SUBJECT
    Idaho Cybersecurity Initiative Progress Report

REFERENCE
March 2020	The Idaho Legislature approved $1M (one-time) for a collaborative statewide cybersecurity initiative across Idaho's public institutions of higher education.

APPLICABLE STATUTE, RULE, OR POLICY
    House Bill 644 (2020)

BACKGROUND/DISCUSSION
    The Presidents Leadership Council (PLC) approved a proposed expenditure plan for $1,000,000 in state funding for: cybersecurity curriculum coordination amongst the eight institutions; improved connectivity and expanded capacity for hands-on learning; increased coordination between the faculty and industry partners in cybersecurity; and increased internships and co-ops for Idaho students. The allocation for this initiative was decreased by 5% to $950,000 as a result of the Governor's budget holdback, however the effort is moving forward with an eye towards educating the state's needed cybersecurity work force.

    Dr. Michael Haney, a University of Idaho faculty member in cybersecurity located in Idaho Falls with a joint appointment with the Idaho National Laboratory, is coordinating a steering committee with academic representatives from each institution to tackle the curriculum coordination and training lab spaces. The steering committee is actively working on creating articulation agreements between the community colleges and the four-year institutions, as well as building a shared curriculum at the bachelor's and master's degree levels between Boise State University (BSU), Idaho State University (ISU), and University of Idaho (UI). Students will be able to register this spring for the first co-offered class at the bachelor's level, with planning underway for expanded offerings in the fall. There are many articulation agreements now in place and more in process.

    An inventory report of all cybersecurity educational offerings across the eight institutions was compiled and updated, showcasing the institutions' financial and time investment in the cybersecurity initiative. Dr. Haney is collaborating with the Office of the State Board of Education to coordinate cybersecurity educational offerings in partnership with the new Online Idaho initiative. Further expanding access to rural Idaho communities via online certificates and degrees in cybersecurity is important to meet the needs of the students where they are, which in turn is expanding the potential labor pool for state industry.

    In fall 2020, an audit was conducted of all eight institutions' capabilities to form a statewide cyber range. The Idaho cyber range will be a state-of-the-art cybersecurity training capability connecting faculty and students across the state, and will directly support the shared curriculum and expanded access for students

at all levels of post-secondary education in Idaho. Each institution will have a node in the cyber range. The node at some institutions will be a security operations center (SOC) training facility. The College of Eastern Idaho has the equipment for their SOC installed, and funding proposals are in process for deploying equipment to the other schools. The cyber range will operate on the backbone of the Idaho Regional Optical Network (IRON). The connectivity assessment determined that the College of Western Idaho would need some additional infrastructure to connect to IRON, so some of the funding will be used to forge this connection.

This spring more competitive student internships and co-ops will be added to the inventory at BSU, ISU and UI, furthering the connection with the cybersecurity industry in the state. There will be projects between the cybersecurity faculty and cybersecurity industry this year to align curricula with workplace needs, and define stronger career pathways for students as they earn two-year, four-year, and alternative credentials in Idaho.

Cybersecurity is a successful model of private and public partnership. Many of the eight institutions have been using state allocated funds for their individual programming and facilities. There are also contributions from private individual and corporate donors flowing to the universities for cyber research. The universities are applying for and receiving federal grant awards for their efforts in cybersecurity. The $950,000 funding from the state has been used to connect these siloed efforts and increase collaboration, with the goal of creating a superior student experience with educational ladders for careers in cybersecurity. Investment by the state, along with leadership by PLC, has helped position the state of Idaho to be a national leader in cybersecurity education

IMPACT
This progress report serves to inform the Board of the progress of the Idaho cybersecurity initiative.

ATTACHMENTS
Attachment 1 – Cybersecurity Initiative Progress Report Slide Deck

STAFF COMMENTS AND RECOMMENDATIONS
The Office of the State Board of Education has worked closely with the PLC, the Council on Academic Affairs and Programs, the cybersecurity initiative director, and faculty throughout the state to support this important effort. In particular, Board staff have collaborated with the institutions to create a new statewide digital campus called Online Idaho, which will serve as a portal for Idahoans to access the cybersecurity courses and degrees being developed by the initiative. Board staff are optimistic that these combined efforts will lead to educational success and increased career opportunities for more Idahoans.

BOARD ACTION
This item is for informational purposes.

# CYBERSECURITY UPDATE

Dr. Michael Haney

Introduction

◦ Many of the institutions were already active in cybersecurity, adding new programming or expanding

◦ The institutions active in cyber have financially invested significantly in the past and will continue to do so

◦ President's Leadership Council (PLC) decided to collaborate on cybersecurity as a state-wide initiative giving extra attention to the partnerships between the institutions

◦ Looking at cybersecurity education and research through a state-wide lens means together we can offer more educational ladders, pathways and options. Allowing the coalition of Idaho public institutions as a group to compete with much larger institutions nationally, that otherwise one institution alone would not have the resources to do.

◦ The legislature provided one-time $950,000 to be used for solidifying the coordination and collaboration amongst the institutions, and will be spent by June 30, 2021

◦ Work will continue after this fiscal year, seeking additional funding from industry and federal grants, and will hopefully lead to a future ask of the Idaho legislature

IDAHO CYBER SECURITY ECOSYSTEM

TO BE THE STATE WITH THE PREMIER EDUCATION IN PHYSICAL CYBER SECURITY

Cyber Range & Connectivity

- We are laying the foundation for a state-wide interconnected cyber range for state-of-the-art hands-on training and education

- Each institution will have at least one 'node' on the range; proposals for each institution due mid-February.

- For some of the institutions that will be a Security Operations Center (SOC) emulating real-world facilities and activities

- College of Eastern Idaho (CEI) has completed their SOC

- Currently working with College of Western Idaho (CWI) on IRON connectivity for complete connection between all schools
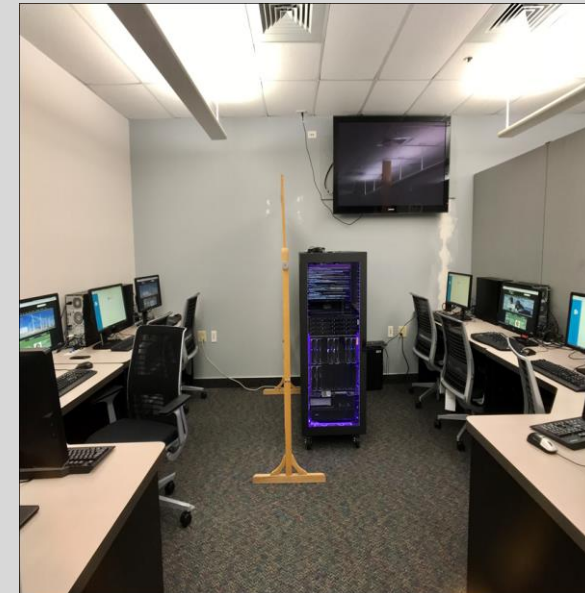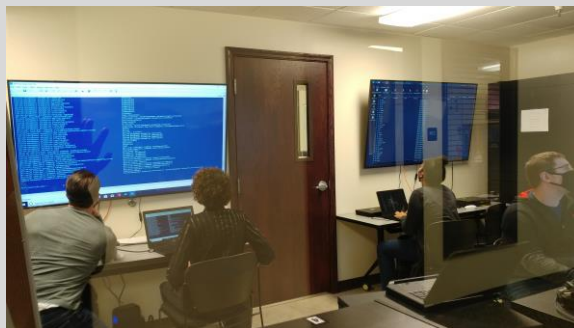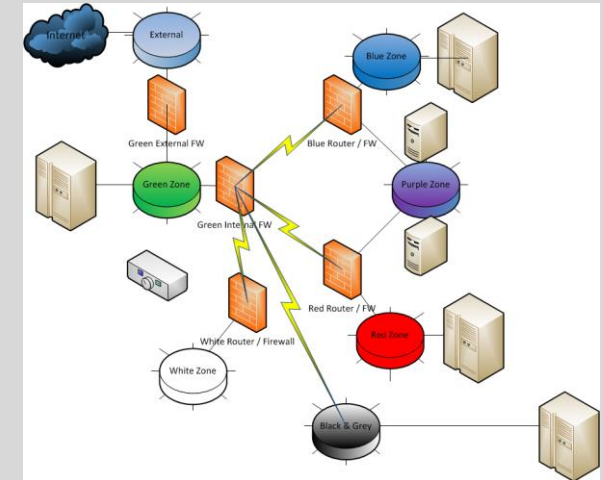
Coordinated Curriculum

◦ Steering committee with representation from each institution formed and routinely meeting

◦ BSU, ISU and UI working on shared curriculum for bachelor's degree course offerings

◦ First bachelors class is taking place Spring 2021 among students from UI, LCSC, BSU, and ISU.

◦ Pilot course is also shaking out technology and platform issues, working with Online Idaho initiative.

◦ Additional courses to be developed and jointly offered in Fall 2021 and Spring 2022

◦ Initiative funding will be used for grants to faculty for professional development and curriculum coordination efforts.

Partnerships with Industry

◦ Faculty grant application announcements in early February with deadline in mid March

◦ Grants are for at least $7,000 and are open to faculty at all 8 institutions

◦ There will be more internships and co-ops offered for students at BSU, ISU and UI to have more students engaging with the cybersecurity employers in the state

◦ Initiative personnel are engaged with WDC, IBE, and ITC to expand work-based education opportunities

◦ Working with steering committee members on process for awarding the student funds.

◦ Summer session starts in mid May, so it will not be a problem for expending the funds by June 30, 2021

◦ We are working to establish a long-term industry engagement in co-op education and apprenticeships

Questions?

SUBJECT
    Board Policy III.Z, Planning and Delivery of Postsecondary Programs and Courses – First Reading

REFERENCE

October 20, 2016	The Board approved the first reading of the proposed amendments to Board Policy III.Z., updating institutions' statewide program responsibilities.
December 15, 2016	The Board approved the second reading of proposed amendments to Board Policy III.Z.
December 21, 2017	The Board approved the first reading of proposed amendments to Board Policy III.Z., changing the planning timeframe from five years to three years.
February 15, 2018	The Board approved the second reading of proposed amendments to Board Policy III.Z.
June 21, 2018	The Board approved the first reading of proposed amendments to Board Policy III.Z., adding responsibilities for applied baccalaureate degrees to each region.
August 16, 2018	The Board approved the second reading of proposed amendments to Board Policy III.Z.
June 10, 2020	The Board approved the first reading of proposed amendments to Board Policy III.Z., changing the name of a statewide program listed for the University of Idaho.
August 26, 2020	The Board approved the second reading of proposed amendments to Board Policy III.Z.

APPLICABLE STATUTE, RULE, OR POLICY
    Idaho State Board of Education Governing Policies and Procedures, Section III.Z. and Section III.G.
    Section 33-113, Idaho Code
    Section 33-2107A, Idaho Code

BACKGROUND/DISCUSSION
    The purpose of Board Policy III.Z, "is to ensure Idaho's public postsecondary institutions meet the educational and workforce needs of the state through academic planning, alignment of programs and courses, and collaboration and coordination." The purpose is to also meet the statutory requirement to "as far as practicable prevent wasteful duplication of effort" by the institutions.

    The Presidents Leadership Council (PLC) identified a need to reexamine Board Policy III.Z to ensure it is promoting collaboration between institutions for the delivery of regional and statewide programs. The Council on Academic Affairs and Programs (CAAP) was charged with coordinating a Board Policy III.Z Working Group, which consisted of provosts from Idaho's institutions and Board staff. This

working group was asked to review Board Policy III.Z., and identify proposed amendments that will incentivize cooperation, coordination, and synergies between institutions; maintain a focus on avoiding duplication; and revise policy language that has fostered an environment of competition in the past.

IMPACT

Proposed amendments include two new definitions for high-demand programs and joint programs that aim to establish a common understanding of terminology and assist institutions and the Board with developing and expanding educational programs. The work group also streamlined the planning and coordination sections that had extraneous guidance, while adding language to other areas that encourage institutions to increase their collaboration with one another and fulfill the state's program requirements. Other proposed amendments include the following:

1. Creation of a specific section on the delivery of high-demand programs.
2. Removal of the statewide program responsibilities list for Boise State University, University of Idaho, and Idaho State University from the policy and placing this list within the official three-year plan document approved by the Board.
3. Clarification of delivery of programs that cross service regions.
4. Specification of requirements for memoranda of understanding between institutions for high-demand programs, joint programs, program transitions, and programs with regional or statewide program responsibilities.

ATTACHMENTS

Attachment 1 – Board Policy III.Z. Planning and Delivery of Postsecondary
                Programs and Courses – First Reading

STAFF COMMENTS AND RECOMMENDATIONS

The Board Policy III.Z Working Group held a series of meetings over the summer and throughout the fall of 2020, and identified policy amendments that refine the current policy by focusing on new areas of emphasis like high-demand and joint programs. Amendments also eliminate or revise portions of the policy that created silos or barriers between institutions.

CAAP, PLC, and the Instruction, Research, and Student Affairs Committee each reviewed the proposed policy amendments at their meetings in December 2020, January 2021, and February 2021, respectively.

Board staff recommends approval.

BOARD ACTION

I move to approve the first reading of proposed amendments to Board Policy III. Z. Planning and Delivery of Postsecondary Education Programs and Courses as submitted in Attachment 1.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

The purpose of this policy is to ensure Idaho's public postsecondary institutions meet the educational and workforce needs of the state through academic planning, alignment of programs and courses (hereinafter referred to collectively as "programs"), and collaboration and coordination. This subsection shall apply to the University of Idaho, Boise State University, Idaho State University, Lewis-Clark State College, College of Eastern Idaho, College of Southern Idaho, College of Western Idaho, and North Idaho College (hereinafter "institutions"). The State Board of Education (the Board) aims to optimize the delivery of academic programs while allowing institutions to grow and develop consistent with their vision and mission with an appropriate alignment of strengths and sharing of resources.

This policy requires the preparation and submission of academic plans to advise and inform the Board in its planning and coordination of educational programs in a manner that enhances access to quality programs, while concurrently increasing efficiency, avoiding unnecessary duplication and maximizing the cost-effective use of educational resources through coordination between institutions. As part of this process, the Board hereby identifies and reinforces the responsibilities of the institutions governed by the Board to deliver Statewide Programs. The provisions set forth herein serve as fundamental principles underlying the planning and delivery of programs pursuant to each institution's assigned Statewide and Service Region Program Responsibilities. These provisions also require collaborative and cooperative agreements, or memorandums of understanding, between and among the institutions.

This policy is applicable to campus-based face-to-face programs, including those that use technology to facilitate and/or supplement a physical classroom experience. It also applies to hybrid and blended programs where a substantial portion of the content is delivered on-line and typically has reduced seat time.

1. Definitions

   a. Designated Institution shall mean an institution whose main campus is located in a service region as identified in subsection 2.b.ii.1) and 2) below; and which possesses the first right to offer programs within its designated service region(s).

      i. ~~For purposes of this policy, w~~With respect to academic programs, Designated Institutions and Partnering Institutions shall have Service Region Program Responsibility for those regions identified in subsection 2.b.ii.1).

      ii. ~~For purposes of this policy, w~~With respect to career technical programs, Designated Institutions and Partnering Institutions shall include only the College of Southern Idaho, College of Western Idaho, North Idaho College,

1

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

College of Eastern Idaho, Lewis-Clark State College, and Idaho State University and shall have Service Region Program Responsibility for those regions identified in subsection 2.b.ii.2).

b. A memorandum of understanding (MOU) is an agreement between two or more institutions offering duplicative programs within the same service region that details how such programs will be delivered in a collaborative manner. An MOU is intended to provide specific, practical details that build upon what has been provided in each Institution's Plan.

c. High-Need Program shall mean a program identified by an institution or the Board as critical to supporting the future growth of a profession.

d. Joint Program shall mean an educational program jointly developed and delivered concurrently by two or more institutions.

e. Partnering Institution shall mean either
    i.   ~~(i)~~ an institution whose main campus is located outside of a Designated Institution's identified service region but which, pursuant to a Memorandum of Understanding, offers Regional Programs in the Designated Institution's primary service region, or ~~(ii)~~
    ~~i.~~ii.   an institution not assigned a Statewide Program Responsibility which, pursuant to a Memorandum of Understanding with the institution assigned the Statewide Program Responsibility, offers and delivers a statewide educational program.

~~d.~~f. Service Region Program shall mean an educational program identified by the Board to be delivered by a Designated Institution within its respective service region that meets regional educational and workforce needs.

~~e.~~g.   Service Region Program Responsibility shall mean an institution's responsibility to offer and deliver a Service Region Program to meet regional educational and workforce needs in its primary service region as defined in subsection 2.b.ii.1) and 2) below. Service Region Program Responsibilities are assigned to the Designated Institution in each service region, but may be offered and delivered by Partnering Institutions in accordance with the procedures outlined in this policy.

~~f.~~h. Statewide Program shall mean an educational program identified by the Board to be delivered by a particular institution which meets statewide educational and workforce needs. Lewis-Clark State College, College of Eastern Idaho, North

2

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

Idaho College, College of Southern Idaho, and College of Western Idaho do not have Statewide Program Responsibilities.

~~g.~~i. Statewide Program Responsibility shall mean an institution's responsibility to offer and deliver a Statewide Program in all regions of the state. Statewide Program Responsibilities are assigned to a specific institution by the Board, taking into account the degree to which such program is uniquely provided by the institution.

2. Planning and Delivery Process and Requirements

   a. Planning

      i. Three-Year Plan

      The Board staff shall, using the Institution Plans submitted, create and maintain a rolling three (3) year academic plan (Three-Year Plan) which includes all current and proposed institution programs. The Three-Year Plan shall be approved by the Board annually at its August Board meeting.

      ii. Institution Plan

      Each institution shall, in accordance with a template to be developed by the Board's ~~Chief Academic Officer~~ Executive Director or designee, create and submit to Board staff a rolling three (3) year academic plan, to be updated annually, that describes all current and proposed programs and services to be offered in alignment with each institution's Statewide and Service Region Program Responsibilities (the Institution Plan). Institution Plans shall be developed pursuant to a process of collaboration and communication with the other institutions in the state.

         1) Statewide Programs

         Institutions assigned a Statewide Program Responsibility shall plan for and determine the best means to deliver such program. Each institution assigned a Statewide Program Responsibility shall include in its Institution Plan all currently offered and proposed programs necessary to respond to the workforce and educational needs of the state relating to such Statewide Program Responsibilities. Each Institution Plan shall include the following information for proposed Statewide programs:

            a) A description of the Statewide Programs to be delivered throughout the state and the anticipated resources to be employed.

3

<div align="right">**ATTACHMENT 1**</div>

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

<div align="right">~~August 2020~~April 2021</div>

    b) A description of the Statewide Programs to be offered by a Designated or Partnering Institution.

    c) A summary of the Memoranda of Understanding (MOU's), if any, to be entered into with Partnering Institutions pursuant to Subsection 2.b.iii. below.

2) Service Region Programs

It is the responsibility of the Designated Institution to plan for and determine the best means to deliver Service Region Programs that respond to the educational and workforce needs of its service region. If, in the course of developing or updating its Institution Plan, the Designated Institution identifies a need for the delivery of a program within its service region, and the Designated Institution is unable to provide the program, then the Designated Institution shall coordinate with a Partnering Institution (including institutions with Statewide Program Responsibilities if applicable) located outside of the service region to deliver the program in the service region.

The Institution Plan developed by a Designated Institution shall include the following:

    a) A description of the proposed academic programs to be delivered in the service region, or outside of the service region, by the Designated Institution and the anticipated resources to be employed.

    b) A description of proposed programs to be offered in the service region by Partnering Institutions, including any anticipated transition of programs to the Designated Institution.

    c) A description of proposed Statewide Programs to be offered in the service region by an institution with Statewide Program Responsibilities, or by the Designated Institution in coordination with the institution holding the Statewide Program Responsibility.

    d) A summary of proposed MOU's, if any, to be entered into between the Designated Institution and any Partnering Institutions in accordance with Subsection 2.b.iii. below.

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

August 2020April 2021

e) A summary of collaborative programs created to meet areas designated as high-need.

3) Institution Plan Updates

Institution Plans shall be updated and submitted to Board staff annually as follows:

a) Preliminary Institution Plans shall be developed according to a template provided by the Board's Chief Academic Officer Executive Director or designee and submitted to the Council for Academic Affairs and Programs (CAAP) for review, discussion and coordination annually in April.

b) Following review by CAAP, Institution Plans shall be submitted to Board staff. Upon submission of the Institution Plans to Board staff, the Board's Chief Academic OfficerExecutive Director or designee shall review the Institution Plans for the purpose of optimizing collaboration and coordination among institutions, ensuring efficient use of resources, and avoiding unnecessary duplication of programs.

c) In the event the Board's Chief Academic Officer Executive Director or designee recommends material changes, he/she shall work with the institutions and then submit those recommendations to CAAP for discussion prior to submission to the Board for inclusion in the Three-Year Plan.

d) The Board's Chief Academic OfficerExecutive Director or designee shall then provide their recommendations to the Board for enhancements, if any, to the Institution Plans at a subsequent Board meeting. The Board shall approve the Institution Plans annually through the Three-Year Plan submitted by Board staff. Board approval of Institution Plans acts as a roadmap for institutional planning and does not constitute Board approval of a program. Institutions are still required to follow the standard program approval process as identified in Board Policy Section III.G to gain program approval.

b. Delivery of Programs

i. Statewide Program Delivery
The Board has established statewide program responsibilities for the following

5

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

~~institutions~~ University of Idaho, Boise State University, and Idaho State University. Each institution must assess the need for, and, when determined by the assessment, ensure the statewide delivery of educational programs assigned by the Board. ~~This~~ A statewide program list consisting of statewide program responsibilities shall be updated by the Board every two years in accordance with a schedule developed by the Executive Director or designee. The program list will be contained in the Board approved three-year plan document and maintained by Board staff.

~~Boise State University must assess the need for and, when determined necessary by the assessment, ensure the statewide delivery of all educational programs in the following degree program areas:~~

Program Name	Degrees
~~Public Policy and Administration~~	~~M.S., Ph.D.~~
~~Community and Regional Planning~~	~~M.C.R.P., Ph.D.~~
~~Social Work (Region V-VI —shared with ISU)~~	~~M.S.W.~~
~~Social Work~~	~~Ph.D.~~

~~Idaho State University must assess the need for and, when determined necessary by the assessment, ensure the statewide delivery of all educational programs in the following degree program areas:~~

Program Name	Degrees
~~Audiology~~	~~Au.D., Ph.D.~~
~~Physical Therapy~~	~~D.P.T., Ph.D.~~
~~Occupational Therapy~~	~~M.O.T.~~
~~Pharmaceutical Science~~	~~M.S., Ph.D.~~
~~Pharmacy Practice~~	~~Pharm.D.~~
~~Nursing (Region III shared w/ BSU)~~	~~M.S., D.N.P.~~
~~Nursing~~	~~Ph.D.~~
~~Physician Assistant~~	~~M.P.A.S.~~
~~Speech Pathology~~	~~M.S.~~
~~Deaf Education~~	~~M.S.~~
~~Sign Language Interpreting~~	~~B.S.~~
~~Health Education~~	~~M.H.E.~~
~~Public Health~~	~~M.P.H.~~
~~Health Physics~~	~~B.S., M.S., Ph.D.~~
~~Dental Hygiene~~	~~B.S., M.S.~~
~~Medical Lab Science~~	~~B.S., M.S.~~
~~Clinical Psychology~~	~~Ph.D.~~

6

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

University of Idaho must assess the need for and, when determined necessary by the assessment, ensure the statewide delivery of all educational programs in the following degree program areas:

Program Name	Degrees
Law	J.D.
Architecture	B.S. Arch., M. Arch.
Integrated Architecture & Design	M.S.
Landscape Architecture	B.S.L.A., M.L.A.
Interior Design	B.I.D., M.S.
Animal & Veterinary Science	B.S.A.V.S.
Animal Science	M.S.
Veterinary Science	D.V.M.
Plant Science	M.S., Ph.D.
Agricultural Economics	B.S.Ag.Econ.
Applied Economics (Agricultural)	M.S.
Food Science	B.S.F.S., M.S., Ph.D.
Forestry	B.S.Forestry
Renewable Materials	B.S.Renew.Mat.
Wildlife Resources	B.S.Wildl.Res.
Fishery Resources	B.S.Fish.Res.
Natural Resource Conservation	B.S.Nat.Resc.Consv.
Rangeland Ecology & Management	B.S.Rangeland.Ecol.Mgmt.
Fire Ecology & Management	B.S.Fire.Ecol.Mgt.
Natural Resource concentrations in: • Forestry • Forest and Sustainable Products • Wildlife Resources • Fishery Resources • Natural Resource Conservation • Rangeland Ecology & Management • Fire Ecology & Management	M.S., M.N.R., Ph.D.

ii. High-Demand Programs

The Board recognizes that the need for high-demand, high-need programs may require joint delivery by multiple institutions statewide. These high-demand programs must be delivered through collaboration between institutions in order to preserve rural and statewide access. Service region restrictions and primary institution first rights to offer a program do not apply to Board identified high-demand programs. Criteria for statewide program high-demand designation

7

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

includes, but is not limited to:

1)   Idaho Department of Labor data,
2)   Idaho industry demand as demonstrated by unfilled positions and industry data,
3)   Demonstrated Idaho state needs for programs supporting underserved populations, and
4)   Requested by the ~~SBOE~~Board.

