulletins).</td>
</tr>
<tr>
<td>A018:</td>
<td>Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).</td>
</tr>
<tr>
<td>A019:</td>
<td>Knowledge of Risk Management Framework (RMF) requirements.</td>
</tr>
<tr>
<td>A020:</td>
<td>Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).</td>
</tr>
<tr>
<td>A021:</td>
<td>Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.</td>
</tr>
<tr>
<td>A022:</td>
<td>Knowledge of new and emerging information technology (IT) and cybersecurity technologies.</td>
</tr>
<tr>
<td>A023:</td>
<td>Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).</td>
</tr>
<tr>
<td>A024:</td>
<td>Knowledge of structural analysis principles and methods.</td>
</tr>
<tr>
<td>A025:</td>
<td>Knowledge of systems diagnostic tools and fault identification techniques.</td>
</tr>
<tr>
<td>A026:</td>
<td>Knowledge of the organization's enterprise information technology (IT) goals and objectives.</td>
</tr>
<tr>
<td>A027:</td>
<td>Knowledge of Supply Chain Risk Management Practices (NIST SP 800-162).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Management Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>A030:</td>
</tr>
<tr>
<td>A031:</td>
</tr>
<tr>
<td>A032:</td>
</tr>
<tr>
<td>A033:</td>
</tr>
<tr>
<td>A034:</td>
</tr>
<tr>
<td>A035:</td>
</tr>
<tr>
<td>A036:</td>
</tr>
<tr>
<td>A037:</td>
</tr>
<tr>
<td>A038:</td>
</tr>
<tr>
<td>A039:</td>
</tr>
<tr>
<td>A040:</td>
</tr>
<tr>
<td>A041:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity Maturity Model Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>X030:</td>
</tr>
<tr>
<td>X031:</td>
</tr>
<tr>
<td>X032:</td>
</tr>
<tr>
<td>X033:</td>
</tr>
<tr>
<td>X034:</td>
</tr>
<tr>
<td>X035:</td>
</tr>
<tr>
<td>X036:</td>
</tr>
<tr>
<td>X037:</td>
</tr>
<tr>
<td>X038:</td>
</tr>
<tr>
<td>X039:</td>
</tr>
<tr>
<td>X040:</td>
</tr>
<tr>
<td>X041:</td>
</tr>
<tr>
<td>X042:</td>
</tr>
<tr>
<td>X043:</td>
</tr>
<tr>
<td>X044:</td>
</tr>
<tr>
<td>X045:</td>
</tr>
<tr>
<td>X046:</td>
</tr>
<tr>
<td>X047:</td>
</tr>
<tr>
<td>X048:</td>
</tr>
<tr>
<td>X049:</td>
</tr>
<tr>
<td>X050:</td>
</tr>
<tr>
<td>X051:</td>
</tr>
<tr>
<td>X052:</td>
</tr>
<tr>
<td>X053:</td>
</tr>
<tr>
<td>X054:</td>
</tr>
<tr>
<td>X055:</td>
</tr>
<tr>
<td>X056:</td>
</tr>
<tr>
<td>X057:</td>
</tr>
<tr>
<td>X058:</td>
</tr>
<tr>
<td>X059:</td>
</tr>
<tr>
<td>X060:</td>
</tr>
<tr>
<td>X061:</td>
</tr>
</tbody>
</table>
K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
K0565: Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network
K0342: Knowledge of penetration testing principles, tools, and techniques.
K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0308: Knowledge of cryptology.
K0292: Knowledge of the operations and processes for incident, problem, and event management.
K0263: Knowledge of information technology (IT) risk management policies, requirements, and procedures.
K0259: Knowledge of malware analysis concepts and methodologies.
K0244: Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.
K0242: Knowledge of organizational security policies.
K0229: Knowledge of applications that can log errors, exceptions, and application faults and logging.
K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating
K0197: Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).
K0180: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or
K0167: Knowledge of system administration, network, and operating system hardening techniques.
K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
K0142: Knowledge of collection management processes, capabilities, and limitations.
K0136: Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
K0135: Knowledge of web filtering technologies.
K0133: Knowledge of web filtering technologies.
K0126: Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
K0108: Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
K0109: Knowledge of physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, network interface cards, data storages).
K0100: Knowledge of the enterprise information technology (IT) architecture.
K0101: Knowledge of the organization's enterprise information technology (IT) goals and objectives.
K0102: Knowledge of the systems engineering process.
K01010: Knowledge of the type and frequency of routine hardware maintenance.
K0104: Knowledge of Virtual Private Network (VPN) security.
K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0107: Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
K0108: Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
K0109: Knowledge of physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, network interface cards, data storages).
K0110: Knowledge of adversarial tactics, techniques, and procedures.
K0111: Knowledge of network tools (e.g., ping, traceroute, nmap).
K0112: Knowledge of defense-in-depth principles and network security architecture.
K0113: Knowledge of different types of network communication (e.g., LAN, WAN, MAN, MAN, WAN, WAN).
K0114: Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic scanners, handheld, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, fax machines, etc.).
K0116: Knowledge of file extensions (e.g., .jpg, .bat, .txt, .xml, .jpg).
K0117: Knowledge of the file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT3]).
K0118: Knowledge of processes for seizing and preserving digital evidence.
K0123: Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
K0125: Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.
K0126: Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
K0128: Knowledge of types and collection of persistent data.
K0129: Knowledge of command-line tools (e.g., mkid, mv, ls, passwd, grep).
K0130: Knowledge of virtualization technologies and virtual machine development and maintenance.
K0135: Knowledge of web filtering technologies.
K0136: Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, RJ, web forums, Direct Video Broadcasts).
K0137: Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WiFi, SCADA).
K0138: Knowledge of Wi-Fi.
A0170: Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

