College of Engineering
Proposed Catalog Changes
Effective Summer 2021

PROPOSAL TO CREATE A NEW B.S. IN CYBERSECURITY

1. Create the following **B.S. in Cybersecurity**:

Cybersecurity (B.S.)

Required course work includes the university requirements (see regulation J-3) and:

COMM 101	Fundamentals of Public Speaking	2
CYB 110	Cybersecurity and Privacy	3
CYB 210	Cybersecurity Architectures and Management	3
CYB 220	Secure Coding and Analysis	3
CYB 310	Cybersecurity Technical Foundations	3
CYB 330	Networking and Control Systems	3
CYB 340	Network Defense	3
CYB 350	Operating System Defense	3
CYB 380	Cybersecurity Lab I	3
CYB 381	Cybersecurity Lab II	3
CYB 401	Cybersecurity as a Profession	1
CYB 420	Computer and Network Forensics	3
CYB 440	Software Vulnerability Analysis	3
CYB 480	Cybersecurity Senior Capstone Design I	3
CYB 481	Cybersecurity Senior Capstone Design II	3
CS 112	Computational Thinking	3
CS 120	Computer Science I	4
CS 121	Computer Science II	3
CS 150	Computer Organization and Architecture	3
CS 240	Operating Systems	3
CS 270	System Software	3
CS 383	Software Engineering	3
ENGL 317	Technical Writing	3
MATH 160	Survey of Calculus	4
or MATH 170	Calculus I	
PHIL 103	Ethics	3
STAT 251	Statistical Methods	3
or STAT 301	Probability and Statistics	

Total Hours 77

Courses to total 120 credits for this degree

Rationale: We have had regular enrollments in our cyber security courses over the past several years, from current computer science students. Most have indicated an interest in focusing their studies in cybersecurity, but are not able to, due to the demands of the current computer science undergraduate degree program.

Studies have shown that there is a major unmet need for cybersecurity professionals. These professionals help businesses protect their assets from cyber criminals. Untrained individuals spend more time and effort, and therefore more corporate resources, developing less than ideal solutions. A trained cybersecurity professional will be able to get the work done with less effort and less resources. Furthermore, our economy and critical infrastructures are today very dependent on digital and computer-based systems. Adequately protecting such systems is of paramount and essential importance, and a likely a prerequisite, for a healthy economy in the State of Idaho and the Nation.

There is a great need for cybersecurity expertise across all businesses and government sectors. Whether it be in the area of e-commerce, web applications, mobile apps, business, military, health, agriculture, critical infrastructures, or processing big-data, there is a need to protect information systems and individual privacy, and to ensure the integrity of our systems. A look at the news every week brings about reports of cybersecurity breaches and loss of private information, financial loss, or the potential for disruption of critical infrastructure.

Cybersecurity experts agree that many of these problems could be fixed if a wider portion of the workforce was aware of best-practice cybersecurity technologies and processes. At the same time, these experts agree that we need to constantly improve these technologies and processes given the advances made by cyber criminals and the constant deployment of new connected technologies which introduce new attack surfaces and vulnerabilities.

Cybersecurity has becoming an increasingly important part of day-to-day life, government and business. It is no longer just the province of the government and banking but touches more and more aspects of our lives.

Our past research and teaching activities have had national and international impact but have primarily focused on technical aspects of cybersecurity. Branching out our core cybersecurity expertise from a subset of computer science to a full, independent degree program will enable us to expand our students' understanding of cybersecurity not only from the technical point of view, but also include societal and business aspects of cyber security. These include issues such as privacy, ethical hacking, and business continuity planning. The full breadth of this education will provide our students with a richer education and make them better able to serve their communities as the needs of cybersecurity continue to grow and expand.

UCC-20-046

Institutional Tracking No. _____

Idaho State Board of Education

Proposal for **Undergraduate/Graduate Degree** Program

Date of Proposal Submission:	October 2019
Institution Submitting Proposal:	University of Idaho
Name of College, School, or Division:	College of Engineering
Name of Department(s) or Area(s):	Computer Science

Program Identification for Proposed New or Modified Program:

Program Title:	Cybersecurity					
Degree:	BS	Degree Designation	X	Undergraduate		Graduate
Indicate if Online Program:		No	X	No		
CIP code (consult IR /Registrar):	**11.1003 COMPUTER AND INFO. SYSTEMS SECURITY/INFORMATION ASSURANCE.**					
`Proposed Starting Date:	Summer 2021					
Geographical Delivery:	Location(s)	Moscow	Region(s)			
Indicate (X) if the program is/has:		Self-Support		Professional Fee		Online Program Fee
Indicate (X) if the program is:	X	Regional Responsibility		Statewide Responsibility		

Indicate whether this request is either of the following:

	New Graduate Certificate (30 credits or more)		Expansion of Existing Program
	New Undergraduate Certificate (30+ cr.)		Consolidation of Existing Program
	New Graduate Program		New Off-Campus Instructional Program
X	New Undergraduate Program		Other _____

Approval Signatures:

College Dean (Institution)	Date	Vice President for Research	Date
Graduate Dean or other official	Date	Academic Affairs Program Manager, OSBE	Date
FVP/Chief Fiscal Officer (Institution)	Date	Chief Academic Officer, OSBE	Date
Provost/VP for Instruction (Institution)	Date	Chief Financial Officer, OSBE	Date
President	Date	SBOE/Executive Director Approval	Date

Before completing this form, refer to Board Policy Section III.G., Postsecondary Program Approval and Discontinuance. This proposal form must be completed for the creation of each new program. All questions must be answered.

Rationale for Creation or Modification of the Program

1. **Describe the request and give an overview of the changes that will result.** *Will this program be related or tied to other programs on campus? Identify any existing program that this program will replace.*

   Since 1991, the Department of Computer Science has offered a variety of Cyber Security courses as technical electives in our undergraduate degree program. In 1999 the University of Idaho was designated a National Center of Academic Excellence (CAE) in Information Assurance Education by the National Security Agency (at the time, Information Assurance was the US Government term for Cybersecurity). We were one of the first seven universities in the nation to receive this designation, and we have maintained it every renewal cycle.

   In the past few years, the CAE certification process has become more proscriptive, requiring more precise course content, and a dedicated degree path forward for Cybersecurity students. ABET (the Engineering accreditation board) now accredits cybersecurity degree programs. Also, the US Government has adopted the NIST Cybersecurity Workforce Framework – a catalog of job duties along with knowledge, skills and abilities for those jobs, for a wide range of cybersecurity careers.

