CLARK COLLEGE
EST. 1933

CLARK COLLEGE

BACCALAUREATE

OF

APPLIED SCIENCE IN CYBERSECURITY

Prepared by Dwight Hughes

Dept. Chair Network Technology

Clark College

COVER SHEET
NEW DEGREE PROGRAM PROPOSAL

Program Information

Institution Name: **Clark College**

Degree: **Bachelor of Applied Science in Cybersecurity** CIP Code: 52.2101

Name(s) of the existing technical associate degree(s) that will serve as the foundation for this program:

Degree:	Network technology AAT	CIP Code:	11.0901	Year Began:	**2010**
Degree:	Cisco Technology AAT	CIP Code:	15.0305	Year Began:	**1995**
Degree:	Computer Support AAT	CIP Code:	15.0305	Year Began:	**1995**

Planned Implementation Date (i.e. Fall 2014): **Fall 2019**

Proposal Criteria: *Please respond to all eight (8) areas listed in proposal criteria FORM D.*
Page Limit: 30 pages

Contact Information

Name: Dwight Hughes

Title: Professor, Department Head of Network Technology

Address: Clark College, 1933 Fort Vancouver Way, Mail-Stop JSH-211, Vancouver WA 98663

Telephone: (360) 992-2417

Fax: (360) 992-2897

Email: dhughes@clark.edu

Chief Academic Officer Date

NEW DEGREE PROGRAM PROPOSAL

Table of Contents

Introduction

As established by our submitted Statement of Need document this proposed program and the curriculum contained within it are desperately needed within our service area. Currently employers, students, and the communities we serve are without a bachelor level education offering specific to cybersecurity.

The proposed BAS program was developed with input and guidance from local employers and our industry advisory committee to meet the needs of working adults. With a blend of hybrid and online courses and block scheduling students only physically come to campus two evenings a week and can complete the program in as little as 18 months. Many of our courses target industry certification attainment, such as: CompTIA PenTest+, CySA+, and Cisco CCNA CyberOps.

The Cybersecurity BAS program and course outcomes for this program are aligned with the Threat Analysis Specialty Area of the National Institute for Science and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, see Appendix C for more information about the NICE Cybersecurity Workforce Framework. The focus of this specialty area is to identify and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produce findings to help initialize or support law enforcement and counterintelligence investigations or activities.

We are meeting the needs of our students graduating from identified AAT feeder programs by providing a relevant and in-demand baccalaureate degree for them while also making their continued education possible with courses designed for working adults and adults with families and complex schedules. With a mix of both hybrid and online courses students only physically come to campus two evenings a week and can complete the program in 18 months.

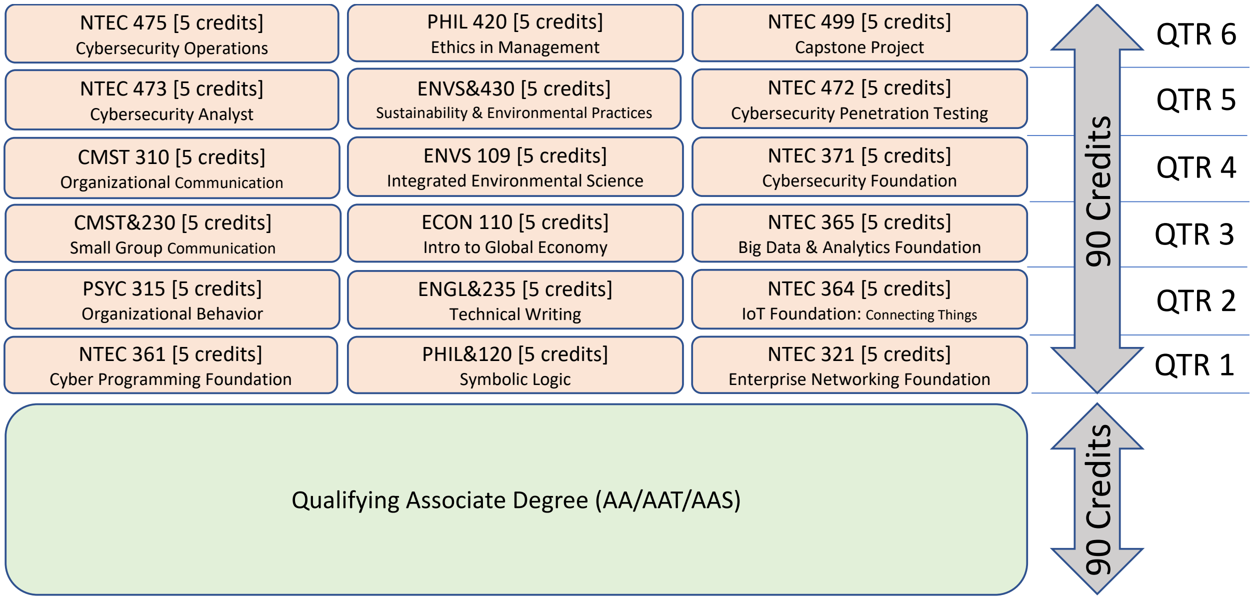
A national standards-based curriculum developed in alignment with the NISTs NICE Framework for cybersecurity education skillsets, courses conceived with the input of local industry partners and industry advisory committee. The program will continue to be mentored and monitored by this committee going forward.

Upon graduation, students are well positioned for success in the job market in network technology cybersecurity job roles, such as a cybersecurity analyst career. Or, they can continue on with their education at WGU in their online master’s degree program in information technology.

Criteria 1: Curriculum demonstrates baccalaureate level rigor.

The Curriculum
The program curriculum is based in industry certifications and alignment to the National Initiative for Cybersecurity Education (NICE) Framework, which defines specific skillsets and careers within cybersecurity. The curriculum is designed to teach students the cybersecurity skills needed for career family wage employment success within our service district and beyond. The curriculum tracks towards several industry certifications of increasing rigor, including: CompTIA Security+, CompTIA PenTest+, CompTIA CySA+, and also Cisco CCNA CyberOps.

The entire degree and a suggested course progression for a full-time student.



NTEC 475 [5 credits] Cybersecurity Operations	PHIL 420 [5 credits] Ethics in Management	NTEC 499 [5 credits] Capstone Project	QTR 6
NTEC 473 [5 credits] Cybersecurity Analyst	ENVS&430 [5 credits] Sustainability & Environmental Practices	NTEC 472 [5 credits] Cybersecurity Penetration Testing	QTR 5
CMST 310 [5 credits] Organizational Communication	ENVS 109 [5 credits] Integrated Environmental Science	NTEC 371 [5 credits] Cybersecurity Foundation	QTR 4
CMST&230 [5 credits] Small Group Communication	ECON 110 [5 credits] Intro to Global Economy	NTEC 365 [5 credits] Big Data & Analytics Foundation	QTR 3
PSYC 315 [5 credits] Organizational Behavior	ENGL&235 [5 credits] Technical Writing	NTEC 364 [5 credits] IoT Foundation: Connecting Things	QTR 2
NTEC 361 [5 credits] Cyber Programming Foundation	PHIL&120 [5 credits] Symbolic Logic	NTEC 321 [5 credits] Enterprise Networking Foundation	QTR 1

BAS General Education Requirements	45 credits
Communication Skills [10 credits]	ENGL&235, CMST&310
Quantitative/Symbolic Reasoning Skills [5 credits]	PHIL&120
Humanities [10 credits]	CMST&230, PHIL420
Social Science [10 credits]	ECON110, PSYC315
Natural Science [10 credits]	ENVS109, ENVS 430
Qualifying AA/AAT/AAS General Education Requirements	15 credits
Communication Skills [5 credits]	ENGL&101
Computational Skills [5 credits]	MATH&107 -or- MATH111
Human Relations Skills [5 credits]	Any courses from approved distribution list.
BAS Core Coursework	45 credits
	NTEC321, NTEC361, NTEC364, NTEC365, NTEC371, NTEC472, NTEC473, NTEC475, NTEC499

The above table illustrates the distribution of the 180 credits in meeting general education requirements. All courses listed in the table are 5 credit courses. Complete course descriptions for all courses within the Cybersecurity BAS are included in Appendix B.

Program Learning Outcomes

The program learning outcomes are aligned with the primary workplace skillsets of a career as a cybersecurity analyst. Program learning outcomes:

A. Implement, administer, and support enterprise information technologies and systems.

B. Implement security measures and practices for an organization's information technology resources.

C. Evaluate organization needs and use those to plan the implementation of information technology systems.

D. Analyze the security vulnerabilities of an organization's information technology resources and use that information to plan the implementation of security measures.

