Bachelor of Applied Science: Cyber Security

Program Proposal—Forms C & D

April 2013

Table of Contents

Form C

COVER SHEET
NEW DEGREE PROGRAM PROPOSAL

Program Information

Program Name: Cyber Security

Institution Name: Columbia Basin College

Degree: BAS Cyber Security__ Level: __Bachelor_ Type: Cyber Security CIP Code: 11.1003
     (e.g. B.S. Chemistry)   *(e.g. Bachelor)*   *(e.g. Science)*

Contact Information (Academic Department Representative)
Name: Deborah Meadows

Title: Dean for Business and IT

Address: 2600 North 20th Ave
                 Pasco, WA 99301

Phone: (509) 542-4863

Fax: (509) 546-0401

Email: dmeadows@columbiabasin.edu

Chief Academic Officer   Date

Name: Curt Freed

Title: Vice President for Instruction

Address: 2600 North 20th Ave
                 Pasco, WA 99301

Phone: (509) 542-4806

Fax: (509) 546-0404

Email: cfreed@columbiabasin.edu

Form D

PROPOSAL for a NEW CYBER SECURITY DEGREE PROGRAM AT COLUMBIA BASIN COLLEGE

Introduction

Columbia Basin College (CBC) proposes to deliver a Bachelor of Applied Science degree in Cyber Security (locally referred to as "BAS-C") and is prepared to enroll junior level students beginning Fall 2013. The degree will build on CBC's computer science certificates and two-year degrees already offered as well as a newly established two-year Associate of Applied Science degree in Cyber Security that began Fall 2012. These certificates and two-year degrees serve both as knowledge and skills foundation for the BAS in Cyber Security and also provide a pathway for students to be prepared to complete junior and senior level coursework in the emerging field of cyber security. The Bachelor of Applied Science degree in Cyber Security will be offered as part of the comprehensive Lockheed Martin Department of Information Science and Technology at CBC.

The BAS degree in Cyber Security is designed to help meet current and future employment needs within CBC's service district of Benton and Franklin Counties. The BAS degree in Cyber Security will provide specialized skills, a bachelor degree that is indicated as an important degree level needed for cyber security employment, and living wage level employment for place bound district citizens in a high demand profession in the Tri-Cities and Washington State.

CBC's capacity to deliver a bachelor degree in a fast emerging high-tech discipline not only builds on existing computer science certificates and degrees that are delivered by well qualified computer science faculty, but also on a campus experienced in delivering a successful BAS degree in Applied Management (see Appendix A). In addition, CBC's success in establishing fruitful public and community partnerships serve to provide funding enhancement, on-going faculty development, adjunct faculty that have extensive cyber security experience, and students with job shadow and internship opportunities.

The program proposal for a BAS degree in Cyber Security includes specific information addressing the eight criteria for new BAS degree program proposals and provides information and evidence regarding CBC's capacity to implement and maintain a BAS degree program.

Criteria 1. Curriculum Demonstrates Baccalaureate Level Rigor

CRITERIA	STANDARD
1. Curriculum demonstrates baccalaureate level rigor.	Describe curriculum including: (1) program learning outcomes; (2) program evaluation criteria and process; (3) course preparation needed by students transferring with a technical associate degree; (4) general education components; and (5) course work needed at junior and senior levels in the BAS.

The cyber security curriculum emerged from an extensive review of current knowledge and skills needed by cyber security professionals, guidance from professional organizations and conferences, and the review of other cyber security degree programs. The resulting collection of cyber security courses addresses the skills and knowledge required of successful cyber security professionals. The degree is designed with continuity between the 100 and 200 level AAS Cyber Security degree and naturally leads to the 300 and 400 level courses to complete the BAS-C core requirements. The general education courses are designed to build general knowledge and help build a mindset needed to respond to the changing world of cyber security. An overview of the entire four-year degree is located in Table 2. The curriculum was reviewed and approved by the Computer Science Advisory Committee, the CBC Curriculum Committee, and by two subject matter experts.

1-1 Program Learning Outcomes and Assessment Process-

The review of and assessment for the BAS degree in Cyber Security, which includes junior and senior level cyber security core courses and two new upper-division general education courses, will use the same assessment process as other Columbia Basin College degrees. The CBC assessment process was developed by the Teaching and Learning Committee, approved by the CBC Faculty Senate,

integrated into the Curriculum Committee's course and degree approval process, and is supported by the Office of Institutional Research.

As illustrated in Figure 1, students who graduate from the Cyber Security BAS program will meet the three levels of the CBC Assessment Model learning outcomes **Classroom/course**, **college-wide Student Learning Outcomes (SLOs)**, and the **Program/Degree** level which incorporates the Computer Science program general outcomes and Cyber Security program outcomes.

Figure 1: Overview of the CBC Assessment Model
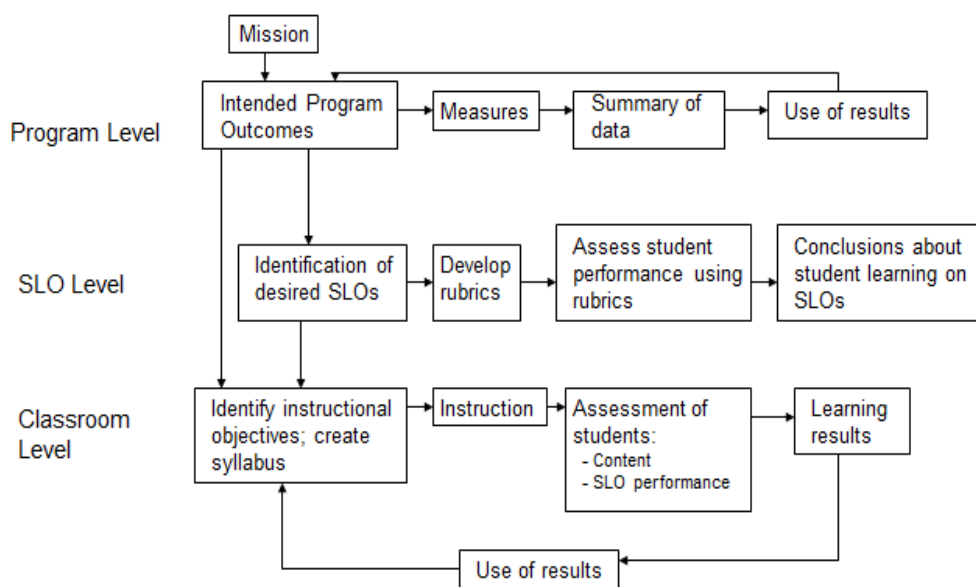
Classroom/Course Level. At the course level, each cyber security and general education course was reviewed and approved by the Curriculum Committee. Student evaluations will be conducted on a regular basis. Each course is mapped to the college-wide student learning outcomes and tracked through the use of a specialized database, a commercial product called TracDat, for ongoing course reviews.

Student Learning Outcomes Level. The CBC college-wide **Student Learning Outcomes (SLOs)** includes the following:

Think Critically
  Understand, analyze, and evaluate the elements of one's environment and one's habits of thought
  Conceptualize alternatives to both

Reason Quantitatively and Symbolically
    Develop a sense of number and pattern
    Analyze, evaluate, and synthesize symbolic statements and quantitative arguments

Communicate Effectively
    Use spoken and written language to express opinions, discuss concepts, and persuade an audience
    Synthesize ideas and supporting information to create effective messages

Apply Information Tools and Resources
    Accurately assess information needs
    Select appropriate information tools and resources and use them efficiently
    Evaluate, manage, and use information effectively and responsibly

Develop Cultural Awareness
    Respect self and others
    Explore and appreciate different cultures in an increasingly diverse, global community
    Challenge culture-bound assumptions

Master Program Learning Outcomes
    Become familiar with a body of knowledge
    Demonstrate ability to know or do the stated program learning outcomes, which are developed by each department and program and assessed annually

As with other CBC degrees, each of the six CBC SLOs are mapped to their location in the cyber security curriculum. Once the SLOs are mapped, Figure 2 illustrates how the SLOs are then tracked and assessed.

Figure 2: Tracking SLOs
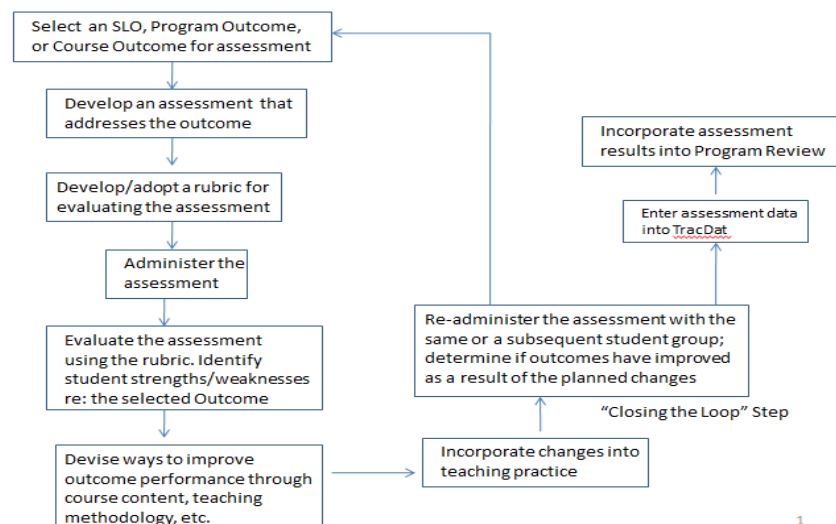
1-2 Program Evaluation Criteria and Process

Program Level. In addition to the college-wide SLOs, all Computer Science degrees including the proposed BAS degree in Cyber Security has five program goals for students to meet. These program goals include the following skills:

1. Students will be able to troubleshoot hardware and software problems **(Problem Solving)**
2. Students will use written, presentation and interpersonal skills to effectively communicate with customers, supervisors and co-workers (**Communication)**
3. Students will be able to demonstrate the basics of programming, applications, Internet usage, creating databases, hardware, networking and operating systems giving them a well-rounded base of core skills. **(Information Tools)**
4. Students will be able to think logically in solving problems. **(Quantitative Skills)**
5. Students will be able to work effectively with other people on assigned tasks. **(Team effort)**

Computer science students who graduate with a BAS degree in Cyber Security will also be able to:

- Protect an organization's critical information systems and assets by integrating cyber security risk management and business continuity best practices throughout an enterprise.
- Implement continuous network monitoring and provide real-time security solutions.
- Analyze advanced persistent threats and deploy countermeasures and conduct risk and vulnerability assessments of planned and installed information systems.
- Formulate, update, and communicate short- and long-term organizational cyber security strategies and policies.

Every five years the program staff will complete a thorough review at the program level. As identified in Figure 3, sample assessment efforts for program review may include but are not limited to:

- Track student and employer interest in the degree
- Develop pre/post surveys and testing items to determine value-added learning from the degree
- Use ePortfolio to track Student Learning Outcomes through the individual classes
- Use ePortfolio to identify changes in learning from the initial BAS courses to the capstone course
- Conduct employer surveys to track BAS graduates capabilities, job fit, wage and job advancement information, and impact on company/organization
- Create a longitudinal BAS study using BAS alumni surveys, interviews, focus groups, etc.

This program outcome process for the two-year applied science degrees, the DTA/AA degree, and the current BAS degree in Applied Management are already in place and the BAS degree in Cyber Security will utilize the same process. Figure 3 illustrates the program review process.

Figure 3: CBC Program Review Process
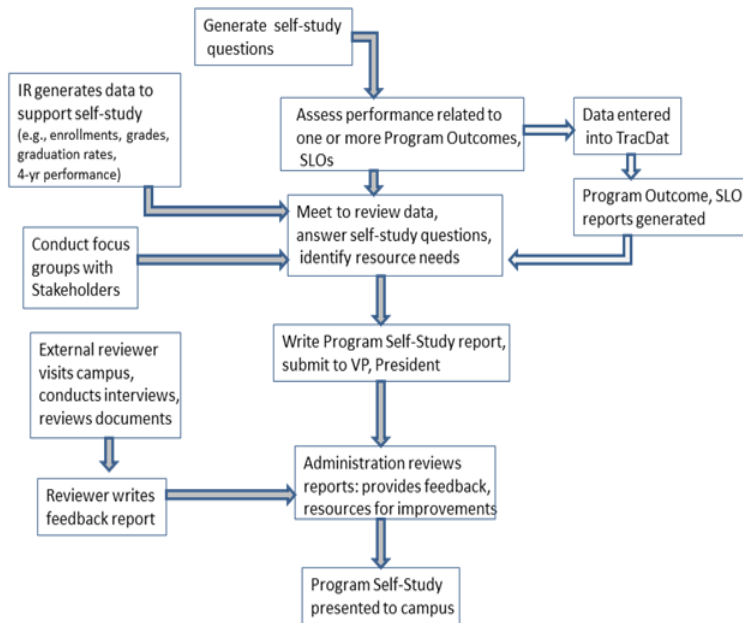
1-3 Preparation for 300 and 400 Level Cyber Security Courses

The Cyber Security BAS prerequisite is the AAS degree in Cyber Security. The two-year cyber security degree provides the foundation for the upper-division courses required in the BAS degree in Cyber Security. Computer science (CS) degrees from CBC or other colleges can serve as an intermediate step. Students can complete courses from the AAS level Cyber Security degree that are missing from their Computer Science (CS) degree or certificate. See Table 1 for the degree pathways.

Table 1: Computer Science Two-year Degree Pathways to Cyber Security BAS

CBC Certificates	CBC Associate Degrees	CBC BAS
Network and Security Certificate (certification & 1 yr. certification)	Cyber Security	
Computer Database Management Certificate (certification & 1 yr. certification)	Database Administrator *(supplemented by Cyber Security AS degree requirements)*	
Computer and Information Technology (certification & 1 yr. certification)	Help Desk Technician *(supplemented by Cyber Security AS degree requirements)*	
Web/Multimedia Management and Webmaster Certificate (certification & 1 yr. certification)	Internet Specialist (supplemented by Cyber Security AS degree requirements)	Cyber Security BAS
Network and Security Certificate (certification & 1 yr. certification)	Network Administrator *(supplemented by Cyber Security AS degree requirements)*	
*C# and Mobile Device Programming (certification & 1 yr. certification) *C++ and Objective-C/iPhone Programming (certification & 1 yr. certification) *Java, Web, and Mobile Device Programming (certification & 1 yr. certification)	Programming and Software Development *(supplemented by Cyber Security AS degree requirements)*	

BAS Degree in Cyber Security Requirements

The BAS-C can be viewed as a combination of the two-year Cyber Security AAS degree, a project management course, 300 and 400 level cyber security courses, and 60 credits of general education requirements. Table 2 provides an overview of all four years of the BAS degree cyber security and specifically identifies the 100 and 200 level courses, major support course, 300 and 400 level courses, and 60 credits of general education courses that are required.