   This growth of standardized program content, along with the tremendous growth in job opportunities for our graduates, has led to the conclusion that we need to establish a dedicated degree path. This degree will be focused on the technical side of cybersecurity, building on the same introductory foundations as computer science but will significantly diverge in the upper-division course requirements. In addition, we are proposing to add introductory courses to cover, in addition to introductory technical knowledge earlier in a student's academic program, several non-technical aspects of cybersecurity, including: planning, contingency and risk management, privacy, ethics, and laws and regulations and human factors.

2. **Need for the Program**. *Describe the student, regional, and statewide needs that will be addressed by this proposal and address the ways in which the proposed program will meet those needs.*

   a) **Workforce need:** *Provide verification of state workforce needs that will be met by this program. Include State and National Department of Labor research on employment potential. Using the chart below, indicate the total projected annual job openings (including growth and replacement demands in your regional area, the state, and nation. Job openings should represent positions which require graduation from a program such as the one proposed. Data should be derived from a source that can be validated and must be no more than two years old.*

      List the job titles for which this degree is relevant.

      The following are US Department of Labor (DOL) Occupation Titles requiring cybersecurity skills:

      1. *Information Security Analysts* – This is the DOL Job title for the following specialized

cybersecurity work roles:

a. System Security Analyst
b. Cyber Defense Analyst
c. Cyber Defense Infrastructure Support Specialist
d. Vulnerability Assessment Analyst
e. Cyber Defense Forensics Analyst

2. *Network Operations Specialist*
3. *Software Developer*
4. *System Administrator*
5. *Technical Support Specialist*

	State DOL data	Federal DOL data	Other data source: (describe)
Local (Service Area)			EMSI Study (see below).
State		520 in 2016 + 150 by 2026	http://www.projectionscentral.com/Projections/LongTerm
Nation		100,000 in 2016 +28,500 by 2026	

Provide (as appropriate) additional narrative as to the workforce needs that will be met by the proposed program.

Our Emsi analysis predicts a 30.4% increase in jobs (510 jobs) in Idaho through 2029 and a 27.8% increase nationally. In our 16-county region, job growth is expected to increase 26.0% (134 jobs) through 2029.

b) Student need. What is the most likely source of students who will be expected to enroll (full-time, part-time, outreach, etc.). Document student demand by providing information you have about student interest in the proposed program from inside and outside the institution. If a survey of s was used, please attach a copy of the survey instrument with a summary of results as **Appendix A.**

We have had regular enrollments in our cyber security courses over the past several years, from current computer science students. Most have indicated an interest in focusing their studies in cybersecurity, but are not able to, due to the demands of the current computer science undergraduate degree program.

Table 1: Past enrollments in the CS courses that have cybersecurity as the focus (undergraduate/ graduate). These courses will become part of the core of the new cybersecurity program.

Course	AY 16-17	AY 17-18	AY 18-19	Fall 2019
CS 336 (Intro course)	19	24	14	24
CS 439 (Applied Security)	10/4	9/10		2/2
CS 437 (Computer Forensics)	1/21		5/32	
CS 438 Network Security		5/10	8/16	
Security Special Topics			0/11	

In addition to internal demand, we expect to see increases in new student enrollment due to the

strong growth of cybersecurity jobs in the region, state, and nationally.

c) Economic Need: *Describe how the proposed program will act to stimulate the state economy by advancing the field, providing research results, etc.*

Studies have shown that there is a major unmet need for cybersecurity professionals. These professionals help businesses protect their assets from cyber criminals. Untrained individuals spend more time and effort, and therefore more corporate resources, developing less than ideal solutions. A trained cybersecurity professional will be able to get the work done with less effort and less resources. Furthermore, our economy and critical infrastructures are today very dependent on digital and computer-based systems. Adequately protecting such systems is of paramount and essential importance, and a likely a prerequisite, for a healthy economy in the Sate of Idaho and the Nation.

d) Societal Need: *Describe additional societal benefits and cultural benefits of the program.*

There is a great need for cybersecurity expertise across all businesses and government sectors. Whether it be in the area of e-commerce, web applications, mobile apps, business, military, health, agriculture, critical infrastructures, or processing big-data, there is a need to protect information systems and individual privacy, and to ensure the integrity of our systems. A look at the news every week brings about reports of cybersecurity breaches and loss of private information, financial loss, or the potential for disruption of critical infrastructure.

Cybersecurity experts agree that many of these problems could be fixed if a wider portion of the workforce was aware of best-practice cybersecurity technologies and processes. At the same time, these experts agree that we need to constantly improve these technologies and processes given the advances made by cyber criminals and the constant deployment of new connected technologies which introduce new attack surfaces and vulnerabilities.

e) If Associate's degree, transferability:

3. Similar Programs. *Identify similar programs offered within Idaho and in the region by other in-state or bordering state colleges/universities.*

The proposed *Bachelor of Science in Cybersecurity* degree was designed from the ground-up to be exceedingly compliant with the criteria, knowledge, and skills detailed in the Center of Academic Excellence in Cyber-Defense (CAE-CD) denomination by the U.S. National Security Agency and the U.S. Department of Homeland Security.

Source: (https://www.iad.gov/NIETP/documents/Requirements/CAE_CDE_criteria.pdf)

Under the Center of Academic Excellence in Cyber-Defense criteria, institutions offering compliant cybersecurity-focused 2-year degrees are denominated as CAE-2Y, and institutions offering compliant Bachelor-level or Graduate-level cybersecurity-focused degrees are denominated CAE-CD (these can be minors, certifications, or emphasis options within a degree). The table below shows the number of CAE-CD and CAE-2Y denominated institutions in Idaho and its neighboring states of Montana, Nevada, Oregon, Utah, and Washington. The state of Wyoming appears to have no CAE-CD nor CAE-2Y denominated educational institutions.

Source: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm (2019-09-09)

Count of Education Institutions with CAE Designation Per State				
State	**CAE-2Y**	**CAE-CD**	**CAE-R**	**Total**
Idaho	1	2		3
Montana	2			2
Nevada	1	1		2
Oregon	2			2
Utah		2		2
Washington	5	2	1	8
Total	**11**	**7**	**1**	**19**

Idaho Public Institutions: Four-year and Graduate:

There are currently two Center of Academic Excellence in Cyber-Defense (CAE-CD) denominated institutions in Idaho: The *University of Idaho* and *Idaho State University*. Source: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

The following table lists programs that we believe to be similar and are being offered by public colleges or universities in Idaho. In this case our definition of similar is that the program is:

a) Offered by an institution also denominated as a Center of Academic Excellence in Cyber-Defense (CAE-CD) and
b) The degree is a Bachelor of Science degree with significant coverage of Cybersecurity knowledge and skills.