Measuring Student Success

A capstone project course taken at the end of the program is designed to evaluate student proficiency in all program outcomes (see program learning outcomes above) through a rigorous research-based team project with a hands-on lab mockup demonstration component. Further, each core course within the program has one or more of their course outcomes that are specifically mapped to one or more of the program outcomes and an identified assessment for measuring success: usually the final exam or a skills-based hands-on evaluation of student skills and abilities. The table below details which courses specifically support a program learning outcome (refer to A-D program learning outcomes above):

Outcome	YEAR ONE					YEAR TWO			
	NTEC	NTEC	NTEC	NTEC	NTEC	NTEC	NTEC	NTEC	NTEC
	321	361	364	365	371	472	473	475	499
A	X	X	X	X	X				X
B					X	X		X	X
C	X		X		X	X	X		X
D				X	X				X

We have already begun to implement an industry advisory committee for this program, as an extension of our existing industry advisory committee for related associate degree network technology degrees this sub-committee of that committee will specifically monitor, advise, and support the growth and success of this program.

Faculty already have a strong voice in this program. Creation of the program and its core coursework was faculty lead and the Network Technology (NTEC) department faculty meet regularly with their chair and dean to discuss feedback, concerns, ideas, and plans for this program.

Assessment Plan

Student satisfaction, progress, and success in the Cybersecurity BAS program will be measured annually as detailed in the table below:

Annual Assessment		
Period	**Data Collected**	**Responsibility**
Spring 2020	• Student survey • Faculty evaluations • Retention data • Faculty survey of student readiness	Program Manager, Program Chair, Program Faculty, Dean, VP Instruction, Office of Planning and Effectiveness, Industry Advisory Committee
Spring 2021	• Student survey • Faculty evaluations • Retention data • Faculty survey of student readiness	Program Manager, Program Chair, Program Faculty, Dean, VP Instruction, Office of Planning and Effectiveness, Industry Advisory Committee
Spring 2022	• Student survey • Faculty evaluations • Retention data • Retention and graduation data • Wage, job and progressions data • Employer Survey • Faculty survey of student readiness	Program Manager, Program Chair, Program Faculty, Dean, VP Instruction, Office of Planning and Effectiveness, Industry Advisory Committee
Spring 2023	• Student survey • Faculty evaluations • Retention data • Retention and graduation data • Wage, job and progressions data • Employer survey • Faculty survey of student readiness	Program Manager, Program Chair, Program Faculty, Dean, VP Instruction, Office of Planning and Effectiveness, Industry Advisory Committee
Spring 2024	Five Year Review. Convene a BAS Professional Work Group to ascertain the relevance of curriculum to employer needs, and perceived strengths and weaknesses of the program. Also continue annual review items, • Student survey • Faculty evaluations • Retention data • Retention and graduation data • Wage, job and progressions data • Employer survey • Faculty survey of student readiness	Program Manager, Program Chair, Program Faculty, Dean, VP Instruction, Office of Planning and Effectiveness, Industry Advisory Committee

Incoming Students
Three AAT degrees at Clark College will provide internal feeder programs and those students will have complete alignment to the entry point for this BAS program. Students should place at the entry placement points for Math and English. There should be zero credit loss for these students, and they should be able to complete the cybersecurity BAS program on time without the need for additional coursework beyond that required within the program.

Currently identified external pathways are too varied to have a systematic approach to accepting incoming credits, instead we must evaluate external coursework on an individual basis until formal articulation agreements are worked out with the institutions behind these external pipelines.

Our currently identified feeder pipeline associate degrees are all heavily related to computer networking and students will have taken several networking related courses within those associate degrees. Many of our program core courses qualify for Credit for Prior Learning, allowing students with a qualifying industry certification related to a course to get credit for the course by providing proof of their valid industry certification. For example, an incoming student could obtain Credit for Prior Learning for the NTEC 321 Enterprise Network Foundation course by having one of these industry certifications: CompTIA Network+, Cisco CCENT, CCNA. This approach allows the program to accept students with a wider range of prior skills and abilities in prerequisite skills like computer networking.

General Education Component
Each general education course has been carefully considered and chosen for this program. All general education courses within this program have been specified for students. General education courses were chosen that met key focus areas we had identified: critical thinking, understanding human behavior, and organization and planning.

Dedicated sections of program required general education courses will be offered specifically for our program cohort. ctcLink will afford us the ability to control student course registrations on an individual section of a course. This will ensure program students are always guaranteed a seat in the courses on their degree path. These courses will be block scheduled to fit with our evening block scheduling for this degree.

General education courses in this program are all shared with other BAS degrees at Clark College, none are uniquely created for this program. The general education and core courses are blended throughout the program duration, with students taking both general education and core courses together each term as part of their course load.

Criteria 2: Qualified faculty.

Total Faculty FTE Allocated to the Program
The total faculty FTE that has been allocated to the program for the first two years of the program is one tenure-track professor for teaching the core curriculum courses. Once the program has been approved through NWCCU then Clark College will begin the process of hiring needed faculty for this program, to include one full-time tenure-track professor. In year three of the program we will add a second annual student cohort and have budgeted for hiring an additional full-time tenure-track professor for this program at that time.

For the first two years of the program there will be one single annual student cohort group start, so the core courses in each term of the program will not exceed the teaching load for a single faculty. However, this new hire full-time tenure-track faculty will most likely only teach some core courses within the Cybersecurity BAS that are most related to their areas of expertise, and the remainder of the program courses will be taught by part-time adjuncts we will also be hiring, and other tenured faculty and adjuncts within other areas of the college, some of those faculty are identified in the faculty profiles below.

Faculty Profiles for Core Courses
There will be a need to find qualified faculty to teach many of the core courses, and those new hire faculty will be required to obtain Vocational Certification within one year. Including hiring a full-time tenure-track professor who will be required to have as a minimum a baccalaureate degree in a related field and five-plus years of related industry experience. Preference will be given to applicants with a master's degree or doctoral degree in a related field. Clark College will be hiring a new tenure track faculty as the primary instructor for many of the core courses for this program, especially the second-year courses. This faculty search will focus on seasoned educators with a curriculum vitae that has a strong cybersecurity focus and advanced skillsets: extensive related industry experience and industry certifications in computer networking and cybersecurity.

Many core courses in the program will be taught by adjunct instructors working actively in their field of expertise. Being an evening block program this will work well with the schedules of these industry professionals.

Professor Dwight Hughes is a tenured faculty member at Clark College that will also teach some of the core coursework. Professor Hughes has been with Clark College for fifteen years and is the department chair for the Network Technology Department that this cybersecurity BAS program will be managed under. Prior to coming to Clark College Professor Hughes managed the Cisco networking programs at Heald College Portland for 4-years and was awarded instructor of the year in 2003.

Professor Hughes has a Masters degree in both Adult Education and Online Learning. He has many industry certifications, including: CompTIA A+, CompTIA Network+, CompTIA Security+, Cisco CCNA, Cisco CCNA Security, Cisco CCNP, and Microsoft MCP. He comes from a 25-year career in the telecom industry: where he has worked for a city government implementing wireless networks and voice-over-IP phones, and as the director of operations for a regional Internet Service Provider (ISP) designing small to large-scale networks for clients throughout the Southwest United States. Professor Hughes meets the certification requirements for professional and technical administrators and instructors in the Washington Administrative Code.

Faculty Profiles for General Education Courses

Key faculty are identified below that will be teaching most of the required general education courses for this degree program. We are currently making a concerted effort now to begin recruiting new adjunct faculty with doctorates for our identified general education courses for the Cybersecurity BAS.