An institution wishing to offer a high-demand program ~~and~~that does not have statewide responsibility in the program area must meet the criteria above, have a signed MOU with the Institution with the Statewide Program Responsibility, and the approval of the Board's Executive Director or designee. At that point, the Partnering Institution shall include the program in its Institution Plan. If the Board determines that an emergency need exists for a program that the Institution with Statewide Program Responsibility cannot meet, then upon Board approval the two Institutions shall enter into an MOU for the delivery of such program.

~~ii.~~iii.   Service Region Program Delivery

The Board has established service regions for the institutions based on the six geographic areas identified in Section 33-2101, Idaho Code. A Designated Institution shall have the Service Region Program Responsibility to assess and ensure the delivery of all educational programs and services necessary to meet the educational and workforce needs within its assigned service region.

1) Academic Service Regions

Region I shall include the area within Area No.1 under Section 33-2101, Idaho Code. Lewis-Clark State College, the University of Idaho, and North Idaho College are the Designated Institutions serving undergraduate needs. The University of Idaho is the Designated Institution serving the graduate education needs. Lewis-Clark State College, and North Idaho College are the Designated Institutions serving applied baccalaureate degree needs.

Region II shall include the area within Area No.2 under Section 33-2101, Idaho Code. Lewis-Clark State College and the University of Idaho are the Designated Institutions serving undergraduate needs. The University of Idaho is the Designated Institution serving the graduate education needs.

8

<div align="right">**ATTACHMENT 1**</div>

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

<div align="right">August 2020April 2021</div>

Region III shall include the area within Area No.3 under Section 33-2101, Idaho Code. Boise State University and College of Western Idaho are the Designated Institutions serving undergraduate needs. Boise State University is the Designated Institution serving graduate education needs. Boise State University and College of Western Idaho are the Designated Institutions serving applied baccalaureate degree needs.

Region IV shall include the area within Area No.4 under Section 33-2101, Idaho Code. Idaho State University and College of Southern Idaho are the Designated Institutions serving undergraduate needs. Idaho State University is the Designated Institution serving the graduate education needs, with the exception that Boise State University will meet undergraduate and graduate business program needs. Idaho State University and College of Southern Idaho are the Designated Institutions serving applied baccalaureate degree needs.

Region V shall include the area within Area No.5 under Section 33-2101, Idaho Code. Idaho State University is the Designated Institution serving undergraduate and graduate education needs.

Region VI shall include the area within Area No.6 under Section 33-2101, Idaho Code. Idaho State University and College of Eastern Idaho are the Designated Institutions serving undergraduate education needs. Idaho State University is the Designated Institution serving the graduate education needs. Idaho State University and College of Eastern Idaho are the Designated Institutions serving applied baccalaureate degree needs.

2) Career Technical Service Regions

Postsecondary career technical education is delivered by six (6) institutions, each having responsibility for serving one of the six geographic areas identified in Section 33-2101.

Region I shall include the area within Area No.1 under Section 33-2101, Idaho Code. North Idaho College is the Designated Institution.

Region II shall include the area within Area No.2 under Section 33-2101, Idaho Code. Lewis-Clark State College is the Designated Institution.

Region III shall include the area within Area No.3 under Section 33-2101, Idaho Code. College of Western Idaho is the Designated Institution

<div align="center">9</div>

<div align="right">

ATTACHMENT 1
</div>

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

<div align="right">

~~August 2020~~April 2021
</div>

Region IV shall include the area within Area No.4 under Section 33-2101, Idaho Code. College of Southern Idaho is the Designated Institution.

Region V shall include the area within Area No.5 under Section 33-2101, Idaho Code. Idaho State University is the Designated Institution.

Region VI shall include the area within Area No.6 under Section 33-2101, Idaho Code. College of Eastern Idaho is the Designated Institution.

3) Program Offerings by Partnering Institutions

If a Partnering Institution (other than an institution with Statewide Program Responsibilities) identifies a Service Region Program not identified, or anticipated to be identified, in a Designated Institution's Plan, and the Partnering Institution wishes to offer such program in the Designated Institution's service region, then the Partnering Institution may communicate with the Designated Institution for the purpose of allowing the Partnering Institution to deliver such program in the service region and to include the program in the Designated Institution's Plan. In order to include the program in the Designated Institution's Plan, the Partnering Institution must demonstrate the need within the service region for delivery of the program, as determined by the Board (or by the Administrator of the Division of Career Technical Education in the case of career technical level programs). In order to demonstrate the need for the delivery of a program in a service region, the Partnering Institution shall complete and submit to the Chief Academic Officer of the Designated Institution, to CAAP and to Board staff, in accordance with a schedule to be developed by the Board's ~~Chief Academic Officer~~Executive Director or designee, the following:

a) A study of business and workforce trends in the service region indicating anticipated, ongoing demand for the educational program to be provided.

b) A survey of potential students evidencing demand by prospective students and attendance sufficient to justify the short-term and long-term costs of delivery of such program.

c) A complete description of the program requested to be delivered, including a plan for the delivery of the program, a timeline for delivery of the program, the anticipated costs of delivery, the resources and support required for delivery (including facilities needs and costs), and program

<div align="center">

10
</div>

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

August 2020April 2021

syllabuses.

4)   Designated Institution's First Right to Offer a Program

In the event the Partnering Institution has submitted the information set forth above to the Board's Chief Academic Officer) for inclusion in the Designated Institution's Plan, and a need is demonstrated by the Partnering Institution for such program in the service region, as determined by the Board (or by the Administrator for the Division of Career Technical Education in the case of career technical level programs), or prior to the submission of an updated Institution Plan by the Designated Institution, it is determined by the Board that an emergency need has arisen for such program in the service region the Designated Institution shall have a first right to offer such program.

The Designated Institution must within six (6) months (three (3) months in the case of associate level or career technical level programs) of receiving the request from a Partnering Institution to offer said program determine whether it will deliver such program on substantially the same terms (with respect to content and timing) described by the Partnering Institution. In the event the Designated Institution determines not to offer the program, the Partnering Institution may offer the program according to the terms stated, pursuant to an MOU to be entered into with the Designated Institution. If the Partnering Institution materially changes the terms and manner in which the program is to be delivered, the Partnering Institution shall provide written notice to the Chief Academic Officer of the Designated Institution and to the Board's Chief Academic Officer of such changes and the Designated Institution shall be afforded the opportunity again to review the terms of delivery and determine within three (3) months of the date of notice whether it will deliver such program on substantially the same terms.

iii.iv.   Memoranda of Understanding

The Board encourages and fosters orderly and productive collaboration between Idaho's public institutions. Memoranda of Understanding can support such collaboration.
When a service region is served by more than one institution for the delivery of an academic or technical credential defined in Board Policy Section III.E., an MOU shall be developed between such institutions as provided herein and submitted to the Board's Chief Academic Officer for review and approval by the Board prior to entering into such agreements. Each MOU shall be entered into based on the following guidelines, unless otherwise approved by the Board.

11

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses
August 2020April 2021

Institutions proposing to offer a joint program shall develop an MOU to identify the specific roles of each participating institution; the student-related processes associated with delivery of the program; and a timeline for review.

When an institution desires to offer a program already being offered by another institution in the latter institution's service region, an MOU shall be developed between the institutions to offer the program.

If a Designated Institution has identified a workforce or educational need for the delivery of a program within its service region and is unable to provide the program, the Designated Institution may collaborate with a Partnering Institution to offer the program. An MOU will not be required for review or approval prior to implementation in this case. Institutions are required to follow the standard program approval processes as identified in Board Policy III.G to obtain program approval.If an institution with Statewide Program Responsibility has submitted the information set forth in Subsection 2.a.ii. above to a Designated Institution and Board staff in a timely manner (as determined by the Board's Chief Academic Officer) for inclusion in the Designated Institution's Plan, then the Designated Institution shall identify the program in its Institution Plan and enter into an MOU with the institution with Statewide Program Responsibility in accordance with this policy. If, prior to the submission of an updated Institution Plan by the Designated Institution, it is determined by the Board that an emergency need has arisen for such program in the service region, then upon Board approval the institution with Statewide Program Responsibility and the Designated Institution shall enter into an MOU for the delivery of such program in accordance with the provisions of this policy.

An institution with Statewide Program Responsibility need not enter into an MOU with any other institutions before offering the statewide program in service regions outside the service region of the institution with Statewide Program Responsibility. If an institution desires to offer a program for which another institution has Statewide Program Responsibility, the institution that does not have Statewide Program Responsibility shall be required to enter into an MOU with the institution that has Statewide Program Responsibility for that program.

When an institution with Statewide Program Responsibility or Service Region Program Responsibility desires to offer a program within a service region where such program is currently being offered by another institution, the institutions shall enter into a transition MOU that includes an admissions plan between the institutions providing for continuity in student enrollment during the transition

12

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

period.

Idaho public postsecondary institutions may enter into MOUs with out-of-state postsecondary institutions or private postsecondary institutions to offer programs. Such MOUs do not require notification or approval by the Board, but shall be shared with the Council on Academic Affairs and Programs. While the Board does not prohibit MOUs with out-of-state postsecondary institutions, agreements with in-state public institutions are preferred. ~~The Board encourages agreements with out-of-state postsecondary institutions, but agreements with in-state public institutions are favorable.~~

Articulation agreements between any postsecondary institutions for the purposes of facilitating course or program transfer do not require approval by the Board. Such agreements shall be managed and tracked by the institutions, and shall be reported to the Board on an annual basis as part of the three-year planning process. All articulation agreements must be in compliance with Section 33-3729, Idaho Code, and Board Policy III.V.

All MOUs shall be submitted in conjunction with related program proposals following the standard program approval processes as identified in Board Policy III.G.

~~iv.~~v.   Facilities

For programs offered by a Partnering Institution (whether an institution with Statewide Program Responsibilities, or otherwise) within a municipal or metropolitan area that encompasses the campus of a Designated Institution, the Partnering Institution's programs offerings shall be conducted in facilities located on the campus of the Designated Institution to the extent the Designated Institution is able to provide adequate and appropriate property or facilities (taking into account financial resources and programmatic considerations), or in facilities immediately adjacent to the campus of the Designated Institution. Renting or building additional facilities shall be allowed only upon Board approval, based on the following:

1) The educational and workforce needs of the local community demand a separate facility at a location other than the campus of the Designated Institution or adjacent thereto as demonstrated in a manner similar to that set forth in Subsection 2.b.ii.1) above, and

2) The use or development of such facilities are not inconsistent with the

13

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

~~August 2020~~April 2021

Designated Institution's Plan.

Facilities rented or built by a Partnering Institution (whether an institution with Statewide Program Responsibilities, or otherwise) on, or immediately adjacent to, the "main" campus of a Designated Institution may be identified (by name) as a facility of the Partnering Institution, or, if the facility is rented or built jointly by such institutions, as the joint facility of the Partnering Institution and the Designated Institution. Otherwise, facilities utilized and programs offered by one or more Partnering Institutions within a service region shall be designated as "University Place at (name of municipality)."

For programs offered by a Partnering Institution (whether an institution with Statewide Program Responsibilities, or otherwise) within a municipality or metropolitan area encompassing a campus of a Designated Institution, to the extent programmatically possible, auxiliary services (including, but not limited to, bookstore, conference and other auxiliary enterprise services) and student services (including, but not limited to, library, information technology, and other auxiliary student services) shall be provided by the Designated Institution. To the extent programmatically appropriate, registration services shall also be provided by the Designated Institution. It is the goal of the Board that a uniform system of registration ultimately be developed for all institutions governed by the Board. The Designated Institution shall offer these services to students who are enrolled in programs offered by the Partnering Institution in the same manner, or at an increased level of service, where appropriate, as such services are offered to the Designated Institution's students. An MOU between the Designated Institution and the Partnering Institution shall outline how costs for these services will be allocated.

~~v.~~vi.   Duplication of Courses

If courses necessary to complete a Statewide Program are offered by the Designated Institution, they shall be used and articulated into the Statewide Program.

~~vi.   Program Transitions~~

~~Institutions with Statewide Program or Service Region Program Responsibilities may plan and develop the capacity to offer a program within a service region where such program is currently being offered by another institution (the Withdrawing Institution) as follows:~~

14

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses

August 2020April 2021

1) The institution shall identify its intent to develop the program in the next update of its Institution Plan. The institution shall demonstrate its ability to offer the program through the requirements set forth in Subsection 2.b.ii.3) above.

Except as otherwise agreed between the institutions pursuant to an MOU, the Withdrawing Institution shall be provided a minimum three (3) year transition period to withdraw its program. If the Withdrawing Institution wishes to withdraw its program prior to the end of the three (3) year transition period, it may do so but in no event earlier than two (2) years from the date of notice (unless otherwise agreed). The Withdrawing Institution shall enter into a transition MOU with the institution that will be taking over delivery of the program that includes an admissions plan between the institutions providing for continuity in student enrollment during the transition period.

vii.   Discontinuance of Programs

Unless otherwise agreed between the applicable institutions pursuant to an MOU, if, for any reason, (i) a Designated Institution offering programs in its service region that supports a Statewide Program of another institution, (ii) a Partnering Institution offering programs in the service region of a Designated Institution, or (iii) an institution holding a Statewide Program Responsibility offering Statewide Programs in the service region of a Designated Institution, wishes to discontinue offering such program(s), it shall use its best efforts to provide the institution with Statewide or Service Region Program Responsibility, as appropriate, at least one (1) year's written notice of withdrawal, and shall also submit the same written notice to the Board and to oversight and advisory councils. In such case, the institution with Statewide or Service Region Program Responsibilities shall carefully evaluate the workforce need associated with such program and determine whether it is appropriate to provide such program. In no event will the institution responsible for the delivery of a Statewide or Service Region Program be required to offer such program (except as otherwise provided herein above).

3. Existing Programs

Programs being offered by a Partnering Institution (whether an institution with Statewide Program Responsibilities, or otherwise) in a service region prior to July 1, 2003, may continue to be offered pursuant to an MOU between the Designated Institution and the Partnering Institution, subject to the transition and notice periods and requirements set forth above.

15

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
Subsection: Z. Planning and Delivery of Postsecondary Programs and Courses
~~August 2020~~April 2021

4. Oversight and Advisory Councils

   The Board acknowledges and supports the role of oversight and advisory councils to assist in coordinating, on an ongoing basis, the operational aspects of delivering programs among multiple institutions in a service region, including necessary resources and support and facility services, and the role of such councils in interacting and coordinating with local and regional advisory committees to address and communicate educational needs indicated by such committees. Such interactions and coordination, however, are subject to the terms of the MOU's entered into between the institutions and the policies set forth herein.

5. Resolutions

   All disputes relating to items addressed in this policy shall be forwarded to the Board's ~~Chief Academic Officer~~ Executive Director or designee for review. The Board's ~~Chief Academic Officer~~ Executive Director or designee shall prescribe the method for resolution. The Board's ~~Chief Academic Officer~~ Executive Director or designee may forward disputes to CAAP and if necessary make recommendation regarding resolution to the Board. The Board will serve as the final arbiter of all disputes.

6. Exceptions

   a. This policy is not applicable to programs for which 90% or more of all activity is required or completed online, or dual credit courses for secondary education.

   b. This policy also does not apply to courses and programs specifically contracted to be offered to a private, corporate entity. However, in the event that an institution plans to contract with a private corporate entity (other than private entities in the business of providing educational programs and course) outside of their Service Region, the contracting institution shall notify the Designated Institutions in the Service Region and institutions with Statewide Program Responsibilities, as appropriate. If the corporate entity is located in a municipality that encompasses the campus of a Designated Institution, the Board encourages the contracting institution to include and draw upon the resources of the Designated Institution insomuch as is possible.

SUBJECT
> Board Policy III.F. Program Prioritization – Second Reading

REFERENCE

May 2013	The Board directed institutions to institute a prioritization of programs process consistent with Robert Dickeson's prioritization principles,[1] and further directed the institutions to use a quintile prioritization approach and communicate to the Board the criteria and weighting to be used after consultation with their respective campuses.
June 2013	The Board approved the program prioritization proposals for Idaho State University (ISU), Boise State University (BSU), and University of Idaho (UI) as presented.
August 2013	The Board approved the program prioritization proposal for Lewis-Clark State College as presented.
October 2013	The Board was presented with an update on program prioritization.
August 2014	The Board was presented with the results of program prioritization and reminded institutions that program prioritization needed to be integrated into their budgeting and planning practices.
June 2015	The Board was presented with an update on the implementation of program prioritization.
August 2016	The Board was presented with an update on the implementation of program prioritization.
December 2018	The Board was presented with an update on the implementation of program prioritization.
August 2019	The Board approved the first reading of new Board Policy III.F., Program Prioritization.
October 2019	The Board approved the second reading of new Board Policy III.F., Program Prioritization, including amendments clarifying process and reporting requirements.
December 2020	The Board approved the first reading of Board Policy III.F., Program Prioritization, removing requirement for non-instructional programs to be placed in quintiles.

APPLICABLE STATUTES, RULE OR POLICY
> Idaho State Board of Education Governing Policies & Procedures, Section III.F. and V.B.
> Section 33-113, Idaho Code

---

[1] *Prioritizing Academic Programs and Services: Reallocating Resources to Achieve Strategic Balance* (Jossey-Bass, 2nd ed; 2010).

BACKGROUND/DISCUSSION

Board Policy III.F. Program Prioritization requires institutions under the Board's governance to integrate program prioritization into their planning and budgeting processes. This policy establishes evaluation criteria for programs and services with specific tangible objectives. The policy currently requires institutions to integrate program prioritization for academic and non-academic programs, and requires both academic and non-academic programs to be "grouped into quintiles based on relative cost efficiency and effectiveness."

The proposed revisions will change the terms "academic and non-academic" to "instructional and non-instructional" and will clarify that "instructional" programs include both academic and career technical education programs. The proposed changes will also remove the requirement for institutions to group non-instructional programs into quintiles based on relative cost efficiency and effectiveness. The policy amendments will require evaluation with quintiling of instructional programs (including both academic and career technical education) and evaluation without quintiling of non-instructional programs.

IMPACT

Approval of the proposed amendments will remove the requirement for non-instructional programs to be placed in quintiles and clarify the program prioritization requirement applies to academic and career technical programs at the four-year institutions.

ATTACHMENTS

Attachment 1 – Board Policy III.F. Program Prioritization – Second Reading

STAFF COMMENTS AND RECOMMENDATIONS

The only change between first and second readings was the addition of the word "only" in subsection 4, to provide additional clarification about which types of programs are required to be quintiled.

Board staff support the proposed policy amendments.

BOARD ACTION

I move to approve the second reading of Board Policy III.F. Program Prioritization as submitted in Attachment 1.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

ATTACHMENT 1

Idaho State Board of Education
GOVERNING POLICIES AND PROCEDURES
SECTION: III. POSTSECONDARY AFFAIRS
SUBSECTION: F. Program Prioritization   ~~October 2019~~ February 2021

Program Prioritization

The University of Idaho, Boise State University, Idaho State University and Lewis-Clark State College shall integrate program prioritization into their respective strategic planning, programming (~~academic~~ instructional and non~~academic~~-instructional) and budgeting processes. As part of the program prioritization process the institutions shall conduct an evaluation of programs and services with specific and tangible objectives, and with a focus on specific evaluation criteria.

1. All ~~academic~~ instructional programs, which include academic and career technical programs, shall be evaluated with an emphasis on:
    a. External demand
    b. Quality of outcomes
    c. Costs and other expenses.

2. Additional criteria may be considered by institutions to evaluate programs. This criteria can be weighted within the evaluation process as the institution determines appropriate. Criteria may include:
    a. History, development and expectations of the program
    b. External demand
    c. Internal demand
    d. Quality of inputs and processes
    e. Quality of outcomes
    f. Size, scope and productivity
    g. Revenue and other resources generated
    h. Costs and other expenses
    i. Impact, justification and overall essentiality
    j. Opportunity analysis

3. Criteria for evaluation of non-~~academic~~instructional programs may include:
    a. Key objectives and how they are measured
    b. Services provided and to which customers
    c. Position-by-position analysis
    d. Unmet needs and demands
    e. Opportunities for collaboration and restructuring
    f. Opportunities to share skill sets and resources
    g. Opportunities for cross-training
    h. Technological improvements that are cost effective
    i. Process improvements to streamline operations

ATTACHMENT 1

   j. Outsourcing exploration to improve service and cut costs

  This criteria may be weighted as each institutions determines appropriate.

4. ~~Academic~~ Instructional and non-~~academic~~instructional programs shall be evaluated as outlined in this policy. ~~and~~Only instructional programs shall be grouped into quintiles ~~based on relative cost efficiency and effectiveness~~.

  All instructional program reviews shall include an indicator of which quintile the program falls into. Annual program prioritization updates shall provide a description of the progress achieved toward implementing findings and recommendations. These are to be submitted annually to the ~~board~~ Board by the institutions in a format and timeline established by the Executive Director.

5. Institutions shall conduct program prioritization at least once every five years. Final reports must include:
   a. Programs that will be improved through advancements in efficiency, quality, productivity, and focus.
   b. Opportunities for improvements to organizational structure and function
   c. Programs considered for consolidation or discontinuation as based on cost of delivery and degree of relevance and impact.
   d. Estimated institutional savings and efficiencies created through implementation of recommendations.

6. As part of program planning processes pursuant to Board Policy III.Z. and postsecondary program approval and discontinuance processes pursuant to Board Policy III.G., institutions must provide the ~~board~~ Board with information on how planned and proposed program action addresses needs identified from program prioritization.

7. Program prioritization processes must involve a diverse range of stakeholder representation at each institution. Methodology will be reported to the Board and must be transparent to institution communities while meeting the outcomes defined in this section of Board Policy.

SUBJECT
    Board Policy III.U. Textbook and Instructional Material Affordability – Partial Waiver

REFERENCE

April 2018	The Board received update on an Open Educational Resources (OER) initiative as part of the work session.
June 2018	The Board discussed system-wide access and affordability strategies including OER and requested an inventory and implementation timeline be provided at the October 2018 Board meeting.
August 2018	The Board approved a line item request for OER funding.
December 2018	The Board was provided with a timeline and inventory update regarding OER and the total number of course sections delivered exclusively with OER throughout Idaho colleges and universities.
April 2019	The Board was provided with an inventory of common-indexed courses for which funding will be focused for OER adoption.
August 2019	The Board approved the first reading of new Board Policy III.U. Textbook and Instructional Material Affordability.
October 2019	The Board approved the second reading of new Board Policy III.U. Textbook and Instructional Materials Affordability.