Under such definition, and to the best of our knowledge, there are no programs, significantly similar to the degree being proposed, currently being offered at other public educational institutions in Idaho. There are however two offerings for Bachelor of Science in Computer Science degrees with Cybersecurity Emphasis degree options: *University of Idaho* and *Boise State University*.

Similar Programs offered by Idaho public institutions (list the proposed program as well)		
Institution Name	**Degree name and Level**	**Program Name and brief description if warranted**
University of Idaho	**B.S. in Cybersecurity (Being proposed)**	**Bachelor of Science in Cybersecurity. The program being proposed in this form.**
University of Idaho	**B.S. in Computer Science.**	**Bachelor of Science in Computer Science plus Cybersecurity Academic Certificate (https://catalog.uidaho.edu/colleges-related-units/engineering/computer-science/cybersecurity-undergraduate-academic-certificate/).**
Boise State University	**B.S. in Computer Science.**	**Bachelor of Science in Computer Science with Cybersecurity Emphasis (https://majors.boisestate.edu/computer-science).**

University of Idaho:

Related degrees and certificates offered by the University of Idaho are listed below.

- Bachelor of Science in Computer Science.
- Master of Science in Computer Science.
- Doctor of Philosophy in Computer Science.
- Undergraduate Academic Certificate in Cybersecurity.
- Graduate Academic Certificate in Secure and Dependable Systems.
- Sources: https://www.uidaho.edu/degree-finder/a-z-index
  https://www.uidaho.edu/academics/dee/programs-courses/certificates

The University of Idaho offers a *Bachelor of Science in Computer Science* degree and a recently approved *Undergraduate Certificate in Cybersecurity*. Students that complete the B.S. in Computer Science degree plus the UG Certificate in Cybersecurity have gained a set of knowledge and skills satisfactorily compliant with the CAE-CD knowledge and skills criteria. Based on such degree and emphasis area, the University of Idaho is currently denominated a CAE-CD until 2021. It is important to note that such denomination was evaluated under the previous and less comprehensive knowledge and skills CAE-CD criteria. Other related degrees at the University of Idaho are graduate level degrees and certificates.

Furthermore, the focus of the proposed B.S. in Cybersecurity degree and the expected positions that graduates will fulfill are different than the focus of the B.S. in Computer Science degree. The field of Cybersecurity has advanced significantly in the last few years and though some of the knowledge and skills covered in a B.S. in Computer Science degree overlap with knowledge and skills to be gained with the proposed B.S. in Cybersecurity degree, there is a still a significant difference in the knowledge and skills expected from graduates that will fulfill positions in the Cybersecurity discipline. These differences are such today that we strongly believe they grant the design and offering of a new degree focused on providing such new set of knowledge and skills with breadth and depth of content in Cybersecurity. One event that crystalized such differences in the knowledge and skills needed for successful practice in Cybersecurity positions is the recent addition by the ABET accreditation board of a new criteria for *Cybersecurity* degrees. ABET is a non-profit international organization that accredits Computer Science, Information Systems, Information Technology, and other Computing-related degrees. Ref: https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2019-2020/. All Bachelor of Science degrees offered by the University of Idaho College of Engineering are ABET accredited.

Boise State University:

To the best of our knowledge the degrees and certificates listed below may offer coverage of Cybersecurity-related knowledge and skills within some of the required and elective courses and with varying degrees of coverage.

- Bachelor of Science in Computer Science.
- *Bachelor of Science in Computer Science with Cybersecurity Emphasis.*
- Bachelor of Science in Computer Science with Secondary Education Emphasis.
- Master of Science in Computer Science.
- Doctor of Philosophy in Computer
- Graduate Certificate in Computer Science.
- Minor in Computer Science.
- Minor in Cybersecurity.
- Minor in Computational Science and Engineering.

- Bachelor of Science in Information Technology Management.
- Sources: https://majors.boisestate.edu/computer-science
  https://majors.boisestate.edu/information-technology-management
  https://coen.boisestate.edu/cs/undergraduates/minor-cybersecurity

Similarly, to the case of the B.S. in Computer Science at the University of Idaho with a cybersecurity emphasis Boise State University offers a *Bachelor of Science in Computer Science degree with Cybersecurity Emphasis*. However, as stated before, an emphasis may cover knowledge and skills in Cybersecurity but maybe not necessarily with the breadth and depth of the B.S. in Cybersecurity proposed in this form.

Lewis-Clark State College:

To the best of our knowledge the degrees listed below may offer some coverage of Cybersecurity-related knowledge and skills within some courses. However, we believe that none of the degrees listed below would qualify as significantly similar under the applied criterion to the degree proposed in this form.

- Bachelor of Science (Arts) in Computer Science.
- Bachelor of Applied Science in Information Technology.
- Bachelor of Applied Science in Web Design and Development.
- Source: http://www.lcsc.edu/degrees/

Idaho State University:

The three degrees offered by ISU that we believe may include significant Cybersecurity knowledge and skills are listed below (first, second, and third). Other degrees that may offer partial coverage of Cybersecurity topics are also listed. Idaho State University is a Center of Academic Excellence in Cyber-Defense (CAE-CD) denominated institution. Given this information, it appears that the degrees offered at ISU that include significant coverage of Cybersecurity content, knowledge, and skills appear to be either Bachelor of Business Administration or Associate of Applied Science degrees and not a Bachelor of Science degree as the one proposed in this form.

- Bachelor of Business Administration in Business Informatics.
- Associate of Applied Science in Information Technology Systems.
- Associate of Applied Science in Industrial Cybersecurity Engineering Technology.
- Master of Science in Computer Science: Data Analysis Emphasis.
- Master of Science in Computer Science: Science Emphasis.
- Intermediate Technical Certificate on Industrial Cybersecurity Engineering Technology.
- Sources: http://coursecat.isu.edu/undergraduate/programs/
  http://coursecat.isu.edu/graduate/programs/
  https://www.isu.edu/cyberphysicalsecurity/

Idaho Public Institutions: Two-year:

The degree proposed in this form is a Bachelor of Science degree. Hence, we are not considering 2-year Associate programs as significantly similar to the degree proposed in this form even if such degrees may appear to have partial knowledge and skills overlap. In addition, there is currently only one two-year Center of Academic Excellence in Cyber-Defense (CAE-2Y) denominated institution in Idaho: *North Idaho College*.
Source: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

College of Eastern Idaho:
2-year institution and not CAE-2Y denominated.
College of Southern Idaho:
2-year institution and not CAE-2Y denominated.
College of Western Idaho:
2-year institution and not CAE-2Y denominated.