Courses	Faculty	Education Credentials	Position within Clark College
PHIL&120 Symbolic Logic	Sacha Greer	PhD, Philosophy, University of South Florida	Philosophy department part-time adjunct professor
PHIL&120, PHIL 420 Ethics in Management	Michael Pankrast	MA, Philosophy, California State University, San Jose	Philosophy department full-time adjunct professor
ENGL 235 Technical Writing	Lindsay Christopher	PhD, English, University of Denver	English department tenured faculty
ENGL 235	Tobias Peterson	MA, English Literature, George Mason University	English department tenured faculty
ENGL 235	Marylynne Diggs	PhD, English, University of Oregon	English department tenured faculty
PSYC 315 Organizational Behavior	Tess Yevka	MS, Counseling Psychology, Portland State University	Psychology department tenured faculty
CMST 230 Small Group Communication, CMST 310 Organizational Communication	Karen Bolton	Ed.D., Organizational leadership, Brandman University	Communication Studies department potential part-time adjunct professor
ENVS 109 Integrated Environmental Science	Rebecca Martin	MS, Environmental Science and Regional Planning, Washington State University	Environmental Science department tenured faculty
ENVS&430 Sustainability and Environmental Practices	Travis Kibota Peter Williams	PhD, Biology, University of Oregon PhD, Adult Higher Education, Oregon State University	Interim Associate VP of Instruction Dean, Science, Technology, Engineering, and Mathematics

Criteria 3: Selective admissions process, if used for the program, consistent with an open-door institution.

Admissions Process
Clark College is proposing a cohort model for the cybersecurity BAS program. Applications will become available in early spring term. The final cohort selection will be determined by the end of the spring term for the fall term start. There will be an established cutoff date for applications for each cohort, and a date for priority consideration.

For the first two years, the program will have one annual student cohort start each fall quarter, and beginning in year three the program will add a second annual student cohort start each spring quarter.

Selection Process
Cybersecurity BAS program entrance consideration is based on the following:

- Completion of the Clark College Application for Admission (if new to Clark College).
- Completion of the Cybersecurity BAS Program Intent Form. (A non-refundable program application fee of $50 is required at the time of application submission.)
- Official transcripts from all other colleges sent to Clark College Enrollment Services.
- Completion of an AA, AAS, AAT, or higher from a regionally accredited institution with a minimum cumulative GPA of 2.00 overall, and 2.50 or above in core program coursework.
- Eligibility for the following courses:
    - PHIL& 120
    - ENGL& 235
- Attend a pre-program advising session with a trained professional or faculty advisor.
- Attend a program orientation session.

Upon admittance to Clark College, the applications will be forwarded to the selective admissions department. The selective admission department will evaluate and track the progress of all the applications that it receives, based on the above outlined criteria. The selective admission department will evaluate all previous degrees and coursework on a course-by-course basis, and all applicable coursework will apply to the program. Date of application will be considered in selecting students for entry into the program, and the program will be deemed full when all available seats in program courses have been filled.

The selective admissions department will notify the department as well as financial aid after the student is admitted to the program.

Waitlist process
Once all seats in the program have been filled, the selective admission department will create and maintain a waitlist and will pull students into the cybersecurity BAS cohort if additional seats become available. These students will also be offered priority into the next available cohort.

Efforts to assure that the program serves as diverse a population as possible.
To insure the inclusion of diverse populations, the strategies and plans will be implemented to include the following:

- Promoting the program to all segments of our service region, by collaborating with Clark's Office of Diversity and Clark's Veterans Resource Center and all student clubs and programs. In addition, recruiting and retaining under-represented populations such as displaced homemakers, the unemployed, and people with disabilities are key goals.
- Creating and providing scholarship opportunities to support BAS students.
- Engaging local businesses and organizations, such as the Vancouver Chamber of Commerce and local service clubs, to support cybersecurity BAS activities and internships.
- Contacting current students and alumni as well as graduates of other higher education institutions in the area to promote the cybersecurity BAS program.
- Regularly checking with Clark College's Office of Planning and Effectiveness to track all the changes in the demographics of the local region, to guide promotional efforts to include diverse populations of Clark College's service district.
- Expanding cultural and educational enrichment activities through college-sponsored events such as field trips, lectures, and community partnerships, as examples.
- Collaborating with Clark College's International Program to better serve this diverse population and provide opportunities to faculty and other students to learn from the international students about their countries and cultures.

Based on the above efforts, changes will be made as necessary to ensure that diverse populations in Clark College's service area are well served.

Criteria 4: Appropriate student services plan.

Student Services

Clark College is strongly committed to student learning initiatives and successful programmatic outcomes. In addition to this instructional philosophy, students at Clark College are also active recipients of procedures and practices in Student Affairs that are thoughtfully implemented in order to increase academic performance, retention, and completion. The Bachelor of Applied Science in Cybersecurity students will be offered these same services as well as other enhanced services that are intrinsic to an applied baccalaureate program.

The first year of the CBAS program will encompass a group of 20 students. The projected impact on student services will be nominal during the initial launch year. By the second academic year, the CBAS program will expand by one additional set of 20 students; this will undoubtedly increase demand for both academic and non-academic services. Fortunately, the projected FTE generation structure for the CBAS program should help to offset impact costs to Student Affairs, both through the CBAS application fee allocation splits and the internal CBAS program support and academic advising.

Registration

Registration into the program will be accomplished by the Registration office after the student has met with the assigned faculty advisor and obtained the course entry codes for the program courses. Registration for the program courses will be handled routinely as for any Clark College student.

Advising

Students' first point of contact for advising will be the Clark College advising center. Students who express an interest in the program will be referred by the advising center advisors to the designated department faculty advisor in the program. Advising will be accomplished at the department level. A designated faculty advisor will advise the current and prospective students. We will utilize a developmental advising approach. Students are required to check-in in each term during registration to secure their course entry code for their classes. This is an opportunity for the faculty advisor to personally check in with them and provide any necessary referrals to campus resources for the student. During registration, the faculty advisor is also available for students after evening classes for them to secure the course entry codes. We will be utilizing developmental advising, which is considered a "high touch" approach to student advising. The faculty advisor is supported by the advising center on campus for referrals and electronic advising resources. Students are entered into the advising center's electronic Advisor Trac system by the designated faculty advisor. This allows the faculty advisor to create and maintain a record of the student advising sessions as enrolled Clark College students.

In the long run, as the program is projected to grow, a separate program advisor might be needed to take on some of the advising and educational planning; the assumption is that the CBAS program would have to absorb the additional costs of this future position. But for years one and two, each CBAS student will be required to develop an educational plan with the CBAS faculty lead/advisor in order to ensure that he or she can complete the program in a timely manner. Methods for CBAS advisement and educational planning will be based on state and institutional best practices, using integrative technologies in accordance with state-mandated record keeping policies. The implementation of ctcLink in Fall 2019 will undoubtedly be part of the technology solutions to keep students on track to completion including predictive analytics advising dashboard tools for intentional outreach and intervention.

Tutoring

Tutoring services are free to Clark students and are available at one of five campus locations, depending on the discipline. Tutoring is also available at each center to assist students in computer skills. The Veteran's Center on main campus also offers tutoring for students who are military veterans. In addition to online tutoring, the Tutoring centers are staffed 8:00-5:00 p.m. weekdays. Cybersecurity BAS students will be able to access tutoring services also.

Advanced students, teachers, and professional tutors will be available to provide the tutoring services needed by the cohort students. An increased schedule of tutoring will be designed during the finals week.

Writing Center

The writing center is located on the main campus. The writing center assists student in writing term papers and various classroom projects. The Writing center will be available to the Cybersecurity BAS students as a campus resource.

Counseling Center

Students who are experiencing personal difficulties or stress due to academic or personal issues, may access the counseling center and are allotted eight free counseling sessions. Personal, academic and mental health issues can be addressed at the counseling center. In addition, the counseling center offers free workshops year-round, on academic and personal subjects, such as test anxiety, essay writing, Notetaking, career decisions, budgeting and others. Workshops are on a drop-in basis and are free to Clark students. CBAS students are able to access all of these services as enrolled Clark College students.

Financial Aid

The Financial Aid Office is located on the Clark College main campus. The Financial Aid Office offers different types of financial aid, which include institution, state, and federal financial aid. There are many resources available to help students cover the costs of expenses to attend college. Students in the Cyber Security BAS program will be eligible to apply for the different types of aid to assist with their cost of education. Depending on student's eligibility, they can apply for grants, loans, student employment, scholarships, workforce education services, and veteran benefits. To determine if they are eligible for the different types of aid, students can complete the Free Application for Federal Student Aid (FAFSA), Washington Application for State Financial Aid (WASFA) or other application as needed. The Financial Aid Office will designate a person for assisting Cyber Security BAS students with their funding needs. In addition, the Financial Aid Office will participate in the open house events and program orientation events for prospective, new, and continuing students in the Cyber Security BAS program.