Table 2: Bachelor of Applied Science (BAS) in Cyber Security			
Major Courses			
CS 102 CS& 131 CS& 141	Programming Fundamentals *or* Computer Science 1C++ *or* Computer Science 1 Java w/ Android Devices	5	Cyber Security Applied Science 2-year degree cyber security major course
CS 106	Database Systems	5	
CS 117	Computer Ethics	2	
CS 140	SharePoint	5	
CS 150	Computer Security	5	
CS 202 CS& 162 CS 236	Programming Fundamentals 2 *or* C++2 *or* Java I/O and Intro to Integration	5	
CS 200	Computer Forensics Fundamentals	5	
CS 206	Database Design	5	

CS221	Database Administration	5	
CS 223	Unix/Linux	5	
CS 228	Windows Server	5	
CS 229	Webmaster	5	
CS 231	Network Infrastructure	5	
CS 232	Network Security	5	
CS 250	Networking Fundamentals	5	
CSIA 300	Cyber Security and Information Assurance	5	300 and 400 Core and Major Support level to complete BAS in Cyber Security
CSIA 310	E-Commerce Security	5	
CSIA 320	Ethical Hacking	5	
CSIA 330	Wireless Security	5	
CSIA 410	Cryptography	5	
CSIA 420	Cyber Crime and Terrorism	5	
CSIA 430	UNIX Administration and Security	5	
CSIA 440	Cyber Testing and Penetration	5	
CSIA 450	Cyber Security Capstone	5	
	Subtotal	**117**	
Major Support			
PROJ 100	Intro to Project Management	5	
	Subtotal	**5**	
General Education			
Communication (10 credits)			
ENGL& 101	English Composition	5	
ENGL& 102	Composition II *or*	5	
ENGL 410	Professional & Organizational Communication	5	
Quantitative Symbolic Reasoning (5 credits)			
MATH& 141+	MATH& 141 *or* higher (except MATH& 171) (see program advisor for best selection)	5	BAS General Education Requirements
Social Science (15 credits)			
PSYC& 100 or SOC&101	General Psychology *or* Intro to Sociology	5	
SOC 305	Cybercrime: A Sociological Perspective	5	
POLS 305	Future of Warfare	5	
Humanities (10 credits)			
PHIL 305	Professional Ethics	5	
	Humanities from DTA distribution list (see program advisor for best selection)	5	
Math/Science (10 credits)			
	Lab science from DTA distribution list (see program advisor for best selection)	5	
	Math from DTA distribution list (see program advisor for best selection)	5	
Additional Requirement (10 credits)			
	Communication, Social Science, Humanities, *or* Math/Science from DTA distribution list (see program advisor for best selection)	10	
	Subtotal	**60**	
	Total Credits Required	**182**	

1-4. General Education Requirements

The BAS degree in Cyber Security general education requirements are designed to meet several

different expectations. These include the BAS general education guidelines, general education required

by the CBC workforce programs, and course selection options established by CBC's transfer distribution degree course options (see Appendix B). Finally, the requirements must help prepare and support students for the rigors of the BAS Cyber Security program and the workplace needs after degree completion. Two-year workforce students will have ENG& 101 and a psychology or sociology course and possibly other courses, depending on the student's background, that will count toward the BAS general education requirements. Table 3 provides an overview of Instruction Committee approved guidelines as well as how CBC has translated those guidelines into the specific BAS degree in Cyber Security general education expectations.

Table 3: Cyber Security General Education Requirements (60 Credits)			
Distribution Area	**SBCTC BAS General Education Requirements**	**CBC Cyber Security BAS General Education Requirements**	**CBC Credits Requirements**
Communications Skills	10 credits	**ENGL& 101** English Composition (5 credits) **ENGL& 102** Composition II (5 credits) **--OR--** **ENGL 410** Professional & Organizational Communication (5 credits)	10 credits
Quantitative/Symbolic Reasoning Skills	5 credits	Quantitative/Symbolic Reasoning Skills course from CBC's Quantitative/Symbolic Reasoning Skills DTA distribution list (see program advisor for best selection)	5 credits
Humanities	10 credits	**PHIL 305** Professional Ethics (5 credits) Humanities course from CBC's DTA distribution list (see program advisor for best selection) (5 credits)	10 credits
Social Science	10 credits	**Psychology 100 or Sociology 101** (5 credits) **SOC 305** Cybercrime: A Sociological Perspective (5 credits) **POLS 305** Future of Warfare (5 credits)	15 credits
Natural Science	10 credits	Lab science from DTA distribution list (see program advisor for best selection) (5 credits) Math from DTA distribution list (see program advisor for best selection) (5 credits)	10 credits
Additional credits selected from distribution options	15 credits	Communication, Social Science, Humanities, *or* Math/Science from DTA distribution list (see program advisor for best selection) (10 credits)	10 credits

1-5 300 and 400 Level Courses for the BAS Degree in Cyber Security

The required BAS 300 and 400 level courses are listed in Table 4. Additional information about the cyber security courses including course description and course outcomes can be found in Appendix C.

Table 4: 300-400 Level Cyber Security Courses and Degree Major Support Course		
CSIA 300	Cyber Security and Information Assurance	5
CSIA 310	E-Commerce Security	5
CSIA 320	Ethical Hacking	5
CSIA 330	Wireless Security	5
CSIA 410	Cryptography	5
CSIA 420	Cyber Crime and Terrorism	5
CSIA 430	UNIX Administration and Security	5
CSIA 440	Cyber Testing and Penetration	5
CSIA 450	Cyber Security Capstone	5
	Subtotal	45
Major Support		
PROJ 100	Intro to Project Management	5
	Subtotal	5

The upper division BAS degree in Cyber Security courses will be delivered in the evening, online and a hybrid mode. Although a number of the students will be working, some could choose to attend full-time. Table 5 illustrates a full-time load with the recommended sequence of core cyber security courses and suggestions as to how the general education courses could best be integrated into a full-time schedule. It is expected that a student will already have taken ENG& 101, a math class that will count as a Quantitative/Symbolic Reasoning Skills course, and a psychology or sociology course.

Table 5: Sample Full-time Cyber Security Course Schedule			
	Fall	**Winter**	**Spring**
Third Year **(Junior)**	**CSIA 300** Security and Info Assurance (5 credits) **CSIA 310** E-Commerce Security (5 credits) **ENGL 410** Professional & Organizational Communication (5 credits)	**CSIA 320** Ethical Hacking (5 credits) **CSIA 330** Wireless Security (5 credits) **PHIL 305** Professional Ethics (5 credits)	**CSIA 410** Cryptography (5 credits) **CSIA 420** Cyber Crimes and Terrorism (5 credits) **PS 305** Future of Warfare (5 credits)
Forth Year **(Senior)**	**CSIA430** UNIX Admin . (5 credits) Distribution Course (5 credits) Humanities Distribution (5 credits)	**CSIA 440** Cyber Testing (5 credits) **SOC 305** Cybercrime: A Sociological Perspective (5 credits) Science Distribution (5 credits)	**CSIA450** Cyber Security Capstone (5 credits) Lab Science (5 credits) Distribution Course (5 credits)

Table 6 illustrates a part-time load with the recommended sequence of core cyber security courses and suggestions as to how the general education courses could best be integrated into a part-time schedule.

Table 6: Sample Part-time Cyber Security Course Schedule (The last two years finished in three years)			
	Fall	**Winter**	**Spring**
Third Year	**CSIA 300** Security and Info Assurance (5 credits) **CSIA 310** E-Commerce Security (5 credits)	**CSIA 320** Ethical Hacking (5 credits) **CSIA 330** Wireless Security(5 credits)	**CSIA 410** Cryptography (5 credits) **CSIA 420** Cyber Crimes and Terrorism (5 credits)
Forth Year	**CSIA430** UNIX Admin . (5 credits) **ENGL 410** Professional & Organizational Communication (5 credits)	**CSIA 440** Cyber Testing (5 credits) **PHIL 305** Professional Ethics (5 credits)	**CSIA450** Cyber Security Capstone (5 credits) **PS 305** Future of Warfare (5 credits)
Fifth Year	**Quantitative Symbolic Reasoning** (5 credits) Science Distribution (5 credits)	Humanities Distribution (5 credits) **SOC 305** Cybercrime: A Sociological Perspective (5 credits)	Lab Science (5 credits) Humanities Distribution (5 credits)

The courses and program are designed to integrate technology into the coursework and support a hybrid model. This is the type of environment that students may experience in the work world. Group projects will encourage students to get to know other students as well as refine their teamwork skills. Virtual labs will be available so students can access the needed virtual environments to complete assignments in the classroom or off campus. Group projects will also use technology to create "virtual teams" so students can work synchronously and asynchronously on their assignments.

To help build team skills, the BAS-C program will also use one or more "social networking" software packages. Social networking will support student interaction beyond a weekly class meeting so BAS-C program students will get to know each other.

To support the hybrid approach, each class will have a Canvas course site. The course site will offer students and faculty opportunities to have course discussions and the delivery of course content that extends well past the face-to-face time in the classroom. The asynchronous discussion will keep students engaged beyond the classroom. The use of Tegrity will offer students the opportunity to replay all or a portion of each class session. Students can download their class session for viewing at their convenience.

Criteria 2. Qualified Faculty

CRITERIA	STANDARD
2. Qualified faculty.	Provide a profile, including education credentials, of anticipated faculty (full-time, part-time, regular, continuing) that will support the program for each year (junior and senior). Include faculty needed to cover the technical course work, general education courses and electives. In addition, provide the total faculty FTE allocated to the program.
	Faculty and administrators responsible for technical courses must meet certification requirements for professional and technical administrators and instructors in the Washington Administrative Code.

CBC's Computer Science program has six highly qualified full-time faculty that have many years of teaching experience. Over the years, the computer science discipline and the needs of the computer science employer have changed dramatically. These changes have required the faculty to continually upgrade their computer science knowledge so as to keep the computer science program updated and aligned to workforce needs. The faculty have continued to upgrade their skills by taking courses, attending workshops, engaging in independent study, completing additional degrees, and participating in back-to-industry experiences. (See Appendix D for more information about the cyber security faculty.)

Since cyber security is an emerging field within the computer science discipline, finding instructors with experience in the field is difficult. Only recently have college cyber security programs begun to provide graduates; competition for cyber security faculty is extremely high. Fortunately, CBC has developed strategies to provide the faculty needed to deliver a high quality BAS degree in Cyber Security.

In preparation for the new two-year degree and the possibility of a four-year BAS degree in Cyber Security, the CBC computer science faculty attended numerous national conferences, participated in back-to-industry experiences, and aligned with CyberWatch West. The faculty are continuing that process this academic year as well. Currently the four full-time faculty, that are the

primary CBC cyber security faculty, are enrolled in a series of cyber security courses, and are completing industry level certification tests.   In addition, CBC is partnering with Pacific Northwest National Lab (PNNL) and Lockheed Martin, two major Hanford employers, to assist the computer science instructors in building their knowledge and skills in cyber security. Battelle is a multinational company that is responsible for PNNL. Battelle has located their chief cyber security administrator at the Richland facility and has multiple cyber security efforts as part of PNNL's mission. Lockheed Martin, a self-described cyber security company, provides the cyber security for the Department of Energy and its Hanford Site contractors, as well as many other programs across the county. Representatives from these organizations have pledged to assist current instructors, provide advisory committee assistance, as well as provide highly skilled cyber security professionals as adjunct faculty members.   Finally, due to the retirement of one of the six computer science faculty, CBC is strategically planning to recruit an additional faculty member to support the new cyber security program and the other computer science degrees. See Table 7 for the cyber security faculty.

Table 7: Core Cyber Security Faculty		
Faculty Name	**Credentials**	**Courses Qualified to Teach**
DeHaan, Melissa	B.A. Washington State University—Computers Columbia Basin College AA degree Columbia Basin College AAS—Computers	**CSIA 300** Security and Information Assurance **CSIA 420** Cyber Crimes and Terrorism
O'Brien, Tym	M.Ed. Heritage University—Adult Learning B.S. Washington State University—Computer Science B.Ed. Srinakarinwirot University--Physics	**CSIA 330** Wireless Security **CSIA 410** Cryptography **CSIA 440** Cyber Testing and Penetration **CSIA 450** Cyber Security Capstone
Sako, Tony	B.S. University of Washington—Numerical Analysis	**CSIA 310** E-Commerce Security **CSIA 410** Cryptography **CSIA 430** UNIX Administration and Security **CSIA 440** Cyber Testing and Penetration **CSIA 450** Cyber Security Capstone
Wolf, Debbie	B.A. Washington State University—Computers	**CSIA 300** Security and Information Assurance **CSIA 320** Ethical Hacking

New Full-time Faculty	Proposed national recruiting efforts for a cyber security specialist prepared at a masters or doctorate level	Cyber Security coursework appropriate for newly selected faculty
Adjunct Faculty	Experienced cyber security professionals from PNNL, Lockheed Martin, etc.	Appropriate Cyber Security coursework matched to individual skill-sets

General Education Faculty

The general education courses are an intentional selection of upper-division courses from the traditional CBC transfer distribution list. Some of the courses such as *SOC 305 Cybercrime: A Sociological Perspective* and *POLS 305 Future of Warfare* are designed to provide general knowledge typical of general education courses but are delivered within the context of the current global cyber security environment. Both classes have course outcomes specifically related to developing a mindset to help students prepare for a cyber-security career.

The BAS degree in Cyber Security general education courses will normally be taught by CBC faculty prepared at the doctorate level in their discipline. Table 8 illustrates the background of faculty who will teach the general education courses. Faculty are very interested in teaching at the 300 and 400 level since the courses are designed not only to build general education knowledge but are also taught within a specific context that is well matched to the instructor's interest. In addition, the experience with the BAS Applied Management students provide evidence that BAS students are well-prepared and highly motivated at a level that is not always manifested in lower division courses. As many of the social science, humanities, and math/science faculty at CBC are doctorate prepared, there are numerous faculty from which to choose. Only the PS 305 and the SOC 305 are courses new to CBC. The other courses are already being taught for the BAS in Applied Management at CBC or for the DTA level general education courses by the instructors identified in Table 8.

Table 8: Sample of General Education Faculty		
Faculty Name	**Credentials**	**Courses Qualified to Teach**
Arnold, David	Ph.D. UCLA--History MA & BA Washington State University--History	**ICS 305** American Diversity
Bourouh, Omar	Ph.D. & M.A. American University—Sociology	**SOC& 101** Intro to Sociology **SOC 305** Cybercrime: A Sociological Perspective
Carbary, Katie	Ph.D. University of Rochester B.S. Reed College	**PSYC& 100** General Psychology
Chakrabarti, Debjani	Ph.D. Mississippi State University--Sociology M.A. Delhi School of Economics--Sociology B.A. Presidency College--Sociology	**ICS 305** American Diversity
Chisholm, Rob	Ph.D. University of Pittsburg--Political Science M.A & B.A. Queen's University—Political Science	**PS 305** Future of Warfare
Kincaid, Matt	Ph.D. Gonzaga--Leadership M.B.A. & B.A. Gonzaga--Business	**PHIL 305** Professional Ethics
Thonney, Teresa	Ph.D. University of Washington--English M.A. & B.A. Eastern Washington University--English	**ENGL 410** Professional & Organizational Communication

Administration and Administrative Support Staff

The administration and administrative support staff are listed in Table 9. The dean is experienced with BAS programs as she was one of two individuals leading the request for the current CBC BAS degree in Applied Management; she designed the BAS-M, and supervised the BAS-M degree startup as well as continuing to supervise the program's operation. As two additional BAS degrees are being requested, the proposal is to identify a BAS director to coordinate and provide continuity between the BAS degrees. The BAS director will be assigned as a .4 FTE to the Cyber Security program. A Student Services Specialist, with computer science expertise, will also be hired to coordinate and deliver the Cyber Security student services program. The computer science department secretary will provide the clerical support Table 9 lists the program support staff.

Table 9: Administrative and Support Staff		
Administrative Staff	**Title/Role**	**Credentials**
Meadows, Deborah	Dean	D.M. University of Maryland University College---Management Ed.D. International Graduate School—Counseling Psychology M.Ed. University of Idaho—Counseling Psychology B.S. University of Idaho—Education *33 years of experience @ CBC*
TBA	BAS Director (to be hired) (.4 FTE)	Master prepared
TBA	Student Services Specialist (to be hired) (1 FTE)	Master prepared
Jack, Deb	Secretary (.2 FTE)	Multiple years as division secretary

Criteria 3. Admissions Process

CRITERIA	STANDARD
3. Selective admissions process, if used for the program, consistent with an open door institution.	• Describe the selection and admission process. Explain efforts that will be used to assure that the program serves as diverse a population as possible.