North Idaho College:

NIC is denominated as a Center of Academic Excellence in Cyber-Defense for two-year programs (CAE-2Y). To the best of our knowledge the degrees and certificates that we believe may be offered under such denomination are listed below. We believe that none of the degrees listed below would qualify as similar under the applied criterion. Several of the courses in Computer Information Technology (CITE) at NIC do cover topics required by the CAE denomination. However, the degrees offered at NIC are applied two-year Associate degrees.

- Associate of Applied Science in Computer Information Technology.
- Associate of Applied Science in Network Security Administration.
- Basic Technical Certificate in Cybersecurity and Networking.
- Source: https://www.nic.edu/programs/

Similar Programs offered by other Idaho institutions and by institutions in nearby states		
Institution Name	**Degree name and Level**	**Program Name and brief description if warranted**
Brigham Young University (Provo, Utah):	Bachelor of Science in Cybersecurity.	Bachelor of Science in Cybersecurity (https://catalog.byu.edu/engineering/school-of-technology/cybersecurity-bs).
City University of Seattle (Seattle, Washington).	Bachelor of Science in Cybersecurity and Information Assurance	Bachelor of Science in Cybersecurity and Information Assurance (https://www.cityu.edu/programs-overview/bachelor-of-science-cybersecurity-and-information-assurance/).
University of Washington (Seattle, Washington).	Bachelor of Science in Informatics.	Bachelor of Science in Informatics with Emphasis in Information Assurance and Cybersecurity (http://www.washington.edu/students/gencat/academic/school_information.html).
University of Washington, Bothell (Bothell, Washington).	M.S. in Cybersecurity Engineering.	M.S. in Cybersecurity Engineering: (https://www.uwb.edu/cybersecurity)

Southern Utah University, (Cedar City, Utah).	Bachelor of Science in Information Systems.	Bachelor of Science in Information Systems: Cybersecurity Emphasis (https://catalog.suu.edu/preview_program.php?catoid=21&poid=7816)

4. **Justification for Duplication with another institution listed above.** (if applicable). *If the proposed program is similar to another program offered by an Idaho public institution, provide a rationale as to why any resulting duplication is a net benefit to the state and its citizens. Describe why it is not feasible for existing programs at other institutions to fulfill the need for the proposed program.*

   There is no similar Bachelor of Science in Cybersecurity program in Idaho.

5. **Describe how this request supports the institution's vision and/or strategic plan.**

   The University Vision: "The University of Idaho will expand the institution's intellectual and economic impact and make higher education relevant and accessible to qualified students of all backgrounds."

   Our strategic plan focuses on an *Engaged Learning Community* supported by *Scholarly and Creative Activity with National and International Impact*.

   Cybersecurity has becoming an increasingly important part of day-to-day life, government and business. It is no longer just the province of the government and banking but touches more and more aspects of our lives.

   Our past research and teaching activities have had national and international impact but have primarily focused on technical aspects of cybersecurity. Branching out our core cybersecurity expertise from a subset of computer science to a full, independent degree program will enable us to expand our students' understanding of cybersecurity not only from the technical point of view, but also include societal and business aspects of cyber security. These include issues such as privacy, ethical hacking, and business continuity planning. The full breadth of this education will provide our students with a richer education and make them better able to serve their communities as the needs of cybersecurity continue to grow and expand.

6. **Assurance of Quality.** *Describe how the institution will ensure the quality of the program. Describe the institutional process of program review. Where appropriate, describe applicable specialized accreditation and explain why you do or do not plan to seek accreditation.*

   The Department of Computer Science and the College of Engineering will conduct annual internal assessment of the program, reviewing attainment of student outcomes for each course as well as program outcomes. We will use the process we use for continual assessment and improvement as recommended by national accreditation organizations.

   The University of Idaho plans to continue certification as a Center of Academic Excellence in Information Assurance Education (in the area of Cyber Defense) through the NSA/DHS sponsored CAE program.

   After an appropriate number of years, we plan to apply for ABET accreditation of the program, meeting the national standards put in place by ABET.

7. **In accordance with Board Policy III.G., an external peer review is required for any new doctoral program.** Attach the peer review report as **Appendix B**.

   Not applicable.

8. **Teacher Education/Certification Programs** All Educator Preparation programs that lead to certification require review and recommendation from the Professional Standards Commission (PSC) and approval from the Board.

   Will this program lead to certification?
   Yes_____ No___X__

   If yes, on what date was the Program Approval for Certification Request submitted to the Professional Standards Commission?

9. **Five-Year Plan: Is the proposed program on your institution's approved 5-year plan? Indicate below.**

   Yes X No _____

   Proposed programs submitted to SBOE that are not on the five-year plan must respond to the following questions and meet at least one criterion listed below.

   a. **Describe why the proposed program is not on the institution's five year plan.** When did consideration of and planning for the new program begin?

      Not applicable.

   b. **Describe the immediacy of need for the program**. What would be lost were the institution to delay the proposal for implementation of the new program until it fits within the five-year planning cycle? What would be gained by an early consideration?

      Not applicable.

   Criteria. As appropriate, discuss the following:

   - **i.** How important is the program in meeting your institution's regional or statewide program responsibilities? Describe whether the proposed program is in response to a specific industry need or workforce opportunity.
   - **ii.** Explain if the proposed program is reliant on external funding (grants, donations) with a deadline for acceptance of funding.
   - **iii.** Is there a contractual obligation or partnership opportunity to justify the program?
   - **iv.** Is the program request or program change in response to accreditation requirements or recommendations?
   - **v.** Is the program request or program change in response to recent changes to teacher certification/endorsement requirements?

Curriculum, Intended Learning Outcomes, and Assessment Plan

10. Curriculum for the proposed program and its delivery.

a. Summary of requirements. Provide a summary of program requirements using the following table.