Scholarships

Clark College Foundation offers approximately one million dollars in scholarship opportunity to new, continuing, and transfer students. Funding for scholarships comes from local high schools, employers, local, civic and community organizations, foundations and private sources. The Clark College Foundation is one of the largest community college foundations in the country. The scholarship application process is separate from the application for state and federal aid. Students in the Cyber Security BAS program will be eligible to apply for Clark College Foundation Scholarships.

Child Care

Clark College also operates an on-campus daycare facility for Clark students. The teacher to child ratio is 1:3 for toddlers, and the facility serves children 1-10 years old. The facility strives to maintain a rich learning environment for the children in their care.

Computing Services

Clark College has 8 computer labs on the 3 campus locations in Clark County. Labs are open as late as 9 p.m. Lab technicians are available in the labs during operation to provide student assistance. The Cybersecurity BAS students will be able to utilize all of the computer labs as registered Clark students.

The eLearning staff provides students with online Canvas and technical support services. The instructors are also provided with training on how to utilize Canvas in their face-to-face, hybrid, and online courses. This office also assists instructors in designing their courses using quality learning models. The CBAS program will utilize the services of this important office throughout the year, especially during the mandatory orientation sessions for CBAS students at the beginning of the year.

Career Services

Career Services provides the resources and strategies for making informed career choices. This includes choosing a college major, developing career plans, creating job search materials, finding internships and full-time jobs, and making successful career transitions. The CBAS faculty lead will work closely with Career Services to ensure CBAS graduates have access to employment opportunities.

Career Services offers a variety of activities to support career development and successful job search endeavors. Events and workshops are free and open to all enrolled students, with no sign-up required. The quarterly Student Success Workshop topics include Resume Building, Interview Skills, Destroy Debt, Conquer Credit, Choosing a Major/Career, and many more. There is a four day Career Days event held each spring featuring workshops, skill-building sessions, resume writing and events designed to assist students and job seekers with career and college transfer preparation.

Marketing
Office of Marketing and Communications is tasked with designing and producing recruitment documents for recruitment of students for the Cybersecurity BAS degree program. The Office of Marketing and Communications will work in tandem with the faculty lead on planning a marketing timeline and marketing program for the degree. The program budget provides for an annual marketing budget. As soon as the institution receives notice of the proposal acceptance by the State Board, the faculty will work with the marketing department to produce the annual plan.

International Programs
International students may apply for admission to the CBAS program. The International Programs office provides international students with a range of services that they need to be successful in the United States. Staff members assist students through the admission process, provide housing contacts, present international student orientations, provide immigration and registration advising, and also organize cultural and social activities. The CBAS Department will collaborate fully with the International Programs office to answer questions about the CBAS program and to assist international students to matriculate into the cohort when it is appropriate to do so.

Library Services
Clark College provides a slate of library services to include instruction, reference, faculty consultation and materials check out. Systems in place to support complete access to material include weekend and evening hours of operation, reservation of materials by faculty and students, use if audio visual equipment, study areas as well as on-site support for students. There have been additional library resources provided for Clark BAS students that are program specific.

The classes in the Cyber BAS will by hybrid on-line and face-to-face. To assist students with these courses the Clark College library offers a 5-module computer assessment entitled *Smarter Measure*, which assesses their readiness for online courses. The library also periodically offers courses in citation and navigation of the library's electronic databases for students. As the Cyber BAS pathway for the degree contains these online components, ascertaining the readiness of a student to take an online course is important to their success. While students may have accessed data base use, citation and navigation within the first two years of study students in the Cyber BAS program will be encouraged to take advantage of these resources.

Program faculty will be including assignments and active learning activities that will require students to gain information literacy with outcomes that include how to obtain material from the library, how to evaluate the efficacy of the material and how to appropriately utilize material in course work and class assignments. The courses in the program that currently provide these outcomes are:

- ENGL &235: Technical Writing
- CMST &310 Organizational communications
- PSYC 315 Organizational Behavior
- ENVS 430: Sustainability and Environmental Practices

In development of the Cyber BAS program, a partnership with the library to develop and design a set of course outcomes and/ or a specific course to address information literacy and library use competency has been undertaken. The goal (s) are to work closely over-time with Library staff to ensure that integration of skills into course curriculum is effective and timely and to ultimately design a specific course for credit for the program. However, due to the structure of internal library approvals and staffing levels, the Cyber BAS was not able to provide the specific course in the program plan.

Book Store

The Clark College bookstore will be able to accommodate the CBAS student by ordering their textbooks and assisting them in their purchases of textbooks as well as supplies for CBAS students. The Clark College Bookstore handles instructor requests for textbooks and works with department and division chairs to ensure Clark College students have access to the most affordable textbook options. The existing services are adequate to accommodate the CBAS program students.

Disability Support Services

The DSS Office will provide information and auxiliary aids or services, as well as serving as a resource to the CBAS students in striving to make Clark College both an accessible and hospitable place for persons with disabilities to enjoy full and equal participation. The DSS office provides accommodations for all Clark College students to assist them in their courses. The DSS has the existing resources to accommodate the CBAS students.

Veteran's Services

The Veterans Resource Center (VRC) is located on the Clark College main campus. The VRC provides student veterans with free tutoring for math and English courses, as well as assistance in applying for Veteran's benefits. The center will also serve the Cyber Security BAS students alongside all other Clark College enrolled students.

Students eligible to receive VA educational benefits will meet with certifying officials to establish benefit eligibility, based on the educational plan developed by the CBAS Department. A certifying official will work closely with the Department to monitor continued eligibility. In addition to existing college resources, veterans can access support services through the Veterans Resource Center that include VA tutoring services, VA Vocational Rehabilitation advising, job resources, and Clark County community assistance programs.

Student Success Programs

The Student Success Programs office is responsible for coordinating the academic Early Warning (AEW) program which monitors students' satisfactory academic performance. When a faculty member provides feedback through the AEW system, trained staff will reach out to students, engage them in academic coaching strategies, and provide campus resources to ensure students remain on track to obtain their educational goals. The office offers several free seminars to help students succeed with topics such as "Test Taking Tips," "Managing Stress," and "How to Study Effectively." The CBAS Department will monitor the academic performance of each of the cohort students and partner with Student Success Programs to ensure the academic success of its students.

Other Services
Clark College provides its students with many more services that make their experiences at the college more convenient and accessible: gym facilities, bookstore, health and medical facilities, dental hygiene facilities that are open for students to utilize at reduced prices, security, food service and vendors, among other services.

Criteria 5: Commitment to build and sustain a high-quality program.

Budget

BAS in Cybersecurity (CBAS)
Revenues & Expenses

	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24
Upper Division FTES Annualized (a)	-	15	30	45	45	45
Revenue						
Tuition Revenue (b)	-	60,721	121,442	182,163	182,163	182,163
Reallocation of Existing Items to CBAS (c)		68,193	68,193	68,193	68,193	68,193
Total Revenue & Reallocation	**-**	**128,914**	**189,635**	**250,356**	**250,356**	**250,356**
Expenses						
Salary, Wages & Benefits						
Faculty						
Full-time Faculty (c)(d)	-	74,355	148,710	148,710	148,710	148,710
Part-time Faculty (e)	-	-	-	51,051	51,051	51,051
Release Time Replacement (f)	-	26,523	26,523	26,523	26,523	26,523
Curriculum Development	14,760	-	-	-	-	-
Staff Support (c)(g)	-	12,514	12,514	12,514	12,514	12,514
Goods & Services	-	2,000	2,500	3,000	3,000	3,000
Marketing/Promotional Activities	10,000	5,000	2,000	1,000	1,000	1,000
Travel	1,000	1,500	2,000	2,500	2,500	2,500
Equipment/Hardware/Software	100,000	10,000	15,000	20,000	20,000	20,000
Accreditation	5,000	-	-	-	-	-
Total Expenses	**130,760**	**131,892**	**209,247**	**265,298**	**265,298**	**265,298**
Net (Shortfall) or Excess	***(130,760)***	***(2,978)***	***(19,612)***	***(14,942)***	***(14,942)***	***(14,942)***

Assumptions

(a) Net annualized FTES with 25% attrition; Year 1 one cohort of 20; Year 2 two cohorts of 20 each; Year 3-5 three cohorts of 20 each

(b) Tuition based on 72% take

(c) 75% of vacant full-time NTEC faculty position (portion not covering current NTEC teaching costs) and .20 FTE NTEC instructional tech will be reallocated to CBAS

(d) Year 1 includes one full-time faculty with 67% release time; Year 2-5 includes two full-time faculty with 67% release time for one faculty

(e) Year 3-5 includes 1.00 FTEF plus 12 months of medical benefits for part-time teaching costs for the third cohort; each class will only be offered once per year per cohort summer through spring

(f) Year 1-5 includes 67% release time part-time backfill for academic year for planning and operational functions

(g) Year 1-5 includes .20 FTE for instructional tech

All figures are based on estimated 2018-19 rates

Clark College has budgeted for the startup costs necessary to begin offering this cybersecurity BAS program and has a budget plan for the ongoing support and operation of the program.