Open Access

Columbia Basin College operates under an open admission policy granting admission to all applicants who are 18 years of age or older and/or graduated from high schools accredited by a regional accrediting association (Administrative Policy 7-010). The Mission Statement specifically mentions CBC's commitment to diversity, fairness, and equity. This mission extends to the Cyber Security BAS program. The College's values also will apply to the Cyber Security BAS program, and therefore will guide the program's selection process. One of the goals of the selection process is that BAS-C participants will mirror or exceed the student diversity in the computer science feeder programs. To help meet this goal, a set of admissions criteria, an applicant selection process, and a participant monitoring and tracking system will support the BAS-C admission process. In addition, the new Cyber Security Student Service Specialist will develop and deploy a recruiting program that is designed to attract a diverse applicant pool beginning at the two-year level and extending to the 300-400 level.

Admissions Criteria

The following admissions criteria have been identified as creating opportunities for a broad spectrum of applicants as well as optimizing the likelihood of successfully completing the cyber security BAS degree.

Admissions Criteria for the BAS degree in Cyber Security:

1. Completion of either an Associate of Applied Science, Associate of Arts and Science degree or the equivalent from an accredited college with a GPA of 2.0 or greater.

2. An application packet which includes:

    o Completed CBC Admissions Form

    o Completed BAS Program Application. The application includes (a) an essay outlining career goals and how a BAS-C degree will support those goals and (b) summary of work experience/resume

    o Official College Transcripts

    o Two Letters of Recommendation

Selection Process

The selection process for the Cyber Security BAS program will be conducted by a committee that includes the BAS-C Student Support Generalist, a BAS-C faculty representative, the BAS director and the dean for the program. The Selection Committee will first review each application packet to identify those who meet the admissions criteria.

If the number of qualified applicants exceeds space availability, the selection committee will proceed to evaluate the individual applicants on specific criteria and identify those to be invited to participate.

This process includes:

1. A thorough review of each application, including transcripts, admissions forms, essays, letters of recommendations and other available documentation.

2. Development of quantified ratings for each applicant on specific dimensions by each committee member. Using the BAS degree in Applied Management strategies as the starting point, these dimensions will be aligned with cyber security expectations and may include relevance of career goals, strength of transcripts, relevance of work experience, and strength of the personal statement. Prior to selection of first cohort, the selection dimensions will be identified, definitions developed, behaviorally-based rating scales developed, and committee members trained to use the dimensions in a reliable and valid manner.

3. Review and discussion of the ratings of each applicant by the committee. Where significant disagreement exists regarding ratings for an applicant, the committee will review the applicant's data and reach a consensus on the rating.

4. Identify the top candidates, based on the ratings, sufficient to fill available spaces. A waiting list of candidates will also be developed in case not all of those selected subsequently enroll in the program.

Program Support for Diversity

CBC is a designated Hispanic Serving Institution. Franklin County, one of the counties in CBC's Service district, is the first Washington State County where the percentages of Hispanic citizens exceed the White Non-Hispanic population.

A key goal for the BAS program is to maintain the diversity levels of the AAS Computer Science feeder programs. The Cyber Security Student Services Specialist and the Office of Diversity and Outreach will work closely with the BAS-C program faculty in this effort. The goal of the CBC Diversity and Outreach Office is to ensure that underrepresented members of our community have fair and equitable access to post-secondary education. The Office will help provide the resources to maintain recruitment and retention of diverse students within the BAS-C program. Outreach efforts will include disseminating BAS-C information to local businesses, both to inform AAS graduates about program opportunities and to educate the business community regarding the upcoming availability of BAS graduates.

Other activities will include involvement in the Multi-Cultural College Night, developing key relationships and BAS-C focused presentations with school districts that maintain large diverse student populations, and hosting events that inform students, parents and the community about the CBC BAS degree in Cyber Security program. Additionally, efforts will be made to qualify and register BAS-C students into federally funded support programs that best fit their needs. By communicating with minority students currently involved in AAS programs through outreach with qualified minorities within the community and by educating employers about the benefits of hiring and promoting BAS-C

graduates, CBC anticipates maintaining or improving the relative proportion of minority students within the current computer science pool and specifically in the BAS-C program.

CBC monitors the representation of minorities within the current BAS degree in Applied Management and all lower division programs on a regular basis and will extend that effort to all new BAS programs. CBC will modify application and selection procedures, as needed, if problems are found. Figure 4 illustrates CBC's student ethnicity and reflects the changing community demographics' impact on ethnicity of CBC's students.

Figure 4: CBC's Student Ethnicity
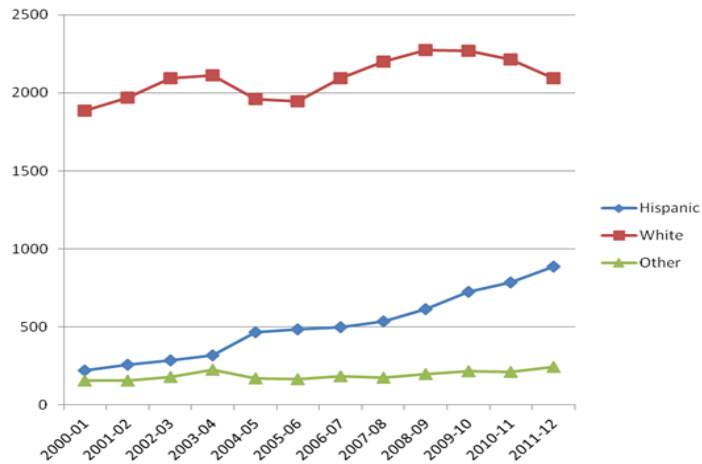
Enrollment Projections

The program's recruiting goals are designed to provide students with courses with enrollment small enough that students receive close personal attention from their teacher. The complexity and need for advanced skill development is best served by advanced and complex assignments that are closely supported by the course's instructor. Table 10 identifies the enrollment goals for the first five years of the program.

| Table 10: Five-Year Goals for Cyber Security BAS FTES					
Year	1 2013-14	2 2014-15	3 2015-16	4 2016-17	5 2017-18
Headcount	25	44	47	50	50
FTES	20	40	40	40	40
Graduates	0	13	15	20	20

Serving Place Bound Students

The CBC Cyber Security BAS degree is designed specifically to serve place-bound students and provide them with a degree in a discipline critically needed for companies and organizations within Benton and Franklin counties and across Washington State. Many CBC students wish to transfer for additional education often choose colleges either nearby or that have distance learning programs suggesting students either feel or actively chose to be place-bound. Figure 5 illustrates the top ten transfer choices for CBC students for 2011-12. The top option, not surprisingly, is Washington State University Tri-Cities. University of Phoenix and Western Governors University are the next two transfer destinations indicating an interest in distance education or that students have chosen not to move. Interestingly, the current CBC BAS degree in Applied Management is the fifth most likely destination for upper-division level education. This suggests when a bachelor's degree program is available at CBC; students will often choose the campus option for that major.

Figure 5: CBC Transfer Destinations

2011-12 Top 4-yr Transfer Destinations for CBC Students
Data Source: SBCTC
2011-12 Annual Report
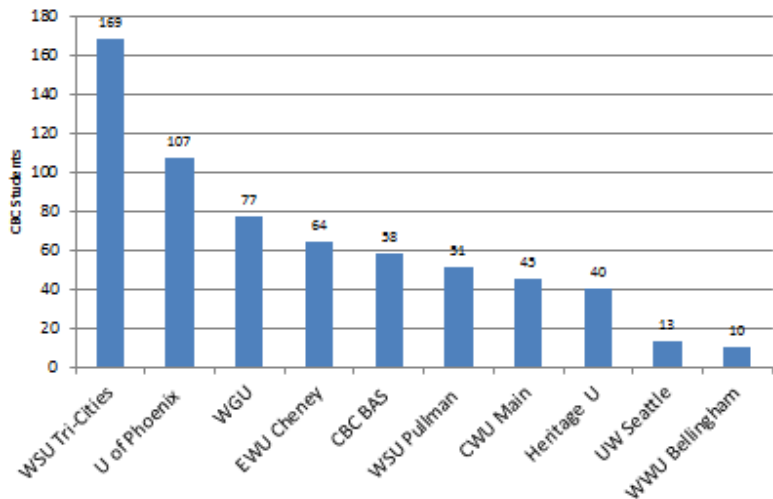
Criteria 4. Appropriate Student Services Plan

CRITERIA	STANDARD
4. Appropriate student services plan.	Describe services that will be needed by the students admitted to the degree program and the college plan for providing those services. Include a description of financial aid services and academic advising for students admitted into the program.

To support the cyber security BAS students, CBC will hire a Student Service Specialist for the program to provide a focused student support system and recruiting program for students. This model will be similar to the already successful student services program for the CBC Applied Management BAS students. The BAS Cyber Security Student Service Specialist will assist in identifying future Cyber Security BAS students, maintain student records, provide program advising, provide retention services, identify and support internships and shadowing experiences, and assist Cyber Security students in accessing other student support services as needed.

The cyber security BAS student services efforts are specifically designed to meet the needs of the adult BAS student that is working, going to school in the evenings, and taking courses through blended learning. These students will be busy, and likely need assistance to keep engaged, focused, avoid feeling overwhelmed, and avoid the feeling of isolation while engaged in the distance learning portion of their program.

The BAS Cyber Security Student Services Specialist and the program instructors will do academic advising and educational planning for the BAS-C student. These program experts will ensure that students receive clear, consistent, and accurate information. A specific BAS-C advising website, to be used with the current CBC online advising site, will also be designed for the students. Students will be trained how to use the site and therefore have 24/7 access to online advising/registration services.

The retention strategies will emphasize both "high touch and high tech." The "high touch" strategy will begin with one-on-one time with the BAS-C Student Services Specialist and the BAS-C faculty members. The staff and the faculty for the BAS program will get to know each student so students will feel the program staff understands them and have committed to their success. The BAS-C Student Services Specialist will be the main contact for many of the student's needs so the student has only to ask for help from the BAS-C Student Services Specialist. The Specialist will either offer personal help or coordinate with other student services staff to provide what is needed. In addition, the BAS-C Student Services Specialist will try to anticipate what the students individually or what the group might need and provide student options. At the beginning of each year, the BAS-C Student Services Specialist will coordinate a gathering that will provide an initial opportunity for students to get to know each other, meet instructors and administrative support staff, and help the student anticipate their BAS experience.

The "high tech" efforts will come in many ways. Since the program is a high tech program and will be designed with integration of eLearning tools into each class, the BAS-C Student Support Services Specialist will also integrate the use of technology in advising and communication. CBC has

recently added AgileGrad software to help support the advising process. Students will experience the use of technology seamlessly throughout the program. Social media will be used to communicate with students, a program specific webpage supporting BAS Cyber Security students and the new campus SharePoint portal will be also used extensively.

The Student Services Specialist will report directly to the BAS Cyber Security director and the program dean. She/he will provide information to the cyber security instructional staff, and liaison with campus student services departments. The specialized student support model will provide student services continuity for evening students and will ensure that cyber security students receive assistance from a staff person that is an expert on the CBC BAS Cyber Security program. This Student Service Specialist will help students access campus student services as well. Examples of the campus student services include the following:

- **Hawk Central:** One-stop student support is available to all CBC students at a newly develop services called Hawk Central. Designed as a one-stop center for student support, students can drop by during designated hours for student assistance and problem solving. Staff is cross-trained in all student services and can provide much of what students need such as cashiering, advising, financial aid, and other campus information. Staff can also quickly refer students to additional specialized services as needed.

- **Online Services:** CBC's newly redesigned website provides online access to campus services such as career information, online registration, financial aid support, student records, and eTutoring. Services are available 24/7 for students not able or interested in driving to campus for face-to-face services.

- **Tutor Center:** High performing cyber security students will be recruited to assist students in mastering cyber security skills. Writing and math tutors are already in place to help students that are struggling or seeking to expedite their skills. A math lab is adjacent to the Tutor Center and online or eTutoring is also available.

- **Financial Aid**: The CBC Financial Aid Office is committed to providing a comprehensive financial aid program for BAS students who have need, apply on time, and meet other requisite conditions for financial aid. CBC offers aid, including loans, work study, and grants or scholarships, to meet the BAS student needs. The Financial Aid Office has provided the current BAS Applied Management students financial aid services for four years. The new BAS Cyber Security students will have the same access as experienced by the current BAS Applied Management students.

- **Resource Center:** The CBC Resource Center will provide assessment and support accommodations for BAS students with documented disabilities. The Center has testing space and the staff coordinates testing for disabled students and assists faculty to provide appropriate accommodation. The Center provides evening hours as needed.

- **Veteran's Services:** As veterans in general are identified as having experiences that help provide a mindset that enhances cyber security professionals focused, recruiting efforts may increase the percentage of veterans in the Cyber Security program. The CBC campus is recognized as a veterans-friendly campus and has specific support services through a drop-in center, specialized veterans financial support, personal counseling services, and specialized veterans services.

- **Placement:** As part of the recruiting plan, the BAS-C Student Services Specialist will also work closely with the Cyber Security Advisory committee and the CBC Student Placement Services to become familiar with the types of businesses that would have need of a cyber security prepared student. This early and ongoing networking will provide the ground work for a successful placement effort both for internships as well as the placement after program completion.

  Since a number of the BAS-C students might opt for an internship experience or will already be working, special attention will be paid to assist students to use their experiences to network or seek initial employment or work with their current employer to identify promotional options.

  The students will be invited to the annual CBC Placement Fair and will have access to CBC workshops on Interviewing, Resume Writing, etc. The CBC Student Placement services have pledged to provide placement assistance to all BAS students. CBC will also have the support of the local WorkSource (who has been recognized nationally as "WorkSource of the Year").

- **Library Services**: Although all of the campus librarians will provide services for the cyber security students, one of the four librarians will be the designated to support the program. Cyber security is a quickly evolving discipline so resources are likely to be digital in the form of newly published government reports, publication databases, websites supporting cyber security, and Listservs. The designated librarian will be an important partner in the cyber security program information delivery and research support. A number of newly published books on related topics will be purchased immediately and ongoing purchases will be made in the future for the library collection. One hundred and fifty lap tops are also available for student checkout from the Library Circulation Desk. The Library maintains day, evening, and Saturday hours.

- **Internet Access and Technology Support**: As one of the first Washington community colleges with Wi-Fi, all students have access to campus networks. Multiple campus sites have networked printers and students also have access to a pre-designated level of free copies each academic quarter. A large open student computer lab is available inside the campus library.

- **Student Study Space:** Although the Library has individual and group student study space, the campus has multiple designated spaces for individual and group study throughout the campus. Wi-Fi access and electrical outlets encourages and supports the use of student technology (BYOD, bring your own device).

- **eLearning:** CBC has a robust online program that is supported by two highly qualified experts. They are available to students for technology trouble-shooting.

In summary, the BAS Cyber Security student services program is designed to provide students with a combination of the personal attention from the Student Services Specialist, services from the campus student services program, and support from the Cyber Security faculty and other computer science staff. In addition to the personal attention, students will also be provided with virtual support services.

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

CRITERIA	STANDARD
5. Commitment to build and sustain a high quality program.	Provide a financial plan for the first five years of program operation. This plan should include (1) types of funds to be used to support the program; (2) projected program expenses; (3) appropriate facilities to be used; (4) equipment, technology, and instructional resources needed for the program.
	Document the college's ability to sustain the program over time.