BACKGROUND/DISCUSSION
    Policy III.U. Textbook and Instructional Materials Affordability establishes definitions of open educational resources (OER) and instructional materials as well as minimum standards for textbook affordability. The policy requires institutions to implement a plan to meet or exceed those standards no later than the start of the 2021-2022 academic year. This includes:

- providing faculty with professional development opportunities;
- incentivizing faculty to explore the adoption, adaption, or creation of OER;
- requiring institutions to develop policies and procedures for minimizing cost of instructional materials for students;
- providing students with a course list that utilizes OER or have no cost instructional materials at the time of enrollment;
- developing OER (or low cost materials where OER is not available) for at least one section of each common-indexed course offered at each institution;
- providing students low cost textbooks or OER for each common-indexed course delivered as dual credit; and
- establishing a standardized review and approval process for OER that ensures quality of materials.

Concerns have been raised about some aspects of this policy by faculty and administrative leaders at institutions throughout the state. In particular, faculty are concerned that the policy's mandate that OER be adopted in common-indexed courses may infringe on faculty academic freedom and responsibility. Academic leaders and faculty have also noted that the policy may be too narrow in scope as it pertains to the larger issues of access and affordability of instructional materials. A comprehensive revision of the policy in consultation with stakeholders across Idaho's institutions is underway.

IMPACT

Approval of a temporary waiver of the implementation deadline in Policy III.U. will allow sufficient time to complete a thorough and appropriate revision of the policy. This will also relieve the requirement of institutions to comply with timelines and standards that may come due, but ultimately be removed or revised, during the policy amendment process.

STAFF COMMENTS AND RECOMMENDATIONS

The concerns with this policy were noted by Board staff in early 2020, and work on the amendment process began with conversations with faculty and academic leaders. However, the conversations and amendment processes were put on hold in response to the COVID-19 pandemic. While the deadline for implementing institutional plans is the start of the 2021-2022 academic year, the policy requires that institutions annotate their course catalogs by the time students begin enrolling for fall semester. Students will begin enrolling for fall semester during the spring 2021 semester.

In December 2020, Board staff resumed the policy amendment process by convening interested faculty and other academic leaders from across the state in a working group. This policy working group will develop a proposed policy amendment to be reviewed by the Council on Academic Affairs and Programs (CAAP) and the Instruction, Research and Student Affairs committee. Staff are targeting a first reading by the full Board in April 2021.

In the meantime, given the imminent deadlines provided in Board Policy III.U and the delay in revision due to the pandemic, the CAAP recommends that the Board temporarily waive the implementation deadline in Policy III.U for one year.

Board staff recognize that developing this policy amendment through a collaborative process with the stakeholders responsible for implementation is the best way to ensure intended long-term policy outcomes.

Board Staff recommends approval of the policy waiver.

BOARD ACTION

I move to waive the fall 2021 implementation deadline in Board Policy III.U. Textbook and Instructional Material Affordability, subsection 2.a., for one year.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

BOISE STATE UNIVERSITY

SUBJECT

Online Graduate Certificates in Analyst and Threat Intelligence, Resilience Engineering, and Governance Policy Administration

APPLICABLE STATUTE, RULE, OR POLICY

Idaho State Board of Education Governing Policies & Procedures, Section III.G. and Section V.R.

BACKGROUND/DISCUSSION

Boise State University (BSU) proposes to create three 9-credit Graduate Certificates in Analyst and Threat Intelligence, Resilience Engineering, and Governance and Policy Administration that will be offered wholly online. The program will operate under the guidelines of Board Policy V.R. as it pertains to wholly online programs. The graduate certificates will be a part of the Cyber Operations and Resilience (CORe) program at BSU. The graduate certificates offer complementary technical and non-technical tracks leading to a master's degree. The unique scaffolding (contribution to a stackable master's degree in CORe) of this program, along with the emerging importance of cyber and physical resilience, prepares students with the knowledge, skills, and expertise needed for maintaining the operational effectiveness of complex business, academic, and government information and physical systems. The program is ideal for students who have a professional, military, or law enforcement background that seek to advance their career within the cyber workforce.

The proposed graduate certificates instruct and produce cybersecurity professionals focused on operational tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. In short, the curriculum in the certificates is about how different aspects of cybersecurity are interrelated and how strengthening the bonds of dependency can lead to a more resilient system/network/society.

Because it is entirely online, the proposed program will enable BSU to reach potential students who need flexibility in their education that result from professional and personal responsibilities. These students may also live in a rural area of Idaho that does not have face-to-face educational opportunities.

IMPACT

The program's size will be scaled to demand for the program, and BSU projects that the total number of enrolled students across all certificates will reach a size of 47 students by the fifth year, graduating approximately 50 students (combined total) per year once the program has reached its target enrollment.

The graduate certificates are intended to be part of a statewide collaboration and initiatives between the higher education institutions in Idaho to meet the growing workforce demand for cyber-related education. Cybersecurity is a multifaceted challenge and these online programs will help fill a gap in Idaho's cybersecurity program offerings. BSU's proposed online graduate certificates focus on early-mid career professionals aspiring to move into leadership roles. These programs will collaborate and coordinate with BSU's new Institute for Pervasive Cybersecurity.

The student fee will be in accordance with the Online Program Fee as defined in Board Policy V.R., 3.a.x. The price-point for this online program fee will be $525 per credit. The total costs for the certificates are as follows:

- Analyst and Threat Intelligence (9 credits): $4,725
- Resilience Engineering (9 credits): $4,725
- Governance Policy Administration (9 credits): $4,725

ATTACHMENTS
Attachment 1 – Proposal for CORe Graduate Certificates
Attachment 2 – Boise State Cybersecurity Curriculum Stack

STAFF COMMENTS AND RECOMMENDATIONS
The proposed graduate certificates will be part of the new Cyber Operations and Resilience program to be considered by the Board under a separate agenda item. The certificates are envisioned to be part of the statewide collaboration between Idaho's eight public postsecondary institutions aimed at meeting the growing workforce demand for cyber-related education. BSU states that the three certificates will serve as stackable, short-term credentials. Additionally, working adults who need to acquire specific skills can enroll in either of the three certificate programs with or without the intent of completing a degree.

BSU anticipates a projected enrollment of 10 students initially, reaching 47 by FY26. These numbers are combined across the three certificates and will be scaled based on demand for each certificate as provided in their program proposal. The following provides a breakdown for each certificate:

- Analyst and Threat Intelligence – 7 initial enrollments in FY22
- Resilience Engineering – 3 initial enrollments in FY22
- Governance Policy Administration – 3 initial enrollments in FY23

Because the certificates will be using the online program fee model, minimum enrollments are based on course registrations, which range from 29.50 to 82.00 annual credits and 1.23 to 3.42 annual FTEs over a five-year period. If enrollments are not met, Boise State University will adjust to reflect actual activity and will be evaluated annually. If the certificate is not fiscally sustainable in the long term, the certificates will be discontinued.

BSU's proposed certificates are consistent with their Service Region Program Responsibilities. At this time, certificates consisting of fewer than 30 credit requirements are not required to be listed on three-year plans. As provided in Board Policy III.Z., no institution has the statewide program responsibility specifically for cybersecurity programs. Additionally, Board Policy III.Z. does not apply to programs for which 90% or more of all activity is required or completed online. Currently, there are no graduate certificates in these areas offered at the other institutions.

Industry support was obtained from Idaho National Laboratory; State of Idaho, Information Technology Services; Ursus Security, LLC; Johnny Security Seed, LLC; and MUFG Union Bank, N.A.

BSU also requests approval to assess an online program fee of $525 per credit for a total program cost of $4,725 for each proposed 9-credit certificate. Based on the information for the online program fee provided in the proposal, staff finds that the criteria have been met for this program.

The proposal completed the program review process and was presented to the Council on Academic Affairs and Programs on February 4, 2021; and to the Committee on Instruction, Research, and Student Affairs and the Business Affairs and Human Resources Committee on February 5, 2021, respectively.

Board staff recommends approval.

BOARD ACTION

I move to approve the request by Boise State University to create three new, online academic programs that will award a Graduate Certificate in Analyst and Threat Intelligence, Resilience Engineering, and Governance Policy Administration as presented in Attachment 1.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

AND

I move to approve the request by Boise State University to charge an online program fee of $525 per credit for each certificate, in conformance with the program budgets submitted to the Board in Attachment 1.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

DocuSign Envelope ID: EB9CFB65-3230-403B-AE22-275CB0B4949E

Institutional Tracking No. _____

Idaho State Board of Education
Proposal for Academic Degree and Certificate Program
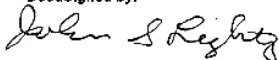
Date of Proposal Submission:	December 2020
Institution Submitting Proposal:	Boise State University
Name of College, School, or Division:	College of Engineering
Name of Department(s) or Area(s):	Electrical and Computer Engineering Department

Official Name of the Programs:	Analyst and Threat Intelligence Graduate Certificate Resilience Engineering Graduate Certificate Governance Policy Administration Graduate Certificate
Implementation Date:	Fall 2021
Degree Information:	Degree Level: Graduate — Degree Type: Graduate Certificate
CIP code (consult IR /Registrar):	43.0404 Cybersecurity Defense Strategy/Policy
Method of Delivery: Indicate percentage of face-to-face, hybrid, distance delivery, etc.	100% Online
Geographical Delivery:	Location(s) Boise — Region(s) III
Indicate (X) if the program is/has: (Consistent with Board Policy V.R.)	Self-Support fee — Professional Fee — X Online Program Fee
Indicate (X) if the program is: (Consistent with Board Policy III.Z.)	Regional Responsibility — Statewide Responsibility

Indicate whether this request is either of the following:

☐ New Degree Programs   ☐ Consolidation of Existing Program

☐ Undergraduate/Graduate Certificates (30 credits or more)   ☐ New Off-Campus Instructional Program

☐ Expansion of Existing Program   ☐ Other (i.e., Contract Program/Collaborative

[signature] 11/24/2020 | 10:04 AM PST			
Date	Vice President for Research (Institution; as applicable)	Date 1//4/21
Dr. Tammi Vacha-Haase 11/25/2020 | 12:11 PM PST			
...ficial Date (Institution: as applicable)	Academic Affairs Program Manager, OSBE	Date
[signature] 12/8/2020 | 3:12 PM MST	_Todd J. Kilburn_	01/15/2021
PVP/Chief Fiscal Officer (Institution) Date	Chief Financial Officer, OSBE	Date
[signature] 12/4/2020 | 12:27 PM PST	_[signature] Bliss_	1/15/21
Instruction (Institution) Date	Chief Academic Officer, OSBE	Date
[signature] 12/15/2020 | 7:58 AM PST		
Date	SBOE/Executive Director Approval	Date
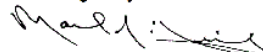
1

> **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. <u>All questions must be answered</u>.

Rationale for Creation or Modification of the Program

1. **Describe the request and give an overview of the changes that will result.** What type of substantive change are you requesting? Will this program be related or tied to other programs on campus? Identify any existing program that this program will replace. If this is an Associate degree, please describe transferability.

   Boise State University proposes the creation of three wholly online graduate certificates programs that will award the following graduate-level certificates:
   - Analyst and Threat Intelligence Certificate
   - Resilience Engineering Certificate
   - Governance Policy Administration Certificate

   The proposed programs will operate under the guidelines of SBOE Policy V.R. as it pertains to wholly online programs.

   The graduate certificates will be a part of the Cyber Operations and Resilience (CORe) program at Boise State University. The graduate certificates offer complementary technical and non-technical tracks leading to a master's degree. The unique scaffolding (contribution to a stackable master's degree) of this program along with the emerging importance of cyber and physical resilience prepares students with the knowledge, skills, and expertise needed for maintaining the operational effectiveness of complex business, academic, and government information and physical systems. The program is ideal for students who have a professional, military, or law enforcement background that seek to advance their career within the cyber workforce.

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

   a. **Workforce and economic need:** Provide verification of state workforce needs that will be met by this program. Include job titles and cite the data source. Describe how the proposed program will stimulate the state economy by advancing the field, providing research results, etc.

   The graduate certificates are intended to be part of a statewide collaboration between eight colleges/universities to meet the growing workforce demand for cyber-related education. Boise State's proposed online graduate program focuses on early-mid career professionals aspiring to move into leadership roles. Most positions listed below either require a master's degree or indicate it is a preferred credential.

   This program is online to accommodate working professionals across Idaho, the western state region, and nation.

   Identifying job titles for the proposed certificates or any cyber operations and resilience program is very difficult and can never encompass all the types of jobs people with a cyber

2

operations and resilience education can pursue. Therefore, we have chosen the following job titles:

- Computer and Information Analysts SOC Code 15-1210
- Information Security Analysts SOC Code 15-1212

2019 National Employment Matrix Title and Code		Employment		Job Openings Due to Growth and Replacement Needs 2019-2029
		2019	**2029**	
Computer and Information Analysts	15-1210	763.4	850.8	87.5
Information Security Analysts	15-1212	131.0	171.9	40.9
TOTAL				**128.4**

2018-2028 Idaho Long Term Employment Projections		Employment		Job Openings Due to Growth and Replacement Needs 2018-2028
		2018	**2028**	
Computer Systems Analyst	15-1121	1,591	1,740	149
Information Security Analysts	15-1122	408	456	48
TOTAL				**197**

b. **Student demand.** What is the most likely source of students who will be expected to enroll (full-time, part-time, outreach, etc.). Provide evidence of student demand/ interest from inside and outside of the institution.

There are three different types of students who will enter these certificates.
- The career advancer who is already employed in the field and is interested in moving up in the field.
- The career starter who is interested in a career that fits his/her personal and professional goals and is currently not employed in the field.
- The career changer who is currently employed in a different field and is interested in changing fields.

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

These certificates serve as stackable, short-term credentials. Working adults who need to acquire specific skills can enroll in a certificate program with or without the intention of completing a degree. This provides an affordable option with curriculum that directly correlates with workforce demand skills, both in Idaho and across the United States.

3. **Program Prioritization**
   Is the proposed new program a result of program prioritization?

Yes_____ No___X__

If yes, how does the proposed program fit within the recommended actions of the most recent program prioritization findings.

N/A

4. **Credit for Prior Learning**
Indicate from the various cross walks where credit for prior learning will be available. If no PLA has been identified for this program, enter 'Not Applicable'.

Not applicable.

5. **Affordability Opportunities**
Describe any program-specific steps taken to maximize affordability, such as: textbook options (e.g., Open Educational Resources), online delivery methods, reduced fees, compressed course scheduling, etc. This question applies to certificates, undergraduate, graduate programs alike.

The program will be offered at a very market competitive rate of $525 per credit hour. The cost for the following certificates are as follows:
- Analyst and Threat Intelligence (9 credits): $4,725
- Resilience Engineering (9 credits): $4,725
- Governance Policy Administration (9 credits): $4,725

The content of the curriculum pushes the boundary of how cyber education is being delivered and will be use cybersecurity working professionals to teach the courses. This curriculum will be offered with asynchronous online mode using a 7-week session that is well suited to working professionals.

Enrollments and Graduates

6. **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 for the most past four years.

Instit.	Program Name	Fall Headcount Enrollment in Program				Number of Graduates From Program (Summer, Fall, Spring)			
		Fall 2017	Fall 2018	Fall 2019	Fall 2020	FY__	FY__	FY__	FY__ (most recent)

7. **Justification for Duplication** (if applicable). If the proposed program is similar to another program offered by an Idaho public higher education 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 duplication as no graduate certificates are offered at the other Idaho public

4

institutions. The proposed graduate certificates instruct and produce Cybersecurity professionals focused on operational tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. In short, the curriculum in the certificates is about how everything is interrelated and how strengthening the bonds of dependency can lead to a more resilient system/network/society.

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

During feasibility it was determined that individual certificate enrollment is unknown. However, for budgetary purposes the following conservative assumptions were made to represent anticipated certificate student behavior:
*   Certificate students make up 50% of the incoming new master's program and certificate students every semester
*   Certificate students are 50% full time (1.5 semesters to complete) and 50% part time (3 semesters to complete)
*   Certificate students only complete one certificate and do not continue on to the Cyber master's degree program.

Proposed Program: Projected Enrollments and Graduates First Five Years											
Program Names: Threat Intelligence Certificate Resilience Engineering Certificate Governance Policy Administration Certificate											
Projected Fall Term Headcount Enrollment in Program						**Projected Annual Number of Graduates From Program**					
F22 (first year)	FY23	FY24	FY25	FY26		FY22 (first year)	FY23	FY24	FY25	FY26	
10	28	36	51	47		4	28	40	44	52	

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

The program's size will be scaled to demand for the program. The numbers in the table above constitute the total combined enrollment across all three graduate certificates, and reflect a reasonable and attainable scaling up of the program.

Marketing and recruitment efforts will include a digital marketing campaign, a web landing page, request for information form and a full program website with details regarding the key program assets, curriculum plan, and costs. In addition, a comprehensive communication plan will be implemented to attract and nurture interested students. Strategic, personalized communications will engage and support students throughout the recruitment life cycle. Our coaching approach to student services will support online students and maintain their connection to Boise State through graduation.

5

Proposed Program: Projected Enrollments and Graduates First Five Years											
Program Name: Analyst and Threat Intelligence Graduate Certificate											
Projected Fall Term Headcount Enrollment in Program						Projected Annual Number of Graduates From Program					
FY22 (first year)	FY23	FY24	FY25	FY26		FY22 (first year)	FY23	FY24	FY25	FY26	
7	16	19	26	24		3	17	21	22	26	

Proposed Program: Projected Enrollments and Graduates First Five Years											
Program Name: Resilience Engineering Graduate Certificate											
Projected Fall Term Headcount Enrollment in Program						Projected Annual Number of Graduates From Program					
FY22 (first year)	FY23	FY24	FY25	FY26		FY22 (first year)	FY23	FY24	FY25	FY26	
3	9	10	15	14		1	10	11	13	15	

Proposed Program: Projected Enrollments and Graduates First Five Years											
Program Name: Governance Policy Administration Graduate Certificate											
Projected Fall Term Headcount Enrollment in Program						Projected Annual Number of Graduates From Program					
FY22 (first year)	FY23	FY24	FY25	FY26		FY22 (first year)	FY23	FY24	FY25	FY26	
0	3	7	10	10		0	1	8	9	11	

10.   **Minimum Enrollments and Graduates.**
    a.   What are the minimums that the program will need to meet in order to be continued, and what is the logical basis for those minimums?

        The numbers below represent the minimum credits and student FTEs for *both* the graduate certificate and the proposed MS in Cyber Operations and Resilience. Since the certificate and master's program share courses, the budgets are intertwined.

        Because the program will be utilizing the online fee model, it is best to put minimum enrollment in terms of course registrations, which are what translate to revenue. Based on estimated expenses for instruction and for support personnel expenses, estimate the minimum number of course registrations to achieve breakeven is:

- Year 1: Annual credits 256, Annual FTEs 10.65
- Year 2: Annual credits 785, Annual FTEs 32.70
- Year 3: Annual credits 1,113, Annual FTEs 46.39
- Year 4: Annual credits 1,336, Annual FTEs 55.65
- Year 5: Annual credits 1,413, Annual FTEs 58.88

        If enrollments do not meet expectations, expenses will adjust to reflect actual activity. The program's financial sustainability will be evaluated at least annually.

    b.   If those minimums are not met, what is the sunset clause by which the program will be considered for discontinuance?

        Programs operating under the online program fee model at Boise State University are expected to be fiscally sustainable. If enrollments do not meet expectations, expenses will be adjusted to reflect actual activity. The program's financial sustainability will be evaluated at least annually. If it is determined to be fiscally unsustainable in the long term, it will be discontinued.

11.   **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 following measures will ensure the high quality of the new program:

Regional Institutional Accreditation: Boise State University is regionally accredited by the Northwest Commission on Colleges and Universities (NWCCU). Regional accreditation of the university has been continuous since initial accreditation was conferred in 1941. Boise State University is currently accredited at all degree levels (A, B, M, D).

Program Development Support: The online certificates are one of several that are being created via the eCampus Expansion Initiative at Boise State University. Boise State's online program development process uses a facilitated program design process to assist program faculty members in the creation of an intentional, cohesive course progression with tightly aligned course and program outcomes. A multi-expert development team, which includes an instructional designer, multimedia specialist, and quality assurance, works collaboratively with the faculty member. One master version of each course is developed for a consistent look and feel of courses across the program; the master course utilizes a professionally created common template aligned with nationally Quality Matters course design standards.

6

Academic Integrity: Academic integrity is vital to the mission of Boise State University and encompasses the totality of academic rigor, ethical behavior, intellectual curiosity, appropriate teamwork, and persistence. All assignments submitted by a student must represent his/her own ideas, concepts, and current understanding or must cite the original source. Boise State proactively supports academic integrity by providing training, maintaining a website dedicated to academic integrity, providing tools such as pedagogical strategies, workshops, and tips for designing tests, as well as establishing policies and procedures for students who violate the academic integrity policy within the Student Code of Conduct. For this new online program, we will use the following strategies to encourage academic integrity:

- During the design and development of the curriculum and assessment of each course, instructors will be informed by staff of Boise State's eCampus Center about best practices for online course design based on Quality Matters ™ and best practice strategies to promote academic integrity in online education based on WCET's recommendations (Version 2.0, June 2009)
- Through the program development process, course production, course launch support provided by the eCampus Center, and other means, instructors will be reminded about the importance of academic integrity and encouraged to report and act upon suspected violations.
- Academic integrity will be addressed within online student orientation. Programs may require online students to complete the university's Academic Integrity Online Workshop.
- At the beginning of each course, the instructor will communicate expectations regarding academic integrity to students in the syllabus and verbally and may require completion of the university's Academic Integrity Online Workshop.

Student Authentication: Because the proposed program will be offered entirely online, it is important to include mechanisms by which we authenticate the identity of students enrolled in the program. We will use the following mechanisms:

- During the admissions process, the university will confirm required official transcripts and other documentation required for admission into the program.
- Associated with access to and use of our Learning Management System, a secure log-in environment will be provided and students will be required to use strong passwords and change them every 90 days.
- When high-stakes exams are required, faculty will be encouraged to utilize remote or online proctoring services when appropriate. In those instances, students will need to provide valid photo identification before gaining access to the graded assessments or other required activities.
- Instructors will utilize Canvas's Turnitin plagiarism detection program when appropriate.
- Instructors are expected to be informed of and aware of the importance of student identity authentication and to report and act upon suspected violations.

12. **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 A**.

    N/A

13. **Teacher Education/Certification Programs** All Educator Preparation programs that lead to certification require review and recommendation from the Professional Standards Commission (PSC) <u>prior</u> to consideration and approval of the program by the State Board of Education.

    Will this program lead to certification?

7

Yes_____ No__X___

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

14.   **Three-Year Plan: If this is a new proposed program, is it on your institution's approved 3-year plan?**

Yes __X__   No _____

If yes, proceed to question 15. If no:

a. **Which of the following statements address the reason for adding this program outside of the regular three-year planning process.**

Indicate (X) by each applicable statement:

	Program is important for meeting your institution's regional or statewide program responsibilities.
	The program is in response to a specific industry need or workforce opportunity.
	The program is reliant on external funding (grants, donations) with a deadline for acceptance of funding.
	There is a contractual obligation or partnership opportunity related to this program.
	The program is in response to accreditation requirements or recommendations.
	The program is in response to recent changes to teacher certification/endorsement requirements.

b. **Provide an explanation for all statements you selected.**

Educational Offerings: Curriculum, Intended Learning Outcomes, and Assessment Plan

15.   **Curriculum. Provide descriptive information of the educational offering.**

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

Analyst and Threat Intelligence Certificate

Credit hours in required courses offered by the department (s) offering the program.	9
Credit hours in required courses offered by other departments:	0
Credit hours in institutional general education curriculum	0
Credit hours in free electives	0
Total credit hours required for degree program:	9

Resilience Engineering Certificate

Credit hours in required courses offered by the department (s) offering the program.	9
Credit hours in required courses offered by other	0

8

departments:	
Credit hours in institutional general education curriculum	0
Credit hours in free electives	0
Total credit hours required for degree program:	9

Governance Policy Administration Certificate

Credit hours in required courses offered by the department (s) offering the program.	9
Credit hours in required courses offered by other departments:	0
Credit hours in institutional general education curriculum	0
Credit hours in free electives	0
Total credit hours required for degree program:	9

b. Curriculum. Provide the curriculum for the program, including credits to completion, courses by title and assigned academic credit granted.