Credit hours in required courses offered by the department (s) offering the program.	62
Credit hours in required courses offered by other departments:	15
Credit hours in institutional general education curriculum	23-24
Credit hours in free electives	19-20
Total credit hours required for degree program:	120

b. Curriculum. *Provide the curriculum for the program, including a listing of course titles and credits in each.*

Required Cybersecurity Courses (40 Credits)

CYB 110 (3cr)	Cybersecurity and Privacy
CYB 210 (3cr)	Cybersecurity Management
CYB 220 (3cr)	Secure Coding and Analysis
CYB 310 (3cr)	Intermediate Cybersecurity
CYB 330 (3cr)	Networking Fundamentals
CYB 340 (3cr)	Network Defense
CYB 350 (3cr)	Operating System Defense
CYB 380 (3cr)	Cybersecurity Practicum I
CYB 381 (3cr)	Cybersecurity Practicum II
CYB 401 (1cr)	Cybersecurity Professional Development
CYB 420 (3cr)	Computer and Network Forensics
CYB 440 (3cr)	Software Vulnerability Analysis
CYB 480 (3cr)	Senior Capstone Design I
CYB 481 (3cr)	Senior Capstone Design II

Required Computer Science Courses (22 cr)

CS 112 (3cr)	Computational Thinking
CS 120 (4cr)	Computer Science I
CS 121 (3cr)	Computer Science II
CS 150 (3cr)	Computer Organization and Architecture
CS 240 (3cr)	Operating Systems
CS 270 (3cr)	System Software
CS 383 (3cr)	Software Engineering

Required Math/Statistics Courses (10 cr)

Math 176 (3cr)	Discrete Math
Math 160 or 170 (4cr)	Survey of Calculus or Calculus I
STAT 251 or Stat 301 (3cr)	Statistical Methods or Probability and Statistics

Other Required Courses (5cr)

Comm 101 (2cr)	Fundamentals of Public Speaking
Phil 103 (3cr)	Ethics
Engl 317 (3cr)	Technical Writing

Other UI Gen Ed Core (23-24 Cr)

ISEM 101 (3 cr)
ISEM 301 (1 cr)
Science (7-8 credits)
Hum/SS (12 credits)

c. Additional requirements. *Describe additional requirements such as comprehensive examination, senior thesis or other capstone experience, practicum, or internship, some of which may carry credit hours included in the list above.*

The proposed program includes a year-long senior capstone experience (CYB 480/481) that parallels the other Engineering Capstone courses.

11. Program Intended Learning Outcomes and Connection to Curriculum.

a. Intended Learning Outcomes. *List the Intended Learning Outcomes for the proposed program, using learner-centered statements that indicate what will students know, be able to do, and value or appreciate as a result of completing the program.*

Graduates of the program will have an ability to:

1. Analyze a complex computing and information management problems and to apply principles of cybersecurity, and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of cyber security.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in cybersecurity practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to cybersecurity.
6. Apply security principles and practices to maintain operations in the presence of risks and threats.

12. Assessment plans

We will use the same general assessment process currently used by the Computer Science Department for its BS degree in Computer Science. The BS in CS degree has been accredited since 1993, first by the CS Accreditation Board (CSAB) and then by ABET, which replaced CSAB.

a. Assessment Process. *Describe the assessment process that will be used to evaluate how well students are achieving the intended learning outcomes of the program.*

There are three main methods by which student outcomes are assessed, divided into direct and indirect measures:

1. Student Work from at least two courses per outcome (direct measure)
2. The Department's Senior Exit Interviews (indirect measure)
3. The University's Graduating Senior Survey (indirect measure)

Each of these measures are described in more detail below. Faculty review and discussion of these measures is a critical part of the overall assessment process and faculty input is included in the analysis of the measures. Faculty review takes place during department meetings in the spring semester and during the department retreat help every fall.

Student Work

Every student outcome is assessed in a minimum of two courses. The focus is on upper division courses to determine the extent to which the students are achieving the outcome when they are approaching graduation.

Faculty select representative material from the course, potentially including assignments, projects, quizzes, exams, presentations, etc., with which to assess the student outcomes. The table given below shows the standard evaluation template used for assessments based on course materials.

Senior Exit Interviews

Every semester the chair conducts exit interviews with the graduating seniors. These include a group interview with all the graduating seniors (based on the graduating class size this is often divided into several smaller groups) and a written survey. The interview allows students to go into depth about the curriculum and their undergraduate experience. The written survey allows all seniors to give input, including anonymously if that is their preference.

No metric of attainment is measured as part of the interview process, but students are asked open ended questions regarding some SOs. This often results in very useful feedback that is not reflected in course materials.

Graduating Senior Surveys

The university conducts annual surveys of all graduating seniors. Many of the questions in the survey map to the program's outcomes. The second table below lists some of the relevant survey questions and responses. All of the questions used for assessment are of the form "Indicate how well the following skill was enhanced by your undergraduate experience". Thus, student answers reflect their belief regarding how well the program enhanced their skill, not necessarily their level of obtainment of the skill in question. Possible answers are 'greatly', 'moderately', 'a little', or 'not at all'. We use the percentage of answers in the 'greatly' and 'moderately' categories as our measure of student obtainment of the outcomes.

Sample Template used to assess student outcomes from a class.

SO	Detail Objective	Material	Question	Question Weight	Median	Score		
1	**Analyze a complex computing and information management problems and to apply principles of cybersecurity, and other relevant disciplines to identify solutions.**	Project 1	N/A	0.25	85%	85%	72%	91%
		Project 2	N/A	0.25	81%	73%	81%	89%
		Exam Two	Problem 4	0.25	85%	65%	85%	95%
		Exam Three	Problem 5	0.25	87%	87%	83%	90%
				WEIGHTED AVG.	**85%**			
2	**Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of cyber security.**	Exam Three	Problem 2	0.5	88%	90%	88%	75%
		Project 4	Problem 5	0.5	84%	92%	84%	69%
				WEIGHTED AVG.	**86%**			

Sample mapping from outcomes to Graduating Senior Survey question used to measure student outcomes. The questions are of the form "Indicate how well the following skill was enhanced by your undergraduate experience:". Possible answers are 'greatly', 'moderately', 'a little', or 'not at all'. We use the percentage of answers in the 'greatly' and 'moderately' categories as our measure of student obtainment of the outcomes.