5-1 Revenue and Funds to Sustain the Cyber Security Program

The Cyber Security BAS program is designed as a self-support program sustained by BAS level tuition from cyber security program students, cyber security student fees, shared hardware and software resources from the existing computer science instructional program, partnership funding or in-kind services opportunities from community businesses and organizations, and potential grant support. To assist in the program startup, Pacific Northwest National Lab (PNNL) has pledged $118,000. The $118,000 will be expended during FY-13 and the first year of operation.

The campus commitment to the program is demonstrated by local funds for initial curriculum development and the use of campus tech fee to replace one of the four computer labs that support the entire computer science program and specifically the BAS Cyber Security program. Table 11 illustrates the program revenue levels for the first five years of the BAS Cyber Security program operations and funding for the current year's development activities.

Table 11: Projected Program Revenue						
	FY-13	**FY-14**	**FY-15**	**FY-14**	**FY-16**	**FY-17**
Tuition & Fees	$ 0	$ 206,344	$ 388,624	$ 388,624	$ 388,624	$ 388,624
PNNL Funds	$ 68,000	$ 50,000	$ 0	0	0	0
Curriculum Development	$ 16,000					
Tech Fees	$ 30,000*					
Total	$ 114,000	$ 256,334	$ 388,624	$ 388,624	$ 388,624	$ 388,624

*$30,000 from tech fee used to upgrade one of the four computer labs$ 388,624

5-2 Cyber Security Program Expenses

Table 12 projects the BAS Cyber Security program expenditures for the program startup costs for FY-13 and the first five years of operation. As additional evidence of institutional commitment to the BAS Cyber Security program, the dean oversight and clerical support will not be charged back to the BAS Cyber Security program nor will indirect or overhead costs be assessed to the program. Part-time instructor costs have been adjusted to accommodate possible faculty sabbaticals for continued ability to promote professional development for the cyber security faculty members.

Table 12: Projected Program Costs

	FY-14	**FY-15**	**FY-14**	**FY-16**	**FY-17**
BAS Director	$ 32,000	$ 32,000	$ 32,000	$ 32,000	$ 32,000
F/T Instruction	$ 48,000	$ 48,000	$ 48,000	$ 48,000	$ 48,000
P/T Instruction	$ 10,000	$ 60,000	$ 60,000	$ 60,000	$ 60,000
Student Support Specialist	$ 45,000	$ 45,000	$ 45,000	$ 45,000	$ 45,000
Back-to-Industry	$ 10,000	$ 28,000	$ 28,000	$ 28,000	$ 28,000
Benefits	$ 51,344	$ 56,000	$ 56,000	$ 57,000	$ 57,000
Travel	$ 20,000	$ 38,000	$ 38,000	$ 38,000	$ 38,000
Registration/ Fees	$ 5,000	$ 18,000	$ 18,000	$ 18,000	$ 18,000
Recruiting	$ 5,000	$ 8,000	$ 8,000	$ 8,000	$ 8,000
Books/Supplies	$ 15,000	$ 20,000	$ 20,000	$ 20,000	$ 20,000
Equipment	$ 15,000	$ 35,624	$ 35,624	$ 35,624	$ 35,624
Total	$ 256,344	$ 388,624	$ 388,624	$ 388,624	$ 388,624

5-3 & 5-4 Program Facilities, Equipment, Technology, and Instructional Resources

The BAS Cyber Security program is scheduled to use the computer science instructional facilities. The instructional space was completely remodeled in 2005 specifically for the computer science instructional program. Included in the 10,000 square foot computer science space are instructional offices, conference room, workroom, reception area, two dedicated classrooms, four computer labs and storage space. Two of the computer labs have new computers, one lab in 2011-2012 and the other lab in 2012-2013. The third lab has a mix of PC and Apple computers allowing two platforms to support the BAS Cyber Security program. The computer labs are updated on a regular replacement schedule so students and instructors have continuously updated hardware. Virtual labs are also available. The campus and the Computer Science department participate in the Microsoft Software Program to ensure software matches the newest version available.

The computer science facilities are intentionally located in the 154,666 square foot Lee Thornton Science, Diversity, and Technology building. The campus Information Services support office is located across the hallway from the computer science instructional area providing opportunity for shared efforts. Also located nearby in the same building are the diversity programs. The diversity staff are located in the same building as science and technology to encourage and support diversity in the STEM programs.

5-5 College Commitment to the Cyber Security Program

CBC is committed to developing and maintaining a BAS degree in Cyber Security. The need for the program is especially acute in CBC's service district; it is a natural progression for many of CBC's two-year computer science graduates; and students, employers; and advisory committee members are strongly supportive of the degree.

The decision to seek a BAS degree in Cyber Security and subsequent preparation for the degree began several years ago. Faculty have and are continuing to participate in back-to-industry experiences

and college funds are dedicated to send several instructors to a series of cyber security conferences and training. Conversations with representatives from CBC's private partnerships at the CBC president and vice president level have been also ongoing for several years. Computer Science faculty have completed coursework, training, and certifications in preparation for the degree.

In addition, CBC is committed to continuing to seek high-demand BAS degrees to provide to the College's service district. CBC students and potential students have welcomed the addition of the BAS degree in Applied Management making it one of the fastest growing campus programs. Although initially the BAS degree in Applied Management had specific state funding the program has now doubled in size with campus support. If approved, the same level of campus backing will also support the BAS degree in Cyber Security.

Criteria 6. Program Specific Accreditation

CRITERIA	STANDARD
6. Program specific accreditation.	Indicate whether the institution will seek specialized program accreditation. If so, describe plans for accreditation and identify appropriate accrediting body.

In addition to submitting the substantive change to NWCCU for a second community college baccalaureate degree, CBC will pursue computer science accreditation with the *Accreditation Board for Engineering and Technology, Inc*. (ABET). ABET accredits higher education degree programs in applied science, computing, engineering, and engineering technology. ABET computer accreditation options begin at the bachelor level degree programs. CBC can request specialized accreditation for the BAS degree in Cyber Security. Currently a number of Washington State bachelors level computer science degrees are accredited through ABET; therefore, as a state instructional standard CBC has decided to also seek ABET accreditation. The Washington computer science degree programs currently accredited by ABET include:

- Eastern Washington University-- Computer Science, BS

- Gonzaga University--Computer Engineering, BS
- Pacific Lutheran University-- Computer Engineering, BS
  Computer Science, BS
- University of Washington--Computer Engineering, BS
- University of Washington Tacoma--Computer Engineering and Systems BS
- Washington State University--Computer Science BS and BA
- Western Washington University--Computer Science BS

Typical of a specialized accreditation process, ABET accreditation requires programs requesting initial accreditation have at least one graduate from the program prior to program's accreditation visit. Given the accreditation process takes approximately 18 months, the BAS Cyber Security program will begin the self-study process in Fall 2013. The timing for the ABET accreditation visit will be arranged for the September-December 2015 time period immediately following the academic year after the first Cyber Security student is expected to graduate in Spring 2015. CBC plans to complete the accreditation process in late 2015 or early 2016. Upon the approval for ABET accreditation, students initially enrolled in the BAS Cyber Security program will retroactively be considered to have graduated from an ABET accredited program.

Criteria 7. Educational Pathways Beyond the BAS Degree

CRITERIA	STANDARD
7. Pathway options beyond baccalaureate degree.	Describe opportunities and articulation agreements for the place-bound BAS graduates to continue their education onto a graduate (Master's) degree program.

BAS Cyber Security graduates will be encouraged to continue their education at the master's level. CBC currently has good success with transferring students from existing BAS to master's level programs. After only two BAS Applied Management classes have graduated, seven of the graduates are already enrolled in master's level education. A similar level of BAS Cyber Security students are expected to continue onto the master's level.

Place-bound BAS Cyber Security graduates, who continue their education in cyber security, have a number of online options available to them. Two online universities with specific cyber security, proven masters programs, and also have a strong presence in Washington are Western Governors University (WGU) and University of Maryland University College (UMUC). A search reveals multiple other online programs such as Florida Tech University, Capella, NYU-ePoly, and Colorado Tech.

For students that are able to relocate, there are a number of Washington State Universities with good face-to-face master's level computer science programs. The University of Washington-Bothell, however, is launching a new master's degree in Cyber Security Engineering beginning Fall 2013. Upon receiving approval for the BAS degree in Cyber Security, CBC will seek articulation agreements with key available masters programs. Table 13 illustrates computer science pathways from the certificate level to sample Cyber Security masters programs.

Table 13: Cyber Security Educational Pathways from Certificates to Masters

CERTIFICATES	ASSOCIATE	BACHELOR'S	MASTER'S
CBC Certificates	**CBC Associate Degrees**	**CBC BAS**	**Examples of Cyber Security Masters Level Options**
Network and Security Certificate (certification & 1 yr. certification)	Cyber Security		Western Governors University MS in Information Security and Assurance (online)
Computer Database Management Certificate (certification & 1 yr. certification)	Database Administrator *(supplemented by Cyber Security AS degree requirements)*		--OR--
Computer and Information Technology (certification & 1 yr. certification)	Help Desk Technician *(supplemented by Cyber Security AS degree requirements)*		Eastern Washington University MS in Computer Science
Network and Security Certificate (certification & 1 yr. certification)	Network Administrator *(supplemented by Cyber Security AS degree requirements)*		--OR—
*C# and Mobile Device Programming (certification & 1 yr. certification) *C++ and Objective-C/iPhone Programming (certification & 1 yr. certification) *Java, Web, and Mobile Device Programming (certification & 1 yr. certification)	Programming and Software Development *(supplemented by Cyber Security AS degree requirements)*	BAS Cyber Security	University of Washington-Bothell Master of Science in Cyber Security Engineering --OR-- University of Maryland University College MS in Cyber Security (online) --OR-- Florida Tech University Masters of Science in Information Technology with a Specialization in Cyber Security (online)

Criteria 8. Expert Evaluation of Program

CRITERIA	STANDARD
8. External expert evaluation of program.	The institution will select two external experts to review the program. In a separate document, provide copies of external evaluators' reports or letters. Summarize the institution's responses and subsequent modifications to the proposal based upon evaluator's recommendations. Attach a short bio of the evaluators.

External Expert Response #1:   **Vicki Wilson**
                                     Manager Support Services
                                     Lockheed Martin

Vicki Wilson is the manager of Support Services in the Service Operations organization for Lockheed Martin Information Technology. Her career at the Hanford site in Richland, WA for more than 28 years has included many different areas of IT services and support.

Vicki is a native of the Tri-Cities. She is a graduate of Pasco High School and Columbia Basin College. She earned her BA from Eastern Washington University in Decision Science. Vicki is also on the Board of Trustees for Eastern Washington University.

External Expert Response #2:   **Gregg A. Serene**
                                     Computer Systems Security Analyst
                                     Lockheed Martin

Gregg Serene is the lead analyst for the Security Testing program at the Department of Energy's Hanford site. The Security Testing program includes web application security testing, penetration testing, and perimeter scanning. Gregg has graduate degrees in Ancient Near Eastern Studies (Cornell University), Theology (Fuller Seminary), and Semitic Languages (also Fuller) and an undergraduate degree in Accounting (University of Maryland, College Park). Gregg serves on the CBC Computer Science Advisory Committee.

Summary

Columbia Basin College proposes to implement a Bachelor's of Applied Science degree in Cyber Security beginning Fall 2013. From the previously approved Form B and this proposed Form D, the College believes it meets or exceeds the following requirements for BAS approval:

- The capacity to commit necessary resources for program success;

- The delivery of courses that will meet the current and emerging needs for the cyber security workforce;
- The ability to engage highly qualified faculty to develop and deliver the cyber security curriculum;
- The identified curriculum prepares students for additional education beyond the bachelors level;
- A student selection process that supports the selection of a diverse student population;
- A robust student services program to support student success;
- Plans to seek specialized program accreditation;
- A review completed by subject matter experts and program was modified as appropriate
- The documented demand for the program in CBC's service area;
- The need for cost-effective access to a baccalaureate program for place-bound students that builds on current computer science two-year degrees; and
- A program that fills a gap in education options offered by the public four-year institutions in the geographic area.

Columbia Basin College has demonstrated, through a variety of other workforce programs, academic programs, and an already successful BAS degree in Applied Management its capacity to deliver high-quality, cost-effective educational programs for Benton and Franklin counties. The Cyber Security BAS program allows graduates of existing AAS computer science programs, and other students with appropriate qualifications, to pursue a bachelor's degree. The degree will provide students with cyber security training while at the same time opening the doors to the students for promotion and higher wages. Students, organizations, and businesses, as well as the community, will gain substantially as a result of implementing this high-demand program.

In conclusion, CBC has a highly qualified faculty and other community experts with strong academic and applied experience to provide high-quality teaching and cyber security education and training. A creative and thoughtful curriculum has been developed to meet program goals. Critical support elements, such as the capability for advising and placement, are in place. A thorough plan for conducting formative and summative program evaluations, and for using the data for continuous improvement, has been developed. Finally, the proposed BAS in Cyber Security program is unique to and vital for the Columbia Basin region and offers considerable benefits to a variety of students, employers and the community without intruding on or duplicating the goals or mission of other

educational programs in the region. In addition, the program will provide an opportunity for a cyber security focused degree to be implemented in the eastern region of the state.

Appendix A: BAS in Applied Management at CBC

Columbia Basin College (CBC) was authorized to offer a Bachelor degree in Applied Management (locally known as BAS-M) beginning Fall 2009. CBC was part of the second round of BAS degrees approved in Washington State. To support the BAS degree, the College was granted 40 FTES funded at the bachelor level and was also granted development funds. Northwest Commission on Colleges and Universities (NWCCU) extended CBC's accreditation approval to bachelor level January 2011. Each year of operation the program has grown, exceeding the FTE program goals on an annual basis. In June 2011, it was decided to double the size of the program for a total of 80 FTES. Table 14 provides an overview of program growth and graduation levels. The program is currently on target to produce approximately 95 annualized FTE during the 2012-2013 academic year.

To accomplish that task, 20 FTES were added at the junior level for 2011-2012 and another 20 FTES at the junior level were added in Fall 2012. The current goal is to operate at approximately 80 FTES on an annual basis. To support a program of 80 FTES and to maintain the quality of the original lower division program, additional faculty have been added. The additional staff include three faculty that consist of one with a PhD in Leadership; one with an MBA and multiple years in the world of business; and finally another faculty member with a JD, a BS in Business, and an MBA. The dean responsible for the program also completed a second doctorate in Management. BAS-M assistant director has also been working on a doctorate since the BAS program has begun and is now ABD in Adult Learning in Higher Education.

The success of the original BAS program helps demonstrate the level of commitment CBC has for their first BAS degree and the College's willingness to maintain a quality program that will extend to the operation of a second BAS degree in Cyber Security.