Analyst and Threat Intelligence Certificate (Online)	
Course Number and Title	**Credits**
CORE 550 Cyber Threat Intelligence	3
CORE 551 Cyber Warfare and Conflicts	3
CORE 552 Cyber Digital and Signal Intelligence	3
TOTAL	**9**

Resilience Engineering Certificate (Online)	
Course Number and Title	**Credits**
CORE 560 Cyber Resilience Systems Design	3
CORE 561 Network Design and Exploitation Techniques	3

9

CORE 562 Resilience Coding and Architecture of Devices	3
TOTAL	**9**

Governance Policy Administration Certificate (Online)	
Course Number and Title	**Credits**
CORE 570 Cyber Risk Management	3
CORE 571 Cyber Law, Ethics, and Policy	3
CORE 572 Cybersecurity Governance and Compliance	3
TOTAL	**9**

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.

N/A

16. **Learning Outcomes: Expected Student 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 students will know, understand, and be able to do, and value or appreciate as a result of completing the program.

The following are six Program Learning Outcomes for the M.S. in Cyber Operations and Resilience degree:

PLO 1: Properly apply the correct fundamentals of cyber operations, resilience, risk assessment, and information assurance to both cyber-physical and information systems.

PLO 2: Make decisions based on the ethics, laws, policies, and governance of the cyber security field.

PLO 3: Apply acceptable tactics, techniques, and procedures necessary to enhance cyber-physical and informational security operations and resiliency.

PLO 4: Apply industry acceptable cyber security model to secure, inform, involve, and educate stakeholders in security/resilience operations and strategies.

PLO 5: Continuously evaluate and monitor the operational and resilient maturity of an entity.

PLO 6: Develop operation and resiliency policies, metrics, testing and security solutions for an entity using both rigorous risk assessment and threat intelligence people, processes, tools and measures.

Each certificate contributes to the learning outcomes in different ways.

Analyst and Threat Intelligence Certificate
- Contributes to all PLO's with a particular focus on PLO 1, PLO 3, PLO 4, and PLO 6.

Resilience Engineering Certificate
- Contributes to all PLO's with a particular focus on PLO 1, PLO 3, PLO 4, and PLO 5.

Governance Policy Administration Certificate
- Contributes to all PLO's with a particular focus on PLO 2, PLO 4, and PLO 6.

17. **Assessment plans.**

   a. **Assessment Process.** Describe the assessment plan for student learning outcomes that will be used to evaluate student achievement and how the results will be used to improve the program.

   The proposed certificates will follow a systematic assessment and improvement process in which multiple approaches will be used, not only to measure student attainment of program outcomes, but to also inform programmatic improvements. The learning outcomes are mapped to courses that provide relevant content. Student work in these courses that address specific outcomes is collected and evaluated by program faculty. The outcomes are assessed on a three-year cycle with data for all outcomes collected each year, and then the results are analyzed every three years. For each outcome, student work across the program is reviewed in a comprehensive review of student work. A group of three faculty members and instructors review the overall attainment of the outcome based on the evidence collected. As part of the review, recommendations for improvement to the program are outlined. All faculty then review these results and make suggestions/changes to improve this process in a program of continuous improvement. Evaluation results inform programmatic, pedagogical, and curricular improvements.

   The key knowledge unit as defined by the National Initiative for Cyber Security Education (NICE) Cybersecurity Workforce Framework, NSA CAE, and UK Cyber Security Body of Knowledge (CyBok) will also be mapped to all the courses. This will ensure the graduate certificate programs are teaching the most important skill sets and critical thinking.

Resources Required for Implementation – fiscal impact and budget.
Organizational arrangements required within the institution to accommodate the change including administrative, staff, and faculty hires, facilities, student services, library; etc.

11

DocuSign Envelope ID: EB9CFB65-3230-403B-AE22-275CB0B4949E

18.   **Physical Facilities and Equipment:** Describe the provision for physical facilities and equipment.

    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 available space and equipment are currently acceptable to operate a successful program.

    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?

       No impact.

    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.

       Operating expenses associated with support staff and new faculty are reflected in the budget.

19.   **Library and Information Resources:** Describe adequacy and availability of library and information 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.

       Online resources are available. No impact on existing programs.

    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 needed. No impact on the library.

20. **Faculty/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?

       The numbers below represent instruction credits and instruction FTEs for both graduate certificate and master's students. Since the certificate and master's programs share courses, their budgets are intertwined.

       The program will fund new adjunct/lecturer instruction to cover the additional

12

instruction credits required by the program:

> Yr 1- 29.50 instruction credits, 1.23 FTE
> Yr 2- 66.50 instruction credits, 2.77 FTE
> Yr 3- 82.00 instruction credits, 3.42 FTE
> Yr 4- 82.00 instruction credits, 3.42 FTE
> Yr 5- 82.00 instruction credits, 3.42 FTE

At maturity, the graduate certificate programs with the master's program will offer a combined total of 40 sections of new courses of which 18 sections will be in cross listed courses with the proposed Bachelor of Science in Cyber Operations and Resilience.

The certificate and master's program will fund a 0.50 FTE program coordinator in years 1, 2 & 3 and convert to a 1.00 FTE program coordinator starting year 4. The certificate and master's program will fund a 0.25 FTE administrative assistant in years 2 & 3 and convert to a 0.50 FTE administrative assistant starting year 4.

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.

Over the first 4 years, the certificate and master's programs will fund partial FTEs of Dr. Sin Ming Loo, a current professor in the Department of Electrical and Computer Engineering.

> Yr 1- 0.10 FTE
>
> Yr 2- 0.10 FTE
>
> Yr 3- 0.08 FTE
>
> Yr 4- 0.05 FTE

Dr. Sin Ming Loo will provide course content and work with the program coordinator to oversee the programs.

c. **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?

Because the graduate certificate programs will fund instruction and administrative support, it is anticipated that limited instructional and administrative support resources from existing programs will be used for the proposed program. There will be a minimal impact on resources available for existing programs.

d. **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.

The following positions will be hired for the graduate certificate programs:
- o   Adjunct Instruction
- o   Program Coordinator
- o   Administrative Assistant

Expenses for these positions are included in the program budget sheet.

13

21. **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?

N/A

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.

No new appropriation will be required.

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?

   The 0.50 FTE certificate and master's Program Coordinator will be funded for one year (January 2021-December 2021) by the Boise State Online Innovation Fund. This fund is funded by online fee revenue and acts as seed funding for online academic programs, online course development stipends to faculty, open education resource grants and eventually innovation grants.

   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?

   N/A

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.

   N/A

   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.

   The student fee will be in accordance with the Online Program Fee as defined in the Board Policy V.R., 3.a.x. That policy enables the institution to set a price-point appropriate for the program; students will pay an online program fee in lieu of tuition. The price-point for our online program fee will be as follows: $525 per credit.
   The cost for the following certificates are as follows:

   o   Analyst and Threat Intelligence (9 credits): $4,725
   o   Resilience Engineering (9 credits): $4,725
   o   Governance Policy Administration (9 credits): $4,725

22. Using the excel budget template provided by the Office of the State Board of Education, provide

14

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).

The budget below represents revenues and expenses for both certificate and master's programs. Since the certificate and master's program share courses, the instruction and support expenses are intertwined.

15

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
- 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).

I. PLANNED STUDENT ENROLLMENT

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	FTE	Headcount	FTE	Headcount	FTE	Headcount	FTE	Headcount	FTE	Headcount
A. New enrollments	9.6	32	33.3	71	51.0	108	67.0	136	74.9	147
B. Shifting enrollments	1.1	4	3.7	8	5.7	12	7.4	15	8.3	16
Total Enrollment	10.7	36	37.0	79	56.6	120	74.5	151	83.2	163
Student Credit Hours Generated	256		889		1,359		1,787		1,997	

16

II. REVENUE

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
1. New Appropriated Funding Request										
2. Institution Funds		$44,978								
3. Federal										
4. New Tuition Revenues from Increased Enrollments										
5. Student Fees		$134,269		$466,548		$713,631		$938,231		$1,081,671
6. Other (i.e., Gifts)										
Total Revenue	$0	$179,247	$0	$466,548	$0	$713,631	$0	$938,231	$0	$1,081,671

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.

Budget Notes:

I.A, B. Calculation of FTE and headcount as follows:
>1 FTE = 24 graduate credits
>Headcount determined as the distinct number of students in the program that year.
>Assume that 90% of the enrollments will be new enrollments and 10% will be shifting enrollments.
>Assume 20% attrition from 1st to 2nd semester, then 3% attrition every semester. No attrition from 2nd to last semester to last semester.

II.2. The University will sponsor the program coordinator for 1 year using funds from the Boise State Online Innovation Fund

II.5. Student Fee revenue calculated as Student Credit Hours * $525 per credit.
>$525 calculated as estimate of 2021-2022 per-credit
>$525 per-credit
>To be conservative, assume in calculations that per-credit fee does not increase over time

17

III. EXPENDITURES

A. Personnel Costs

	FY 2022 On-going	FY 2022 One-time	FY 2023 On-going	FY 2023 One-time	FY 2024 On-going	FY 2024 One-time	FY 2025 On-going	FY 2025 One-time	FY 2026 On-going	FY 2026 One-time
1. FTE		1.98		3.52		4.67		4.92		4.92
2. Faculty		$0		$0		$0		$0		$66,967
3. Adjunct Faculty		$50,150		$116,442		$162,180		$174,182		$139,944
4. Graduate/Undergrad Assistants										
5. Research Personnel										
6. Directors/Administrators		$60,550		$45,275		$78,398		$76,927		$73,158
7. Administrative Support Personnel				$8,498		$8,752		$18,030		$18,571
8. Fringe Benefits		$26,811		$31,483		$48,027		$53,370		$73,905
9. Other:										
Total Personnel and Costs	$0	$137,510	$0	$201,697	$0	$297,358	$0	$322,509	$0	$372,545

Budget Notes (continued)
III.A.2 Lecturer FTE: Calculated using (Credit hour load)/24
III.A.3 Adjunct FTE: Calculated using (Credit hour load)/24
III.A.6 Administrator: Program Coordinator (0.5 FTE in years 1,2,3, 1.0 FTE in years 4+). Additional expense included in year 1 to reflect anticipated Jan 2021 start date. Institutional funds will fund position Jan-Dec 2021
III.A.7 Administrative Support: Administrative Assistant (0.25 FTE in years 2 & 3, 0.50 FTE in years 4+)
III.A.8 Benefits calculated at staff fringe rate of $11,650+(annual wage*20.47%) professional staff and $11,650+(annual wage*21.57%) classified staff

B. Operating Expenditures	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	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										
5. Materials and Supplies										
6. Rentals										
7. Materials & Goods for Manufacture & Resale										
8. Miscellaneous - Computer Hardware/Software		$500		$500		$500		$1,000		$2,000
Total Operating Expenditures	$0	$500	$0	$500	$0	$500	$0	$1,000	$0	$2,000

Budget Notes (continued):
III.B.8   Miscellaneous: Computer hardware/software

19

DocuSign Envelope ID: EB9CFB65-3230-403B-AE22-275CB0B4949E

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
C. Capital Outlay										
1. Library Resources										
2. Equipment										
Total Capital Outlay	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
D. Capital Facilities Construction or Major Renovation										
E. Other Costs										
1. Boise State University Support		$67,134		$233,274		$356,815		$469,115		$540,835
Utilities										
Maintenance & Repairs										
Other										
Total Other Costs	$0	$67,134	$0	$233,274	$0	$356,815	$0	$469,115	$0	$540,835
TOTAL EXPENDITURES:	$0	$205,145	$0	$435,471	$0	$654,673	$0	$792,625	$0	$915,380
Net Income (Deficit) to College	$0	-$25,898	$0	$31,077	$0	$58,958	$0	$145,606	$0	$166,291

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

III.E.1   Boise State University Support is defined as follows:

Boise State Central Services (10.00% of revenue): A fund dedicated to funding support services for online students.

Boise State eCampus Center (8.75% of revenue): Provide funding for initiative management, online course/program development and other support services

Boise State Online Innovation Fund (3.80% of revenue): Seed funding for academic programs, course development stipends to faculty, open education resource grants and eventually innovation grants

Boise State Online Marketing, Recruitment, Enrollment, Advising and Retention Fund (27.45% of revenue): A fund dedicated to marketing the program, recruiting students, enrolling qualified students, advising students and retaining students throughout the life of the program

APPENDIX B- LETTERS OF SUPPORT

Idaho National Laboratory – Scott Cramer, Director Cybercore Integration Center

State of Idaho, Information Technology Services – Keith Tresh, Chief Information Security Officer

Ursus Security, LLC – Kim L. Jones, Founder and Managing Director

Johnny Security Seed, LLC – Richard W. Owen, CEO and Chief Evangelist

MUFG Union Bank, N.A. – Stanley R. Jarocki, Vice President

21

Idaho National Laboratory **INL**

October 13, 2020　　　　　　　　　　　　　　　　　　CCN 248073

Idaho State Board of Education
650 West State St.
Suite 307
Boise, ID 83720

Subject: Letter of Support Regarding Boise State Course Offerings in Cyber Operations and Resilience

Dear Board Members,

As part of our continued collaboration with Boise State University (BSU) and in support of the Cybercore Integration Center (CIC) mission at Idaho National Laboratory (INL), this letter expresses our strong endorsement of the proposed Cyber Operations and Resilience course offerings.

INL is a world leader in research and technologies for securing and protecting the critical infrastructure of the United States and is focused on fundamental challenges with greatest impact. Building on the current success of BSU and CIC collaborations, these competency-based learning models will help to reach additional students while addressing outstanding needs in the current workforce.

INL has been observing the cybersecurity security curriculum development across the state of Idaho. University of Idaho offers a BS in Cybersecurity, a degree focused on computer science and programming. Idaho State University is now offering a BAS in Cyber-Physical Systems Engineering Technology, concentrated on industrial cybersecurity. There is another identified need for cyber operations, which targets frontline workers who continually face security concerns and address challenges across the enterprise. We are delighted that BSU has taken the appropriate steps to address this gap, at both the BS and MS level, and are prepared to make course offerings available as soon as next fall.

The fact that the courses will be available as an asynchronous online program, opens the instruction to much broader audiences across the state and affords full-time workers and remote learners the ability to build skills outside of the traditional classroom setting. This progressive and flexible platform offers broad reach and greater access to a variety of students, from diverse backgrounds and skill sets, to advance education and workforce development efforts necessary to meet cybersecurity needs now, and in the future.

In short, we see these programs as beneficial to industry, local governments, counties, and state entities in training cybersecurity frontline workers to protect and defend, enhance critical thinking skills and provide more resilience within our cyber environments, which addresses elements currently in short supply and which will only grow in demand. Increasing the number

of people capable of cyber operations and accelerating their development, is core to our mission and vital to both our state and the nation.

We applaud BSU efforts and continued contributions in supporting the Idaho cyber-education ecosystem and willingness to advance offerings designed to provide access to a wide range of students, while addressing identified needs is the workforce.

We believe these efforts will be of benefit to the community, the state and the region, as well as INL, and strongly support the proposed offerings being put into practice and made available.

Sincerely,

Scott Cramer, Director Cybercore Integration Center
National & Homeland Security

SC:KL

Distribution:
Sin Ming Loo, Boise State University

cc: Z.D. Tudor, MS 3750
        W.C. Kiestler, MS 3750
        S.F. McAraw, MS 1444
        E.J. Taylor, MS 1444
        M.T. Bingham, MS 3605

23

State of Idaho

Information Technology Services
Office of the Governor

BRAD LITTLE
Governor
JEFF WEAK
Administrator
GREG ZICKAU
Deputy Administrator/
Chief Information Officer

11331 W. Chinden Blvd, Suite B201
P.O. Box 83720
Boise, ID 83720-0042
Telephone (208) 605-4000 or FAX (208) 605-4093
http://its.idaho.gov

September 23, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear Board Members,

I am writing this letter in support of Boise State University's proposed Bachelor of Science and Master of Science Degree in Cyber Operations and Resilience (CORe).

Given the importance of cybersecurity in every aspect of modern life and the shortage of trained cybersecurity professionals nationwide, this program and the graduates it produces will benefit the public and private sectors inside Idaho and the nation a whole. The proposed Cyber Operations and Resilience programs will build a pathway for professionals to change careers and help existing cybersecurity professionals deepen their expertise. This program will also help cybersecurity professionals progress into management level positions and will feed some of the PhD programs statewide if these same professionals choose to continue their education by pursuing a doctorate degree.

Boise State University already offers a Bachelor of Science in Computer Science with a Cybersecurity emphasis and a PhD in Computing with Cybersecurity emphasis, so these proposed programs fill a missing level that would be attractive to many potential students. Idaho employers need multiple universities inside our state to offer programs that specialize in all aspects of cybersecurity to satisfy the demand and need for trained cybersecurity professionals. To that end, Boise State University is participating in conversations within our state to codify an agreement for all major universities to share courses, curriculum and resources within the cybersecurity area of concentration.

I also want to highlight the fact that Boise State University hired several faculty members with operational cybersecurity experience in the last five years. They have also worked hard to seek and maintain many key industry/government relationships within the cybersecurity field including the State of Idaho, Information Technology Services as well as the Idaho National Lab.

As an example, and a matter of fact, I was hired in August of 2019 to teach in their current baccalaureate program. I also participate in all of their Cybersecurity planning and sit on the Board of Boise State's up-and-coming Institute for Pervasive Cybersecurity.

In closing, I would like to add that as a public servant with over 25 years of information technology and cybersecurity operational experience, I feel these programs can and will dramatically increase the available number of trained cybersecurity professionals within Idaho and nationwide. I wholeheartedly support the creation and implementation of both the Bachelor of Science and Master of Science degrees in Cyber Operations and Resilience!

If you have questions or need more information, please feel free to contact me at (208) 605-4054 or keith.tresh@its.idaho.gov.

Sincerely,

Keith Tresh
Chief Information Security Officer
Office of Information Technology Services
Office of the Governor
Keith.Tresh@its.idaho.gov
Office: (208) 605-4054
Cell: (208) 407-8509

25

Ursus Security LLC
"Standing in the Gap"

October 8th, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Esteemed Board Members:

I am writing this letter to express my strongest possible support for Boise State University's Cyber Operations and Resilience (CORe) degree programs.

As a senior cybersecurity profession and former senior cyber executive, I have long struggled with the challenge of finding skilled professionals to fill the ranks of my supported organizations. As the cyber talent gap widened and universities took up the call for support, I was disappointed at the caliber of students produced by our institutes of higher learning. In far too many cases "cyber graduates" had only theoretical knowledge of cybersecurity principles across a narrow portion of the career field; they were inadequately prepared to face the fluid (and often non-standard) real-world dilemmas faced by today's cyber warriors.

When I was asked to evaluate Boise State University's CORe program and approach, I entered the process with a high degree of skepticism. I am pleased to say that I left the process more excited and impressed than I have been with a university-led program in a long time. Boise State's curricula (at both the Bachelors and Masters levels) remains entrenched in a real world, practical approach which prepares students to meet the challenges of a cybersecurity career head on. Further, the modular approach is extremely well suited for those looking to transition careers – something which must be embraced if we are ever to close the cyber job-talent gap. Boise State's commitment to hiring top tier cyber talent – including senior cyber executives and not just educational professionals – gives me an extremely high degree of confidence around the caliber of graduates these programs will produce. I look forward to introducing Boise State's first crop of graduates into the companies I advise and support.

Boise State University is to be commended for taking a proactive, thought-leading approach to solving one of our nation's most vexing problems. I urge you to support these efforts wholeheartedly.

26

Ursus Security LLC
"Standing in the Gap"

Please feel free to contact me if you have questions.

Sincerely,

Kim L. Jones CISM, CISSP, CDGSE, M.Sc.
Founder and Managing Director
Ursus Security LLC
(480) 253-9120
Kim.Jones@UrsusWorldwide.com
https://www.linkedin.com/in/kimjones-cism/

DocuSign Envelope ID: EB9CFB65-3230-403B-AE22-275CB0B4949E

Johnny Security Seed, LLC.
4412 E la Estancia Cir
Cave Creek, AZ 85331
www.JohnnySecuritySeed.com

September 30, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear Board Members,

I am writing this letter in support of Boise State University's Bachelor of Science (BS) and Master of Science (MS) Degree programs in Cyber Operations and Resiliency (CORe). I understand that Boise State and other universities offer degrees in Computer Science with an emphasis in Cyber Security, but Cyber Security can no longer be just an extra area of study.

In today's world we continue to collect, process and store more information and base many decisions on this ever-growing collection of data. This simply adds greater importance and risk to those systems and data. However, we have a nation-wide shortage of skilled and educated people who can provide the protection that we require. The Cybersecurity Industry is in a need of not only more qualified people, but those who are trained to think and address rapidly changing threats.

I applaud Boise State University for creating programs that start first with the high school student. Johnny Security Seed has a similar effort and approach. As one who has significant technical training and many certifications stacked on top of my formal college education, I have found that the combination has been a key element in my success. I see these programs as vital to creating professionals who can address ever-changing operational issues to ensure the resiliency of critical data and systems. I also support the program's experiential learning credit approach. Hackers follow no formal education road map and to respond we need to create a workforce capable of accomplishing the mission, oftentimes in a less structured fashion. I believe that the proposed curriculums would provide my current and prior businesses a more capable employee to help in this ongoing fight.

As a point of reference, I have spent over 50 years protecting information of which over 30 years was focused on creating and managing cyber security programs. I created the Information Security Program for Mission Operations at Johnson Space Center, NASA. While there, I was awarded a "Silver Snoopy" by the astronauts for the program and a Continuous Improvement Award by the NASA Administrator for avoiding over $25M in costs. After that, I created four other very successful security programs across various industries. I am a past International President of the Information Systems Security Association (ISSA) and a member of the Information Security Hall of Fame. Most recently I was honored with Fellow status of the world renowned Ponemom Institute (https://www.ponemon.org).

Should you have any questions of if I may be of other assistance, I can be contacted at Rich@JohnnySecuritySeed.com or on my cell at 480-686-5527.

28

Sincerely,

Richard W. Owen, Jr.
CEO and Chief Evangelist

29

◉ MUFG

MUFG Union Bank, N.A.
Information Risk Management
Risk Management Division for the
Americas
6802 E Bobwhite Way
Scottsdale, AZ 85266
T: +1-480-381-0887

Stanley.Jarocki@unionbank.com

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear State Board Members:

I am writing this letter in full support of the proposed Cybersecurity Bachelor and Master programs at Boise State. These programs incorporate fundamental aspects of Cybersecurity that are needed to maintain a key core element – Cyber Operations and Resiliency – that are so desperately needed and which require trained individuals to cover all critical infrastructure sectors today and in the future.

Today, as a veteran of many attacks that I have experienced in the Federal Government sector, the critical infrastructure sectors – financial, healthcare, retail – and having lived through 911 at ground zero, I speak from experience. Cyber resources that drive the systems of our environment must be secure, auditable, compliant, and resilient. Knowledgeable talent is needed at the entry level and senior executive level to promote the proper planning, testing and execution to keep these systems running. Just imagine what would happen if hospital cyber system went down and doctors, nurses and staff had to resort to pen and pencil. Today in the time of the pandemic huge numbers of lives would be lost, treatment would have to stop and those needing care would not be able to get it. And it could be your family members or yourself. Sounds farfetched? Well, it is happening as they are being attacked not only by natural disasters but by Bad Actors using Ransomware, DDoS attacks and other extortion attempts. Cyber is the nervous system, communications paths, and knowledge repositories upon which our lives are built and depend. Therefore, the need for Cyber professionals and cyber warriors to support and build strong infrastructure is needed. Where are they going to get this knowledge? They will be able to get this critical knowledge base from Boise State's Bachelor and Master's programs in Cyber Operations and Resiliency.

The key to these powerful new programs - the Cyber Operations and Resilience (CORe) Bachelor of Science (BS) and Master of Science (MS) programs – lies in their ability to develop focused curriculum that provide needed skill sets that they can use day one. These programs are geared to instruct and produce Cybersecurity professionals focused on operational tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. The goal of the CORe curriculums is to prepare learners at the beginning levels to view and think of systems as holistic models while determining how resiliency can be achieved. CORe presents the interdependencies infrastructure has between cyber and physical to achieve operational effectiveness. In short, CORe is about business, real life and the world of cybersecurity and their interrelationships and how strengthening the bonds of dependency can lead to a more robust and resilient system/network/society.