Student Outcome	GSS Question
1. Analyze a complex computing problem	Identify and solve problems
	Think analytically and critically
2. Design, implement, and evaluate a computing-based solution	Formulate creative/original ideas and solutions
	Use computers and other technology
3. Communicate	Communicate well orally
	Write Effectively
4. Recognize professional responsibilities	Develop a sense of values and ethical standards
	Make decisions and act ethically
	Identify moral and ethical issues

b. Closing the loop. *How will you ensure that the assessment findings will be used to improve the program?*

As noted above, the measures of student obtainment of the outcomes are discussed during faculty meetings in the spring as the data become available – direct measure of student performance in class is normally measured in the fall classes. In addition, the entire curriculum is reviewed both in the spring as part of the meeting with the department's Industrial Advisory Board and in the fall as part of the department's annual retreat.

c. **Measures used.** *What direct and indirect measures will be used to assess student learning?*

These are discussed under **a. Assessment Process** above.

d. **Timing and frequency**. *When will assessment activities occur and at what frequency?*

Assessments based on students' performance in courses are typically conducted during the fall semester so that they can be reviewed in the spring. Senior exit interviews are held near the end of both the fall and spring semesters in order to give all graduating seniors the opportunity to participate. The UI's graduating senior survey is completed by students when they apply for graduation – typically the semester before they graduate and more or less continuously throughout the year.

Enrollments and Graduates

13. Existing similar programs at Idaho Public Institutions. Using the chart below, provide

enrollments and numbers of graduates for similar existing programs at your institution and other Idaho public institutions.

As noted above although there are certificates and minors in Cybersecurity and BS programs in Computer Science, no Idaho Public Institution currently offers a BS in Cybersecurity. Minors in Cybersecurity and BS programs in Computer Science are not similar enough to a BS in Cybersecurity to accurately represent either interest or competition.

Existing Similar Programs: Historical enrollments and graduate numbers								
Institution and Program Name	**Fall Headcount Enrollment in Program**				**Number of Graduates From Program (Summer, Fall, Spring)**			
	FY_16_	FY_17_	FY_18_	FY_19_ (most recent)	FY_16_	FY_17_	FY_18_	FY_19_ (most recent)
BSU	0	0	0	0	0	0	0	0
ISU	0	0	0	0	0	0	0	0
UI	0	0	0	0	0	0	0	0
LCSC	0	0	0	0	0	0	0	0
CEI	0	0	0	0	0	0	0	0
CSI	0	0	0	0	0	0	0	0
CWI	0	0	0	0	0	0	0	0
NIC	0	0	0	0	0	0	0	0

14. Projections for proposed program: Using the chart below, provide projected enrollments and number of graduates for the proposed program:

Proposed Program: Projected Enrollments and Graduates First Five Years											
Program Name:											
Projected Fall Term Headcount Enrollment in Program						**Projected Annual Number of Graduates From Program**					
FY 21 (first year)	FY 22	FY 23	FY 24	FY 25	FY 26	FY 21 (first year)	FY 22	FY 23	FY 24	FY 25	FY 26
16	31	45	60	66	72	-	-	-	-	10	14

15. Describe the methodology for determining enrollment and graduation projections. Refer to information provided in Question #2 "Need" above. What is the capacity for the program? Describe your recruitment efforts? How did you determine the projected numbers above?

Maximum capacity is determined by the size of the labs for the junior and senior level courses. These labs hold 20 students. Currently we only anticipate offering one section of each course, which limits us to upper division classes being no more than 20 students. Lower division classes can be slightly larger, assuming some attrition.

The numbers in the table are based on current demand within computer science, and a somewhat higher retention rate. Experience shows that students coming into the computer science major are often not prepared for the amount of mathematics, logical thinking, and workload of the discipline. Many students, even high performing students, transfer out of computer science in the first two years.

We believe a conservative estimate is having 16 new freshmen enter the program the first year, and slow growth in new freshmen, two additional per year, as news of the program spreads.

16. Minimum Enrollments and Graduates.

a. Have you determined minimums that the program will need to meet in order to be continued? What are those minimums, what is the logical basis for those minimums?

To maintain a viable program, we need to provide a regular offering of cybersecurity courses. Some of these courses can be taken by students in other majors (for example the upper division lecture courses can be take computer science students as technical electives). To provide these courses, we need to maintain a minimum enrollment in the classes (assumed to be an average of 15 undergraduate students per section).

If we have least 15 students in each "upper-division cadre", then we will easily make these numbers. Such numbers will place the program within the median size of bachelor programs at the University of Idaho, and thus will be sustainable.

We believe a sustained enrollment of at least 80 undergraduate students will be a minimum to maintain this program.

b. What is the sunset clause by which the program will be considered for discontinuance if

the projections or expectations outlined in the program proposal are not met?

We anticipate that the program will undergo an ABET accreditation review in Fall 2025. If the program is unable to become accredited at that time, we will need to evaluate our shortcomings, and if the program is not sustainable, begin the process of terminating the program. Similarly, if we can't reach sustained enrollments of at least 24 upper division students (Juniors and Seniors), we will need to sunset the program. In either case students in the initial years of the program (Freshmen and Sophomores) can transition to the CS degree with minimal difficulty.

Resources Required for Implementation – fiscal impact and budget

17. Physical Resources.

a. Existing resources. Describe equipment, space, laboratory instruments, computer(s), or other physical equipment presently available to support the successful implementation of the program.

The full program will be offered in Moscow. In the near future we plan to create a 2+2 programs in Coeur d'Alene (CdA) and in Idaho Falls (IF). We will partner with North Idaho College (NIC) in CdA and with the College of Eastern Idaho (CEI) in Idaho Falls (IF). Students will take the first two years of the program, earning an Associate's degree in the process, at NIC or CEI and finish the last two years, earning the BS, through UI. We will used live video conferencing between all three campuses (Moscow, CdA, and IF) to maximize our use of existing faculty in offering the degree. We currently have a 2+2 Bachelor's of CS program with NIC that will serve as the model for these 2+2 programs.

Although the program will initially be available only in Moscow – it will likely be at least two years before students from NIC or CEI would enter the program - the following discussion includes the resources at all three campuses to cover the anticipated expansion.

RADICL Lab, this is a specially designed, secure computing lab used to teach advanced cybersecurity courses that include attack and defense. In Moscow this lab is in JEB6. In Idaho Falls this lab is in CHE104. In Coeur d'Alene this lab is in iDen104.

General Computing Lab, this is a standard computing lab designed to teach programming and defense oriented cybersecurity. In Moscow this lab is in JEB321. In IF this lab is in CHE204. In CdA this lab is currently in HC240B.

If this program is eventually to be offered in Coeur d'Alene, and Idaho Falls via live video conferencing video capable classrooms are critical. In Moscow there are two available video classrooms EP202 and EP204, both of which hold 35 students. The CS Department currently gets priority scheduling for EP204. In Coeur d'Alene two video classrooms are available in the Harbor Center. In Idaho Falls video classrooms are available in the CHE building.

b. Impact of new program. What will be the impact on existing programs of increased use of physical resources by the proposed program? How will the increased use be accommodated?