Table 14: CBC's BAS in Applied Management Enrollment and Graduation Levels

Academic Year	FTE Goal	Actual FTES**	Graduates
2009-2010*	20	29	
2010-2011	40	49	27
2011-2012	60	65	21
2012-2013	80	***	

*First Academic Year of CBC's BAS Applied Management Degree

**Annualized FTES

***Summer (32 FTES) & Fall FTES levels indicate the 2012-2013 enrollment goal will be accomplished

Appendix B: General Distribution Course Options

Communication

CMST 101 Speech Essentials [C]
CMST 110 Communication Behavior [C]
CMST&210 Interpersonal Communication [C]
CMST&220 Public Speaking [C]
CMST 260 Multicultural Communication [C]
ENGL&101 English Composition I [C]
ENGL&102 Composition II [C]
ENGL&235 Technical Writing [C]
ENGL 410 Professional & Organizational Communication [C]

Humanities

ARAB 121 Arabic [H]
ARAB 122 Arabic II [H]
ARAB 123 Arabic III [H]
ART& 100 Art Appreciation [H]
ART 116 Art History Ancient World [H]
ART 117 Art History Medieval-Baroque [H]
ART 118 Art History Modern Times [H]
ART 119 Art History of Asia [H]
ART 120 Art History Of the Americas [H]
ART 121 Women In Art [H]
CHIN&121 Chinese I [H]
CHIN&122 Chinese II [H]
CHIN&123 Chinese III [H]
CMST 246 Oral Interpretation [H]
DRMA&101 Intro to Theatre [H]
DRMA 215 Survey of Theatre History [H]
EFL 101 Written English Language I [H]
EFL 111 Written English Language II [H]
ENGL&111 Intro to Literature [H]
ENGL 140 The Cinema [H]
ENGL 160 Women's Literature [H]
ENGL 180 Multicultural Literature [H]
ENGL 195 Bible as Literature [H]
ENGL 203 Mythology [H]
ENGL 210 Intro to Linguistics [H]
ENGL&220 Intro to Shakespeare [H]
ENGL&236 Creative Writing I [H]
ENGL&237 Creative Writing II [H]
ENGL&244 American Literature I [H]
ENGL&245 American Literature II [H]
ENGL&246 American Literature III [H]
ENGL&254 World Literature I [H]
ENGL&255 World Literature II [H]
ENGL&256 World Literature III [H]
ENGL 257 English Grammar [H]
ENGL 264 English Literature [H]
ENGL 265 English Literature [H]
ENGL 266 English Literature [H]
ENGL 280 Gay and Lesbian Studies [H]
FRCH&121 French I [H]
FRCH&122 French II [H]
FRCH&123 French III [H]
FRCH&221 French IV [H]
FRCH&222 French V [H]
FRCH&223 French VI [H]
GERM&121 German I [H]
GERM&122 German II [H]
GERM&123 German III [H]
GERM&221 German IV [H]
GERM&222 German V [H]
GERM&223 German VI [H]
HEB 121 Hebrew I [H]
HEB 122 Hebrew II [H]
HEB 123 Hebrew III [H]
HIST&126 World Civilizations I [H]
HIST&127 World Civilizations II [H]
HIST&128 World Civilizations III [H]
ICS 120 Survey of Hispanic Culture [H]
ICS 125 Native American Culture [H]
ICS 130 Survey of Asian American Culture [H]
ICS 135 Survey of African American Cultures [H]
ICS 222 Columbia Basin Cultures [H]
ICS 310 American Diversity [H]
JAPN&121 Japanese I [H]
JAPN&122 Japanese II [H]
JAPN&123 Japanese III [H]
JAPN&221 Japanese IV [H]
JAPN&222 Japanese V [H]
JAPN&223 Japanese VI [H]
MUSC&105 Music Appreciation [H]
MUSC 116 History of Jazz [H]
PHIL&101 Intro to Philosophy [H]
PHIL&106 Intro to Logic [H]
PHIL 131 World Religions [H]
PHIL 150 Introduction to Ethics [H]
PHIL 305 Professional Ethics [H]
RUSS&121 Russian I [H]
RUSS&122 Russian II [H]
RUSS&123 Russian III [H]
SPAN 104 Intensive 1st Year Spanish [H]
SPAN 110 Beginning Spanish for Professionals [H]
SPAN 111 Intermediate Spanish for Professionals [H]
SPAN 112 Advanced Spanish for Professionals [H]
SPAN&121 Spanish I [H]
SPAN&122 Spanish II [H]
SPAN&123 Spanish III [H]
SPAN 205 Spanish for Spanish Speakers [H]
SPAN 206 Spanish for Spanish Speakers [H]
SPAN 207 Spanish For Spanish Speakers [H]
SPAN&221 Spanish IV [H]
SPAN&222 Spanish V [H]
SPAN&223 Spanish VI [H]
WS 155 Women's Cultural Heritage [H]
WS 160 Women in Literature and Art [H]

Mathematical & Natural Sciences

ANTH&205 Biological Anthropology [M/S]
ANTH 214 Biological Anthropology Lab [M/S]

ASTR&101 Intro To Astronomy w/ Lab [M/S]
ASTR&101L Intro To Astronomy Lab [M/S]
BIOL&100 Survey of Biology w/ Lab [M/S]
BIOL 120 Bioethics [M/S]
BIOL 140 Fundamentals of Botany [M/S]
BIOL 140L Fundamentals of Botany Lab [M/S]
BIOL 148 Plant Identification [M/S]
BIOL 148L Plant Identification Lab [M/S]
BIOL&160 ....General Biology w/ Lab [M/S]
BIOL&175 Human Biology w/ Lab [M/S]
BIOL 186 Extended Topics in Biology [M/S]
BIOL 186L Extended Topics in Biology Lab [M/S]
BIOL 201 Soils [M/S]
BIOL 201L Soils Lab [M/S]
BIOL&211 Majors Cellular w/ Lab [M/S]
BIOL&212 Majors Plant w/ Lab [M/S]
BIOL&213 Majors Animal w/ Lab [M/S]
BIOL 240 General Ecology [M/S]
BIOL 240L General Ecology Lab [M/S]
BIOL&241 Human A&P 1 w/ Lab [M/S]
BIOL&242 Human A&P 2 w/ Lab [M/S]
BIOL 250 General Genetics [M/S]
BIOL 250L General Genetics Lab [M/S]
BIOL 252 Insects of Economic Importance [M/S]
BIOL 252L Insects of Economic Importance Lab [M/S]
BIOL 253 Plant Pathology [M/S]
BIOL 253L Plant Pathology Lab [M/S]
BIOL 254 Plant Systematics [M/S]
BIOL 254L Plant Systematics Lab [M/S]
BIOL&260 Microbiology w/ Lab [M/S]
CHEM&110 Chemical Concepts w/ Lab [M/S]

CHEM&121 Intro to Chemistry w/ Lab [M/S]
CHEM&122 Intro to Organic Chemistry w/ Lab [M/S]
CHEM&123 Intro to Biochemistry w/ Lab [M/S]
CHEM&131 Intro to Organic/Biochemistry w/ Lab [M/S]
CHEM&140 General Chemistry Prep w/ Lab [M/S]
CHEM&161 General Chemistry I w/ Lab [M/S]
CHEM&162 General Chemistry II w/ Lab [M/S]
CHEM&163 General Chemistry III w/ Lab [M/S]
CHEM&241 Organic Chemistry I [M/S]
CHEM&242 Organic Chemistry II [M/S]
CHEM&243 Organic Chemistry III [M/S]
CHEM&251 Organic Chemistry I Lab [M/S]
CHEM&252 Organic Chemistry II Lab [M/S]
CHEM&253 Organic Chemistry III Lab [M/S]
CHEM 254 Quantitative Analysis [M/S]
CHEM 255 Instrumental Analysis [M/S]
CHEM 264 Quantitative Analysis Lab [M/S]
CHEM 265 Instrumental Analysis Lab [M/S]
CHEM 2861 Undergraduate Research, Special Topics [M/S]
CHEM 2862-9 Undergraduate Research, Special Topics [M/S]
CHEM 2901-9 Undergraduate Research, Special Topics [M/S]
ENVS&101 Intro to Environmental Science w/ Lab [M/S]
ENVS 174 Intro to Meteorology and the Atmosphere [M/S]
ENVS 310 Environmental Issues [M/S]
GEO 101 Physical Geography [M/S]
GEO 120 Introduction to Atmospheric Science [M/S]
GEO 1201 Introduction to Atmospheric Science Lab [M/S]
GEOL&101 Intro to Physical Geology w/ Lab [M/S]

GEOL 102 Physical Geology II [M/S]
GEOL 102L Physical Geology II Lab [M/S]
GEOL&103 Historical Geology w/ Lab [M/S]
GEOL&110 Environmental Geology w/ Lab [M/S]
MATH 113 Geometry/Trigonometry [M/S]
MATH 121 Structure of Elementary Math [M/S]
NUTR&101 Nutrition [M/S]
PHYS&100 Physics For Non-Science Majors [M/S]
PHYS&101 Physics Lab For Non-Science Majors [M/S]
PHYS&124 General Physics Lab I [M/S]
PHYS&125 General Physics Lab II [M/S]
PHYS&126 General Physics Lab III [M/S]
PHYS&134 General Physics I [M/S]
PHYS&135 General Physics II [M/S]
PHYS&136 General Physics III [M/S]
PHYS&231 Engineering Physics Lab I [M/S]
PHYS&232 Engineering Physics Lab II [M/S]
PHYS&233 Engineering Physics Lab III [M/S]
PHYS&241 Engineering Physics I [M/S]
PHYS&242 Engineering Physics II [M/S]
PHYS&243 Engineering Physics III [M/S]
SCI 110 Natural Hist of the Columbia Basin Region [M/S]
SCI 1101 Natural History of the Col Basin Region Lab [M/S]

Mathematical & Natural Science OR Quantitative/Symbolic Reasoning
MATH&107 Math In Society [M/S] [Q/SR]
MATH 122 Informal Geometry/Elementary Teachers [M/S][Q/SR]
MATH 123 Algebra,Probability,Stats Elementary [M/S] [Q/SR]
MATH&141 Precalculus I [M/S] [Q/SR]

MATH&142 Precalculus II [M/S] [Q/SR]
MATH&144 Precalculus I & II [M/S] [Q/SR]
MATH&146 Introduction to Stats [M/S] [Q/SR]
MATH 147 Finite Math [M/S] [Q/SR]
MATH&148 Business Calculus [M/S] [Q/SR]
MATH&151 Calculus I [M/S] [Q/SR]
MATH&152 Calculus II [M/S] [Q/SR]
MATH&153 Calculus III [M/S] [Q/SR]
MATH&171 Math for Elementary Education I [M/S] [Q/SR]
MATH&172 Math for Elementary Education II [M/S] [Q/SR]
MATH&173 Math for Elementary Education III [M/S] [Q/SR]
MATH 243 Linear Algebra [MS/] [Q/SR]
MATH 246 Discrete Structures [M/S] [Q/SR]
MATH&254 Calculus IV [M/S] [Q/SR]
MATH 255 Differential Equations [M/S] [Q/SR]

Quantitative/Symbolic Reasoning
CS 102 Programming Fundamentals [Q/SR]
CS 162 C++2 [Q/SR]
CS 202 Programming Fundamentals 2 [Q/SR]
CS&131 Computer Science I C++ [Q/SR]
PHIL 121 Symbolic Logic [Q/SR]

Social & Behavioral Sciences
ANTH&100 Survey on Anthropology [S/B]
ANTH&204 Archeology [S/B]
ANTH&206 Cultural Anthropology [S/B]
ANTH&234 Religion & Culture [S/B]
ECON 110 Economic Trends, Issues and Policy [S/B]
ECON&201 Micro Economics [S/B]
ECON&202 Macro Economics [S/B]

ECON 291 History of American Economic Development [S/B]
ECON 305 Managerial Economics [S/B]
GEO 150 Cultural Geography [S/B]
HIST 107 Chicano History [S/B]
HIST 108 History of Immigration in the U.S. [S/B]
HIST 110 History of Modern East Asia [S/B]
HIST 111 Colonial Latin America [S/B]
HIST 112 Modern Latin America [S/B]
HIST 113 Mexico Since Independence [S/B]
HIST 115 History of Modern Middle East [S/B]
HIST 116 History of Africa [S/B]
HIST 117 History of India [S/B]
HIST&146 U.S. History I [S/B]
HIST&147 U.S. History II [S/B]
HIST&148 U.S. History III [S/B]
HIST&220 African American History [S/B]
HIST 233 War In History [S/B]
ICS 255 Race and Ethnic Relations [S/B]
POLS&101 Intro to Political Science [S/B]
POLS 104 State and Local Government [S/B]
POLS&201 Intro Political Theory [S/B]
POLS&202 American Government [S/B]
POLS&203 International Relations [S/B]
POLS&204 Comparative Government [S/B]
POLS 205 American Political Thought [S/B]
PSYC&100 General Psychology [S/B]
PSYC 103 Applied Psychology [S/B]
PSYC&200 Lifespan Psychology [S/B]
PSYC 201 Social Psychology [S/B]
PSYC 205 Psychology of Adjustment [S/B]
PSYC&220 Abnormal Psychology [S/B]
SOC&101 Intro to Sociology [S/B]

SOC 110 Gender, Media, and Popular Culture [S/B]
SOC 150 Marriage-Family [S/B]
SOC&201 Social Problems [S/B]
SOC 269 Sociology of World Cinema [S/B]
SSCI 290 Social Research Methods [S/B]
SSCI 2901 Social Research Methods Lab [S/B]

Appendix C: Course Descriptions and Outcomes

CS 101 Introduction to Computer & Information Technology   Credits: 5.0

CS 101 is a 5 credit introductory class designed to meet the needs of all students as defined in CBC's "Using Information Technology & Tools Student Learning Outcome." The class emphasizes the cognitive aspects of dealing with Information Technology (IT): evaluating information, learning practical IT skills, solving problems, and dealing with information related issues such as privacy, security, ethics, etc. Students will also learn computer basics, using Windows, Word, Excel, PowerPoint, email, and Internet skills to locate, present and report information.

COURSE OUTCOMES:

Introduction to Computer & Information Technology is intended to develop familiarity with use of information technologies and basic understanding of computer components through the following outcomes:

- Create, edit, and format Word documents to include borders, shading, graphics, tables, pictures, and Web addresses (SLO 1)
- Evaluate accuracy of online information (SLO 1 & 3)
- Summarize and judge new technologies beyond the desktop (SLO 6)
- Explain the fundamental principles of security (SLO 3 & 6)
- Demonstrate computer problem solving (SLO 3 & 6)
- Demonstrate the use of Windows, Word, Excel, and PowerPoint to accomplish assigned tasks SLO (1 & 6)
- Demonstrate email and Internet skills to locate, present, and report information (SLO 1, 3, & 4)

CS 102 Programming Fundamentals Credits: 5.0

An introduction to programming using current technologies. It is designed for those with little or no programming experience. Topics include: program development cycle, fundamentals of programming and logic, decisions, repetitions, controls, functions, and procedures. Prerequisite: MATH 095 or MATH 098 with a 2.0 or better.

COURSE OUTCOMES:

CS 102 is intended to develop understanding and skills in programming fundamentals through the following outcomes:

- Demonstrate basic computer concepts (SLO 6)
- Define terms used in programming (SLO 6)
- Identify what data types to be used when solving problems (SLO 6)
- Distinguish what variables are and how to declare them (SLO 1 & 6)
- Distinguish when to use loop, events, and conditional statements (SLO 1, 3, 5, & 6)
- Demonstrate how to define and call functions (SLO 1 & 6)
- Write, compile, debug, and run simple programs successfully (SLO 1 , 3, 5, & 6)

- Create a GUI using appropriate controls (SLO 1 – 6)
- Perform loops, decisions, and computations (SLO 1, 3, 5, & 6)

CS 106 Database Systems   Credits: 5.0

This is a beginning database course in which the student will create, modify, and implement relational databases using Microsoft Access. Topics include: tables, queries, forms, reports, sharing information with other programs, data access pages, advanced queries, managing database objects, and creating macros and navigation boards. Prerequisite: CS 101 recommended.