Cost savings have been realized in several key areas:

- Technology lab. The network technology department where this BAS program will be managed also manages two AAT degrees, both feeders to this BAS program. With much of the AAT coursework comprised of extensive hands-on lab work the department already has a laboratory facility that will require a minimal additional equipment investment to support the BAS specific courses over the cost of an entirely new technology laboratory.
- Instructional Tech. The network technology department already has a 9-month benefited lab technician to support and maintain the laboratory facility and assist both instructors and students. This position will be expanded to a 12-month full-time position to encompass laboratory support for the BAS program at minimal additional cost compared to an entirely new position.
- Tenure Track Faculty. The network technology department has an approved and budgeted tenure-track faculty vacancy that will be used to hire the new core courses faculty for this BAS program.

Criteria 6: Program specific accreditation.

Accreditation through NWCCU
Clark College will seek accreditation for this applied baccalaureate program from the Northwest Commission on Colleges and Universities (NWCCU) before promoting or starting this program. The plan is to begin the accreditation process as soon as the program is approved by SBCTC. The college currently offers three other applied baccalaureate programs: one in Dental Hygiene, one in Health Services, and one in Applied Management. All three degrees are accredited through NWCCU.

There are no plans to seek any other accreditation at this time for the Cybersecurity BAS beyond NWCCU.

Criteria 7: Pathway options beyond baccalaureate degree.

Post Program Pathway

While our primary goal for the cybersecurity BAS program is to provide our graduating students with family wage careers within their communities, we do recognize the need for further educational opportunities for students that may elect to pursue them.

Western Governors University (WGU) offers an online master degree in cybersecurity. They have a signed MOU with the Washington SBCTC affirming their pathway for BAS graduating students within our state.

We will continue to seek out partnerships and work with other institutions on articulations and program alignments with the cybersecurity BAS program to provide additional post graduate educational opportunities for our graduates. For example, we have reached out professor Yan Bai at UW Tacoma about their Master of Cybersecurity and Leadership (MCL) degree and developing an articulated pathway for our students, while this is an ongoing and developing discussion we mention it to illustrate the progress we are making in developing these post graduate pathways for our students.

Criteria 8: External expert evaluation of program

External Evaluator Bios

Alan Carter -- IT BAS Program Director – Green River College

- Full time faculty member at Green River College since 2004
- Director: Green River College Cyber Center (GRC is a center of academic excellence in cyber defense (CAE2Y), by the NSA and Department of Homeland security)
- MS IT Network Architecture and Design: Capella University
- BS Computer Information Systems Troy University
- BA Religious Studies Saint Leo University
- AAS Instructor in Technology Community College of the Air Force

Alan has been teaching others to work in the IT field since 1992. He has taught for a variety of training companies, and has been a full time faculty member at Green River College since 2004. Alan has many industry certifications including: MCSE + Security Windows 2000, Security+, CCNA Cybersecurity Operations, CCNA Routing and Switching. In addition to his teaching career, Alan has written several books on certification, including Windows NT 4.0 MCSE study guide, and Windows 2000 MCSE study guide.

Charles Costarella -- full time faculty at the University of Washington Tacoma in the School of Engineering and Technology

- Charles has been teaching in the UW Tacoma IT program since 2013
- Master in Computer Science at University of Washington Tacoma
- BS in Computer Science at Chapman University at Edwards

His background in IT began in the 1990s when he worked as a C++ and Java developer at the United States Air Force Flight Test Center at Edwards Air Force Base in California. He built flight test systems to do real time loads/flutter and performance and flying qualities post-test analysis for supersonic jet aircraft. He also had a brief opportunity to do some early server side web application development for the 412th Test wing at AFFTC.

After completing his BSCS he left AFFTC to go to work for a startup that was acquired by Ask Jeeves, the Internet Search Engine, where he stayed on for a couple of years. He ended his programming work in industry with a professional services position for Trintech, an International Financial transaction software company where he did custom C++ and Java development for customers such as Unibanco in Brazil, Korean National Bank, Sprint PCS, VISA, and MasterCard.

Charles teaching career path began in 1999 almost as soon as he received his BSCS, teaching Java and Data Structures at Antelope Valley College in California. He has been teaching IT in the classroom ever since. After moving to Washington in 2011, he returned to school (UWT) to get my Masters in CS on a National Science Foundation Scholarship for Service and stayed on at UWT to teach in the BSIT program and the Masters in CyberSecurity and Leadership program, a joint venture between the SET and the Milgard Business School. His current subject areas are Networking, System Administration, Cybersecurity (Incident Response), and all things .NET programming, from C# to full stack web application development using ASP.NET Core MVC. He is also the faculty advisor for the campus GrayHat security group and a representative of SET on the University's Executive Council.

External Evaluator's Recommendations & Institutional Response

Both external evaluators have provided overwhelmingly positive and supportive reports indicating no changes are needed.

> "I find this to be a current, relevant, high-quality program that addresses a job market that is expanding rapidly and has a large shortage of qualified applicants. The graduates of this program will be well prepared for jobs in the cybersecurity field."
>
> -- Alan Carter

> "As it stands, what is presented is a very strong proposal for a program that will cover a wide range of cyber op topics, give usable, marketable skills and breadth of knowledge that can be built on and specialized from. It will serve the students well, and nicely dovetail between feeder programs and programs that it could, in turn, feed into."
>
> -- Charles Costarella

See Appendix A for external evaluator's full reports.

Conclusion

The proposed cybersecurity BAS program meets the needs of working adults. With a blend of hybrid and online courses and block scheduling students only physically come to campus two evenings a week and can complete the program in as little as 18 months.

A national standards based curriculum developed in alignment with the NISTs NICE Framework for cybersecurity education skillsets, courses conceived with the input of local industry partners and industry advisory committee. The program will continue to be mentored and monitored by this committee going forward.

Upon graduation, students are well positioned for success in the job market in network technology cybersecurity job roles, such as a cybersecurity analyst career. Or, they can continue on with their education at WGU in their online master's degree program in information technology.

Applied Baccalaureate External Review Rubric

College Name:	Clark College	**BAS Degree Title:**	BAS Cybersecurity
Reviewer Name/ Team Name:	Alan Carter IT Faculty	**Institutional or Professional Affiliation:**	Green River College/IT Faculty
Professional License or Qualification, if any:	CCNA Cybersecurity Operations	**Relationship to Program, if any:**	None
Please evaluate the following Specific Elements			
a) Concept and overview	Is the overall concept of the degree program relevant and appropriate to current employer demands as well as to accepted academic standards? Will the program lead to job placement?		
	Comment **This proposed degree is very relevant to current employer demands – there is a huge shortage of qualified applicants in the cybersecurity field. This program will definitely lead to job placement.** **The curriculum proposed is very appropriate to current academic standards for BAS degrees.**		
b) Degree Learning Outcomes	Do the degree learning outcomes demonstrate appropriate baccalaureate degree rigor?		
	Comment **Yes, the outcomes do represent appropriate rigor for baccalaureate degrees. In addition, the choice of course material is very well matched to industry needs for cybersecurity professionals.**		

c) Curriculum Alignment	Does the curriculum align with the program's Statement of Needs Document?
	Comment **The curriculum is directly aligned with the statement of need. It is spot on!**
d) Academic Relevance and Rigor	Do the core and elective courses align with employer needs and demands? Are the upper level courses, in particular, relevant to industry? Do the upper level courses demonstrate standard academic rigor for baccalaureate degrees?
	Comment **Both the core and elective courses demonstrate the high level of academic rigor that is associated with Baccalaureate degrees.** **Both the core and elective classes are very relevant to industry. Each of the core classes build skills required on the job. This degree will do an outstanding job of preparing students for jobs, and they will be well prepared to continue on into master's level coursework should they choose to continue on.**
e) General Education Requirements	Are the general educations requirements suitable for a baccalaureate level program? Do the general education courses meet breadth and depth requirements?
	Comment **It appears that each of the general education requirements was chosen specifically to help IT professionals succeed and excel in the workforce. Each class helps students develop the soft skills and technical skills outside of IT that employers tell us they need. This degree not only prepares students for technical careers, but for**