A holistic system level thinking approach is at the heart of the CORe program. The asynchronous online curriculum provides for a challenging set of achievement modalities:

30

1. Pathways for high school students (traditional and career & technical education), community college graduates, and working professionals with an undergraduate degree in any field,
2. Stackable certification pathways for learners to achieve career alignment without the need for long-term program commitments,
3. A curriculum that awards experiential learning credits in an affordable manner,
4. A potential for strong internship with local and national industries and critical infrastructure sectors, and
5. Accelerated BS/MS curriculum for learners looking to achieve maximum career opportunity in the shortest time frame possible.

As an early practitioner in the field of Cybersecurity I had to boot strap my knowledge with a lot of "OJT" (On the Job Training) to get the job done. Adding needed skills such as audit, risk management and executive leadership was not easy. Holding CISO positions in a variety of industries and major companies in the financial, healthcare and retail sectors. - I can attest that finding individuals with these skills is extremely hard. Nationally, there is estimated to be over 3 million job openings creating a dire shortage of talent. This is exasperated even more due to the increased attacks by bad actors and nation states who feel we are too preoccupied with the "Pandemic." Trained people are desperately needed with practical operational skills who can contribute day one.

As the editor / contributor of the USA National Security Plan for the financial sector and chief architect of the Financial Services Information Sharing and Analysis Center and presently as a VP of Information Risk Management for the 5th largest bank in the World – MUFG – I can attest that quality trained talent is desperately needed. Additionally, as an advisor to higher education intern programs, it is extremely important that Cybersecurity needs to start with K-12 to show that diversity and excitement does exist in the world of Cybersecurity. I believe the curriculum that I have reviewed is the right start in our battle to cultivate passionate and talented individuals who will be practically trained to jump in and defend the cyber world of today and, more importantly, tomorrow.

I also believe local Boise Headquartered companies such as Albertsons is another example of an organization that requires cybersecurity and resiliency as we have observed in recent disasters and the Pandemic. Food supplies are critical and the supply chain systems that support operations and get the goods to the stores and people is critical to humanity's survival.

So it is extremely important that support for the ability to produce learners with the caliber of talent needed for the state of Idaho, the nation, and worldwide, be provided at the highest level of state government – through the governor's office, and through approval of these programs through the state board of education.

Sincerely,

Stanley R. Jarocki

Vice President

Cybersecurity Education Opportunities
Fall 2021 and Beyond

Knowledge

PhD in Computing, Cybersecurity Emphasis - Now / In-person

*MS, Cyber Operations & Resilience - Fall 2021 / Online
*MS, Cybersecurity - Fall 2021 / In-person

Certificate in Cryptography and Cryptanalysis - Fall 2021 / Online

BS, Computer Science w/ Cybersecurity Emphasis - Now / In-person

*BS, Cyber Operations & Resilience - Fall 2021 / Online
BS, Computer Systems Engineering - Fall 2021 / In-person

Cybersecurity Minor - Now / In-person

Four Cyber/Physical Certificates for STEM Students - Now / Hybrid
(Power, Process, Software, Hardware)

Cryptography and Cryptanalysis Certificate - Fall 2021 / Online

Cyber Operations Certificate and Certification - Now / Online

Cybersecurity For All Certificate - Now / Online

Legend:
- Graduate Degrees
- Graduate Certs
- Undergrad Minors or Degrees
- Undergrad Certs
- Certifications

*Under Review. Forthcoming subject to the Board approval.

IRSA

Student Involvement (not to scale)

TAB 5 Page 1

BOISE STATE UNIVERSITY

SUBJECT
Online Bachelor of Science and Master of Science in Cyber Operations and Resilience

APPLICABLE STATUTE, RULE, OR POLICY
Idaho State Board of Education Governing Policies & Procedures, Section III.G. and Section V.R.

BACKGROUND/DISCUSSION
Boise State University (BSU) proposes to create a Bachelor of Science and a Master of Science in Cyber Operations and Resilience (CORe) program that will be offered wholly online. These programs will operate under the guidelines of Board Policy V.R. as it pertains to wholly online programs.

CORe programs are designed around the realities of today's cyber and physical landscape: It's not *if* a security (cyber and/or physical and/or interdependencies) breach will occur, it's a matter of *when*. A resilient system will be able to be restored in a timely and orderly fashion. Businesses, while maintaining a secure posture, are investing in people, processes, and technology to ensure operational continuity under adverse conditions, such as from cyber-attacks, physical attacks, insider threats, malfunctioning equipment/software, or failure of infrastructures. The proposed programs will prepare students to anticipate, detect, mitigate, and manage cyber, physical, and interdependencies infrastructure threats.

The unique scaffolding of these programs (which are designed as a stackable degree program both at the undergraduate and graduate levels, along with the emerging importance of cyber and physical resilience) prepares students with the knowledge, skills, and expertise needed for maintaining the operational effectiveness of complex business, academic, and government information and physical systems. The Bachelor's degree program utilizes and stacks existing undergraduate certificates, including Cyber Physical Systems (as optional electives) and Cyber Operations (required) into the degree plan. Moreover, the degree has the flexibility for students to stack related industry certifications, existing minor and certificates, and dual-listed courses, prior learning, internships, and experiential learning. The MS in CORe is a stackable Master's degree program that offers graduate certificates with complementary technical and non-technical tracks leading to a master's degree. The program is ideal for students who have a professional, military, or law enforcement background that seek to advance their career within the cyber workforce.

Because they are entirely online, the proposed programs will enable BSU to reach potential students who need flexibility in their education that result from

professional and personal responsibilities. These students may also live in a rural area of Idaho that do not have face-to-face educational opportunities.

IMPACT

The proposed CORe degree programs are intended to be a part of the statewide cybersecurity initiatives and the collaboration between the Idaho's higher education institutions to meet the growing workforce demand for cyber-related education. Cybersecurity is a multifaceted challenge and these online programs will help fill a gap in Idaho's cybersecurity program offerings. They are designed to prepare learners to think in systems about how resilience can be achieved. These programs will collaborate and coordinate with BSU's new Institute for Pervasive Cybersecurity. The unique and flexible scaffolding of these programs will allow them to be part of joint programming opportunities in cybersecurity education in Idaho.

BSU projects that the Bachelor's CORe program will reach a size of 116 students by the fifth year, graduating approximately 47 students per year once the program is up and running. BSU projects that the master's program will reach a size of approximately 100 students by the fifth year, graduating approximately 39 students per year once the program is up and running. Both programs are scalable to meet the demand for the program.

The proposed Bachelor's program is different from Idaho State University's undergraduate Cyber-Physical System Engineering Technology program and the University of Idaho's undergraduate Cybersecurity program because the proposed program instructs and produces cybersecurity professionals focused on operational thinking, tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. There is no duplication at the master's level, as no Idaho public institution offers a similar program. The proposed MS in CORe program concentrates on cybersecurity people, process, and technology.

The student fees will be in accordance with the Online Program Fee as defined in Board Policy V.R., 3.a.x. The price-point for the online BS CORe program fee will be $350 per credit. For the 120 credits required for completion of the proposed program, the total cost will be $42,000. The price-point for the online MS CORe program fee will be $525 per credit. For the 30 credits required for completion of the proposed program, the total cost will be $15,750.

ATTACHMENTS

Attachment 1- Proposal for Bachelor of Science in Cyber Operations and Resilience
Attachment 2- Proposal for Master of Science in Cyber Operations and Resilience
Attachment 3- Boise State University Cybersecurity Curriculum Stack

STAFF COMMENTS AND RECOMMENDATIONS

Boise State University anticipates 20 enrollments initially reaching 116 by FY26 for the Bachelor's program and anticipates 10 enrollments for the Master's program

initially reaching 107 by FY26. The program will be scaled based on demand for the degree offerings as provided in their program proposal. Because the program will be using the online program fee model, minimum enrollments are based on course registrations, which range from 405 to 1,876 annual credits and 13.50 to 62.53 annual FTEs (BS program) and 256 to 1,413 annual credits and 10.65 to 58.88 annual FTEs (MS program) over a five-year period. If enrollments are not met, BSU will adjust to reflect actual activity and will be evaluated annually. If in the long term it is not fiscally sustainable, the program will be discontinued.

While the proposed program is currently not listed on BSU's approved three-year plan, it was included in their draft plan submitted in 2020. Due to the pandemic, program planning was postponed last academic year. Draft plans were in progress and were shared with the Instruction, Research, and Student Affairs Committee to demonstrate impacts on program planning and immediate plans for the future. In accordance with Board Policy III.Z, no institution has the statewide program responsibility specifically for cybersecurity programs. Additionally, Board Policy III.Z does not apply to programs for which 90% or more of all activity is required or completed online.

As provided in the program proposal, University of Idaho (U of I) currently offers a Bachelor of Science in Cybersecurity, which is a computer science based degree, and Idaho State University offers a Bachelor of Applied Science in Cyber-Physical Systems Engineering Technology, which is an industry control cybersecurity program that focuses on operational technology cybersecurity. BSU's baccalaureate program is focused on cyber operations in dealing with security issues. All three universities also offer a Bachelor of Science in Computer Science. There are currently no similar Master's level programs being offered. Both BSU and the U of I have plans to bring forward a Master's level Cybersecurity program in the future. Staff notes that BSU has recently submitted a proposal for their Master of Science in Cybersecurity, which will come before the Board at next meeting, and the U of I has a Master of Science in Cybersecurity projected for summer 2022.

Industry support was obtained from Idaho National Laboratory; State of Idaho, Information Technology Services; Ursus Security, LLC; Johnny Security Seed, LLC; and MUFG Union Bank, N.A.

BSU also requests approval to assess an online program fee of $350 per credit for the Bachelor's program consisting of 120 credits, which amounts to $42,000; and $525 per credit for the Master's program consisting of 30 credits, which totals $15,750. Based on the information for the online program fee provided in the proposal, staff finds that the criteria have been met for this program.

The proposal completed the program review process and was presented to the Council on Academic Affairs and Programs (CAAP) on February 4, 2021; and to

the Instruction, Research, and Student Affairs (IRSA), and Business Affairs and Human Resources (BAHR) Committees on February 5, 2021.

Board staff recommends approval.

BOARD ACTION

I move to approve the request by Boise State University to create an online Bachelor of Science and Master of Science in Cyber Operations and Resilience, as presented in Attachments 1 and 2.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

AND

I move to approve the request by Boise State University to charge an online program fee of $350 per credit for the Bachelor of Science in Cyber Operations and Resilience, in conformance with the program budget submitted to the Board in Attachment 1.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

AND

I move to approve the request by Boise State University to charge an online program fee of $525 per credit for the Master of Science in Cyber Operations and Resilience, in conformance with the program budget submitted to the Board in Attachment 2.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

DocuSign Envelope ID: F1B13D98-9F7F-4D55-B24B-1541DFA5DDF4

Institutional Tracking No. _____

Idaho State Board of Education
Proposal for Academic Degree and Certificate Program

Date of Proposal Submission:	December 2020
Institution Submitting Proposal:	Boise State University
Name of College, School, or Division:	College of Engineering
Name of Department(s) or Area(s):	Department of Electrical and Computer Engineering

Official Name of the Program:	Bachelor of Science in Cyber Operations and Resilience	
Implementation Date:	Fall 2021	
Degree Information:	Degree Level: Bachelor	Degree Type: Bachelor of Science
CIP code (consult IR /Registrar):	43.0404	
Method of Delivery: Indicate percentage of face-to-face, hybrid, distance delivery, etc.	100% online	

Geographical Delivery:	Location(s)	Boise	Region(s)	III

Indicate (X) if the program is/has: (Consistent with Board Policy V.R.)		Self-Support fee		Professional Fee	X	Online Program Fee

Indicate (X) if the program is: (Consistent with Board Policy III.Z.)		Regional Responsibility		Statewide Responsibility

Indicate whether this request is either of the following:

[X]	New Degree Program	[ ]	Consolidation of Existing Program
[ ]	Undergraduate/Graduate Certificates (30 credits or more)	[ ]	New Off-Campus Instructional Program
[ ]	Expansion of Existing Program	[ ]	Other (i.e., Contract Program/Collaborative

11/24/2020 | 10:07 AM PST

_____ on)   Date

Vice President for Research (Institution; as applicable)   Date
Jan 8, 2021

_____ er official)   Date

12/9/2020 | 4:42 PM MST

Academic Affairs Program Manager, OSBE   Date
Todd J. Kilburn
January 12, 2021

_____ cal Officer (Institution)   Date

11/24/2020 | 10:48 AM PST

Chief Financial Officer, OSBE   Date

_____ or Instruction (Institution)   Date

T J Bliss
Jan 12, 2021

Chief Academic Officer, OSBE   Date

12/10/2020 | 10:53 AM PST

President   Date

SBOE/Executive Director Approval   Date

1

> **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. <u>All questions must be answered</u>.

Rationale for Creation or Modification of the Program

1. **Describe the request and give an overview of the changes that will result.** What type of substantive change are you requesting? Will this program be related or tied to other programs on campus? Identify any existing program that this program will replace. If this is an Associate degree, please describe transferability.

   Boise State University proposes the creation of a wholly online program that will award a Bachelor of Science in Cyber Operations and Resilience.   The proposed program will operate under the guidelines of SBOE Policy V.R. as it pertains to wholly online programs.

   Cyber Operations and Resilience (CORe) is an asynchronous online program that prepares students to anticipate, detect, mitigate, and manage cyber, physical, and interdependencies infrastructure threats. CORe is to prepare learners to think in systems and how resilience can be achieved. It is not only cybersecurity. It is not just cyber and physical. It is also about interdependencies infrastructure for cyber and physical to operate. It is how everything is interrelated and how strengthening the dependency can lead to a more resilience system. CORe is designed around the realities of today's cyber and physical landscape: it's not if a security (cyber and/or physical and/or interdependencies) breach will occur, it's a matter of when. A resilient system will be able to be restored and bounced back timely and orderly. Businesses, while maintaining a secure posture, are investing in people, processes, and technology to ensure operational continuity under adverse conditions, such as from cyber attacks, physical attacks, insider threats, malfunctioning equipment/software or failure of infrastructures.

   The unique scaffolding of this program (it is designed as a stackable degree program) along with the emerging importance of cyber and physical resilience prepares students with the knowledge, skills, and expertise needed for maintaining the operational effectiveness of complex business, academic, and government information and physical systems. This new degree utilizes and stacks our existing undergraduate certificates, including Cyber Physical Systems (as optional electives) and Cyber Operations (required) into the degree plan. Moreover, the degree has the flexibility for students to stack related industry certifications, existing minor and certificates, and dual-listed courses, prior learning, internships, and experiential learning. This program will be ideal for traditional students, non-traditional students, community college transfer students, and other transfer students. The program has a large number of elective credit hours to accommodate needs and wants of any students.

   A holistic system level thinking approach is at the heart of the CORe program. The asynchronous online curriculum provides for a number of achievement modalities:
   1. Pathways for high school students, community college graduates, and working professionals with an undergraduate degree in any field.
   2. Stackable certification pathways for learners to achieve career alignment without the need for long-term program commitments.
   3. A curriculum that awards experiential learning credits in affordable manner.
   4. Accelerated BS/MS curriculum for learners looking to achieve maximum career opportunity in the shortest time frame possible.

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

   a. **Workforce and economic need:** Provide verification of state workforce needs that will be met by this program. Include job titles and cite the data source. Describe how the proposed program will stimulate the state economy by advancing the field, providing research results, etc.

   The proposed program will stimulate the state economy by training top notch workforce that can work for any companies operating at any physical locations. This online program will provide the learning opportunities to anyone in Idaho to be trained as a security professional.

   The proposed BS in Cyber Operations and Resilience degree is intended to be part of a statewide collaboration between eight colleges/universities to meet the growing workforce demand for cyber-related education. Boise State's proposed online program is ideal for anyone interested in this field.

   Job posting data from 2018-2020, collected using EMSI Analyst, indicates 452 Cyber-related job postings in Idaho required or preferred a graduate credential. The primary market is local and regional, i.e., Idaho + 10 western states. From 2018 - 2020, approximately 21,000 cyber-related job postings indicated a graduate-level credential. Military personnel are a subset of the primary market. A larger and more competitive secondary market is a national and international audience.

   Identifying job titles for the proposed program or any cyber operations and resilience program is very difficult and can never encompass the types of jobs people with a cyber operations and resilience education can pursue. Therefore, we have chosen the following job titles:

   - Computer and Information Analysts SOC Code 15-1210
   - Information Security Analysts SOC Code 15-1212

2019 National Employment Matrix Title and Code		Employment		Job Openings Due to Growth and Replacement Needs 2019-2029
		2019	**2029**	
Computer and Information Analysts	15-1210	763.4	850.8	87.5
Information Security Analysts	15-1212	131.0	171.9	40.9
TOTAL				**128.4**

3

2018-2028 Idaho Long Term Employment Projections		Employment		Job Openings Due to Growth and Replacement Needs 2018-2028
		2018	**2028**	
Computer Systems Analyst	15-1121	1,591	1,740	149
Information Security Analysts	15-1122	408	456	48
TOTAL				**197**

b. **Student demand.** What is the most likely source of students who will be expected to enroll (full-time, part-time, outreach, etc.). Provide evidence of student demand/ interest from inside and outside of the institution.

Career Starter - a student who just completed a high school education, a student who just completed high school with courses in cyber career and technical education, a student who already completed an associate's degree. A student who may be employed, underemployed, or unemployed.

Career Advancer - typically a nontraditional student who is currently employed in an entry or mid-level position, looking to move into senior-level position but needs a degree and specific skill sets.

Degree Finisher - typically a nontraditional student who has made some progress toward an associate or bachelor's degree in a related field and wants to complete a degree. This often includes military students and/or those employed in technical professions but want to transition into managerial positions.

Career Changer - employed in a field other than cyber but wants to shift to a cyber career and needs a bachelor's degree. This may include those with a bachelor's degree (e.g., biology, history, finance, etc.).

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

A recent study by Cybersecurity Ventures[1], a respected publisher of cybersecurity content, predicts that 3.5 million cybersecurity jobs around the world will be unfilled by 2021. In the United States, the demand for professionals with cybersecurity expertise is outpacing all other occupations[2]. These reports, along with many others, underpin the need for increasing workforce development initiatives founded in cybersecurity principles. The workforce shortage is across all cybersecurity domains, yet our adversaries are always advancing, always probing for vulnerabilities in corporate enterprise systems, critical infrastructure systems, and vital national security systems.

To combat this persistent threat, which is a 24/7 operation, we need all hands on deck. It is important to ensure students are positioned to fully support the cyber world; people are

---

[1] https://cybersecurityventures.com/jobs/
[2] https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating

Student demand is tied to the high number of job openings in the region, and nation, as well as looking at the number of students graduating from cyber-related program. The gCORE program expects that a growing number of students with a cyber-related background will be attracted to the program because of the vast employment opportunities that exist within the field.

According to Cyberseek (www.cyberseek.org, January 5, 2021), there are 1,597 cyber job openings in Idaho. There are 23,531 cyber jobs in Idaho and surrounding states (Washington, Oregon, Nevada, Utah, Wyoming, and Montana). Some of these job openings have been difficult to fill as the graduates are not trained in the right skill sets. The need to fill these positions is a large part of why we designed the BS and MS in Cyber Operations and Resilience degrees (uCORe and gCORe) and the gCORE certificates. The curriculums have been designed to prepare the graduates for short-term and long-term learning outcomes.

According to the program feasibility research, from February 2018- April 2020, 466 job postings in Idaho required a credential in a field related to cybersecurity. Of which, 116 jobs either prefer or require an advanced degree (i.e., post-baccalaureate) which the gCORE certificates can provide (in addition to the MS degree).

The program feasibility research identified the regional workforce demand (Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Utah, Washington and Wyoming) as 22,532 total jobs posted that required a credential in a field related to cybersecurity (February 2018- April 2020). Of which, 3,308 jobs either prefer or require an advanced degree (i.e., post-baccalaureate). California and Washington states dominate the job market. The average salary is estimated at $100.1K.

Additionally, research for the national workforce demand, identified 130,322 total jobs posted that required a credential in a field related to cybersecurity (February 2018- April 2020). Of which, 19,223 jobs either prefer or require an advanced degree (i.e., post-baccalaureate). California and Washington states dominate the job market. The average salary is estimated at $95.1K.

In addition to the vast job opportunities that we anticipate will attract students to the program, the current the undergraduate Cyber Operations certificate that was started as part of the effort funded by Idaho Workforce Development Council, already has 30 students enrolled (new program as of August 2020).

As part of the program feasibility study, completion data for both undergraduate and graduate degree programs for the western US state region was analyzed (Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Utah, Washington, and Wyoming), which indicate a growth in enrollment.
Regional undergraduate degree completions in cyber-related programs
2016 - 1,030
2017 - 1,134 = 10% year over year growth in regional degree completions
2018 - 1,164 = 2.6% year over year growth in regional degree completions

2019 - 2,630 = 125% year over year growth in regional degree completions

The increase year over year of undergraduate students in cyber-related programs indicates that increasing number of students will likely pursue advanced educational opportunities to increase their employability, salary potential, advance their careers, and grow their skills and knowledge in the field.

Regional graduate degree completions in cyber-related programs
2016 - 527
2017 - 688 = 30.5% year over year growth in regional degree completions
2018 - 807 = 17% year over year growth in regional degree completions
2019 - 1,100 = 36% year over year growth in regional degree completions

needed with different perspectives, approaches, ways of thinking, and methods to solve the cyber challenges our society is facing and will face. This need is especially pressing when assessing the current and future digital landscape — a tireless and ever expanding connectivity supported by societal needs and economic development, yet compromised by the common criminal to nation-state sponsored criminal activity.

At the center of this program is getting learners to think differently and understanding how a resilient system and network can be built for the society to be more resilient. With the upcoming wide deployment of 5G network, it is even more important that we have a program that is a societal need. Also, how we educate learners that are able to protect our critical infrastructure and our homes with resiliency in mind.

3. Program Prioritization
Is the proposed new program a result of program prioritization?

Yes_____ No_X_____

If yes, how does the proposed program fit within the recommended actions of the most recent program prioritization findings.

4. Credit for Prior Learning
Indicate from the various cross walks where credit for prior learning will be available. If no PLA has been identified for this program, enter 'Not Applicable'.

This program is interested in providing opportunities for credit for prior learning. As the program begins to scale, it will evaluate how credit for prior learning can be awarded. If a student has earned industry certifications, the program can award credits for certifications.

5. Affordability Opportunities
Describe any program-specific steps taken to maximize affordability, such as: textbook options (e.g., Open Educational Resources), online delivery methods, reduced fees, compressed course scheduling, etc. This question applies to certificates, undergraduate, graduate programs alike.

Boise State University will offer this program at a very market competitive rate of $350 per credit hour. This program has been designed to be able to accommodate all of 60 credit hours transfer from state and community colleges. If a student has earned industry certifications, the program can award credits for certifications. Students will also be able to earn internships credits, and earn prior learning credits and experiential learning credits, thus, reducing the total cost of their education.

Enrollments and Graduates

6. 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 for the most past four years.

Cyber education programs can be classified in three categories: (1) Cyber awareness program for everyone, (2) cyber for STEM where STEM majors learn how to design and code with security in mind, (3) cyber operations for dealing with security issues 24/7. This degree is in category (3).

5

At Boise State University, there is currently no similar program. Currently, there is no such program across Idaho. University of Idaho's new BS in Cybersecurity is a Computer Science based degree. It is to teach how to program securely. The Idaho State University's BAS Cyber-Physical Systems Engineering Technology degree, which launched in Fall 2020, is an industry control cybersecurity program. This degree concentrates on operational technology cybersecurity.

The proposed BS in Cyber Operations and Resilience is focused on cyber operations. It is to meet the needs of any organizations, from local governments, counties governments, state governments, national security, and private entities.