COURSE OUTCOMES:
CS 106 Database Systems is intended to develop understanding and beginning skills in database creation, modification, and implementation through the following outcomes:

- Demonstrate basic database concepts (SLO 1, 3, 4, 5, & 6)
- Design, create and modify Access tables and data (SLO 1, 3, 5, & 6)
- Create and run select, crosstab, find duplicates, and unmatched queries (SLO 1, 3, 5, & 6)
- Develop and print custom forms and reports (SLO 1, 3, 4, 5, & 6)
- Demonstrate how to import and export Access database objects (SLO 1 & 6)
- Create hyperlinks to external documents and web sites (SLO 1, 3, & 6)
- Demonstrate the ability to sort and filter data (SLO 1, 3, 5, & 6)
- Demonstrate how to create advanced queries (SLO 1, 3, 5, & 6)
- Demonstrate the ability to link and embed objects in a report (SLO 1, 3, 5, & 6)
- Export Access objects in various file formats (SLO 1, 3, 5, & 6) design and plan a user interface (SLO 1, 3, 4, 5, & 6)
- Create macros, custom toolbars, switchboards and menus (SLO 1, 3, 4, 5, & 6)

CS 117 Computer Ethics   Credits: 2.0

Covers essential topics of information and technology ethics. Students will understand what to do and what not to do as a user and an employee. Topics include: ethics and information technology, IT configured societies, information flow, privacy and surveillance, digital intellectual property, and professional ethics in computing. Students work in small groups to discuss important issues based on scenarios given.

COURSE OUTCOMES:

CS 117 is intended to develop SLO 1, and 3-6 through the following outcomes:

- Define terms associated with IT Ethics (SLO 6)
- Describe certain policies and laws dealing with software (SLO 4 & 6)
- Demonstrate their ability to work in a group (SLO 4)
- Critique and discuss today's misused software issues based on scenarios given (SLO 3 & 6)
- Compare and contrast Micro- and Macro-Level Analysis (SLO 6)
- List activities most people do with software and technologies and analyze possible unethical matters (SLO 3 & 6)
- Explain Virtual Rape (SLO 6)

- Explain complexity if ethical issues (SLO 6)
- Describe Democracy and the Internet issues and arguments (SLO 6)
- Describe Digital Intellectual Property and what to be avoided (SLO 4 & 6)
- Describe Law and Order on the Internet (SLO 4 & 6)
- Explain why care about "Information Flow and Privacy" (SLO 4 & 6)

CS& 131 Computer Science I C++   Credits: 5.0

This class is the first in a series of three in which the student will learn the C++ programming language. C++ is an extension of C language, which includes both procedural and object- oriented programming. It is the basis for most PC based windows programs. Students will learn C++ keywords, control structures, functions, arrays, strings, and introduction to classes and objects. All prerequisites must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES:
C++1 is intended to develop understanding and skills in the C++ programming language through the following outcomes:

- Explain basic computer concepts and C++ program development environment (SLO 1, 3, 5, & 6)
- Define terms used in programming (SLO 1, 3, 5, & 6)
- Select what data types to be used when solving problems (SLO 1, 3, 5, & 6)
- Prescribe what variables and addresses are (SLO 1, 3, 5 , & 6)
- Determine when to use loop, arrays, and conditional statements (SLO 1, 3, 5, & 6)
- Demonstrate how to define and call functions (SLO 1, 3, 5, & 6)
- Write, compile, link, load, and execute simple C++ programs successfully (SLO 1 – 6)
- Apply C++'s powerful structured programming and object-oriented features (SLO 1 – 6)
- Develop programs using standard C++ class libraries (SLO 1 – 6)
- Produce software tools for C++ development (SLO 1 – 6)
- Describe and call functions (SLO 1, 3, 5, & 6)
- Perform loops, decisions, and computations (SLO 1, 3, 5, & 6)

CS140 SharePoint Server   Credits: 5.0

The purpose of this course is to offer the critical information students need to successfully move into a role as an IT professional and support Microsoft Office SharePoint in a business environment. This class teaches SharePoint specific skills that will enable students to effectively implement, support, and troubleshoot SharePoint deployment. Prerequisite: CS 101 with 2.0 grade or better or instructor's permission.

COURSE OUTCOMES:

SharePoint Server is intended to develop the understanding and skills to work with SharePoint through the following outcomes:

- Install and configure SharePoint (SLO 1, 4, & 6)
- Distinguish and create SharePoint Users and groups (SLO 1, 4, & 6)

- Configure Authentication and Security (SLO 1, 4, & 6)
- Configure and create a collaborative environment with sites, blogs, and wiki's (SLO 1, 4, & 6)
- Create custom workflows (SLO 1, 4, & 6)
- Create and configure Document Libraries and Web content (SLO 1, 4, & 6)

CS& 141 Computer Science I JAVA with Android Devices   Credits: 5.0

JAVA is an object oriented programming language that is widely used to enhance information delivery on the Web. The topics include: compiling and running a Java Program, use of selection, loop structures, arrays, Graphical User Interface, and introduction to classes and objects. Students will learn how to write and debug Java programs with and without Graphical User Interfaces. Students will also learn to create simple Android Apps. Prerequisite: Math 095 or Math 098. The prerequisite must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES:

Computer Science I Java is intended to develop understanding and skills in the Java programming language through the following outcomes:

- Compare and contrast JAVA with other programming languages (SLO 1 & 3)
- Explain how the JAVA concept of "write-once run anywhere" is implemented (SLO 3, 5, & 6)
- Describe the relationship between JAVA and the Web (SLO 3 & 5)
- Explain how objects are created and how methods are inherited or over-ridden (SLO 1-6)
- Create, edit, run, and debug JAVA programs (SLO 1, 5, & 6)
- Create and manipulate selection, loops, and arrays in a Java application (SLO 5 & 6)
- Utilize JAVA toolkits (SLO 1, 3, & 5)
- Write a GUI Java Application (SLO 1 - 6)

CS 150 Computer Security   Credits: 5.0

This class covers the basics of computer security. Students will learn about virus protection, installing security patches, using firewalls to protect networks, cryptography and Public Key Infrastructure (PKI), and legal issues. Prerequisite: CS 101 recommended.

COURSE OUTCOMES:
CS 150 Computer Security is intended to develop understanding and skills in computer security through the following outcomes:

- Describe the vulnerabilities faced by computer and network users, and how to reduce exposure (SLO 1, 3, 4, & 6)
- Compare and contrast the various cryptographic methods such as simple encryption, steganography, DES, and PKI (SLO 1, 3, 4, & 6)
- Describe how the PKI exchange functions (SLO 4 & 6)
- Implement and maintain virus scanning software (SLO 1, 3, & 6)
- Develop an adequate security plan Given a list of conditions and requirements, (SLO 1, 3, 4, & 6)

- Prepare list of public keys and trusted authorities (SLO 1 & 6)
- Evaluate the security exposure of a given computer and operating system (SLO 1, 3, & 6)
- Research and write papers on new technologies pertaining to this class (SLO 1, 3, 4, & 6)

CS 162 C++2 Credits: 5.0

This is an intermediate C++ course that provides students an understanding of key object- oriented programming (OOP) theories and concepts; and how to create and manipulate objects in a GUI environment. The students will learn advanced features of C++ including: arrays, strings, file processing, classes, inheritance, composition, pointers, virtual functions, templates, and introduction to linked lists. All prerequisites must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES:
C++2 is intended to develop understanding and intermediate skills in the C++ programming language through the following outcomes:

- Utilize arrays in C++ programs (SLO 1, 3, 5, & 6)
- Apply concepts of classes and objects in C++ programs (SLO 1, 3, 5, & 6)
- Apply inheritance and composition in C++ programs (SLO 1, 3, 5, & 6)
- Apply pointers, classes, and virtual functions in C++ programs (SLO 1, 3, 5, & 6)
- Perform overloading and templates in C++ programs (SLO 1, 3, 5, & 6)
- Explain a linked list structure (SLO 1, 3, 5, & 6)
- Develop and maintain programs using standard C++ library functions and different data such as arrays, and linked list (SLO 1 – 6)
- Modify and analyze C++ programs for best solutions (SLO 1 – 6)
- Allocate memory dynamically (SLO 1, 3, 5, & 6)
- Maintain and document a C++ program (SLO 1 – 6)
- Develop complex C++ programs for business applications (SLO 1 – 6)

CS 200 Computer Forensics Fundamentals   Credits: 5.0

This class provides the student with the fundamentals of computer forensics, cyber crime scene analysis and electronic discovery; along with associated investigation tools and techniques. The students will explore computer forensic theory and focus on various forensic skills including conducting security incident investigations; file system and storage analysis and data hiding techniques. Students will also learn about legal issues and standards.

COURSE OUTCOMES
Computer Forensics is intended to develop Critical Thinking, Quantitative and Symbolic Reasoning, Effective Communication, Applying Information Tools and Resources, Developing Cultural Awareness and Mastering Program Learning Outcomes through the following outcomes:

- Explain how to deal with categories of electronic evidence including media, email, and networks. (SLO 4 & 6)
- Detect and prevent intrusion and attacks. (SLO 4 & 6)
- Gain experience in structured digital evidence collection and evaluation. (SLO 4 & 6)

- Apply commercial and open-source computer forensics tools. (SLO 4 & 6)
- Depict the legal issues involved in computer forensic analysis. (SLO 1 & 5)
- Prepare written reports and deliver presentations showing investigative results. (SLO 3, 4, & 6)

CS 202 Programming Fundamentals 2   Credits: 5.0

This is an intermediate programming course using current technologies. Students will learn to write, design, and debug Windows applications using a variety of controls and events, procedures, functions, arrays, structures, files, classes /Object Oriented design, database programming, and calculations to solve problems. Class projects involve writing games and business applications. Prerequisite: CS 102 with 2.0 grade or better.

COURSE OUTCOMES:

CS 202 is intended to develop understanding and gain programming skills through the following outcomes:

- Demonstrate how to create a sub and function procedure. (SLO 6)
- Summarize how to define and call functions and sub procedures. (SLO 1, 3, 5, & 6)
- Demonstrate the use of value and reference parameters. (SLO 6)
- Explain the importance of why using a sub and/or function procedure.(SLO 3 & 6)
- Understand how to declare arrays. (SLO 6)
- Explain when to use a one dimensional and a two dimensional array. (SLO 3 & 6)
- Connect to a database and manipulate the data using LINQ. (SLO 1 & 6)
- Explain Structured Query Language (from research). (SLO 6)
- Demonstrate how to declare a structure and manipulate it in a program.(SLO 1, 3 , 5, & 6)
- Demonstrate how to manipulate strings.(SLO 1 , 3, & 6)
- Create a menu.(SLO 1 & 6)
- Create a Web Application. (SLO 1 & 6)
- Demonstrate how to create a class and object. (SLO 1 & 6)
- Create objects of classes to execute desired tasks. (SLO 1, 3, 5, & 6)
- Apply loops, classes, arrays, events, and conditional statements in programs. (SLO 1, 3, 5, & 6)
- Write, compile, debug, and execute business and game programs successfully (SLO 1, 3, 5, & 6)
- Develop programs using appropriate controls for an advanced GUI. (SLO 1, 3, 5, & 6)

CS 206 Database Design   Credits: 5.0

An advanced course designed to help students understand concepts including: SQL, integrity constraints, relational database design, normalization, and physical database design. Students also gain hands-on experience using Microsoft. Prerequisite: CS 106, MATH 095 or MATH 098, and/or instructor's permission. All prerequisites must be passed with a 2.0 or better.

COURSE OUTCOMES:

Database Design is intended to develop advanced understanding and skills in database design through the following outcomes:

- Identify when to use SQL (SLO 1, 3, & 6)
- Implement data integrity constraints (SLO 1, 3, 4, & 6)
- Design a relational database and why relational databases are useful (SLO 1, 3, 4, & 6)
- Summarize basic concepts of indexing (SLO 3, 4, & 6)
- Identify and apply query processing (SLO 1, 4, & 6)
- Create transactions (SLO 1, 4, & 6)
- Design bound and unbound forms and subforms (SLO 1, 4, & 6)
- Create reports that display data requested (SLO 1, 4, & 6)

CS 221 SQL Server Administration   Credits: 5.0

This course provides students with the knowledge and skills to install, configure, administer, and troubleshoot Microsoft SQL Server client/server database management systems. It will help prepare students for the MCDBA Certificate. Prerequisite: CS 106, CS 228, and MATH 095 or MATH 098. All prerequisites must be passed with a 2.0 or better.

COURSE OUTCOMES:

SQL Server Administration is intended to develop the knowledge and skills to install, configure, administer, and troubleshoot Microsoft SQL server database management systems through the following outcomes:

- Describe SQL Server Architecture (SLO 1, 3, 4, & 6)
- Choose and configure a login security method (SLO 1, 4, & 6)
- Plan and implement database permissions (SLO 1, 4, & 6)
- Develop a backup and restore plan (SLO 1, 3, 4, & 6)
- Troubleshoot SQL Server problems (SLO 1, 4, & 6)
- Install and configure SQL server (SLO 1, 4, & 6)
- Manage files on an SQL server (SLO 1, 4, & 6)
- Monitor and maintain SQL server performance (SLO 1, 4, & 6)

CS 223 UNIX/LINUX   Credits: 5.0

This course will prepare students to administer UNIX and Linux. This course covers topics related to: installation, configuration, troubleshooting, and optimization of a Linux Server. Students will learn to set up and maintain users, groups, and file systems. The students will learn how to use critical thinking and troubleshooting tools to troubleshoot the server, printers, and workstations. Prerequisite: CS 110, CS 123 PC Hardware recommended MATH 095 or MATH 098, or instructor's permission. All prerequisites must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES:

UNIX/LINUX is intended to develop the understanding and skills for working with other operating systems through the following outcomes:

- Compare and contrast Linux with Unix, Windows Operating System, DOS, and NT (SLO 3 & 6)
- Explain the Unix file system (SLO 4 & 6)
- Describe how multi-user OSs differ from single user systems, and how it affects security (SLO 3, 4, & 6)
- Utilize telnet to connect and log on a Unix host (SLO 1 & 6)
- Perform basic functions such as listing directories, copying files, and moving around the file system (SLO 1 & 6)
- Illustrate the use FTP to move files between Unix and Windows (SLO 1 & 6)
- Demonstrate the use of the *man* utility to get help (SLO 1 & 6)
- Manage Unix file permissions (SLO 1 & 6)
- Explain the use the *Vi* Editor to create files (SLO 1 & 3)
- Create simple batch scripts (SLO 6)
- Customize the Unix environment (SLO 6)

CS 228 Windows Server   Credits: 5.0

This course will prepare students to work with Windows Server. This course covers topics related to installation, configuration, troubleshooting, and optimization of a Windows Server. The students will learn to set up and maintain users, groups, and file systems. Students will learn how to use critical thinking and troubleshooting tools to troubleshoot the server, printers, and workstations. This class will help to prepare students to pass one of the Windows exams. Prerequisites: CS 127 recommended, MATH 095 or MATH 098, or instructor's permission. All prerequisites must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES:

Windows Server is intended to develop the understanding and skills to work with Windows Server through the following outcomes:

- Summarize the hardware requirements and installation procedures for Windows Server (SLO 1 & 3)
- Identify resources and how to manage them (SLO 1, 3, & 6)
- Install and configure the Server software (SLO 1, 3, & 6)
- Create users and groups, attach printers, map drives, apply directory permissions (SLO 1, 3, & 6)
- Install, configure, and support applications (SLO 1, 3, 4, & 6)
- Utilize monitoring tools to isolate and solve performance related problems (SLO 1, 3, & 4)
- Apply troubleshooting tools to identify and correct problems (SLO 1, 3, & 4)
- Install and configure printers, file systems, disks and partitions (SLO 1 & 3)
- Implement Group Policy (SLO 1, 3, 4, & 6)
- Research and write papers on new technologies pertaining to this class (SLO 1, 3, & 4)

CS229 Webmaster   5 Credits

The goal of this course is to provide knowledge of Internet technologies and prepare students to pass CompTIA's broad-based, vendor-independent internet technology certification exam, i-Net+. This course covers a wide range of material about Internet, from using the Internet to demonstrating how the

