Cybersecurity
at Columbus State

Associate of Applied Science in Cybersecurity
Launching 2017

NSF ATE Grant 14-577
Ohio Region Cyber Security Technician Training Pipeline

Evaluation Plan for Programming Developed by:
Columbus State Community College

Prepared by:

Justin Sullivan, M.S.
University of Wisconsin-Stout Applied Research Center
Associate Institutional Planner – Project Manager

Jason Nicholas, M.S.
University of Wisconsin-Stout Applied Research Center
Associate Institutional Planner – Project Manager

September 19, 2014

COLUMBUS STATE
CYBERSECURITY

The evaluation will be conducted by the UW-Stout Applied Research Center (ARC). The ARC, established in 2007, specializes in providing clients with results that can directly influence decision making, particularly in the area of evaluation. UW-Stout ARC staff have received formal training in evaluation studies, and several hold Doctoral and Master degrees in this field. The staff have over 50 years of combined experience working with clients in survey development and administration, statistical analysis, qualitative analysis, designing evaluation instruments, and other aspects of research design. The ARC has provided evaluation services for approximately $35 million in grant funded programs, through grants from the National Science Foundation, Department of Education, Education Trust, UW System and UW-Stout.

The purpose of the evaluation plan is twofold: 1) *Summative:* to measure achievement of the overall project goal and identified outcomes, including an assessment of the broader impacts of the program and impact on student learning, and 2) *Formative:* to assess implementation, participation, and satisfaction with the identified program activities, in order to provide data for program improvement and data to increase interest and enrollment in the program. Tables 1 through 3 describe the evaluation methods.

Table 1. Summative Evaluation Plan

Goal:	**Student Outcomes:**	**Evaluation Methods:**
Establish a CyberSecurity Training Pipeline in the Ohio region to increase the supply of qualified CyberSecurity professionals for industry and government	High levels of student learning	-Course artifacts *(see Table 3)* -Course grades
	Retention and completion rates exceed that of comparative groups	-First to second year retention rates -Three year associate degree completion rates -Six year bachelor's degree completion rates -Self-reported intentions for persistence and completion *(see CSCC Student Entry/Exit Survey in Table 3)*
	Performance on SSCP certification exam exceeds national comparisons	-Pass rates on the SSCP certification exam for program participants vs. national comparisons -Scores on the SSCP certification exam for program participants vs. national comparisons
	High student placement rates and levels of employer satisfaction	Determine when data will be collected

Table 2. Formative Evaluation Plan

Project Objectives:	**Major Program Activities:**	**Evaluation Methods:**
Develop and implement a 60-credit hour Associate of Applied Science degree and related academic certificates in CyberSecurity	-Establish CyberSecurity Technology program -Recruit program participants	-Program enrollments -Applications to the program -CSCC Student Entry/Exit Survey *(see Table 3)*
Develop a pre-college initiative model for regional high schools to serve as the first link in a 2+2+2 CyberSecruity training pipeline by developing and implementing a CyberSecruity education workshop for high school teacher professional devt.	-Conduct educators workshop for regional high schools	-Post-educators workshop survey *(see Table 3)* -Pre/post CyberSecurity education for faculty *(see Table 3)*
Develop a model articulation agreement for regional four-year universities to serve as the final link in a 2+2+2 CyberSecurity training pipeline, ensure seamless transfer.	-Establish training pipeline	-Program enrollments -Applications to the program -CSCC Student Entry/Exit Survey *(see Table 3)*

The following data collection methods will be used for both formative and summative assessment:

Table 3. Data Collection Methods

Data Collection Method	**Description**	**Usage in evaluation**

CSCC Student Entry/Exit Survey	A survey to be administered to students when they enter the program and again when they exit (either through graduation or if they drop out) to collect information on: demographics, how they learned about the program, and intentions for transfer to 4-year university.	Formative and Summative
Course artifacts	Each instructor will identify one artifact that best demonstrates student learning in each course. Examples might include exams, course projects or presentations. A common rubric will be used to assess student learning	Summative
Enrollment, Retention and completion rates	Data for the new CyberSecurity program will be gathered directly from the Placement Office at CSCC and compared to data published by Ohio Higher Ed, University System of Ohio, and national benchmarks to compare applications, enrollment, retention and graduation rates.	Formative and Summative
Course grades	Final course grades will be examined and compared to college-wide data	Summative
Placement data and employer satisfaction	Determine when data will be collected	Summative
SSCP certification exam	Scores and pass rates on the SSCP certification exam will be calculated for the program participants and compared to national comparisons.	Summative
Post-educators workshop survey	Two surveys to high school faculty members who participate in the Educator's Workshop: -The first will be quantitative and designed to measure the level of satisfaction among faculty in regard to the training they received during the Educators Workshop. -A second qualitative survey will be administered 3 months later to identify strengths and weaknesses of strategies provided in the workshop and how they might be applied at the participant's site. Insight from this review can be used to identify potential barriers and successes on a larger scale.	Formative
Pre/Post CyberSecurity education for faculty	As outlined in section D.2 CyberSecurity of the proposal, High school faculty attending the Educator's Workshop will be administered a pre and post-test to measure levels of CyberSecurity education.	Formative