Instit.	Program Name	Fall Headcount Enrollment in Program				Number of Graduates From Program (Summer, Fall, Spring)			
		Fall 2017	Fall 2018	Fall 2019	Fall 2020	FY17	FY18	FY19	FY2020
BSU	BS in Computer Science	706	710	684	698	69	98	98	111
ISU	BS in Computer Science	175	185	176	175	17	15	23	22
U of I	BS in Cybersecurity	n/a	n/a	n/a	Not available	n/a	n/a	n/a	n/a
U of I	BS in Computer Science	284	278	268	Not available	22	32	27	30

7. **Justification for Duplication** (if applicable). If the proposed program is similar to another program offered by an Idaho public higher education 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.

The proposed program is different from the Idaho State University's Cyber-Physical System Engineering Technology (UG) program and the University of Idaho's Cybersecurity (UG) program because the proposed program instructs and produces cybersecurity professionals focused on operational thinking, tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. The goal of the CORe curriculum is to prepare learners to view and think of systems as holistic models while determining how resiliency can be achieved. CORe presents the interdependencies infrastructure has between cyber and physical in order to achieve operational effectiveness. In short, CORe is about how everything is interrelated and how strengthening the bonds of dependency can lead to a more resilient system/network/society.

8. **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

6

Program Name: BS in Cyber Operations and Resilience											
Projected Fall Term Headcount Enrollment in Program						Projected Annual Number of Graduates From Program					
FY22 (first year)	FY23	FY24	FY25	FY26		FY22 (first year)	FY23	FY24	FY25	FY26	
20	58	93	107	116		0	9	29	42	47	

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

    The program's size will be scaled to demand for the program. The numbers in the table above reflect a reasonable and attainable scaling up of the program.

    Marketing and recruitment efforts will include a digital marketing campaign, a web landing page, request for information form and a full program website with details regarding the key program assets, curriculum plan, and costs. In addition, a comprehensive communication plan will be implemented to attract and nurture interested students. Strategic, personalized communications will engage and support students throughout the recruitment life cycle. Our coaching approach to student services will support online students and maintain their connection to Boise State through graduation.

10. **Minimum Enrollments and Graduates.**
    a. What are the minimums that the program will need to meet in order to be continued, and what is the logical basis for those minimums?

        Because the program will be utilizing the online fee model, it is best to put minimum enrollment in terms of course registrations, which are what translate to revenue. Based on estimated expenses for instruction and for support personnel expenses, estimate the minimum number of course registrations to achieve breakeven is:

        • Year 1: Annual credits 405, Annual FTEs 13.50
        • Year 2: Annual credits 943, Annual FTEs 31.43
        • Year 3: Annual credits 1,519, Annual FTEs 50.62
        • Year 4: Annual credits 1,748, Annual FTEs 58.26
        • Year 5: Annual credits 1,876, Annual FTEs 62.53

        If enrollments do not meet expectations, expenses will adjust to reflect actual activity. The program's financial sustainability will be evaluated at least annually.

    b. If those minimums are not met, what is the sunset clause by which the program will be considered for discontinuance?

        Programs operating under the online program fee model at Boise State University are expected to be fiscally sustainable. If enrollments do not meet expectations, expenses will

7

be adjusted to reflect actual activity. The program's financial sustainability will be evaluated at least annually. If it is determined to be fiscally unsustainable in the long term, it will be discontinued.

11. **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 following measures will ensure the high quality of the new program:

Regional Institutional Accreditation: Boise State University is regionally accredited by the Northwest Commission on Colleges and Universities (NWCCU). Regional accreditation of the university has been continuous since initial accreditation was conferred in 1941. Boise State University is currently accredited at all degree levels (A, B, M, D).

Program Review: Boise State has instituted a new program review procedure. At the inception of new programs, the programs will submit to the Office of the Provost a three-year assessment plan to be scheduled into the Periodic Review/Assessment Reporting Cycle. The plan includes program learning outcomes; and an implementation plan with a timeline identifying when and what will be assessed, how the programs will gather assessment data, and how the program will use that information to make improvements. Then, every three years, the programs will provide Program Assessment Reports (PAR), which will be reviewed by a small team of faculty and staff using a PAR Rubric, which includes feedback, next steps, and a follow-up report with a summary of actions.

Program Development Support: The online B.S. in Cyber Operations and Resilience is one of several that are being created via the eCampus Expansion Initiative at Boise State University. Boise State's online program development process uses a facilitated program design process to assist program faculty members in the creation of an intentional, cohesive course progression with tightly aligned course and program outcomes. A multi-expert development team, which includes an instructional designer, multimedia specialist, and quality assurance, works collaboratively with the faculty member. One master version of each course is developed for a consistent look and feel of courses across the program; the master course utilizes a professionally created common template aligned with nationally Quality Matters course design standards.

Academic Integrity: Academic integrity is vital to the mission of Boise State University and encompasses the totality of academic rigor, ethical behavior, intellectual curiosity, appropriate teamwork, and persistence. All assignments submitted by a student must represent his/her own ideas, concepts, and current understanding or must cite the original source. Boise State proactively supports academic integrity by providing training, maintaining a website dedicated to academic integrity, providing tools such as pedagogical strategies, workshops, and tips for designing tests, as well as establishing policies and procedures for students who violate the academic integrity policy within the Student Code of Conduct. For this new online program, we will use the following strategies to encourage academic integrity:
- During the design and development of the curriculum and assessment of each course, instructors will be informed by staff of Boise State's eCampus Center about best practices for online course design based on Quality Matters ™ and best practice strategies to promote academic integrity in online education based on WCET's recommendations (Version 2.0, June 2009)
- Through the program development process, course production, course launch support provided by the eCampus Center, and other means, instructors will be reminded about the importance of academic integrity and encouraged to report and act upon suspected

8

violations.
- Academic integrity will be addressed within online student orientation. Programs may require online students to complete the university's Academic Integrity Online Workshop.
- At the beginning of each course, the instructor will communicate expectations regarding academic integrity to students in the syllabus and verbally and may require completion of the university's Academic Integrity Online Workshop.

Student Authentication: Because the proposed program will be offered entirely online, it is important to include mechanisms by which we authenticate the identity of students enrolled in the program. We will use the following mechanisms:
- During the admissions process, the university will confirm required official transcripts and other documentation required for admission into the program.
- Associated with access to and use of our Learning Management System, a secure log-in environment will be provided and students will be required to use strong passwords and change them every 90 days.
- When high-stakes exams are required, faculty will be encouraged to utilize remote or online proctoring services when appropriate. In those instances, students will need to provide valid photo identification before gaining access to the graded assessments or other required activities.
- Instructors will utilize Canvas's Turnitin plagiarism detection program when appropriate.
- Instructors are expected to be informed of and aware of the importance of student identity authentication and to report and act upon suspected violations.

12. **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 A**.

   N/A

13. **Teacher Education/Certification Programs** All Educator Preparation programs that lead to certification require review and recommendation from the Professional Standards Commission (PSC) prior to consideration and approval of the program by the State Board of Education.

   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?

14. **Three-Year Plan: If this is a new proposed program, is it on your institution's approved 3-year plan?**

   Yes __X__ No _____

   If yes, proceed to question 15. If no:

   a. **Which of the following statements address the reason for adding this program outside of the regular three-year planning process.**

      Indicate (X) by each applicable statement:

9

	Program is important for meeting your institution's regional or statewide program responsibilities.
	The program is in response to a specific industry need or workforce opportunity.
	The program is reliant on external funding (grants, donations) with a deadline for acceptance of funding.
	There is a contractual obligation or partnership opportunity related to this program.
	The program is in response to accreditation requirements or recommendations.
	The program is in response to recent changes to teacher certification/endorsement requirements.

   b. **Provide an explanation for all statements you selected.**

Educational Offerings: Curriculum, Intended Learning Outcomes, and Assessment Plan

15.   **Curriculum. Provide descriptive information of the educational offering.**

   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.	36-43
Credit hours in required courses offered by other departments:	
Credit hours in institutional general education curriculum	37-38
Credit hours in free electives	39-47
Total credit hours required for degree program:	120

   b. **Curriculum.** Provide the curriculum for the program, including credits to completion, courses by title and assigned academic credit granted.

B.S. Degree Completion in Cyber CORe	Credits
University Foundations	**37-38**
University Foundations requirements indicated in bold. See page 48 for details and lists of approved courses.	
UF 100 Foundations of Intellectual Life	3
UF 200 Foundations of Ethics and Diversity	3
FW ENGL 101 Writing and Rhetoric I	3
FW ENGL 102 Writing and Rhetoric II	3
FC Foundations of Oral Communication	3
FM Foundations of Mathematics course (MATH 254 Intro to Statistics)	3-4

FN Foundations of Natural, Physical, & Applied Sciences course with lab	4
FN Foundations of Natural, Physical, & Applied Sciences course in a second field	3
FA Foundations of Arts course	3
FH Foundations of Humanities course	3
FS Foundations of Social Sciences course	3
FS Foundations of Social Sciences course in a second field	3
Required Courses	**27**
CPS 301 Information Assurance and Critical Thinking (Cyber Ops Cert)	3
CPS 401 Defensive Security (Cyber Ops Cert)	3
CPS 402 Offensive Security (Cyber Ops Cert)	3
CPS 403 Recovery and Forensics (Cyber Ops Cert)	3
CPS 412 Foundational Essential for IT Cyber Security Practitioner (CompTIA Security+) (Cyber Ops Cert)	3
CPS 411 Networking (CompTIA Network+)	3
CORE 405 Cyber Project Management and Design	3
CORE 470 Cyber Risk Management (Governance)	3
CORE 400 Cyber Systems Thinking (Essential and CORe Masters)	3
Choose at least 3 Courses (Cyber Essentials)	**3**
CORE 421 Cyber Business and Regulatory Operations (Essentials)	1
CORE 413 Internet of Things Architecture (Essentials)	1
CORE 420 Cyber Security Operations Center (Essentials)	1
CORE 401 Cyber Risk Assessment (Essentials)	1
CORE 422 Cyber Red and Blue Teams (Essentials)	1
CORE 411 Artificial Intelligence & Machine Learning (Essentials)	1
CORE 410 Applied Cyber Security Programming	1
Choose at least 1 Course (Cyber Depth)	**3**
CORE 450 Cyber Threat Intelligence (Threat Intelligence)	3
CORE 460 Cyber Resilience Systems Design (Resilience Analyst)	3
Finishing Foundation (FF)	**3**
FF CORE 480 Cyber Capstone	**3**
Electives	**39-47**
Electives to total 120 credits	
Total	**120**

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.

There will be a 3-credit capstone experience course, which will fulfill the finishing foundations requirements of the University. The brief description of this capstone course is:

11

CORE 480 Cyber Capstone Capstone design experience integrating previous coursework with cyber operations and resilience design theory and methodology. Prereq: CORE 405, CORE 470, CPS 301.

16. **Learning Outcomes: Expected Student 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 students will know, understand, and be able to do, and value or appreciate as a result of completing the program.

    - Recognize the correct fundamentals of cyber operations, resilience, risk assessment, and information assurance to both cyber-physical and information systems.
    - Make decisions based on the ethics, laws, policies, and governance of the cyber security field.
    - Practice acceptable tactics, techniques, and procedures necessary to enhance cyber-physical and informational security operations and resiliency.
    - Recognize industry acceptable cyber security model to secure, inform, involve, and educate stakeholders in security/ resilience operations and strategies.
    - Continuously evaluate and monitor the operational and resilient maturity of an entity.
    - Analyze operation and resiliency policies, metrics, testing and security solutions for an entity using both rigorous risk assessment and threat intelligence people, processes, tools and measures

17. **Assessment plans.**

    a. **Assessment Process.** Describe the assessment plan for student learning outcomes that will be used to evaluate student achievement and how the results will be used to improve the program.

    The B.S. in Cyber Operations and Resilience degree program will follow a systematic assessment and improvement process in which multiple approaches will be used, not only to measure student attainment of program outcomes, but to also inform programmatic improvements. The learning outcomes are mapped to courses that provide relevant content. Student work in these courses that address specific outcomes is collected and evaluated by program faculty. The outcomes are assessed on a three-year cycle with data for all outcomes collected each year, and then the results are analyzed every three years. For each outcome, student work across the program is reviewed in a comprehensive review of student work. A group of three faculty members and instructors review the overall attainment of the outcome based on the evidence collected. As part of the review, recommendations for improvement to the program are outlined. All faculty then review these results and make suggestions/changes to improve this process in a program of continuous improvement. Evaluation results inform programmatic, pedagogical, and curricular improvements.

    The key knowledge unit as defined by the National Initiative for Cyber Security Education (NICE) Cybersecurity Workforce Framework, NSA CAE, and UK Cyber Security Body of Knowledge (CyBok) will also be mapped to all the courses. This will ensure we are teaching the most important skill sets and critical thinking.

12

<u>Resources Required for Implementation – fiscal impact and budget.</u>
Organizational arrangements required within the institution to accommodate the change including administrative, staff, and faculty hires, facilities, student services, library; etc.

18. **Physical Facilities and Equipment:** Describe the provision for physical facilities and equipment.

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

   No impact. Since this is a cyber-focused program, the hands-on activities can either be carried out using student's computers or using cloud computing services.

   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?

   No impact is anticipated.

   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.

   N/A

19. **Library and Information Resources:** Describe adequacy and availability of library and information 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.

   No impact is anticipated.

   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.

   No impact. We have ACM and IEEE subscriptions. Most publications are online and we can get access to those publicly available resources.

20. **Faculty/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?

13

The program will fund new adjunct/lecturer instruction to cover the additional instruction credit required by the program:

> Yr 1- 25.50 instruction credits, 1.06 FTE
> Yr 2- 48.50 instruction credits, 2.02 FTE
> Yr 3- 90.00 instruction credits, 3.75 FTE
> Yr 4- 90.00 instruction credits, 3.75 FTE
> Yr 5- 90.00 instruction credits, 3.75 FTE

At maturity, the program will offer a combined total of 34 sections of new courses of which 31 sections will be in cross listed courses with the proposed Master of Science in Cyber Operations and Resilience.

The program will fund a 0.50 FTE program coordinator in years 1, 2 & 3 and convert to a 1.00 FTE program coordinator starting year 4. The program will fund a 0.25 FTE administrative assistant in years 2 & 3 and convert to a 0.50 FTE administrative assistant starting year 4.

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.

Over the first 4 years of the program, the program will fund partial FTEs of Dr. Sin Ming Loo, a current professor in the Department of Electrical and Computer Engineering:

> Yr 1- 0.10 FTE
> Yr 2- 0.10 FTE
> Yr 3- 0.08 FTE
> Yr 4- 0.05 FTE

Dr. Sin Ming Loo will provide course content and work with the program coordinator to oversee the program.

c. **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?

Because the program will fund instruction and administrative support, it is anticipated that limited instructional and administrative support resources from existing programs will be used for the proposed program. There will be a minimal impact on resources available for existing programs.

d. **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.

The following positions will be hired for the program:
- Adjunct Instruction
- Program Coordinator
- Administrative Assistant

Expenses for these positions are included in the program budget sheet.

21. **Revenue Sources**

14

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?

N/A

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.
No new appropriation will be required.

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?

    The 0.50 FTE Program Coordinator will be funded for one year (January 2021-December 2021) by the Boise State Online Innovation Fund. This fund is funded by online fee revenue and acts as seed funding for online academic programs, online course development stipends to faculty, open education resource grants and eventually innovation grants.

    When startup funding is exhausted, it is anticipated that program student fee revenue will cover the cost of the program coordinator.

  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?

    Starting at program launch (Fall 2021) through Fall 2022, the course instruction expenses will be funded by an Idaho Workforce Development Grant.

    When startup funding is exhausted, it is anticipated that program student fee revenue will cover the cost of instruction of the program courses.

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.

    N/A

  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.

    The student fee will be in accordance with the Online Program Fee as defined in the Board Policy V.R., 3.a.x. That policy enables the institution to set a price-point appropriate for the program; students will pay an online program fee in lieu of tuition. The price-point for the online program fee will be as follows: $350 per credit.
    For the 120 credits required for completion of the proposed program, the total cost will be $42,000.

    We project that by the fourth year of the program, it will generate 1,922 SCH, which

will yield a total revenue of $672,847.

22. Using the excel <u>budget template</u> 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).

DocuSign Envelope ID: F1B13D98-9F7F-4D55-B24B-1541DFA5DDF4

I. PLANNED STUDENT ENROLLMENT

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	FTE	Headcount	FTE	Headcount	FTE	Headcount	FTE	Headcount	FTE	Headcount
A. New enrollments	12.2	27	30.2	59	51.3	86	57.7	94	63.6	104
B. Shifting enrollments	1.4	3	3.4	7	5.7	10	6.4	10	7.1	12
Total Enrollment	13.5	30	33.6	66	57.0	96	64.1	104	70.7	115
Student Credit Hours Generated	405		1,007		1,710		1,922		2,121	

II. REVENUE

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
1. New Appropriated Funding Request										
2. Institution Funds		$44,978								
3. Federal										
4. New Tuition Revenues from Increased Enrollments										
5. Student Fees		$141,750		$352,307		$598,480		$672,847		$742,522
6. Other (i.e., Gifts)		$30,575		$18,763						
Total Revenue	$0	$217,303	$0	$371,069	$0	$598,480	$0	$672,847	$0	$742,522

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.

Budget Notes:

I.A., B.   Calculation of FTE and headcount as follows:
>1 FTE = 30 credits
>Headcount determined as the distinct number of students in the program that year.
>Assume that 90% of the enrollments will be new enrollments and 10% will be shifting enrollments.
>Assume 25% attrition from 1st to 2nd semester, then 3% attrition every semester. No attrition from 2nd to last semester to last semester.

II.2.   The University will sponsor the program coordinator for 1 year using funds from the Boise State Online Innovation Fund.

II.5.   Student Fee revenue calculated as Student Credit Hours * $350 per credit.
$350 calculated as estimate of 2021-2022 per credit rate.
To be conservative, assume in calculations that per-credit fee does not increase over time to align with the amount charged to traditional resident students.

II.6.   An Idaho Workforce Development Council grant will fund instruction of CPS courses through Fall of 2022.

17

18

III. EXPENDITURES

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
A. Personnel Costs										
1. FTE		1.81		2.77		4.50		5.25		5.25
2. Faculty										
3. Adjunct Faculty		$43,350		$84,924		$162,180		$166,770		$171,360
4. Graduate/Undergrad Assistants										
5. Research Personnel										
6. Directors/Administrators		$60,550		$45,275		$43,919		$76,927		$73,158
7. Administrative Support Personnel		$0		$8,498		$8,752		$18,030		$18,571
8. Fringe Benefits		$26,199		$28,839		$35,528		$53,087		$52,263
9. Other: Teaching Assistants				$4,808		$9,615		$9,615		$9,615
Total Personnel and Costs	$0	$130,098	$0	$172,342	$0	$259,995	$0	$324,430	$0	$324,968

Budget Notes (continued)
III.A.3 Adjunct FTE: Calculated using (Credit hour load)/24
III.A.6 Administrator: Program Coordinator (0.5 FTE in years 1,2,3, 1.0 FTE in years 4+). Additional expense included in year 1 to reflect anticipated Jan 2021 start date. Institutiona funds will fund position Jan-Dec 2021
III.A.7 Administrative Support: Administrative Assistant (0.25 FTE in years 2 & 3, 0.50 FTE in years 4+)
III.A.8 Benefits calculated at staff fringe rate of $11,650+(annual wage*20.47%) professional staff and $11,650+(annual wage*21.57%) classified staff
III.A.9 Other: Teaching Assistants hired to support high enrollment courses starting year 2

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
B. Operating Expenditures										
1. Travel										
2. Marketing and Promotion										
3. Other Services										
4. Communications										
5. Materials and Supplies										
6. Rentals										
7. Materials & Goods for Manufacture & Resale										
8. Miscellaneous - Computer Hardware/Software		$2,500		$2,500		$2,500		$2,500		$2,500
Total Operating Expenditures	$0	$2,500	$0	$2,500	$0	$2,500	$0	$2,500	$0	$2,500

Budget Notes (continued):
III.B.8 Miscellaneous: Computer hardware/software

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
C. Capital Outlay										
1. Library Resources										
2. Equipment										
Total Capital Outlay	$0	$0								$0
D. Capital Facilities Construction or Major Renovation										
E. Other Costs										
1. Boise State University Support		$70,875		$176,153		$299,240		$336,423		$371,261
Utilities										
Maintenance & Repairs										
Other										
Total Other Costs	$0	$70,875	$0	$176,153	$0	$299,240	$0	$336,423	$0	$371,261
TOTAL EXPENDITURES:	$0	$203,473	$0	$350,995	$0	$561,735	$0	$663,353	$0	$698,729
Net Income (Deficit) to College	$0	$13,829	$0	$20,074	$0	$36,745	$0	$9,493	$0	$43,794

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

III.E.1   Boise State University Support is defined as follows:

Boise State Central Services (10.00% of revenue): A fund dedicated to funding support services for online students.

Boise State eCampus Center (8.75% of revenue): Provide funding for initiative management, online course/program development and other support services

Boise State Online Innovation Fund (3.80% of revenue): Seed funding for academic programs, course development stipends to faculty, open education resource grants and eventually innovation grants

Boise State Online Marketing, Recruitment, Enrollment, Advising and Retention Fund (27.45% of revenue): A fund dedicated to marketing the program, recruiting enrolling qualified students, advising students and retaining students throughout the life of the program

19

APPENDIX A – Program Map

College of Engineering
Cyber Operations and Resilience (CORe)
Bachelors Degree

BOISE STATE UNIVERSITY

20

Program Purpose

The online Cyber Operations and Resilience (CORe) Bachelor of Science (BS) degree completion program is to instruct and produce Cybersecurity professionals focused on operational tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. The goal of the CORe curriculum is to prepare learners to view and think of systems as holistic models while determining how resiliency can be achieved. CORe presents the interdependencies infrastructure has between cyber and physical in order to achieve operational effectiveness. In short, CORe is about how everything is interrelated and how strengthening the bonds of dependency can lead to a more resilient system/network/society.

1. Recognize the correct fundamentals of cyber operations, resilience, risk assessment, and information assurance to both cyber-physical and information systems.
2. Make decisions based on the ethics, laws, policies, and governance of the cyber security field.
3. Practice acceptable tactics, techniques, and procedures necessary to enhance cyber-physical and informational security operations and resiliency.
4. Recognize industry acceptable cyber security model to secure, inform, involve, and educate stakeholders in security/resilience operations and strategies.
5. Continuously evaluate and monitor the operational and resilient maturity of an entity.
6. Analyze operation and resiliency policies, metrics, testing and security solutions for an entity using both rigorous risk assessment and threat intelligence people, processes, tools and measures.

Stakeholders
- College of Engineering
- Institute of Pervasive Cybersecurity

Required Course
CORE 480
Finishing Foundations/
Capstone
3 Credits

Choose at least 3 Courses

CORE 401/501
Cyber Risk
Assessment
1 Credit

CORE 410/510
Applied Cybersecurity
Programming
1 Credit

CORE 420/520
Cyber Security
Operations Center
1 Credit

CORE 411/511
AI & Machine Learning
1 Credit

CORE 421/521
Cyber Business &
Regulatory Ops
1 Credit

CORE 413/513
Internet of Things
Architecture
1 Credit

CORE 422/522
Cyber Red & Blue
Teams
1 Credit

Choose at least 1 Course

CORE 450/550
Cyber Threat
Intelligence
3 Credits

CORE 460/560
Cyber Resilience
Systems Design
3 Credits

CORE 400/500
Cyber Systems Thinking
3 Credits

CORE 405
Cyber Project Mgmt &
Design
3 Credits

CORE 470/570
Cyber Risk
Management
3 Credits

Required Courses

CPS 301
Information Assurance
& Critical Thinking
3 Credits

CPS 403
Recovery & Forensics
3 Credits

CPS 401
Defensive Security
3 Credits

CPS 411
Networking
3 Credits

CPS 402
Offensive Security
3 Credits

CPS 412
Found Essential for IT
Cyber Security Practitioner
3 Credits

Can be used for Cyber
Operations Certificate

Undergraduate Degree
- Admission to Boise State University

APPENDIX B- LETTERS OF SUPPORT

Idaho National Laboratory – Scott Cramer, Director Cybercore Integration Center

State of Idaho, Information Technology Services – Keith Tresh, Chief Information Security Officer

Ursus Security, LLC – Kim L. Jones, Founder and Managing Director

Johnny Security Seed, LLC – Richard W. Owen, CEO and Chief Evangelist

MUFG Union Bank, N.A. – Stanley R. Jarocki, Vice President

Idaho National Laboratory **INL**

October 13, 2020   CCN 248073

Idaho State Board of Education
650 West State St.
Suite 307
Boise, ID 83720

Subject: Letter of Support Regarding Boise State Course Offerings in Cyber Operations and Resilience

Dear Board Members,

As part of our continued collaboration with Boise State University (BSU) and in support of the Cybercore Integration Center (CIC) mission at Idaho National Laboratory (INL), this letter expresses our strong endorsement of the proposed Cyber Operations and Resilience course offerings.