Internet works, using different Internet protocols, programming on the Internet, the Internet infrastructure, security, an e-commerce. It not only introduces a variety of concepts, but also discusses in-depth the most significant aspects of Internet, such as the OSI model of networking. In addition to explaining concepts, the course uses a multitude of real world examples of networking issues from a professional's standpoint, making it practical preparation for the real world In this course, the student will gain the knowledge and skills needed to design and manage an Intranet for an Internet Web site. Specifically, the student will learn how to set up and configure a Web server and the applications needed to support it. Familiarity with building Web pages and with basic programming concepts are assumed. All prerequisites must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES

- Explain what the Internet is, and describe in detail its various components and describe the relationship between the various application protocols and TCP/IP (SLO 2, 4, & 6)
- Describe in detail how HTTP is used to transfer Web pages (4 & 6)
- Install, customize and troubleshoot different browsers (SLO 1, 2, 4, & 6)
- Install, configure and troubleshoot an IIS Web Server and the Apache web service on a Linux server (SLO 1, 4, & 6)
- Create and manage virtual server and virtual directories (SLO 4 & 6)
- Create and manage the interface between Web servers and existing database applications (SLO 4 & 6)
- Configure a web server to meet a given set of customer requirements and specifications (SLO 1, 3, 4, & 6)

CS 231 Network Infrastructure Credits: 5.0

This course will prepare students to install, manage, monitor, configure, and troubleshoot DNS, DHCP, Remote Access, Network Protocols, IP Routing, and WINS in a Windows network infrastructure. In addition, this class will also prepare students to manage, monitor, and troubleshoot Network Address Translation and Certificate Services. It also prepares the student to pass one of the MCSA/MCSE exams. All prerequisites must be passed with a 2.0 or better before taking this class. CS 228, and MTH 95 or MTH 98

COURSE OUTCOMES:

Windows Network Administration is intended to develop the knowledge and skills to install, manage, monitor, configure, and troubleshoot DNS, DHCP, Remote Access, Network Protocols, IP Routing, and WINS in a Windows network infrastructure through the following outcomes:

- Install, configure, manage, monitor, and troubleshoot DNS (SLO 1)
- Troubleshoot DHCP (SLO 3)
- Configure and troubleshoot remote access (SLO 3)
- Install, configure, and troubleshoot network protocols (SLO 6)
- Install, configure, manage, a WINS server (SLO 6)
- Install, configure, manage, Certificate Services (SLO 6)
- Install DNS server service (SLO 5)

- Manage and monitor DNS (SLO 6)
- Create and manage DHCP scopes (SLO 5)
- Install Certificate Servers (SLO 6)
- Configure a virtual private network (SLO 6)
- Install and configure TCP/IP (SLO 6)
- Secure access for remote access users (SLO 6)
- Configure and troubleshoot IPSEC (SLO 6)

CS 232 – Network Security

This course will prepare students to design network security solutions. This will focus on the networking side of security including firewall implementations, and network encryption and authentication. This course will also look at identifying security needs and business requirements for a corporate environment. Topics covered include: firewall configurations, Web and distributed systems security, and specific implementation of security models and architectures.   All prerequisites must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES:

- Identify security risks (SLO 1, 3, 6)
- Secure resources on windows servers (SLO 1, 3, & 6
- Design and implement Security Policies (SLO 1, 3, 4, & 6)
- Secure network services (SLO 1, 3, & 6)
- Use analysis tools to find network vulnerabilities (SLO 6)
- Plan and design firewall (SLO 1, 3, 5, & 6)
- Configure and administer a firewall (SLO 1, 3, 5, & 6)
- Describe and implement the principles of encryption (SLO 1, 3, 5, & 6)
- Demonstrate the components of contingency planning (SLO 1, 3, 5, & 6)
- Summarize the basics of digital forensics (SLO 6)

CS 236 Java I/O with Android Devices and Intro to Integration   Credits: 5.0

Students who have a programming background will learn to develop Java applications to manipulate data and databases. Topics include: classes, methods, interfaces, inheritance, exceptions, streams and files processing. Students will also be introduced to Enterprise Tools such as Spring, Ant, JUnit, Struts, and/or Hibernate, and integration libraries such as Java Database Connectivity (JDBC) API and Remote Method Invocation (RMI). Students will also learn to create Android Apps. Prerequisite: CS& 141, or instructor's permission. All prerequisites must be passed with a 2.0 or better before taking this class.

COURSE OUTCOMES:

CS 236 is intended to develop SLO 1, 3-6 through the following outcomes:

- Summarize how to work in input and output streams (SLO 6)
- Recognize file types (SLO 6)

- Describe data sources (SLO 4 & 6)
- Describe how to compress files in an application (SLO 4 & 6)
- Identify java classes needed for streams (SLO 6)
- Identify objects of streams (SLO 6)
- Describe a common way to encrypt data (SLO 4 & 6)
- Explain JAR Archive (SLO 6)
- Explain why using Object Serialization (SLO 3, 4, & 6)
- Create an application using classes and their objects to create tasks dealing with files to solve a problem (SLO 1, 3, 5, & 6)
- Maintain an application dealing with files to solve a problem (SLO 1, 3, 5, & 6)
- Identify essential classes used when working files and streams (SLO 1 & 6)
- Identify integration libraries and explain what they are for (SLO 1 & 6)
- Prepare an application sample that uses an integration library (SLO 1 & 6)
- Identify important components of the Enterprise Tools of the Spring, Ant, Struts, and/or Hibernate used to develop applications when using (SLO 1 & 6)
- Describe the importance of JUnit and why using it (SLO 4 & 6)

CS 250 Network Fundamentals Credits: 5

This class focuses on implementing, managing, protecting, and troubleshooting small to medium size enterprise branch networks. Topics covered include OSI model, Cisco devices, wireless networks, switching, IP routing, troubleshooting routing and advanced TCP/IP configuration. This course prepares students for the Cisco Certified Network Associate (CCNA) exam.

COURSE OUTCOMES:
Network Fundamentals is intended to develop *understanding and skills used in network technologies and security* through the following outcomes:

- Describe the purpose and functions of various network devices (SLO 1, 3, 4, & 6)
- Utilize the OSI and TCP/IP models and their associated protocols to explain how data flows in a network (SLO 1, 4, & 6)
- Perform and verify initial switch configuration tasks including remote access management (SLO 1, 4, & 6)
- Connect, configure, and verify operation status of a device interface (SLO 1, 4, & 6)
- Demonstrate the steps to configure a routing protocol and commands for configuring the Routing Information Protocol (RIP). (SLO 1, 4, & 6)
- Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point (SLO 1, 4, & 6)
- Calculate and apply an addressing scheme including VLSM IP addressing design to a network (SLO 1, 2, 4, & 6)
- Configure, verify, and troubleshoot VLANs   (SLO 1, 4, & 6)
- Describe enhanced switching technologies (SLO 1, 3, 4, & 6)
- Explain general methods to mitigate common security threats to network devices, hosts, and applications (SLO 1, 3, 4, & 6)

CSIA 300 Security and Information Assurance   Credits: 5.0

This course provides students with the tools and resources they need to develop an understanding of the CISSP certification body of knowledge. Using a variety of pedagogical features students will learn security basics such as security laws, access control, cryptography and security architecture and design. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE) CS 150, CS 231, and CS 250

COURSE OUTCOMES

- Interpret and apply application threats and countermeasures. (SLO 1,4, 6)
- Explain the types of recovery plan testing. (SLO 3,4, 6)
- Describe the steps in security incident response and investigations. (SLO 1,2, 6)
- Apply security concepts to computer and business operations. (SLO 1, 2, & 6)
- Describe how network routing, addressing, authentication, and tunneling work. (SLO 1, 4, & 6)

CSIA 310 E-Commerce Security Credits: 5.0

This course provides students with tools and resources they need to develop a thorough understanding of four major aspects of security; policies and procedures, technology orientation, computer and network security, and managing organizations securely.   PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE) CS 150, CS 206, CS 229, and CSIA 300. CSIA 300 can be taken concurrently

COURSE OUTCOMES

- Demonstrate how to use security principles in designs to improve the security of systems. (SLO 1, 4, & 6)
- Explain how to effectively manage security behaviors. (SLO 1, 3, & 6)
- Demonstrate how to apply the appropriate security tools effectively. (SLO 1, 4, & 6)
- Describe how to plan for existing and future needs and emerging security issues. (SLO 1, 3, & 6)
- Illustrate how to improve decision making and problem solving about security issues. (SLO 1, 2, & 6)
- Identify how to establish organization- wide security of information systems that align technical with business needs and goals. (SLO 1, 4, & 6)

CSIA 320 Ethical Hacking Credits: 5.0

This course provides students with the tools and resources they need to develop an understanding of Ethical Hacking. The student will be taken through an interactive environment where they will be shown how to scan, test, hack and secure information systems. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE) CS 232 and CSIA 300. CSIA 300 can be taken concurrently

COURSE OUTCOMES Understand the importance of and elements of information security in today's world. (SLO 1 & 6)

- Identify the phases of the hacking cycle and the different types of hacker attacks. (SLO 1 & 6)
- Summarize scanning methodology and perform different scanning techniques. (SLO 1, 4, & 6)

- Apply the various tools used in hacking. (SLO 1, 4, & 6)
- Perform penetration testing. (PT). (SLO 1, 4, & 6)

CSIA 330 Wireless Security   Credits: 5.0

This class provides students with the conceptual knowledge and hands-on skills needed to work with wireless technology. Topics include planning, designing, installing, and configuring wireless LANs with an emphasis on security. It also details common wireless LAN uses including maintenance, security, and business applications. It is designed to help students pass the Certified Wireless Network Administrator (CWNA) exam, as well as the new IEEE 802.11 standard. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE): CS 150 and 250 and CSIA 300. CSIA300 can be taken concurrently.

COURSE OUTCOMES:

Wireless Security is intended to develop *understanding and skills in wireless technologies and security* through the following outcomes:

- Describe the vulnerabilities faced by wireless communications, and how to reduce exposure. (SLO 1, 3, 4, & 6)
- Define the terms and concepts involved in wireless signal propagation. (SLO 1, 3, & 6)
- Compare and contrast the IEEE and ETSI standards. (SLO 1, 3, 4, & 6)
- Setup and configure a WLAN. (SLO 1 3 4, & 6)
- Know the wireless protocols and programming languages used in wireless devices and how they are used in different situations. (SLO 1, 4, & 6)
- Evaluate wireless devices that make up a typical wireless infrastructure. (SLO 1, 3, 4, & 6)
- Compare the security scenarios for a wired and wireless network. (SLO 1, 3, 4, & 6)
- Perform a penetration test on a wireless network using a variety of tools. (SLO 1, 4, & 6)
- Research and write papers on new technologies pertaining to this class. (SLO 1, 3, 4, & 6)

CSIA 410 Cryptography Credits: 5.0

This class will provide students with an operational understanding of basic cryptographic systems. Students will learn about symmetric cryptography, block ciphers and secure hash functions, asymmetric cryptography, key exchange and public-key systems, and authentication and encryption in an adversarial model. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE) CS 102 OR CS& 131 OR CS 141 and CS 228 OR CS 229

COURSE OUTCOMES

Cryptography is intended to develop Critical Thinking, Quantitative and Symbolic Reasoning, Effective Communication, Applying Information Tools and Resources, Developing Cultural Awareness and Mastering Program Learning Outcomes through the following outcomes:

- Demonstrate and apply the principles of cryptology and steganography. (SLO 2 & 6)
- Describe the evolution of cryptanalysis of historical ciphers. (SLO 1, 2, 3, & 5)
- Utilize Public Key certificates, by either applying for and using 3rd party certificates, or

administering a server to create and distribute and validate certificate. (SLO 4 & 6)
- Describe and apply the theory and practice of modern cryptographic systems and network protocols such as SSL for secure electronic communication. (SLO 4 & 6)
- Classify the social, ethical, and political issues surrounding cryptography and its use in communications, especially electronic communications. (SLO 1, 3, 5, & 6)

CSIA 420 Cyber Crimes and Terrorism   Credits: 5.0

The class begins with a broad introduction to the field of computer crime, discussing the history of computer crime, basic criminal techniques, and the relevant laws. It walks students through forensics, litigation, depositions, expert reports, trials, and how to select an appropriate expert witness. The class also covers specific techniques and tricks that hackers use and how to defend against such attacks. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE): CS 250 and CS 232 and CSIA 300 and CSIA 320.

COURSE OUTCOMES:

Cyber Crime and Terrorism is intended to develop *skills in understanding computer crimes and the laws and procedures to protect us* through the following outcomes:

- Describe the vulnerabilities faced by computer and network users, and how to reduce exposure. (SLO 1, 3, 4, & 6)
- Research the history of computer crime and computer laws in the United States. (SLO 1, 3, 4, & 6)
- Appraise and select proper techniques and tools for obtaining and securing data. (SLO 1, 3, 4, & 6)
- Identify experts in the field and verify their credentials. (SLO 1, 3, 4, & 6)
- Discuss the rules for being deposed. (SLO 1, 3, 4, &6)
- Describe the different types of civil matters relating to computer crime. (SLO 1, 3, & 6)
- Identify and assess the tactics used by online predators and the tools to keep children safe. (SLO 1, 3, 4, & 6)
- Discuss the impact of identity theft and rules for online safety. (SLO 1, 3, 6)
- Research online harassment and discuss federal laws regarding cyber stalking/threats. (SLO 1, 4, & 6)

CSIA 430 UNIX Administration and Security   Credits: 5.0

Students in this class will study UNIX/Linux system administration and security. System administration topics include installation, kernel configuration and customization, user administration, package management and backup, automating and scheduling tasks, filesystem management and maintenance, system initialization and services. Students will also learn how to assess security on UNIX/Linux systems, take appropriate actions to correct security deficiencies and prepare administrative reports. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE) CS 150, CS 223

COURSE OUTCOMES

UNIX Administration and Security is intended to develop Critical Thinking, Effective Communication, Applying Information Tools and Resources, Developing Cultural Awareness and Mastering Program Learning Outcomes through the following outcomes:

- Discuss concepts and capabilities of the Unix/Linux computing and network environment. (SLO 4 &6)
- Install and configure Linux servers. (SLO 4 & 6)
- Add and manage user accounts. (SLO4 & 6)
- Employ system administration tools to add, configure and manage applications and system resources; ensuring that both business requirements and security considerations are met. (SLO1, 4, & 6)
- Apply UNIX/Linux data security tools and techniques to secure system against local and network attacks and to monitor system for potential security threats. (SLO4 & 6)
- Produce and use well-documented system security assessment reports for clients. (SLO 3, 4, & 6)

CSIA 440 Cyber Testing and Penetration Credits: 5.0

This course covers a broad base of topics in advanced penetration testing and information security analysis. Students are exposed to techniques and tools to perform a thorough penetration test along with legal requirements, rules of engagement, how to plan and schedule a test, how to perform vulnerability analysis, external and internal penetration testing, and techniques to conduct an advanced penetration test. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE): CSIA 300, CSIA 320, and CSIA 330.