	career progression into IT management.
f) Preparation for Graduate Program Acceptance	Do the degree concept, learning outcomes and curriculum prepare graduates to enter and undertake suitable graduate degree programs?
	Comment **Yes, there are many available graduate programs that these students would be very successful in. For example, I believe that articulations could be developed with the University of Washington Tacoma for their master's in cybersecurity and leadership, with Western Governors University, and Capella university to name a few.**
g) Faculty	Do program faculty qualifications appear adequate to teach and continuously improve the curriculum?
	Comment **Looking at this program, and the needs of the community, I believe that the planned staffing levels for this program may need to be increased faster than indicated. My experience with a similar program shows growth from one cohort in the beginning to 4 total cohorts in 5 years.** **Each of the faculty teaching both the core classes and the general education classes look more than qualified to teach and improve the curriculum.**
h) Resources	Does the college demonstrate adequate resources to sustain and advance the program, including those necessary to support student and library services as well as facilities?

	Comment **The college does demonstrate adequate resources to sustain and continue to expand this program.**
i) Membership and Advisory Committee	Has the program received approval from an Advisory Committee? Has the program responded appropriately to it Advisory Committee's recommendations?
	Comment **The advisory committee minutes reflect that the committee unanimously supports the program, and all recommended changes have been implemented.**
j) Overall assessment and recommendations	Please summarize your overall assessment of the program.
	Comment **I find this to be a current, relevant, high-quality program that addresses an job market that is expanding rapidly and has a large shortage of qualified applicants. The graduates of this program will be well prepared for jobs in the cybersecurity field.**
Reviewer Bio or Resume Evaluator, please insert a short bio here Alan Carter IT BAS Program Director – Green River College Director: Green River College Cyber Center (GRC is a center of academic excellence in cyber	

defense (CAE2Y), by the NSA and Department of Homeland security).

MS IT Network Architecture and Design: Capella University

BS Computer Information Systems Troy University

BA Religious Studies Saint Leo University

AAS Instructor in Technology Community College of the Air Force

Alan has been teaching others to work in the IT field since 1992. He has taught for a variety of training companies, and has been a full time faculty member at Green River College since 2004.

Alan has many industry certifications including: MCSE + Security Windows 2000, Security+, CCNA Cybersecurity Operations, CCNA Routing and Switching

In addition to his teaching career, Alan has written several books on certification, including Windows NT 4.0 MCSE study guide, and Windows 2000 MCSE study guide.

Applied Baccalaureate External Review Rubric

College Name:	Clark College	**BAS Degree Title:**	CYBER SECURITY BAS
Reviewer Name/ Team Name:	Charles Costarella	**Institutional or Professional Affiliation:**	University of Washington Tacoma School of Engineering and Technology
Professional License or Qualification, if any:	CCNA R&S, CCNA Sec.	**Relationship to Program, if any:**	Clark College serves as UW Tacoma's Cisco NetAcad ASC
Please evaluate the following Specific Elements			
k) Concept and overview	Is the overall concept of the degree program relevant and appropriate to current employer demands as well as to accepted academic standards? Will the program lead to job placement?		
	Program is extremely relevant to demand in the area for Cyber Security operational positions, both government and private industry. As threats continue to evolve and bad actors multiply, positions will continue to have to be filled by trained individuals with specific, in depth training. Alignment with NICE framework is documented.		
l) Degree Learning Outcomes	Do the degree learning outcomes demonstrate appropriate baccalaureate degree rigor?		
	Outcomes look to be designed to produce a very highly skilled graduate who is ready to fill critical roles in an organization's front line of defense against network and device intrusion. More and more, organizations are recognizing that their data is a critically valuable business asset and the trust to be placed in recent grads who would be manning these positions puts focus on the critical nature of the education and training those personnel received. This is in line with a baccalaureate level degree.		

m) Curriculum Alignment	Does the curriculum align with the program's Statement of Needs Document?
	Is aligned with Statement of Needs doc.
n) Academic Relevance and Rigor	Do the core and elective courses align with employer needs and demands? Are the upper level courses, in particular, relevant to industry? Do the upper level courses demonstrate standard academic rigor for baccalaureate degrees?
	All upper division courses are very relevant to the major. Like CS, IT, and other tech fields, this is a discipline that is already stuffed full of topics and the real expertise of the faculty may determine which niche areas are eventually developed.
o) General Education Requirements	Are the general educations requirements suitable for a baccalaureate level program? Do the general education courses meet breadth and depth requirements?
	This is not an area of expertise, either in my teaching, or service to the University. Most of my focus at UW is at the school and program level. I get students when they are already admitted to the BSIT program, or grad students, typically from industry in the MCL.
p) Preparation for Graduate Program Acceptance	Do the degree concept, learning outcomes and curriculum prepare graduates to enter and undertake suitable graduate degree programs?
	Yes, and this is of keen interest to UW Tacoma with regard to the UW's MCL program. There is a demonstrated need for graduates to feed the Masters program we are running and I think this proposed Cyber Ops program is a nice feeder to it. Further, for those students who are thinking all the way to a terminal degree, our MCL has an

	articulation agreement to the University of Colorado at Colorado Springs PhD program with a focus on Cyber Security. So, there could be a nice series of steps here that afford a student access to progress as far as s/he wants to in the field.
q) Faculty	Do program faculty qualifications appear adequate to teach and continuously improve the curriculum?
	Yes. I also have some limited, but first-hand, knowledge of some faculty at Clark and I found them to be excellent in all respects.
r) Resources	Does the college demonstrate adequate resources to sustain and advance the program, including those necessary to support student and library services as well as facilities?
	Everything looks in order. I am specifically encouraged by the mention of the lab and lab hours of availability to the students. This is often an overlooked item in programs when launching, but accreditation bodies such as ABET (or others as appropriate) are tracking closely.
s) Membership and Advisory Committee	Has the program received approval from an Advisory Committee? Has the program responded appropriately to it Advisory Committee's recommendations?
	Paperwork that I looked over seems to indicate this is being handled correctly. No additional comments here.

t) Overall assessment and recommendations	Please summarize your overall assessment of the program.
	The program, as designed and described, will be a benefit to the state and the geographic area to provide a path forward for students interested in this growing career field. It is nicely dovetailed with existing programs at Clark and in turn, can function as a nice feeder program to advanced degree programs nearby. **It is my opinion that a CyberOps program's success will depend heavily on the hands on component of the program, the specific delivery of course material, the labs and supplemental materials chosen, the expertise of the instructors, and school's support of the program in terms of resources, such as the mention of $100,000 towards virtualization. (I personally feel that cloud and virtualization are the 2 most under-represented areas of tech in most programs across the board currently).** **The recognition that there should be a plan moving forward to transition from cohort model to open scheduling is positive. The UW SET IT program is currently wrestling with this exact issue. Once a program has established as a cohort arrangement, schedules and budgets get set and established, and like any momentum, it is difficult to re-target the vector. I think the schedule as outlined is overly optimistic, but the fact that there is a schedule for the transition outweighs any negative here.** **I am personally negative on the topic of integrating a CEH certification. I don't think this particular cert is of the same level of value as say industry recognized standards such as CCNA, MCSA, CISSP, etc. I am talking about the actual value, not the perceived value, but that is my opinion.** **There was mention of Python's usefulness as a security tool and I concur with this assessment. I am a member of The Honeynet Project org and there is no question Python is the most widely used language in that arena, showing up as the implementation language of choice among security coders in honeypots, honeynets, botnets, and security scripts. I would expand the language study however, to reach out to another language as well. I am heavily involved in .NET programming and Microsoft technologies and for that reason (there**

isn't a copy of Windows around that isn't running some version of .NET), C# is appearing more and more as a security language being used for penetration testing and network programming. It has the advantage of clean decompiling because of the managed code environment and the tools available in Visual Studio, ILasm and ILdasm, ILSpy are very accessible. I am convinced we will be seeing more and more C# code in the security arena moving forward. Reverse malware engineering and secure coding are two areas that might be explored for integration in to the program as well (I apologize in advance if they are mentioned and I've missed it).