INL is a world leader in research and technologies for securing and protecting the critical infrastructure of the United States and is focused on fundamental challenges with greatest impact. Building on the current success of BSU and CIC collaborations, these competency-based learning models will help to reach additional students while addressing outstanding needs in the current workforce.

INL has been observing the cybersecurity security curriculum development across the state of Idaho. University of Idaho offers a BS in Cybersecurity, a degree focused on computer science and programming. Idaho State University is now offering a BAS in Cyber-Physical Systems Engineering Technology, concentrated on industrial cybersecurity. There is another identified need for cyber operations, which targets frontline workers who continually face security concerns and address challenges across the enterprise. We are delighted that BSU has taken the appropriate steps to address this gap, at both the BS and MS level, and are prepared to make course offerings available as soon as next fall.

The fact that the courses will be available as an asynchronous online program, opens the instruction to much broader audiences across the state and affords full-time workers and remote learners the ability to build skills outside of the traditional classroom setting. This progressive and flexible platform offers broad reach and greater access to a variety of students, from diverse backgrounds and skill sets, to advance education and workforce development efforts necessary to meet cybersecurity needs now, and in the future.

In short, we see these programs as beneficial to industry, local governments, counties, and state entities in training cybersecurity frontline workers to protect and defend, enhance critical thinking skills and provide more resilience within our cyber environments, which addresses elements currently in short supply and which will only grow in demand. Increasing the number

of people capable of cyber operations and accelerating their development, is core to our mission and vital to both our state and the nation.

We applaud BSU efforts and continued contributions in supporting the Idaho cyber-education ecosystem and willingness to advance offerings designed to provide access to a wide range of students, while addressing identified needs is the workforce.

We believe these efforts will be of benefit to the community, the state and the region, as well as INL, and strongly support the proposed offerings being put into practice and made available.

Sincerely,

Scott Cramer, Director Cybercore Integration Center
National & Homeland Security

SC:KL

Distribution:
Sin Ming Loo, Boise State University

cc: Z.D. Tudor, MS 3750
        W.C. Kiestler, MS 3750
        S.F. McAraw, MS 1444
        E.J. Taylor, MS 1444
        M.T. Bingham, MS 3605

23

DocuSign Envelope ID: F1B13D98-9F7F-4D55-B24B-1541DFA5DDF4

State of Idaho

Information Technology Services
Office of the Governor

BRAD LITTLE
Governor
JEFF WEAK
Administrator
GREG ZICKAU
Deputy Administrator/
Chief Information Officer

11331 W. Chinden Blvd, Suite B201
P.O. Box 83720
Boise, ID 83720-0042
Telephone (208) 605-4000 or FAX (208) 605-4093
http://its.idaho.gov

September 23, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear Board Members,

I am writing this letter in support of Boise State University's proposed Bachelor of Science and Master of Science Degree in Cyber Operations and Resilience (CORe).

Given the importance of cybersecurity in every aspect of modern life and the shortage of trained cybersecurity professionals nationwide, this program and the graduates it produces will benefit the public and private sectors inside Idaho and the nation a whole. The proposed Cyber Operations and Resilience programs will build a pathway for professionals to change careers and help existing cybersecurity professionals deepen their expertise. This program will also help cybersecurity professionals progress into management level positions and will feed some of the PhD programs statewide if these same professionals choose to continue their education by pursuing a doctorate degree.

Boise State University already offers a Bachelor of Science in Computer Science with a Cybersecurity emphasis and a PhD in Computing with Cybersecurity emphasis, so these proposed programs fill a missing level that would be attractive to many potential students. Idaho employers need multiple universities inside our state to offer programs that specialize in all aspects of cybersecurity to satisfy the demand and need for trained cybersecurity professionals. To that end, Boise State University is participating in conversations within our state to codify an agreement for all major universities to share courses, curriculum and resources within the cybersecurity area of concentration.
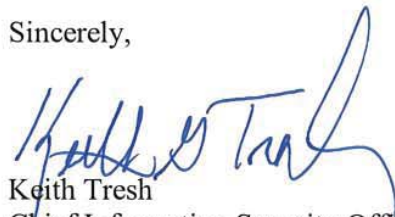
I also want to highlight the fact that Boise State University hired several faculty members with operational cybersecurity experience in the last five years. They have also worked hard to seek and maintain many key industry/government relationships within the cybersecurity field including the State of Idaho, Information Technology Services as well as the Idaho National Lab.

24

As an example, and a matter of fact, I was hired in August of 2019 to teach in their current baccalaureate program. I also participate in all of their Cybersecurity planning and sit on the Board of Boise State's up-and-coming Institute for Pervasive Cybersecurity.

In closing, I would like to add that as a public servant with over 25 years of information technology and cybersecurity operational experience, I feel these programs can and will dramatically increase the available number of trained cybersecurity professionals within Idaho and nationwide. I wholeheartedly support the creation and implementation of both the Bachelor of Science and Master of Science degrees in Cyber Operations and Resilience!

If you have questions or need more information, please feel free to contact me at (208) 605-4054 or keith.tresh@its.idaho.gov.

Sincerely,

Keith Tresh
Chief Information Security Officer
Office of Information Technology Services
Office of the Governor
Keith.Tresh@its.idaho.gov
Office: (208) 605-4054
Cell: (208) 407-8509

25

DocuSign Envelope ID: F1B13D98-9F7F-4D55-B24B-1541DFA5DDF4

Ursus Security LLC
"Standing in the Gap"

October 8th, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Esteemed Board Members:

I am writing this letter to express my strongest possible support for Boise State University's Cyber Operations and Resilience (CORe) degree programs.

As a senior cybersecurity profession and former senior cyber executive, I have long struggled with the challenge of finding skilled professionals to fill the ranks of my supported organizations. As the cyber talent gap widened and universities took up the call for support, I was disappointed at the caliber of students produced by our institutes of higher learning. In far too many cases "cyber graduates" had only theoretical knowledge of cybersecurity principles across a narrow portion of the career field; they were inadequately prepared to face the fluid (and often non-standard) real-world dilemmas faced by today's cyber warriors.

When I was asked to evaluate Boise State University's CORe program and approach, I entered the process with a high degree of skepticism. I am pleased to say that I left the process more excited and impressed than I have been with a university-led program in a long time. Boise State's curricula (at both the Bachelors and Masters levels) remains entrenched in a real world, practical approach which prepares students to meet the challenges of a cybersecurity career head on. Further, the modular approach is extremely well suited for those looking to transition careers – something which must be embraced if we are ever to close the cyber job-talent gap. Boise State's commitment to hiring top tier cyber talent – including senior cyber executives and not just educational professionals – gives me an extremely high degree of confidence around the caliber of graduates these programs will produce. I look forward to introducing Boise State's first crop of graduates into the companies I advise and support.
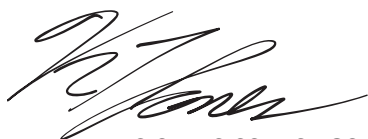
Boise State University is to be commended for taking a proactive, thought-leading approach to solving one of our nation's most vexing problems. I urge you to support these efforts wholeheartedly.

Ursus Security LLC
"Standing in the Gap"

Please feel free to contact me if you have questions.

Sincerely,

Kim L. Jones CISM, CISSP, CDGSE, M.Sc.
Founder and Managing Director
Ursus Security LLC
(480) 253-9120
Kim.Jones@UrsusWorldwide.com
https://www.linkedin.com/in/kimjones-cism/

Johnny Security Seed, LLC.
4412 E la Estancia Cir
Cave Creek, AZ 85331
www.JohnnySecuritySeed.com

September 30, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear Board Members,

I am writing this letter in support of Boise State University's Bachelor of Science (BS) and Master of Science (MS) Degree programs in Cyber Operations and Resiliency (CORe). I understand that Boise State and other universities offer degrees in Computer Science with an emphasis in Cyber Security, but Cyber Security can no longer be just an extra area of study.

In today's world we continue to collect, process and store more information and base many decisions on this ever-growing collection of data. This simply adds greater importance and risk to those systems and data. However, we have a nation-wide shortage of skilled and educated people who can provide the protection that we require. The Cybersecurity Industry is in a need of not only more qualified people, but those who are trained to think and address rapidly changing threats.

I applaud Boise State University for creating programs that start first with the high school student. Johnny Security Seed has a similar effort and approach. As one who has significant technical training and many certifications stacked on top of my formal college education, I have found that the combination has been a key element in my success. I see these programs as vital to creating professionals who can address ever-changing operational issues to ensure the resiliency of critical data and systems. I also support the program's experiential learning credit approach. Hackers follow no formal education road map and to respond we need to create a workforce capable of accomplishing the mission, oftentimes in a less structured fashion. I believe that the proposed curriculums would provide my current and prior businesses a more capable employee to help in this ongoing fight.

As a point of reference, I have spent over 50 years protecting information of which over 30 years was focused on creating and managing cyber security programs. I created the Information Security Program for Mission Operations at Johnson Space Center, NASA. While there, I was awarded a "Silver Snoopy" by the astronauts for the program and a Continuous Improvement Award by the NASA Administrator for avoiding over $25M in costs. After that, I created four other very successful security programs across various industries. I am a past International President of the Information Systems Security Association (ISSA) and a member of the Information Security Hall of Fame. Most recently I was honored with Fellow status of the world renowned Ponemom Institute (https://www.ponemon.org).

Should you have any questions of if I may be of other assistance, I can be contacted at Rich@JohnnySecuritySeed.com or on my cell at 480-686-5527.

1

28

Sincerely,

Richard W. Owen, Jr.
CEO and Chief Evangelist

29

◉ MUFG

MUFG Union Bank, N.A.
Information Risk Management
Risk Management Division for the
Americas
6802 E Bobwhite Way
Scottsdale, AZ 85266
T: +1-480-381-0887

Stanley.Jarocki@unionbank.com

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear State Board Members:

I am writing this letter in full support of the proposed Cybersecurity Bachelor and Master programs at Boise State. These programs incorporate fundamental aspects of Cybersecurity that are needed to maintain a key core element – Cyber Operations and Resiliency – that are so desperately needed and which require trained individuals to cover all critical infrastructure sectors today and in the future.

Today, as a veteran of many attacks that I have experienced in the Federal Government sector, the critical infrastructure sectors – financial, healthcare, retail – and having lived through 911 at ground zero, I speak from experience. Cyber resources that drive the systems of our environment must be secure, auditable, compliant, and resilient. Knowledgeable talent is needed at the entry level and senior executive level to promote the proper planning, testing and execution to keep these systems running. Just imagine what would happen if hospital cyber system went down and doctors, nurses and staff had to resort to pen and pencil. Today in the time of the pandemic huge numbers of lives would be lost, treatment would have to stop and those needing care would not be able to get it. And it could be your family members or yourself. Sounds farfetched? Well, it is happening as they are being attacked not only by natural disasters but by Bad Actors using Ransomware, DDoS attacks and other extortion attempts. Cyber is the nervous system, communications paths, and knowledge repositories upon which our lives are built and depend. Therefore, the need for Cyber professionals and cyber warriors to support and build strong infrastructure is needed. Where are they going to get this knowledge? They will be able to get this critical knowledge base from Boise State's Bachelor and Master's programs in Cyber Operations and Resiliency.

The key to these powerful new programs - the Cyber Operations and Resilience (CORe) Bachelor of Science (BS) and Master of Science (MS) programs – lies in their ability to develop focused curriculum that provide needed skill sets that they can use day one. These programs are geared to instruct and produce Cybersecurity professionals focused on operational tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. The goal of the CORe curriculums is to prepare learners at the beginning levels to view and think of systems as holistic models while determining how resiliency can be achieved. CORe presents the interdependencies infrastructure has between cyber and physical to achieve operational effectiveness. In short, CORe is about business, real life and the world of cybersecurity and their interrelationships and how strengthening the bonds of dependency can lead to a more robust and resilient system/network/society.

A holistic system level thinking approach is at the heart of the CORe program. The asynchronous online curriculum provides for a challenging set of achievement modalities:

1. Pathways for high school students (traditional and career & technical education), community college graduates, and working professionals with an undergraduate degree in any field,

2. Stackable certification pathways for learners to achieve career alignment without the need for long-term program commitments,

3. A curriculum that awards experiential learning credits in an affordable manner,

4. A potential for strong internship with local and national industries and critical infrastructure sectors, and

5. Accelerated BS/MS curriculum for learners looking to achieve maximum career opportunity in the shortest time frame possible.

As an early practitioner in the field of Cybersecurity I had to boot strap my knowledge with a lot of "OJT" (On the Job Training) to get the job done. Adding needed skills such as audit, risk management and executive leadership was not easy. Holding CISO positions in a variety of industries and major companies in the financial, healthcare and retail sectors. - I can attest that finding individuals with these skills is extremely hard. Nationally, there is estimated to be over 3 million job openings creating a dire shortage of talent. This is exasperated even more due to the increased attacks by bad actors and nation states who feel we are too preoccupied with the "Pandemic." Trained people are desperately needed with practical operational skills who can contribute day one.

As the editor / contributor of the USA National Security Plan for the financial sector and chief architect of the Financial Services Information Sharing and Analysis Center and presently as a VP of Information Risk Management for the 5th largest bank in the World – MUFG – I can attest that quality trained talent is desperately needed. Additionally, as an advisor to higher education intern programs, it is extremely important that Cybersecurity needs to start with K-12 to show that diversity and excitement does exist in the world of Cybersecurity. I believe the curriculum that I have reviewed is the right start in our battle to cultivate passionate and talented individuals who will be practically trained to jump in and defend the cyber world of today and, more importantly, tomorrow.

I also believe local Boise Headquartered companies such as Albertsons is another example of an organization that requires cybersecurity and resiliency as we have observed in recent disasters and the Pandemic. Food supplies are critical and the supply chain systems that support operations and get the goods to the stores and people is critical to humanity's survival.

So it is extremely important that support for the ability to produce learners with the caliber of talent needed for the state of Idaho, the nation, and worldwide, be provided at the highest level of state government – through the governor's office, and through approval of these programs through the state board of education.

Sincerely,

Stanley R. Jarocki

Vice President

31

DocuSign Envelope ID: E4BC928A-D5CB-447D-9FD4-C80A95F162EF

Institutional Tracking No. _____

Idaho State Board of Education
Proposal for Academic Degree and Certificate Program

Date of Proposal Submission:	December 2020
Institution Submitting Proposal:	Boise State University
Name of College, School, or Division:	College of Engineering
Name of Department(s) or Area(s):	Electrical and Computer Engineering Department

Official Name of the Program:	Master of Science in Cyber Operations and Resilience	
Implementation Date:	Fall 2021	
Degree Information:	Degree Level: Master	Degree Type: M.S.
CIP code (consult IR /Registrar):	43.0404 Cybersecurity Defense Strategy/Policy	
Method of Delivery: Indicate percentage of face-to-face, hybrid, distance delivery, etc.	100% online	

Geographical Delivery:	Location(s)	Boise	Region(s)	III

Indicate (X) if the program is/has: (Consistent with Board Policy V.R.)		Self-Support fee		Professional Fee	X	Online Program Fee
Indicate (X) if the program is: (Consistent with Board Policy III.Z.)		Regional Responsibility		Statewide Responsibility		

Indicate whether this request is either of the following:

X	New Degree Program			Consolidation of Existing Program
	Undergraduate/Graduate Certificates (30 credits or more)			New Off-Campus Instructional Program
	Expansion of Existing Program			Other (i.e., Contract Program/Collaborative

11/24/2020 | 10:06 AM PST

_____ (Institution)   Date

Vice President for Research (Institution; as applicable)   Date
Jan 8, 2021

Dr. Tammi Vacha-Haase   11/25/2020 | 12:09 PM PST

_____ fficial   Date

Academic Affairs Program Manager, OSBE   Date

12/8/2020 | 3:11 PM MST

_____ er (Institution)   Date

Todd J. Kilburn
Chief Financial Officer, OSBE   Date
January 12, 2021

12/4/2020 | 12:27 PM PST

_____ Instruction (Institution)   Date

TJ Bliss
Chief Academic Officer, OSBE   Date
Jan 12, 2021

12/8/2020 | 9:28 PM PST

_____   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. <u>All questions must be answered</u>.

<u>Rationale for Creation or Modification of the Program</u>

1. **Describe the request and give an overview of the changes that will result.** What type of substantive change are you requesting? Will this program be related or tied to other programs on campus? Identify any existing program that this program will replace. If this is an Associate degree, please describe transferability.

   Boise State University proposes the creation of a wholly online program that will award a Master of Science in Cyber Operations and Resilience.   The proposed program will operate under the guidelines of SBOE Policy V.R. as it pertains to wholly online programs.

   Cyber Operations and Resilience (CORe) is an asynchronous online program that prepares students to anticipate, detect, mitigate, and manage cyber, physical, and interdependencies infrastructure threats. The MS in CORe is to prepare learners to think in systems and how resilience can be achieved. It is not only cybersecurity. It is not just cyber and physical. It is also about interdependencies infrastructure for cyber and physical to operate. It is how everything is interrelated and how strengthening the dependency can lead to a more resilience system. The MS in CORe is designed around the realities of today's cyber and physical landscape: it's not if a security (cyber and/or physical and/or interdependencies) breach will occur, it's a matter of when. A resilient system will be able to be restored and bounced back timely and orderly. Businesses, while maintaining a secure posture, are investing in people, processes, and technology to ensure operational continuity under adverse conditions, such as from cyber attacks, physical attacks, insider threats, malfunctioning equipment/software or failure of infrastructures.

   The MS in CORe is a stackable master's degree program that offers graduate certificates with complementary technical and non-technical tracks leading to a master's degree. The unique and flexible scaffolding of this program along with the emerging importance of cyber and physical resilience prepares students with the knowledge, skills, and expertise needed for maintaining the operational effectiveness of complex business, academic, and government information and physical systems. The program is ideal for students who have a professional, military, or law enforcement background that seek to advance their career within the cyber workforce.

   This program is focused on the interplay of systems, technical, program management, and policy skills necessary to design, remediate, and operate resilient information systems, physical systems, networks. The program provides students with stackable credentials, certificates, hands-on experiential learning, learning by teaching, and practical operation resilience problem solving scenarios — all which culminate in a capstone tabletop exercise in support of regional businesses, government institutions, military facilities, or law enforcement agencies. Practitioners experienced in physical operations, cyber operations and resilience will be recruited to advise, support course development, and teach.

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

2

a. **Workforce and economic need:** Provide verification of state workforce needs that will be met by this program. Include job titles and cite the data source. Describe how the proposed program will stimulate the state economy by advancing the field, providing research results, etc.

The proposed program will stimulate the state economy by training a top notch workforce that can work for any company operating at any physical locations. This online program will provide the learning opportunities to anyone in Idaho to be trained as a security professional.

The master's degree and the graduate certificates are intended to be part of a statewide collaboration between eight colleges/universities to meet the growing workforce demand for cyber-related education. Boise State's proposed online graduate program focuses on early-mid career professionals aspiring to move into leadership roles. Most positions listed below either require a master's degree or indicate it is a preferred credential. This program is online to accommodate working professionals across Idaho, western state region, and nation.

Job posting data from 2018-2020, collected using EMSI Analyst, indicates 452 Cyber-related job postings in Idaho that required or preferred a graduate credential. The primary market is local and regional, i.e., Idaho + 10 western states. From 2018 - 2020, approximately 21,000 cyber-related job postings indicated a graduate-level credential. Military personnel are a subset of the primary market. A larger and more competitive secondary market is a national and international audience.

Identifying job titles for the proposed program or any cyber operations and resilience program is very difficult and can never encompass all the types of jobs people with a cyber operations and resilience education can pursue. Therefore, we have chosen the following job titles:

- Computer and Information Analysts SOC Code 15-1210
- Information Security Analysts SOC Code 15-1212

2018 National Employment Matrix Title and Code		Employment		Job Openings Due to Growth and Replacement Needs 2018-2028
		2018	2028	
Computer and Information Analysts	15-1210	763.4	850.8	87.5
Information Security Analysts	15-1212	131.0	171.9	40.9
TOTAL				**128.4**

2018-2028 Idaho Long Term	Employment	Job Openings Due to

Employment Projections		2018	2028	Growth and Replacement Needs 2018-2028
Computer Systems Analyst	15-1121	1,591	1,740	149
Information Security Analysts	15-1122	408	456	48
TOTAL				197

b. **Student demand.** What is the most likely source of students who will be expected to enroll (full-time, part-time, outreach, etc.). Provide evidence of student demand/ interest from inside and outside of the institution.

There are three different types of students who will enter this program.
- The career advancer who is already employed in the field and is interested in moving up in the field.
- The career starter who is interested in a career that fits his/her personal and professional goals and is currently not employed in the field.
- The career changer who is currently employed in a different field and is interested in changing fields.

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

A recent study by Cybersecurity Ventures[1], a respected publisher of cybersecurity content, predicts that 3.5 million cybersecurity jobs around the world will be unfilled by 2021. In the United States, the demand for professionals with cybersecurity expertise is outpacing all other occupations[2]. These reports, along with many others, underpin the need for increasing workforce development initiatives founded in cybersecurity principles. The workforce shortage is across all cybersecurity domains, yet our adversaries are always advancing, always probing for vulnerabilities in corporate enterprise systems, critical infrastructure systems, and vital national security systems.

To combat this persistent threat, which is a 24/7 operation, we need all hands on deck. It is important to ensure students are positioned to fully support the cyber world; there is a need people with different perspectives, approaches, ways of thinking, and methods to solve the cyber challenges all are facing and will face. This need is especially pressing when assessing the current and future digital landscape — a tireless and ever expanding connectivity supported by societal needs and economic development, yet compromised by the common criminal to nation-state sponsored criminal activity.

At the center of this program is getting learners to think differently and understanding how a resilient system and network can be built for the society to be more resilient. With the upcoming wide deployment of 5G network, it is even more important that Boise State

---

[1] https://cybersecurityventures.com/jobs/
[2] https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating

Student demand is tied to the high number of job openings in the region, and nation, as well as looking at the number of students graduating from cyber-related program. The gCORE program expects that a growing number of students with a cyber-related background will be attracted to the program because of the vast employment opportunities that exist within the field.

According to Cyberseek (www.cyberseek.org, January 5, 2021), there are 1,597 cyber job openings in Idaho. There are 23,531 cyber jobs in Idaho and surrounding states (Washington, Oregon, Nevada, Utah, Wyoming, and Montana). Some of these job openings have been difficult to fill as the graduates are not trained in the right skill sets. The need to fill these positions is a large part of why we designed the BS and MS in Cyber Operations and Resilience degrees (uCORe and gCORe) and the gCORE certificates. The curriculums have been designed to prepare the graduates for short-term and long-term learning outcomes.

According to the program feasibility research, from February 2018- April 2020, 466 job postings in Idaho required a credential in a field related to cybersecurity. Of which, 116 jobs either prefer or require an advanced degree (i.e., post-baccalaureate) which the gCORE certificates can provide (in addition to the MS degree).

The program feasibility research identified the regional workforce demand (Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Utah, Washington and Wyoming) as 22,532 total jobs posted that required a credential in a field related to cybersecurity (February 2018- April 2020). Of which, 3,308 jobs either prefer or require an advanced degree (i.e., post-baccalaureate). California and Washington states dominate the job market. The average salary is estimated at $100.1K.