COURSE OUTCOMES:

Penetration testing is intended to develop *skills in procedures and methodologies of penetration testing* through the following outcomes:

- Explain fundamentals of penetration testing, techniques and process. (SLO 1, 3, 4, & 6)
- Discuss the professional duties and legal issues involved in penetration testing. (SLO 3, 4, & 6)
- Prepare and execute a test plan. (SLO 1,3,4,6)
- Utilize an array of tools for information gathering and social engineering penetration testing. (SLO 1, 4, & 6)
- Apply tools to test the security weaknesses and strengths of an organizations computer device. (SLO 1, 4, & 6)
- Describe the components of a penetration testing report and describe how to create the final report. (SLO 1, 3, 4, & 6)
- Discuss the actions that an organization should take following the completion of a penetration test. (SLO 1, 3, & 6)

- Explain the concept of simulating an attack by experienced hackers including techniques to conduct the testing. (SLO 1, 3, 4, & 6)

CSIA 450 Cyber Security Capstone Credits: 5.0

This course *integrates* all the various cyber security knowledge and skills learned in previous courses into a simulated project. Emphasis is placed on security policy, process planning, procedure definition, business continuity, and systems security architecture. Upon completion, students should be able to design and implement comprehensive information security architecture from the planning and design phase through implementation. PREREQUISITE OR ASSET/COMPASS SCORE (AS APPROPRIATE) CSIA 440 or concurrent enrollment

COURSE OUTCOMES

- Design and establish organization-wide security policies that align technical with business needs and goals of a system. (SLO 1, 4, & 6)
- Utilize tools to test the security weaknesses and strengths of your designed systems. (SLO 1, 4, & 6)
- Describe components of your system in a written final report and presentation. (SLO 1, 3, 4, & 6)

SOC 305 Cybercrime: A Sociological Perspective Credits: 5.0

Cybercrime is a deviant behavior involving the illegal use of computer technology and the internet against individuals, social groups, and institutions. This course will examine cybercrime and its various types (such as identity theft, bullying and cyber-terrorism), as a social problem in the US and the world. The goal of the course is to introduce students to the theories and methods used by sociologists to understand the different dimensions of cybercrime including their causes, costs and challenges to society, and possible solutions. Topics include: cyber-sociology, crime and deviance, types of cybercrime, challenges to social order, society's responses to cybercrime, and socio-economic and ethical consequences of cybercrime.

COURSE OUTCOMES

Cybercrime is intended to develop critical thinking, application of information tools and resources, and cultural awareness through the following outcomes:

- Develop cultural awareness by learning about cybercrime across cultures and its impact on various social groups and societies. (SLO 1, 4, 5, & 6)

- Formulate opinions on the various dimensions of cybercrime. (SLO 1, 4, 5, & 6)

- Research and analyze deviant behavior in cybercrime. (SLO 1, 4, 5, & 6)

- Acquire theoretical knowledge on the nature, causes, and consequences of cybercrime as they relate to particular situations and students' own life experiences. (SLO 2)

- Compare and contrast various theoretical and social perspectives used to explain cybercrime. (SLO 1, 4, 5, & 6)

- Discuss and analyze the impact the cybercriminals can create on cybercrime victims, society and economic, as well as predicting emerging and controversial cybercrime issues. (SLO 1, 4, 5, & 6)

POLS 305 Future of War Credits: 5.0

The Future of War is designed to introduce students to the use of force in contemporary international politics and to examine transformations in the purpose, conduct, and theory of war that appear to be unsettling the post-WWII arrangements. The course will cover the use of force in international politics by state and non-state actors, theories of strategy and war, the relation of war to technology and culture, and case studies that exemplify the issues of contemporary war and threats of conflict.

COURSE OUTCOMES

The Future of War is intended to develop critical thinking, application of information tools and resources, and cultural awareness through the following outcomes:

- Define the role of force in the international system of states and explain various theories purporting to explain its use by states and non-state actors. (SLO 1, 3, & 4)
- Define the various factors that influence the use of force, its effectiveness, and its legitimacy by examining both empirical evidence and philosophical arguments. (SLO 1, 2, 4, & 5)
- Formulate reasoned opinions on current political issues to exercise their rights as citizens to influence foreign policy and to complete assigned work at a level appropriate for university courses in the social sciences. (SLO 1, 3, & 4)

Appendix D: Faculty Experience

Melissa DeHaan, Associate Professor Computer Science Department

Education

- BA Washington State University Computer Science
- AA Columbia Basin College
- AAS Columbia Basin College Computer Science

Program Related Experience

- Teaches CS102 Programming Fundamentals, CS 150 Computer Security, CS 228 Windows Server, CS230 Active Directory, CS231 Network Infrastructure, CS232 Network Security, CS207 Word Implementation and CS208 Adv. Excel

- Certifications in Windows Server, Active Directory, and Security +

Tym O'Brien, Associate Professor Computer Science Department

Education

- Trained in mobile device programming
- Master of Education in Adult Education from Heritage University
- Bachelor of Science in Computer Science from Washington State University
- Bachelor of Education in Physics from Sirnakarinwirot University, Thailand

Program Related Experience

- **Associate Professor at Columbia Basin College**: Currently teach a series of C++, Java, C# courses, and mobile device programming courses for iOS and Android platforms. Served as Computer Science Department lead for two terms from the fall of 2001 to the fall of 2003 and the fall of 2012-current. Currently serve on the Curriculum Committee and Teaching and Learning Committee.

- **Computer Programmer at Lamb Weston, Richland, WA**: Worked as a programmer writing and maintaining in-house applications for various departments.

- **Cyber Security Courses Qualified to Teach –**CS117 Computer Ethics, CS150 Computer Security, CS200 Computer Forensics Fundamentals, CS223 UNIX/Linux, CS229 Webmaster, CS250 Networking Fundamentals

Tony Sako, Associate Professor Computer Science Department

Education

- B.S. University of Washington Numerical Analysis

- Additional Graduate level coursework in Computer Science

Program Related Experience

- **Associate Professor at Columbia Basin College**: 17 years teaching experience in programming, networking, UNIX/Linux Computer graphics and animation, and Internet Development. Currently teaches classes for the Internet Developer degree. Served as Computer Science Department lead from the fall of 1999 to the fall of 2003. Have worked as professional training instructor for Columbia Basin Advanced Technologies and Microsoft Summer Institute in PC Hardware, TCP/IP, Asp.Net and Web 2.0.

- **Senior Systems Analyst Boeing Computer Services and Lockheed Martin Hanford**: 13 years experience in various aspects of computer and network programming and support.

- **Owner Internet Associates Consulting Group:** Web site development on a consulting basis.

Debbie Wolf, Associate Professor Computer Science Department

Education

- BA   Washington State University Management Information Systems
- AAS Degree Columbia Basin College Computer Science

Certifications

- EC-Council Certified Ethical Hacker
- Novell CNE

Program Related Experience

- Associate Professor at Columbia Basin College: 15 years teaching experience in programming, networking, SharePoint, database design and administration. Currently teaches classes for the Databases Administration degree. Served as Computer Science Lead for 4 years.
- Recognized by teaching peers for the CBC 2013 National Institute for Staff and Organizational Development Award.

Appendix E: Content Expert Evaluations

Columbia Basin College
Program Proposal
Bachelor of Applied Science: Cyber Security
Review by Vicki Wilson

Criteria 1. Curriculum Demonstrates Baccalaureate Level Rigor

CRITERIA	STANDARD
8. Curriculum demonstrates baccalaureate level rigor.	Describe curriculum including: (1) program learning outcomes; (2) program evaluation criteria and process; (3) course preparation needed by students transferring with a technical associate degree; (4) general education components; and (5) course work needed at junior and senior levels in the BAS.

I believe CBC has captured the correct curriculum for a higher understanding of the world of cyber security. It will be very important to make sure employer/corporate feedback is gathered for recommendations to keep current in the applied practice of cyber security. It is stated that a thorough review of the Cyber Security program will be conducted every 5 years. If at all possible, I would recommend at least an every 3 year review. I would like to understand where the study of evaluating, analyzing and auditing of the ever- changing cyber security policies, regulations and requirements from a government and corporate America perspective will be taught.

Response:
The five year review process corresponds to the college accreditation schedule. Ongoing assessments are done throughout the academic year. If it becomes evident a shorter review period is needed, it will be implemented at that time.

The study of evaluating, analyzing and auditing of cyber security policies, regulations and requirements from a government and corporate America perspective will be covered in the CSIA 450 Capstone class.

Course Description: This course integrates all the various cyber security knowledge and skills learned in previous courses into a simulated project. Emphasis is placed on security policy, process planning, procedure definition, business continuity, and systems security architecture. Upon completion, students should be able to design and implement comprehensive information security architecture from the planning and design phase through implementation.

The instructors work closely with the advisory committee members from government and private industry to assure current policies and requirements for both sectors will be included in the course.

Criteria 2. Qualified Faculty

CRITERIA	STANDARD
9. Qualified faculty.	Provide a profile, including education credentials, of anticipated faculty (full-time, part-time, regular, continuing) that will support the program for each year (junior and senior). Include faculty needed to cover the technical course work, general education courses and electives. In addition, provide the total faculty FTE allocated to the program. Faculty and administrators responsible for technical courses must meet certification requirements for professional and technical administrators and instructors in the Washington Administrative Code.

As Lockheed Martin is an employer of many CBC graduates, I know first-hand of the quality of many CBC faculty who will be supporting the BAS – Cyber Security. The employees who have received education from the CBC Computer Science programs have a thorough understanding of their areas with outstanding mentoring and counseling. I would encourage CBC faculty to take advantage of and seek out mentoring and shadowing opportunities with companies to gain practical and real life experience in cyber security. This is a very important element given the fast-paced ever changing IT environment and the even faster changing world of cyber security.

Criteria 3. Admissions Process

CRITERIA	STANDARD
10. Selective admissions process, if used for the program, consistent with an open door institution.	• Describe the selection and admission process. Explain efforts that will be used to assure that the program serves as diverse a population as possible.

CBC's selection and admission process seems very well thought out and reasonable. One element perhaps to consider would be to have candidates evaluated by outside sources, rather than the all CBC based selection committee. I would like to understand how CBC would modify the application and selection procedures as needed, if problems are found as stated in the following statement: "CBC monitors the representation of minorities within the current BAS in Applied Management and all lower division programs on a regular basis and will extend that effort to all new BAS programs. **CBC will modify application and selection procedures, as needed, if problems are found."**

Response:

Having very competitive programs such as nursing and dental hygiene, CBC has a lot of experience working with programs to select a diverse population. A wide variety of educational professionals from CBC serve on the committees.

CBC will continue to employ successful methods to attract a diverse student body for all of its programs. Outreach efforts concentrate on attracting a diverse student population.

I would also like clarification on Table 10 and the reasoning behind the figure of 18 graduates in Yr. 5 of the program. This is a drop from Yr. 4.

Response:

This was a typographical error. The total for year five should be 20.

Criteria 4. Appropriate Student Services Plan

CRITERIA	STANDARD
11. Appropriate student services plan.	Describe services that will be needed by the students admitted to the degree program and the college plan for providing those services. Include a description of financial aid services and academic advising for students admitted into the program.

Students' services for the BAS-C appear more than adequate and will service the students of the program very well. The Cyber Security Advisory committee is discussed in the Placement section and doesn't seem to appear anywhere else. What is this committee's charter and who makes up this committee?

Response:

Advisory committees are organized to provide advice and assistance to the instructors and administrators of specific programs. The primary purpose for advisory committees is to promote greater cooperation between the educational environment and the private sector in preparing individuals for employment, promoting quality professional-technical education, and making the educational delivery system more responsive to the labor market.

The Computer Science Advisory Committee is made of a number of employees from various private sectors such as MEIER Enterprises Inc., Cayuse Technologies, HAPO Credit Union, Washington State University, Lockheed Martin, PNNL, Tilite, Senske, GESA Credit Union, Bechtel, and Play Plus Benefits. In addition, Computer Science faculty members, CBC administrators and counselors serve on the committee.

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

CRITERIA	STANDARD
12. Commitment to build and sustain a high quality program.	Provide a financial plan for the first five years of program operation. This plan should include (1) types of funds to be used to support the program; (2) projected program expenses; (3) appropriate facilities to be used; (4) equipment, technology, and instructional resources needed for the program.
	Document the college's ability to sustain the program over time.

CBC's commitment to this program is very sound and along with the communities' involvement with the College this program should easily be sustained over time. One question – when will the replacement of one of the four computer labs be accomplished?

Response:

The replacement of the computer lab will be completed August 2013 prior to the start of the new school year. CBC has a rotating schedule to replacement computers in labs on a regular basis approximately every three years. The "high end" courses use the newest computer labs and less demanding software courses use the older computers.

With the high demand of cyber security across any company, anywhere in the world, I believe the Bachelors of Applied Science – Cyber Security will be in much demand.

Criteria 6. Program Specific Accreditation

CRITERIA	STANDARD
13. Program specific accreditation.	Indicate whether the institution will seek specialized program accreditation. If so, describe plans for accreditation and identify appropriate accrediting body.

CBC's commitment to the pursuit of accreditation is a very sound strategic accomplishment and solidifies the commitment of this program.

Criteria 7. Educational Pathways Beyond the BAS Degree

CRITERIA	STANDARD
14. Pathway options beyond baccalaureate degree.	Describe opportunities and articulation agreements for the place-bound BAS graduates to continue their education onto a graduate (Master's) degree program.

CBC has cited numerous pathways for BAS graduates to pursue graduate degrees and seem committed to helping with those choosing that path. The future in cyber security will demand higher levels of education.

Criteria 8. Expert Evaluation of Program

CRITERIA	STANDARD
9. External expert evaluation of program.	The institution will select two external experts to review the program. In a separate document, provide copies of external evaluators' reports or letters. Summarize the institution's responses and subsequent modifications to the proposal based upon evaluator's recommendations. Attach a short bio of the evaluators.

I believe Columbia Basin College is strongly positioned to successfully implement and sustain a Bachelor of Applied Science degree in Cyber Security. I would highly recommend CBC be granted this program. Cyber security experts and employees are in high demand and this program will help to fulfill this need in Eastern Washington, as well as across the county.

========================

Vicki Wilson is the manager of Support Services in the Service Operations organization for Lockheed Martin Information Technology. Her career at the Hanford site in Richland, WA for more than 28 years has included many different areas of IT services and support.

Vicki is a native of the Tri-Cities. She is a graduate of Pasco High School and Columbia Basin College. She earned her BA from Eastern Washington University in Decision Science. Vicki is also on the Board of Trustees for Eastern Washington University.

Columbia Basin College
Program Proposal
Bachelor of Applied Science: Cyber Security
Review by Greg A. Serene

Comments:

Page 8

Computer science students who graduate with a BAS degree in Cyber Security will also be able to:
- *Protect an organization's critical information systems and assets by integrating cyber security risk management and business continuity best practices throughout an enterprise.*
- *Implement continuous network monitoring and provide real-time security solutions.*
- *Analyze advanced persistent threats and deploy countermeasures and conduct risk and vulnerability assessments of planned and installed information systems.*
- *Formulate, update, and communicate short- and long-term organizational cyber security strategies and policies.*

I thought about this list for a while. What our country most needs right now is deep technical skills, but I think a BAS needs to develop more than just technical skills, however important. This list seems to strike a good balance.

Page 53 CSIA 310 E-Commerce Security

The course title is specific but the content description and outcomes are quite general. At a minimum you need to discuss PCI DSS, but issues like authentication, confidentiality, and availability are also big in E-Commerce.

Response:

The course instructor will make sure to include the suggested topics. If necessary, a course description change will be submitted to the CBC curriculum committee for approval.

Page 54 CSIA 320 Ethical Hacking

The relationship between CSIA 320 and CSIA 440 isn't clear to me. Penetration testing and ethical hacking are often treated as synonyms. You seem to be doing so; is 440 a continuation of 320? Or are you covering other topics like fuzzing and reverse engineering in 320?

Response:

CSIA 440 is a continuation of CSIA 320.

Overall I like CBC's vision for the BAS-C degree. There is a balance between general education and the specific course of study. This is important; the ability to find security flaws is good, for example, but if you can't effectively describe the flaws and persuade management that they must be fixed then you won't be an effective security professional. I also like the emphasis on programming and on systems administration. The more a security tester knows about the systems and applications being tested, the more effective he or she will be at finding vulnerabilities. Specialties like incident detection and forensics also require a very detailed understanding of how specific systems (e.g. Windows, Linux) and applications function.

Great job!

Gregg