I strongly endorse the inclusion of the Capstone component of the program with the goal being an academic paper. I would consider an internship component as well. It is of great benefit to many students. Many students grow to feel safe and acclimated to their routines while in school, but need whatever help they can get making that transition from school to work. In a program such as this, that employment after graduation is an important goal for almost all of them. The percentage of internships that we see which are really an in depth job interview masquerading as an internship is significant.

These are just some opinions and thoughts about where the program could go and what might be reconsidered. As it stands, what is presented is a very strong proposal for a program that will cover a wide range of cyber op topics, give usable, marketable skills and breadth of knowledge that can be built on and specialized from. It will serve the students well, and nicely dovetail between feeder programs and programs that it could, in turn, feed into.

V/R

--charles costarella

Reviewer Bio or Resume

Evaluator Bio:

Appendix A – External Evaluator Reports

My name is Charles Costarella, I am currently on the full time faculty at the University of Washington Tacoma in the School of Engineering and Technology where I have been teaching in the IT program since 2013. My background in IT began in the 1990s when I worked as a C++ and Java developer at the United States Air Force Flight Test Center at Edwards Air Force Base in California. We built flight test systems to do real time loads/flutter and performance and flying qualities post-test analysis for supersonic jet aircraft. I also had a brief opportunity to do some early server side web application development for the 412th Test wing at AFFTC.

After completing my BS in Computer Science at Chapman University at Edwards, I left AFFTC to go to work for a startup that was acquired by Ask Jeeves, the Internet Search Engine, where I stayed on for a couple of years. I ended my programming work in industry with a professional services position for Trintech, an International Financial transaction software company where I did custom C++ and Java development for customers such as Unibanco in Brazil, Korean National Bank, Sprint PCS, VISA, and MasterCard. We built automated dispute resolution systems as well as early payment wallet systems and a number of other cutting edge applications for that time period.

My teaching career path began in 1999 almost as soon as I received my BSCS, teaching Java and Data Structures at Antelope Valley College in California, and I have been teaching IT in the classroom ever since. After moving to Washington in 2011, I returned to school (UWT) to get my Masters in CS on a National Science Foundation Scholarship for Service and stayed on at UWT to teach in the BSIT program and the Masters in CyberSecurity and Leadership program, a joint venture between the SET and the Milgard Business School. My current subject areas are Networking, System Administration, Cybersecurity (Incident Response), and all things .NET programming, from C# to full stack web application development using ASP.NET Core MVC. I am the faculty advisor for the campus GrayHat security group and I am a representative of SET on the University's Executive Council.

Appendix B –Course Descriptions for Cybersecurity BAS

Detailed overviews of each core curriculum course, presented in the order they are taken by students:

NTEC 321 - **Enterprise Network Foundation**

This course provides a wide overview of computer networking concepts. Students learn to configure, manage, and maintain essential network devices. Implement network security, standards, and protocols. Troubleshoot network problems and create virtualized networks. The course may help prepare students to attain the industry certification CompTIA Network+.

- Analyze user requirements to design and implement functional networks.
- Configure, manage, and maintain essential network devices.
- Evaluate benefits and drawbacks of existing network configurations.
- Create resilient networks.
- Implement network security, standards, and protocols.
- Evaluate available information to troubleshoot network problems.

NTEC 361 - **Cybersecurity Programming Foundation**

Students learn to use the Python programming language to accomplish coding tasks related to the basics of programming and the fundamental notions and techniques used in object-oriented programming. The course may help prepare students to attain the industry certification PCAP (Certified Associate in Python Programming) from the Python Institute.

- Apply the fundamentals of computer programming to real world problems.
- Create programs that using the basic methods of formatting and outputting data offered by Python.
- Implement Boolean values to compare difference values and control the execution paths.
- Apply defining and using of functions.
- Create programs using Python modules.
- Apply the fundamentals of OOP (Object Oriented Programming) the way they are adopted in Python.

NTEC 364 - **IoT Foundation: Connecting Things**

The course explores how nearly every object can be connected to the Internet. From washing machines to an airplane's jet engine, even organic items like crops and cows. Students learn the basis of this exciting and emerging field using hands-on activities to model securely connecting sensors to cloud services over IP networks and collecting data in an end-to-end IoT (Internet of Things) system.

- Create a solution that incorporates design thinking, prototyping and troubleshooting.
- Evaluate proposed solutions using critical thinking and problem-solving skills.
- Apply an interdisciplinary understanding of IoT systems (electronics, networking, and programming)
- Apply teamwork skills to network security.
- Analyze and Evaluate problems and solutions in a business context.

NTEC 365 - **Big Data & Analytics Foundation**

The course explores modern, real-time applications, IoT (Internet of Things) systems and the data they collect. Students learn how to collect, store, and visualize data obtained from IoT sensors and to use data analytics to gain insights from the intelligence produced.

- Implement Python to create code that reads data from sensors and stores it in a SQL database.
- Explain fundamental principles of Big Data platforms like Hadoop.
- Visualize, clean, manipulate and integrate data sets.
- Apply storytelling to present insights gained from extracted data.

NTEC 371 - **Cybersecurity Foundation**

This course provides a wide overview of cybersecurity concepts and places an emphasis on mitigating specific security issues. Students apply what they learn through extensive hands-on lab activities. The course may help prepare students to attain the industry certification CompTIA Security+.

- Evaluate risks and risk mitigation activities.
- Differentiate infrastructure, application, information and operational security.
- Apply security controls to maintain confidentiality, integrity and availability.
- Evaluate appropriate technologies and products for given scenarios.
- Evaluate available information to troubleshoot security events and incidents.
- Analyze policies, laws and regulations related to cybersecurity

NTEC 472 - **Cybersecurity Penetration Testing**

This course covers the penetration testing and vulnerability assessment and management. Students learn skills necessary to determine the resiliency of a network against attacks. How to customize assessment frameworks to effectively collaborate on and report findings. And best practices to communicate recommended strategies to improve the overall state of IT security. The course may help prepare students to attain the industry certification CompTIA PenTest+.

- Analyze the knowledge and skills required to plan and scope an assessment.
- Analyze legal and compliance requirements.
- Execute a vulnerability scanning analysis
- Analyze data, and effectively report and communicate results.

NTEC 473 - **Cybersecurity Analyst**

The course covers the behavioral analytics skills to identify and combat malware, and advanced persistent threats. Students learn to perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization. Configure and use threat-detection tools. And to secure and protect applications and systems within an organization. The course may help prepare students to attain the industry certification CompTIA CySA+.

- Analyze and interpret the results of available information to identify vulnerabilities, threats and risks to an organization.
- Apply threat-detection tools to a network.
- Implement technologies to secure and protect applications and systems within an organization.

NTEC 475 - **Cybersecurity Operations**
The course focuses on how to monitor, detect and respond to cybersecurity threats. Students learn cryptography, host-based security analysis, security monitoring, computer forensics, attack methods and incident reporting and handling. The course may help prepare students to attain the industry certification Cisco CCNA CyberOps.
• Detect and respond to security incidents. • Apply incident handling critical thinking and problem-solving skills • Apply understanding of cybersecurity basic principles • Apply network intrusion analysis • Apply an appropriate incident response for a given scenario • Apply data and event analysis

NTEC 499 – **Capstone Project**
The capstone project integrates and synthesizes competencies from across the degree program. Each project consists of a technical work proposal, the proposal's implementation, and a post-implementation report that describes the student's experience in developing and implementing the capstone project.
• Analyze, implement, administer, and support enterprise information technologies and systems. • Analyze the security vulnerabilities of an organization's information technology resources. • Analyze and implement security measures and practices for an organization's information technology resources. • Evaluate organization needs, and use those needs to plan the implementation of information technology systems.

Detailed overviews of each general education course, presented in the order they are taken by students:

PHIL&120 – **Symbolic Logic**
Rigorous examination of logical theory emphasizing modern symbolic or formal logic, including truth-functional logic, propositional logic with proofs, predicate logic with quantifiers and proofs. Applications include computer science, cognitive science, artificial intelligence, linguistics, mathematics, and philosophy.

CMST&230 – **Small Group Communication**
Small group communication emphasizing theoretical principles and their application, enabling students to become more comfortable and competent participants in the group communication process. Emphasis will be on the study and application of the dynamics of group development, problem solving methodologies, and the use of power, including leadership and conflict.