There will be increased use of the RADICL lab at all three campuses. Currently there is sufficient available timeslots and room in these labs to manage the increased use on the Moscow and Idaho Falls campuses.

There will be increased use of the General Computer Labs at all campuses. Currently there is sufficient available timeslots and room in these labs to manage the increased use on the Moscow and Idaho Falls campuses. However, neither of the general computing labs are equipped with video conferencing equipment. So, before the program can be offered at either CdA or IF video capabilities will need to be added to JEB321 and to the general computing labs in CdA and IF.

c. Needed resources. List equipment, space, laboratory instruments, etc., that must be obtained to support the proposed program. Enter the costs of those physical resources into the budget sheet.

To offer the program in Moscow only, no additional resources are needed.

18. Library resources

a. Existing resources and impact of new program. Evaluate library resources, including personnel and space. Are they adequate for the operation of the present program? Will there be an impact on existing programs of increased library usage caused by the proposed program? For off-campus programs, clearly indicate how the library resources are to be provided.

Library resources are sufficient.

b. Needed resources. What new library resources will be required to ensure successful implementation of the program? Enter the costs of those library resources into the budget sheet.

None.

19. Personnel resources

a. Needed resources. Give an overview of the personnel resources that will be needed to implement the program. How many additional sections of existing courses will be needed? Referring to the list of new courses to be created, what instructional capacity will be needed to offer the necessary number of sections?

Resources for additional Sections:

We expect to add two sections of the existing CS120 course. This is taught as a large lecture course with separate lab sections, so the additional sections will be covered by TAs who teach the labs.

Resources for new Courses:

A review of the program curriculum shows that many of the courses are currently being taught as CS courses (they will become Cybersecurity CYB courses or cross-listed CS/CYB courses). When we reach year 3 and begin teaching the lab courses two

additional TAs will be needed.

b. Existing resources. Describe the existing instructional, support, and administrative resources that can be brought to bear to support the successful implementation of the program.

This program will be offered as an additional degree option within the Department of Computer Science. Hence all of the existing support, administrative staff, office space, etc. that is currently available within CS will be available to this program.

Impact on existing programs. What will be the impact on existing programs of increased use of existing personnel resources by the proposed program? How will quality and productivity of existing programs be maintained?

We will create a separate curriculum/petitions committee from the Cyber Security faculty to oversee the program. This will minimize the impact on existing personnel and the existing BS in Computer Science degree.

There will be an increase in size in some CS courses that are also required courses for students in the proposed CYB program. We have instructional capability to accommodate the additional students.

There will be a general shift in the elective CS course available to students in the CS program. Existing faculty will need to shift some of their teaching duties to the new CYB courses. Thus, some of the existing CS technical electives may be taught less frequently, but there will be more technical electives in the domain of Cybersecurity available to students. Overall students will still be able to select from a range of technical electives and there will be more than sufficient technical electives to allow students to graduate on time.

c. Needed resources. List the new personnel that must be hired to support the proposed program. Enter the costs of those personnel resources into the budget sheet.

Personnel:

To offer the program in Moscow only no additional faculty are required. As noted above some of the non-cybersecurity electives currently taught may be taught less frequently to account for the additional cybersecurity courses (many of which will be available as technical electives).

20. Revenue Sources

a) **Reallocation of funds:** If funding is to come from the reallocation of existing state appropriated funds, please indicate the sources of the reallocation. What impact will the reallocation of funds in support of the program have on other programs?

No existing funds will be reallocated.

b) **New appropriation**. If an above Maintenance of Current Operations (MCO) appropriation is required to fund the program, indicate when the institution plans to include the program in the legislative budget request.

c) **Non-ongoing sources**:

i. If the funding is to come from one-time sources such as a donation, indicate the sources of other funding. What are the institution's plans for sustaining the program when that funding ends?

ii. Describe the federal grant, other grant(s), special fee arrangements, or contract(s) that will be valid to fund the program. What does the institution propose to do with the program upon termination of those funds?

d) **Student Fees**:

i. If the proposed program is intended to levy any institutional local fees, explain how doing so meets the requirements of Board Policy V.R., 3.b.

There will be student lab fees to support the client computers, used by the students in the lab courses to connect to the secure servers. These fees will be used only for resources used in class. The exact amount of the fee will be dependent upon estimated enrollment and will be amortized over 3 years – the standard replacement cycle for the computers.

ii. Provide estimated cost to students and total revenue for self-support programs and for professional fees and other fees anticipated to be requested under Board Policy V.R., if applicable.

See attached budget.

21. Using the budget template provided by the Office of the State Board of Education, provide the following information:

- Indicate all resources needed including the planned FTE enrollment, projected revenues, and estimated expenditures for the first **four** fiscal years of the program.
- Include reallocation of existing personnel and resources and anticipated or requested new resources.
- Second and third year estimates should be in constant dollars.
- Amounts should reconcile subsequent pages where budget explanations are provided.
- If the program is contract related, explain the fiscal sources and the year-to-year commitment from the contracting agency(ies) or party(ies).
- Provide an explanation of the fiscal impact of any proposed discontinuance to include impacts to faculty (i.e., salary savings, re-assignments).

University of Idaho
Bachelor of Science in Cybersecurity

Freshman Fall			Freshman Spring		
CYB 110	Cybersecurity and Privacy **CSP, CSF,** PLE, PRI	3	CS 120	Computer Science I BSP	4
CS 112	Computational Thinking	3	Math 176	Discrete Math	3
ISEM 101	Integrated Seminar	3	Comm 101	Fundamentals of Public Speaking	2
ENGL 101	Introduction to College Writing	3	Phil 103	Ethics	3
Math 143	Pre-calculus Algebra and Analytic Geometry	3	ELECTIVE	Science Elective w/Lab	4
	Total Credits	**15**		**Total Credits**	**16**

Sophomore Fall			Sophomore Spring		
CS 121	Computer Science II	3	CS 270	System Software	3
CS 150	Computer Organization & Arch.	3	CS 240	Operating Systems OSC, OTH	3
CYB 210	Cybersecurity Management CPM, SPM, **ISC**	3	CYB 220	Secure Coding and Analysis SPP, SSA, QAT	3
ENGL 102	College Writing and Rhetoric	3	ELECTIVE	Science Elective w/Lab	4
MATH 160 or 170	Survey of Calculus or Calc I	4	STAT 251 or 301	Statistical Methods	3
	Total Credits	**16**		**Total Credits**	**16**