A0111: Ability to work across departments and business units to implement an organization's strategy and/or planning products.

A0063:Ability to operate different electronic communication systems and methods (e.g., e-mail, phone, fax, other communications).

A0062: Ability to monitor measures or indicators of system performance and availability.

A0058: Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).

A0055: Ability to operate common network tools (e.g., ping, traceroute, nslookup).

K0624: Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list).

K0420: Knowledge of database theory.

K0344: Knowledge of an organization's threat environment.

K0297: Knowledge of countermeasure design for identified security risks.

K0276: Knowledge of security management.

K0263: Knowledge of information technology (IT) risk management policies, requirements, and procedures.

K0259: Knowledge of malware analysis concepts and methodologies.

K0229: Knowledge of applications that can log errors, exceptions, and application faults and logging.

K0222: Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.

K0200: Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).

K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

K0169: Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.

K0161: Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).

K0159: Knowledge of Voice over IP (VoIP).

K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).

K0144: Knowledge of social dynamics of computer attackers in a global context.

K0140: Knowledge of secure coding techniques.

K0139: Knowledge of interpreted and compiled computer languages.

K0123: Knowledge of legal governance related to admissibility (e.g., Rules of Evidence).

K0112: Knowledge of defense-in-depth principles and network security architecture.

K0101: Knowledge of the organization's enterprise information technology (IT) goals and objectives.

K0077: Knowledge of server and client operating systems.

K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).

K0069: Knowledge of query languages such as SQL (structured query language).

K0065: Knowledge of policy-based and risk adaptive access controls.

K0059: Knowledge of new and emerging information technology (IT) and cybersecurity technologies.

K0054: Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, and management techniques.

K0053: Knowledge of measures or indicators of system performance and availability.

K0051: Knowledge of low-level computer languages (e.g., assembly languages).

K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, accountability).

K0040: Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).

K0036: Knowledge of human-computer interaction principles.

K0028: Knowledge of organization's evaluation and validation requirements.

K0019: Knowledge of cryptography and cryptographic key management concepts.

K0018: Knowledge of encryption algorithms.

K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
MACE

A0001: Ability to identify systemic security issues based on the analysis of vulnerability and system problems.
A0032: Ability to develop curriculum for use within a virtual environment.
A0063: Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
A0055: Ability to operate common network tools (e.g., ping, traceroute, nslookup).
A0010: Ability to analyze malware.
A0015: Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
A0018: Ability to develop clear directions and instructional materials.
A0019: Ability to develop curriculum for use within a virtual environment.
A0041: Ability to use data visualization tools (e.g., Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js).
A0042: Knowledge of telecommunication and broadcast technologies and systems (e.g., satellite, radio, cellular, microwave, fiber optic, cable, ISDN, T1, T3, POTS, Ethernet, Token Ring, Broadband).
The text contains various knowledge areas related to computer networking, security, and protocols. Some specific areas include:

- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Knowledge of risk management processes and methodologies.
- Knowledge of laws, regulations, policies, and as they relate to cybersecurity and privacy.
- Knowledge of cybersecurity and privacy principles.
- Knowledge of cyber threats and vulnerabilities.
- Knowledge of specific operational impacts of cybersecurity/laws.
- Knowledge of critical infrastructure systems with information communication technology that were designed without a system security consideration.
- Knowledge of software reverse engineering techniques.
- Knowledge of covert communication techniques.
- Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Knowledge of systems and applications security threats and vulnerabilities.
- Knowledge of communication methods, principles, and concepts that support the network infrastructure.
- Knowledge of incident response and handling methodologies.
- Knowledge of covert communication techniques.
- Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Knowledge of systems and applications security threats and vulnerabilities.
- Knowledge of communication methods, principles, and concepts that support the network infrastructure.

These areas cover a broad spectrum of cybersecurity and networking knowledge, from basic concepts to advanced methodologies.
Knowledge of computer networking concepts and protocols, and network security methodologies.

Addressed in a contract and that the contractor meets the functional and security to determine the effectiveness of the controls (i.e., management, operational, and technical security controls and control enhancements).

Ability to conduct a comprehensive assessment of the confidentiality, integrity, availability, authentication, non-repudiation.

Ability to apply techniques for detecting host and network-based intrusions using relevant to confidentiality, integrity, availability, authentication, non-repudiation.

Ability to accurately and completely source all data used in intelligence, assessment.

Ability to monitor traffic flows across the network.

Ability to operate the organization’s LAN/WAN pathways.

Ability to operate common network tools (e.g., ping, traceroute, nslookup).

Ability to operate network equipment including hubs, routers, switches, bridges, logic.

Ability to identify systemic security issues based on the analysis of vulnerability and.

Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list).

Knowledge of controls related to the use, processing, storage, and transmission of data.

Knowledge of principles and methods for integrating system components.

Knowledge of operating system command-line tools.

Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).

Knowledge of systems engineering theories, concepts, and methods.

Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi), paging, telephones, copiers, facsimile machines, etc.).

Knowledge of the range of existing networks (e.g., PEX, LAN, WAN, WiFi, SCADA).

Knowledge of 802.11.

Knowledge of interpreted and compiled computer languages.

Knowledge of collection management processes, capabilities, and limitations.

Knowledge of front-end collection systems, including traffic collection, filtering, and selection.

Knowledge of security event correlation tools.

Knowledge of electronic evidence law.

Knowledge of legal rules of evidence and court procedure.

Knowledge of cyber defense and information security policies, procedures, and regulations.

Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).

Knowledge of Voice over IP (VoIP).

Knowledge of the common attack vectors on the network layer.

Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).

Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-reason state sponsored, and nation sponsored).

Knowledge of system administration, network, and operating system hardening techniques.

Knowledge of applicable laws, statutes (e.g. in Titles 10, 18, 32, 50 U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal/legal guidelines and procedures.

Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).

Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.

Knowledge of data caring tools and techniques (e.g., Forensics).

Knowledge of reverse engineering concepts.

Knowledge of anti-forensics tactics, techniques, and procedures.

Knowledge of forensic lab design configuration and support applications (e.g., VMWare, WinExpert).

Knowledge of debugging procedures and tools.

Knowledge of file type abuse by adversaries for anomalous behavior.

Knowledge of malware analysis tools (e.g., OleView, MalPills).

Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer’s display device).

Knowledge of cloud service models and how those models can limit incident response.

Knowledge of industry best practices for service desk.

Knowledge of organizational security policies.

Knowledge of remote access protocols, tools, and capabilities related to customer support.

Knowledge of binary analysis.

Knowledge of network architecture concepts including topology, protocols, and components.

Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).

Knowledge of malware analysis concepts and methodologies.

Knowledge of Personally Identifiable Information (PII) data security standards.

Knowledge of Payment Card Industry (PCI) data security standards.

Knowledge of Personal Health Information (PHI) data security standards.

Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.

Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), infrared, Wi-Fi, wireless fidelity, packet level analysis using appropriate tools (e.g., WinExpert, tcpdump).

Knowledge of the basic operation of computers.

Knowledge of the use of sub-netting tools.

Knowledge of concepts and practices of processing digital forensic data.

Knowledge of cryptography.

Knowledge of trademarking.

Knowledge of procedures used for documenting and querying reported incidents, problems, and events.

Knowledge of operating system command line tools.

Knowledge of embedded systems.

Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.

Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.
K0032: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0034: Knowledge of network traffic analysis (tools, methodologies, processes).
K0039: Knowledge of how to use network analysis tools to identify vulnerabilities.
K0042: Knowledge of penetration testing principles, tools, and techniques.
K0046: Knowledge of principles and methods for integrating system components.
K0047: Knowledge and understanding of operational design.
K0050: Knowledge of the common networking and routing protocols (e.g., TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
K0052: Knowledge of controls related to the use, processing, storage, and transmission of data.
K0064: Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list)

Network Basics

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004: Knowledge of cybersecurity and privacy principles.
K0005: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0006: Knowledge of specific operational impacts of cybersecurity/apes.
K0009: Knowledge of application vulnerabilities.
K0010: Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, data).
K0011: Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
K0012: Knowledge of Virtual Private Network (VPN) security.
K0013: Knowledge of interpreted and compiled computer languages.
K0014: Knowledge of deployable forensics.
K0015: Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
K0016: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
K0017: Knowledge of organizational security policies.
K0018: Knowledge of encryption algorithms.
K0019: Knowledge of cyber defense and information security policies, procedures, and regulations.
K0020: Knowledge of legal rules of evidence and court procedure.
K0021: Knowledge of cyber defense activities.
K0022: Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
K0024: Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list)
K0025: Knowledge of organizational security policies.
K0026: Knowledge of malware analysis concepts and methodologies.
K0027: Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, etc.).
K0028: Knowledge of Personal Health Information (PHI) data security standards.
K0029: Knowledge of organization’s Local and Wide Area Network connections.
K0030: Knowledge of payment card industry (PCI) data security standards.
K0031: Knowledge of nationally and internationally recognized certification programs (e.g., CompTIA, Certified Ethical Hacker, Certified Information Systems Security Professional (CISSP), etc.).
K0032: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0033: Knowledge of development policies, plans, and strategy in compliance with laws, regulations, and standards in support of organizational cyber activities.
K0034: Knowledge of network traffic analysis (tools, methodologies, processes).
K0035: Knowledge of how to use network analysis tools to identify vulnerabilities.
K0036: Knowledge of penetration testing principles, tools, and techniques.
K0037: Knowledge of principles and methods for integrating system components.
K0038: Knowledge and understanding of operational design.
K0039: Knowledge of the common networking and routing protocols (e.g., TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
K0040: Knowledge of controls related to the use, processing, storage, and transmission of data.
K0041: Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list)

EOI-Enclave and Structure

K0042: Knowledge of computer networking concepts and protocols, and network security methodologies.
K0043: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0044: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0045: Knowledge of cybersecurity and privacy principles.
K0046: Knowledge of cyber threats and vulnerabilities.
K0047: Knowledge of emerging security issues, risks, and vulnerabilities.
K0048: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0049: Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.
K0050: Knowledge of network architecture concepts including topology, protocols, and components.
K0051: Knowledge of binary analysis.
K0052: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
K0053: Knowledge of countermeasure design for identified security risks.
K0054: Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.
K0055: Knowledge of local area and wide area networking principles and concepts including bandwidth management technologies.
K0056: Knowledge of principles and methods for integrating system components.
K0057: Knowledge and understanding of operational design.
K0058: Knowledge of network traffic analysis methods.
K0059: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0060: Knowledge of remote access technology concepts.
K0061: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0062: Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
K0063: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
K0064: Knowledge of operational impact from system and application security vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
Summary

The CFI Training met its initial objectives in teaching an introductory cybersecurity course to its testees. The modular training took over a half a year to create. The curriculum developer, Tiffany Dinh, primarily based the training around industry standard certifications and desires from CCRE customers. Utilizing her curriculum in a three-month timespan, Dinh tested a diverse pool of students to evaluate the effectiveness of the project. Dinh found her training to be a success but sees continuous improvements that can be made regarding accommodating different learning styles and future module developments. Her analysis of student results found three distinctive indicators of higher success amongst students: high school level of education, prior exposure to material, and having parents with graduate-level education. Upon submission of this Honors Capstone Project, Dinh will continue to modify the training to better meet the needs of the research center and the cybersecurity needs of the nation.
Acknowledgements

The author would like to especially thank Mrs. Sharon Johnson for her continuous support in not
only her Honors Capstone but her efforts in education and industry.

The author would also like to thank all the faculty and student employees at The University of
Alabama in Huntsville Center for Cybersecurity Research and Education. Without their
assistance, this project would not have even been a possibility.