ENGL&235 – **Technical Writing**
Study of advanced writing skills for typical work-world documents in a business/technical environment, with emphasis on document format, audience analysis, correspondence, formal and informal reports, research, and documentation.

CMST 310 – **Organizational Communication**

Introduction to the communication dynamics of an organization, including the major theories of organizational communication, identifying and defining primary concepts and applying them to discussions of real-world situations. Students will analyze relationships between structural variables in the organization and informal communication channels, organizational culture, and strategic communication. Topics include public and human relations, conflict resolution, motivation, coaching, leadership, informal communication networks, corporate culture, socialization, globalization, the role of technology, and external communication as they relate to organizations.

ECON 110 – **Introduction to the Global Economy**

Introduction to economic concepts and their use in the global economy. Topics include basic microeconomics and macroeconomics, international trade, balance of payments, exchange rates, international institutions, energy, war, and terrorism.

PSYCH 315 – **Organizational Behavior**

Focuses on managing relationships in organizations. Students will gain practical experience in managing teams, resolving conflict, and building professional and effective relationships. Special emphasis will be placed on managing difficult behavioral human situations, whether among employees within the organization or with external stakeholders.

ENVS 109 – **Integrated Environmental Science**

Introduction to scientific inquiry using the foundations of physical, earth and life sciences. Focus on developing the skills to answer basic questions about scientific phenomena through scientific investigations and the ability to assist and guide others through this process.

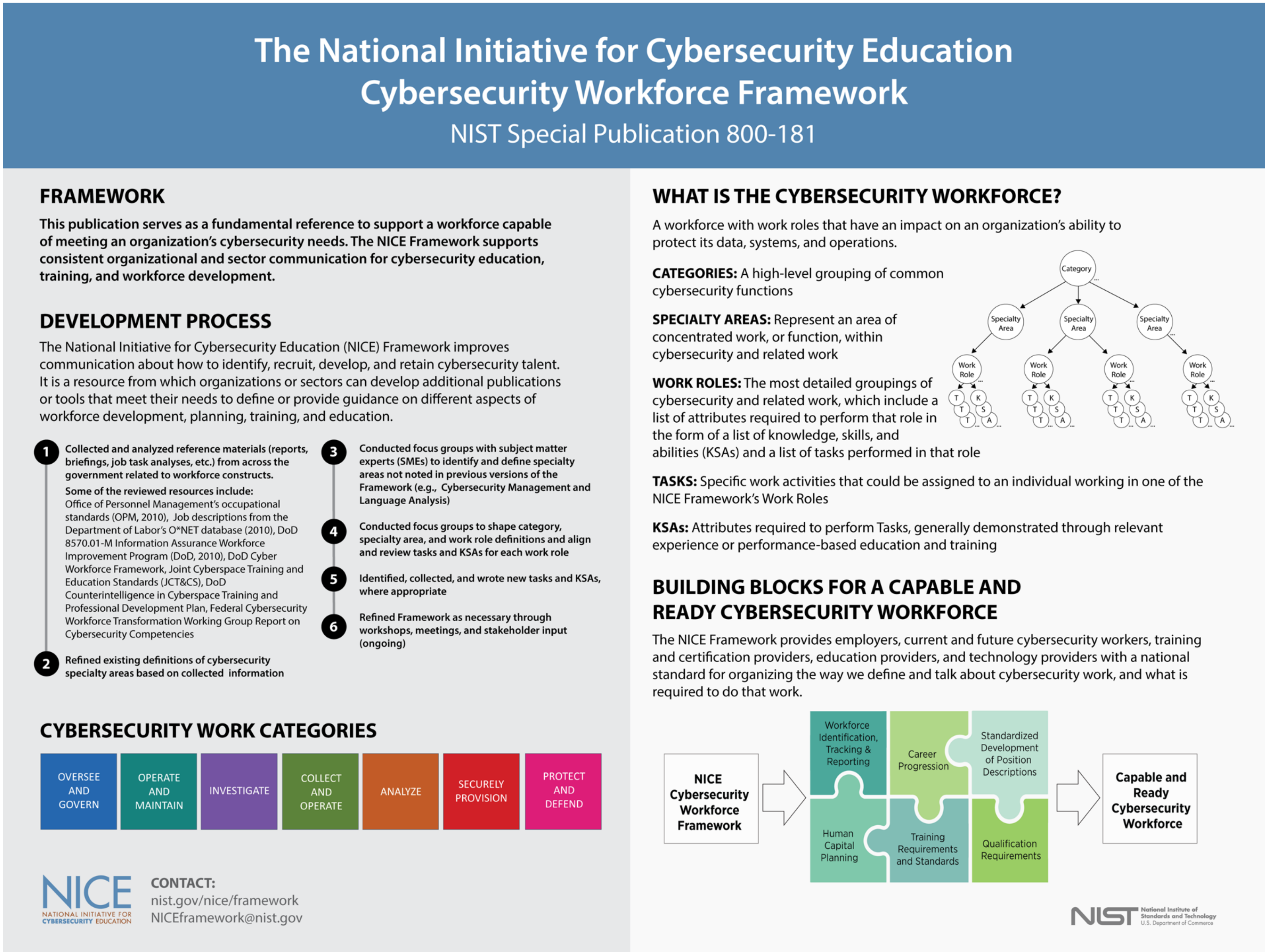
ENVS&430 – **Sustainability & Environmental Practices**

Investigate how environmental problems have arisen due to human activities (global warming, air pollution, waste disposal) and their impact on corporate practices, to include the corporate mission, competitive strategy, technology choices, production development decisions, production processes, and corporate responsibilities. Regulations and permits will be reviewed from the perspective of local planning departments. Changes to the environment by using resources at rates that exceed the system's ability to replenish them will also be covered.

PHIL 420 – **Ethics in Management**

Examines the role of ethics and social responsibility in the management of public and private sectors of organizations and businesses. Theoretical concepts in business ethics will be applied to real-world situations based on challenges managers face. An emphasis on contemporary trends and corporate responsibilities with respect to ethical, legal, economic, regulatory conditions, and the needs of stakeholders in the global marketplace will be included. Case studies will be used to explore real-world ethical and social responsibility situations.

Appendix C –NICE Cybersecurity Workforce Framework



The National Initiative for Cybersecurity Education Cybersecurity Workforce Framework

NIST Special Publication 800-181

FRAMEWORK

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

DEVELOPMENT PROCESS

The National Initiative for Cybersecurity Education (NICE) Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

1. **Collected and analyzed reference materials (reports, briefings, job task analyses, etc.) from across the government related to workforce constructs.**

   Some of the reviewed resources include:
   Office of Personnel Management's occupational standards (OPM, 2010), Job descriptions from the Department of Labor's O*NET database (2010), DoD 8570.01-M Information Assurance Workforce Improvement Program (DoD, 2010), DoD Cyber Workforce Framework, Joint Cyberspace Training and Education Standards (JCT&CS), DoD Counterintelligence in Cyberspace Training and Professional Development Plan, Federal Cybersecurity Workforce Transformation Working Group Report on Cybersecurity Competencies

2. **Refined existing definitions of cybersecurity specialty areas based on collected information**

3. **Conducted focus groups with subject matter experts (SMEs) to identify and define specialty areas not noted in previous versions of the Framework (e.g., Cybersecurity Management and Language Analysis)**

4. **Conducted focus groups to shape category, specialty area, and work role definitions and align and review tasks and KSAs for each work role**

5. **Identified, collected, and wrote new tasks and KSAs, where appropriate**

6. **Refined Framework as necessary through workshops, meetings, and stakeholder input (ongoing)**

CYBERSECURITY WORK CATEGORIES

OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CONTACT:
nist.gov/nice/framework
NICEframework@nist.gov

WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

BUILDING BLOCKS FOR A CAPABLE AND READY CYBERSECURITY WORKFORCE

The NICE Framework provides employers, current and future cybersecurity workers, training and certification providers, education providers, and technology providers with a national standard for organizing the way we define and talk about cybersecurity work, and what is required to do that work.

NICE Cybersecurity Workforce Framework
Workforce Identification, Tracking & Reporting
Career Progression
Standardized Development of Position Descriptions
Human Capital Planning
Training Requirements and Standards
Qualification Requirements
Capable and Ready Cybersecurity Workforce

NIST National Institute of Standards and Technology U.S. Department of Commerce