Junior Fall			Junior Spring		
CYB 310	Intermediate Cybersecurity (was CS 336) CTH, BCY, IAA	3	CS 383	Software Engineering	3
ISEM 301	Great Issues Seminar	1	CYB 340	Network Defense (was CS 438) NDF, IDS	3
CYB 330	Networking Fundamentals BNW, NTP	3	CYB 350	Operating System Defense OSH, OSA, BCO	3
CYB 380	Cybersecurity Lab I	3	CYB 381	Cybersecurity Lab II (was CS 439)	3
ELECTIVE	Hum/Social Science	3	ELECTIVE	Hum/Social Sciences	3
ENGL 317	Technical Writing	3			
	Total Credits	**16**		**Total Credits**	**15**

Senior Fall			Senior Spring		
CYB 401	Cybersecurity Professional Development (can be CS 400)	1	CYB 440	Software Vulnerability Analysis SAS, VLA	3
CYB 420	Computer and Network Forensics (was CS 447) DFS, HOF, NWF	3	CYB 481	Senior Capstone Design II (can be same as CS 481?)	3
CYB 480	Senior Capstone Design I (can be same as CS 480?)	3			
ELECTIVE	Free Electives	3	ELECTIVE	Free Electives	4
ELECTIVE	Hum/Social Science	3	ELECTIVE	Hum/Social Science	3
	Total Credits	**13**		**Total Credits**	**13**

Courses in RED are new Cybersecurity Courses
Courses in BLUE are modified existing CS courses
Foundational KU are in **BOLD Underline GREEN**
Core Technical KU are in Underlined RED
Core Non-technical KU are Underline Brown
Other Optional KUs are in Purple

Program Resource Requirements.

- Indicate all resources needed including the planned FTE enrollment, projected revenues, and estimated expenditures for the first **four** fiscal years of the program
- Include reallocation of existing personnel and resources and anticipated or requested new resources.
- Second and third year estimates should be in constant dollars.
- Amounts should reconcile subsequent pages where budget explanations are provided.
- If the program is contract related, explain the fiscal sources and the year-to-year commitment from the contracting agency(ies) or party(ies).
- Provide an explanation of the fiscal impact of any proposed discontinuance to include impacts to faculty (i.e., salary savings, re-assignments).

Start FY **21**

I. PLANNED STUDENT ENROLLMENT

	FY 21		FY 22		FY 23		FY 24	
	FTE	Headcount	FTE	Headcount	FTE	Headcount	FTE	Headcount
A. New enrollments	11	11	31	31	45	45	60	60
B. Shifting enrollments	5	5	0	0	0	0	0	0
Total Enrollment	**16**	**16**	**31**	**31**	**45**	**45**	**60**	**60**

II. REVENUE

	FY 21		FY 22		FY 23		FY 24	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
1. New Appropriated Funding Reques	-	-	-	-	-	-	-	-
2. Institution Funds	-	-	-	-	-	-	-	-
3. Federal	-	-	-	-	-	-	-	-
4. New Tuition Revenues from Increased Enrollments	154,823	N/A	433,504	N/A	628,299	N/A	846,965	N/A
5. Student Fees	3,300	N/A	9,240	N/A	13,392	N/A	18,053	N/A
6. Other (i.e., Gifts)	-	-	-	-	-	-	-	-
Total Revenue	158,123	-	442,744	-	641,691	-	865,018	-

Ongoing is defined as ongoing operating budget for the program which will become part of the base.
One-time is defined as one-time funding in a fiscal year and not part of the base.

III. EXPENDITURES

	FY 21		FY 22		FY 23		FY 24	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time

A. Personnel Costs

1. FTE	0	N/A	0	N/A	0	N/A	0	N/A
2. Faculty	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
3. Adjunct Faculty	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
4. Graduate/Undergrad Assistants	$ -	N/A	$ -	$ -	$ 33,000	$ -	$ 33,000	$ -
5. Research Personnel	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6. Directors/Administrators		N/A		N/A		N/A		N/A
7. Administrative Support Personnel	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
8. Fringe Benefits	$ -	N/A	$ -	N/A	$ 1,122	N/A	$ 1,122	N/A
9. Other: _____	$ -	N/A	$ -	N/A	$ 4,032	N/A	$ 4,032	N/A
Total Personnel and Costs	$ -	$ -	$ -	$ -	$ 38,154	$ -	$ 38,154	$ -

	FY 21		**FY 22**		**FY 23**		**FY 24**	
B. Operating Expenditures	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
1. Travel	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
2. Professional Services	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
3. Other Services	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
4. Communications	$ 500	$ 2,000	$ 500	$ -	$ 500	$ -	$ 500	$ -
5. Materials and Supplies	$ 7,150	$ -	$ 7,150	$ -	$ 7,150	$ -	$ 7,150	$ -
6. Rentals	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
7. Materials & Goods for Manufacture & Resale	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
8. Miscellaneous	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Operating Expenditures	$ 7,650	$ 2,000	$ 7,650	$ -	$ 7,650	$ -	$ 7,650	$ -

	FY 21		**FY 22**		**FY 23**		**FY 24**	
C. Capital Outlay	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
1. Library Resources	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

2. Equipment	$40,000.00	$0.00	$40,000.00	$0.00	$40,000.00	$0.00	$40,000.00	$0.00	Grant funded
Total Capital Outlay	$40,000	$0	$40,000	$0	$40,000	$0	$40,000	$0	

	FY 21		**FY 22**		**FY 23**		**FY 24**	
D. Capital Facilities Construction or Major Renovation								
E. Other Costs								
Utilites								
Maintenance & Repairs								
Other								
Total Other Costs	$0	$0	$0	$0	$0	$0	$0	$0
TOTAL EXPENDITURES:	$47,650	$2,000	$47,650	$0	$85,804	$0	$85,804	$0
Net Income (Deficit)	$110,473	-$2,000	$395,094	$0	$555,887	$0	$779,214	$0

Budget Notes (specify row and add explanation where needed; e.g., "I.A.,B. FTE is calculated using…"):

I.A.B.	
Row 84	Communication expenses are for advertising the program - these will come from CS funds: F&A returns, EO, etc.
Row 107	Renewing client machines in the computer labs, covered by lab fees. Initially the bulk of the lab fees will come from CS (non-CYB) students using the labs.
Row 105	This is grant funded
Row 51	Two TAs, these will be reallocated from another department within the College if necessary.
Row 78	No travel funds for recruiting are included because the chair and members of the program already travel around the state extensively, these trips will incorporate advertising.