Additionally, research for the national workforce demand, identified 130,322 total jobs posted that required a credential in a field related to cybersecurity (February 2018- April 2020). Of which, 19,223 jobs either prefer or require an advanced degree (i.e., post-baccalaureate). California and Washington states dominate the job market. The average salary is estimated at $95.1K.

In addition to the vast job opportunities that we anticipate will attract students to the program, the current the undergraduate Cyber Operations certificate that was started as part of the effort funded by Idaho Workforce Development Council, already has 30 students enrolled (new program as of August 2020).

As part of the program feasibility study, completion data for both undergraduate and graduate degree programs for the western US state region was analyzed (Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Utah, Washington, and Wyoming), which indicate a growth in enrollment.
Regional <u>undergraduate degree completions</u> in cyber-related programs
2016 - 1,030
2017 - 1,134 = 10% year over year growth in regional degree completions
2018 - 1,164 = 2.6% year over year growth in regional degree completions

2019 - 2,630 = 125% year over year growth in regional degree completions

The increase year over year of undergraduate students in cyber-related programs indicates that increasing number of students will likely pursue advanced educational opportunities to increase their employability, salary potential, advance their careers, and grow their skills and knowledge in the field.

Regional <u>graduate degree completions</u> in cyber-related programs
2016 - 527
2017 - 688 = 30.5% year over year growth in regional degree completions
2018 - 807 = 17% year over year growth in regional degree completions
2019 - 1,100 = 36% year over year growth in regional degree completions

University offer a program to meet this pressing societal need.

3.   **Program Prioritization**
Is the proposed new program a result of program prioritization?

Yes_____ No__X___

If yes, how does the proposed program fit within the recommended actions of the most recent program prioritization findings.

4.   **Credit for Prior Learning**
Indicate from the various cross walks where credit for prior learning will be available. If no PLA has been identified for this program, enter 'Not Applicable'.

Not applicable

5.   **Affordability Opportunities**
Describe any program-specific steps taken to maximize affordability, such as: textbook options (e.g., Open Educational Resources), online delivery methods, reduced fees, compressed course scheduling, etc. This question applies to certificates, undergraduate, graduate programs alike.

We will be offering this program at a very market competitive rate of $525 per credit hour. This degree can be completed at the cost of $15,750. The content of this curriculum pushes the boundary of how cyber education is being delivered and will be use cybersecurity working professionals to teach the courses. This curriculum will be offered with asynchronous online mode using a 7-week session that is well suited working professionals.

The stackable building blocks of this program allow learners to work through required courses and one certificate at time, and complete the experiential learning activities to gain the MS in Cyber Operations and Resilience degree.

Enrollments and Graduates

6.   **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 for the most past four years.

Cyber education programs can be classified in three categories: (1) Cyber awareness program for everyone, (2) cyber for STEM where STEM majors learn how to design and code with security in mind, (3) cyber operations for dealing with security issues 24/7. This degree is in category (3).

Currently Boise State University, does not have a similar program. Currently, there is no such program across Idaho.

Instit.	Program Name	Fall Headcount Enrollment in Program				Number of Graduates From Program (Summer, Fall, Spring)			
		Fall 2016	Fall 2017	Fall 2018	Fall 2019	FY17	FY18	FY19	FY20

Boise State University	MS in Computer Science	51	42	54	43	16	10	17	21
University of Idaho	MS in Computer Science	27	30	52	49	10	11	11	23
Idaho State University	MS in Computer Science	Not available	Not available	Not available	Not available	Not available	Not available	Not available	Not available

7.   **Justification for Duplication** (if applicable). If the proposed program is similar to another program offered by an Idaho public higher education 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 duplication, as no Idaho public institution offers a similar program. The proposed MS in CORe program concentrates on cybersecurity people, process, and technology. The proposed program is different from the existing master's programs in Computer Science, and Boise State University's proposed MS in Cybersecurity. These programs are concentrated on programming, providing cyber related education for people with STEM background to learn how to design and code with security in mind. The proposed MS in CORe program instructs and produces Cybersecurity professionals focused on operational tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. The goal of the CORe curriculum is to prepare learners to view and think of systems as holistic models while determining how resiliency can be achieved. CORe presents the interdependencies infrastructure has between cyber and physical in order to achieve operational effectiveness. In short, CORe is about how everything is interrelated and how strengthening the bonds of dependency can lead to a more resilient system/network/society.

Currently Boise State University does not have a similar program. Currently, there is no such program across Idaho.

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

For budgetary purposes the following conservative assumptions were made to represent anticipated master's student behavior:
  • Master's students make up 50% of the incoming new master's program and certificate students every semester
  • Master's students are 35% full time (4 semesters to complete) and 65% part time (8 semesters to complete)

Proposed Program: Projected Enrollments and Graduates First Five Years

6

Program Name: MS in Cyber Operations and Resilience											
Projected Fall Term Headcount Enrollment in Program						**Projected Annual Number of Graduates From Program**					
FY22 (first year)	FY23	FY24	FY25	FY26		FY22 (first year)	FY23	FY24	FY25	FY26	
10	40	67	92	107		0	6	16	31	39	

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

    The program's size will be scaled to demand for the program. The numbers in the table above reflect a reasonable and attainable scaling up of the program.

    Marketing and recruitment efforts will include a digital marketing campaign, a web landing page, request for information form and a full program website with details regarding the key program assets, curriculum plan, and costs. In addition, a comprehensive communication plan will be implemented to attract and nurture interested students. Strategic, personalized communications will engage and support students throughout the recruitment life cycle. Our coaching approach to student services will support online students and maintain their connection to Boise State through graduation.

10. **Minimum Enrollments and Graduates.**
    a. What are the minimums that the program will need to meet in order to be continued, and what is the logical basis for those minimums?

        The numbers below represent the minimum credits and student FTEs for *both* master's and certificate students. Since the master's and certificate programs share courses, the budgets are intertwined.

        Because the program will be utilizing the online fee model, it is best to put minimum enrollment in terms of course registrations, which are what translate to revenue. Based on estimated expenses for instruction and for support personnel expenses, estimate the minimum number of course registrations to achieve breakeven is:

        • Year 1: Annual credits 256, Annual FTEs 10.65
        • Year 2: Annual credits 785, Annual FTEs 32.70
        • Year 3: Annual credits 1,113, Annual FTEs 46.39
        • Year 4: Annual credits 1,336, Annual FTEs 55.65
        • Year 5: Annual credits 1,413, Annual FTEs 58.88

        If enrollments do not meet expectations, expenses will adjust to reflect actual activity. The program's financial sustainability will be evaluated at least annually.

    b. If those minimums are not met, what is the sunset clause by which the program will be

7

considered for discontinuance?

Programs operating under the online program fee model at Boise State University are expected to be fiscally sustainable. If enrollments do not meet expectations, expenses will be adjusted to reflect actual activity. The program's financial sustainability will be evaluated at least annually. If it is determined to be fiscally unsustainable in the long term, it will be discontinued.

11. **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 following measures will ensure the high quality of the new program:

Regional Institutional Accreditation: Boise State University is regionally accredited by the Northwest Commission on Colleges and Universities (NWCCU). Regional accreditation of the university has been continuous since initial accreditation was conferred in 1941. Boise State University is currently accredited at all degree levels (A, B, M, D).

Program Review: Boise State has instituted a new program review procedure. At the inception of new programs, the programs will submit to the Office of the Provost a three-year assessment plan to be scheduled into the Periodic Review/Assessment Reporting Cycle. The plan includes program learning outcomes; and an implementation plan with a timeline identifying when and what will be assessed, how the programs will gather assessment data, and how the program will use that information to make improvements. Then, every three years, the programs will provide Program Assessment Reports (PAR), which will be reviewed by a small team of faculty and staff using a PAR Rubric, which includes feedback, next steps, and a follow-up report with a summary of actions.

Program Development Support: The online MS in Cyber Operations and Resilience is one of several that are being created via the eCampus Expansion Initiative at Boise State University. Boise State's online program development process uses a facilitated program design process to assist program faculty members in the creation of an intentional, cohesive course progression with tightly aligned course and program outcomes. A multi-expert development team, which includes an instructional designer, multimedia specialist, and quality assurance, works collaboratively with the faculty member. One master version of each course is developed for a consistent look and feel of courses across the program; the master course utilizes a professionally created common template aligned with nationally Quality Matters course design standards.

Academic Integrity: Academic integrity is vital to the mission of Boise State University and encompasses the totality of academic rigor, ethical behavior, intellectual curiosity, appropriate teamwork, and persistence. All assignments submitted by a student must represent his/her own ideas, concepts, and current understanding or must cite the original source. Boise State proactively supports academic integrity by providing training, maintaining a website dedicated to academic integrity, providing tools such as pedagogical strategies, workshops, and tips for designing tests, as well as establishing policies and procedures for students who violate the academic integrity policy within the Student Code of Conduct. For this new online program, we will use the following strategies to encourage academic integrity:
  - During the design and development of the curriculum and assessment of each course, instructors will be informed by staff of Boise State's eCampus Center about best practices for online course design based on Quality Matters ™ and best practice strategies to

8

promote academic integrity in online education based on WCET's recommendations (Version 2.0, June 2009)

- Through the program development process, course production, course launch support provided by the eCampus Center, and other means, instructors will be reminded about the importance of academic integrity and encouraged to report and act upon suspected violations.
- Academic integrity will be addressed within online student orientation. Programs may require online students to complete the university's Academic Integrity Online Workshop.
- At the beginning of each course, the instructor will communicate expectations regarding academic integrity to students in the syllabus and verbally and may require completion of the university's Academic Integrity Online Workshop.

<u>Student Authentication:</u> Because the proposed program will be offered entirely online, it is important to include mechanisms by which we authenticate the identity of students enrolled in the program. We will use the following mechanisms:

- During the admissions process, the university will confirm required official transcripts and other documentation required for admission into the program.
- Associated with access to and use of our Learning Management System, a secure log-in environment will be provided and students will be required to use strong passwords and change them every 90 days.
- When high-stakes exams are required, faculty will be encouraged to utilize remote or online proctoring services when appropriate. In those instances, students will need to provide valid photo identification before gaining access to the graded assessments or other required activities.
- Instructors will utilize Canvas's Turnitin plagiarism detection program when appropriate.
- Instructors are expected to be informed of and aware of the importance of student identity authentication and to report and act upon suspected violations.

12. **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 A**.

     N/A

13. **Teacher Education/Certification Programs** All Educator Preparation programs that lead to certification require review and recommendation from the Professional Standards Commission (PSC) <u>prior</u> to consideration and approval of the program by the State Board of Education.

     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?

14. **Three-Year Plan: If this is a new proposed program, is it on your institution's approved 3-year plan?**

     Yes _X_ No _____

     If yes, proceed to question 15. If no:

9

a. **Which of the following statements address the reason for adding this program outside of the regular three-year planning process.**

Indicate (X) by each applicable statement:

	Program is important for meeting your institution's regional or statewide program responsibilities.
	The program is in response to a specific industry need or workforce opportunity.
	The program is reliant on external funding (grants, donations) with a deadline for acceptance of funding.
	There is a contractual obligation or partnership opportunity related to this program.
	The program is in response to accreditation requirements or recommendations.
	The program is in response to recent changes to teacher certification/endorsement requirements.

b. **Provide an explanation for all statements you selected.**

Educational Offerings: Curriculum, Intended Learning Outcomes, and Assessment Plan

15. **Curriculum. Provide descriptive information of the educational offering.**

   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.	30
Credit hours in required courses offered by other departments:	0
Credit hours in institutional general education curriculum	
Credit hours in free electives	
Total credit hours required for degree program:	30

   b. **Curriculum.** Provide the curriculum for the program, including credits to completion, courses by title and assigned academic credit granted.

Master of Science in Cyber Operations and Resilience (Online)	
Course Number and Title	**Credits**
Complete required courses, two certificates, and capstone option	
Required Courses:	
CORE 500 Cyber Systems Thinking	3

10

CORE 501 Cyber Risk Assessment	1
Choose 6 out of 10 (1 credit courses):	6
CORE 502 Cyber Threat Modeling	
CORE 503 Information Assurance	
CORE 510 Applied Cybersecurity Programming	
CORE 511 Artificial Intelligence & Machine Learning	
CORE 512 Introduction to Deep Learning	
CORE 513 Internet of Things Architecture	
CORE 514 Cyber-Informed Engineering	
CORE 520 Cyber Security Operations Center	
CORE 521 Cyber Business and Regulatory Operations	
Elective (potential transfer credit)	3
TOTAL	**10**
Complete two out of following three certificates	
Analyst and Threat Intelligence Certificate	
CORE 550 Cyber Threat Intelligence	3
CORE 551 Cyber Warfare and Conflicts	3
CORE 552 Cyber Digital and Signal Intelligence	3
TOTAL	**9**
Resilience Engineering Certificate	
CORE 560 Cyber Resilience Systems Design	3
CORE 561 Network Design and Exploitation Techniques	3

DocuSign Envelope ID: E4BC928A-D5CB-447D-9FD4-C80A95F162EF

CORE 562 Resilience Coding and Architecture of Devices	3
TOTAL	**9**
Governance Policy Administration Certificate	
CORE 570 Cyber Risk Management	3
CORE 571 Cyber Law, Ethics, and Policy	3
CORE 572 Cybersecurity Governance and Compliance	3
TOTAL	**9**
Capstone - Choose 2	**2**
CORE 578 Teaching	
CORE 579 Certification	
CORE 591 Project	
TOTAL	**30**

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.

- **CORE 578 Teaching** one semester/one course composed of supervised cyber and physical resilience teaching at regional community college and above
- **CORE 579 Certification (obtain one certification)**
  - Certified SCADA Security Architect (CSSA)
  - Certified Information Systems Auditor (CISA)
  - Certified Ethical Hacking (CEH)
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP) certification
  - Certified Project Manager (PMP)
  - Kali Linux Certified Professional (KLCP)
  - Certified Red Team Operations Professional (CRTOP)
- **CORE 591 Project** A comprehensive systems, cyber and physical resilience tabletop exercise accompanied by a post-action report detailing the scenario design, tabletop exercise activities, timeline of events, with recommendations on improving incident detection, response, containment, and remediation.

16.   **Learning Outcomes: Expected Student Learning Outcomes and Connection to**

12

Curriculum.

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

- Properly apply the correct fundamentals of cyber operations, resilience, risk assessment, governance, information assurance, ethics, laws, and policies related to both cyber-physical and information systems.
- Apply acceptable tactics, techniques, and procedures necessary to enhance both operational and resiliency for both cyber-physical and informational security operations.
- Develop, test, implement and access appropriate modalities to secure, inform, involve, and educate stakeholders in security/resilience operations and strategies.
- Evaluate and continuously monitor the operational and resilient maturity of an entity.
- Develop operation and resiliency policies, metrics, testing and security solutions for an entity using both rigorous risk assessment and threat intelligence people, processes, tools and measures.

17. **Assessment plans.**

a. **Assessment Process.** Describe the assessment plan for student learning outcomes that will be used to evaluate student achievement and how the results will be used to improve the program.

The MS in Cyber Operations and Resilience will follow a systematic assessment and improvement process in which multiple approaches will be used, not only to measure student attainment of program outcomes, but to also inform programmatic improvements. The learning outcomes are mapped to courses that provide relevant content. Student work in these courses that address specific outcomes is collected and evaluated by program faculty. The outcomes are assessed on a three-year cycle with data for all outcomes collected each year, and then the results are analyzed every three years. For each outcome, student work across the program is reviewed in a comprehensive review of student work. A group of three faculty members and instructors review the overall attainment of the outcome based on the evidence collected. As part of the review, recommendations for improvement to the program are outlined. All faculty then review these results and make suggestions/changes to improve this process in a program of continuous improvement. Evaluation results inform programmatic, pedagogical, and curricular improvements.

The key knowledge unit as defined by the National Initiative for Cyber Security Education (NICE) Cybersecurity Workforce Framework, NSA CAE, and UK Cyber Security Body of Knowledge (CyBok) will also be mapped to all the courses. This will ensure we are teaching the most important skill sets and critical thinking.

Resources Required for Implementation – fiscal impact and budget.
Organizational arrangements required within the institution to accommodate the change including administrative, staff, and faculty hires, facilities, student services, library; etc.

18. **Physical Facilities and Equipment:** Describe the provision for physical facilities and

13

equipment.

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 available space and equipment is currently acceptable to operate a successful program.

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?

No impact.

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.

Operating expenses associated with support staff and new faculty are reflected in the budget.

19. **Library and Information Resources:** Describe adequacy and availability of library and information 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.

Online resources are available. No impact on the library. No impact on existing programs.

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 needed. No impact on the library.

20. **Faculty/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?

The numbers below represent instruction credits and instruction FTEs for both master's and certificate students. Since the master's and certificate programs share courses, their budgets are intertwined.

The program will fund new adjunct/lecturer instruction to cover the additional

14

instruction credit required by the program:

> Yr 1- 29.50 instruction credits, 1.23 FTE
> Yr 2- 66.50 instruction credits, 2.77 FTE
> Yr 3- 82.00 instruction credits, 3.42 FTE
> Yr 4- 82.00 instruction credits, 3.42 FTE
> Yr 5- 82.00 instruction credits, 3.42 FTE

At maturity, the program will offer a combined total of 40 sections of new courses of which 18 sections will be in cross listed courses with the proposed Bachelor of Science in Cyber Operations and Resilience.

The master's and graduate certificate programs will fund a 0.50 FTE program coordinator in years 1, 2 & 3 and convert to a 1.00 FTE program coordinator starting year 4. The program will fund a 0.25 FTE administrative assistant in years 2 & 3 and convert to a 0.50 FTE administrative assistant starting year 4.

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.

Over the first 4 years of the program, the program will fund partial FTEs of Dr. Sin Ming Loo, a current professor in the Department of Electrical and Computer Engineering:

> Yr 1- 0.10 FTE
> Yr 2- 0.10 FTE
> Yr 3- 0.08 FTE
> Yr 4- 0.05 FTE

Dr. Sin Ming will provide course content and work with the program coordinator to oversee the program.

c. **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?

Because the program will fund instruction and administrative support, it is anticipated that limited instructional and administrative support resources from existing programs will be used for the proposed program, there will be a minimal impact on resources available for existing programs.

d. **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.

The following positions will be hired for the program:
- Adjunct Instruction
- Program Coordinator
- Administrative Assistant

Expenses for these positions are included in the program budget sheet.

21. **Revenue Sources**

15

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?

   N/A

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.

   No new appropriation will be required.

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?

         The 0.50 FTE Program Coordinator will be funded for one year (January 2021-December 2021) by the Boise State Online Innovation Fund. This fund is funded by online fee revenue and acts as seed funding for online academic programs, online course development stipends to faculty, open education resource grants and eventually innovation grants.

   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?

         N/A

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.

         N/A

   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.

         The student fee will be in accordance with the Online Program Fee as defined in the Board Policy V.R., 3.a.x. That policy enables the institution to set a price-point appropriate for the program; students will pay an online program fee in lieu of tuition. The price-point for our online program fee will be as follows: $525 per credit.
         For the 30 credits required for completion of the proposed program, the total cost will be $15,750.

         We project that by the fourth year of the program, it will generate 1,787 SCH, which will yield a total revenue of $938,231.

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

16

- 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).

The budget below represents revenues and expenses for both master's and certificate programs. Since the certificate and master's program share courses, the instruction and support expenses are intertwined.

17

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
- 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).

I. PLANNED STUDENT ENROLLMENT

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	FTE	Headcount	FTE	Headcount	FTE	Headcount	FTE	Headcount	FTE	Headcount
A. New enrollments	9.6	32	33.3	71	51.0	108	67.0	136	74.9	147
B. Shifting enrollments	1.1	4	3.7	8	5.7	12	7.4	15	8.3	16
Total Enrollment	10.7	36	37.0	79	56.6	120	74.5	151	83.2	163
Student Credit Hours Generated	256		889		1,359		1,787		1,997	

18

19

II. REVENUE

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
1. New Appropriated Funding Request										
2. Institution Funds		$44,978								
3. Federal										
4. New Tuition Revenues from Increased Enrollments										
5. Student Fees		$134,269		$466,548		$713,631		$938,231		$1,081,671
6. Other (i.e., Gifts)										
Total Revenue	$0	$179,247	$0	$466,548	$0	$713,631	$0	$938,231	$0	$1,081,671

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.

Budget Notes:

I.A, B. Calculation of FTE and headcount as follows:
>1 FTE = 24 graduate credits
>Headcount determined as the distinct number of students in the program that year.
>Assume that 90% of the enrollments will be new enrollments and 10% will be shifting enrollments.
>Assume 20% attrition from 1st to 2nd semester, then 3% attrition every semester. No attrition from 2nd to last semester to last semester.

II.2. The University will sponsor the program coordinator for 1 year using funds from the Boise State Online Innovation Fund

II.5. Student Fee revenue calculated as Student Credit Hours * $525 per credit.
>$525 calculated as estimate of 2021-2022 per-credit
>To be conservative, assume in calculations that per-credit fee does not increase over time

III. EXPENDITURES

A. Personnel Costs

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
1. FTE		1.98		3.52		4.67		4.92		4.92
2. Faculty		$0		$0		$0		$0		$66,967
3. Adjunct Faculty		$50,150		$116,442		$162,180		$174,182		$139,944
4. Graduate/Undergrad Assistants										
5. Research Personnel										
6. Directors/Administrators		$60,550		$45,275		$78,398		$76,927		$73,158
7. Administrative Support Personnel				$8,498		$8,752		$18,030		$18,571
8. Fringe Benefits		$26,811		$31,483		$48,027		$53,370		$73,905
9. Other:										
Total Personnel and Costs	$0	$137,510	$0	$201,697	$0	$297,358	$0	$322,509	$0	$372,545

Budget Notes (continued)
III.A.2 Lecturer FTE: Calculated using (Credit hour load)/24
III.A.3 Adjunct FTE: Calculated using (Credit hour load)/24
III.A.6 Administrator: Program Coordinator (0.5 FTE in years 1,2,3, 1.0 FTE in years 4+). Additional expense included in year 1 to reflect anticipated Jan 2021 start date. Institutional funds will fund position Jan-Dec 2021
III.A.7 Administrative Support: Administrative Assistant (0.25 FTE in years 2 & 3, 0.50 FTE in years 4+)
III.A.8 Benefits calculated at staff fringe rate of $11,650+(annual wage*20.47%) professional staff and $11,650+(annual wage*21.57%) classified staff

B. Operating Expenditures	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	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										
5. Materials and Supplies										
6. Rentals										
7. Materials & Goods for Manufacture & Resale										
8. Miscellaneous - Computer Hardware/Software		$500		$500		$500		$1,000		$2,000
Total Operating Expenditures	$0	$500	$0	$500	$0	$500	$0	$1,000	$0	$2,000

Budget Notes (continued):
III.B.8   Miscellaneous: Computer hardware/software

22

	FY 2022		FY 2023		FY 2024		FY 2025		FY 2026	
	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time	On-going	One-time
C. Capital Outlay										
1. Library Resources										
2. Equipment										
Total Capital Outlay	$0	$0		$0		$0		$0		$0
D. Capital Facilities Construction or Major Renovation										
E. Other Costs										
1. Boise State University Support		$67,134		$233,274		$356,815		$469,115		$540,835
Utilities										
Maintenance & Repairs										
Other										
Total Other Costs	$0	$67,134	$0	$233,274	$0	$356,815	$0	$469,115	$0	$540,835
TOTAL EXPENDITURES:	$0	$205,145	$0	$435,471	$0	$654,673	$0	$792,625	$0	$915,380
Net Income (Deficit) to College	$0	-$25,898	$0	$31,077	$0	$58,958	$0	$145,606	$0	$166,291

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

III.E.1   Boise State University Support is defined as follows:

Boise State Central Services (10.00% of revenue): A fund dedicated to funding support services for online students.

Boise State eCampus Center (8.75% of revenue): Provide funding for initiative management, online course/program development and other support services

Boise State Online Innovation Fund (3.80% of revenue): Seed funding for academic programs, course development stipends to faculty, open education resource grants and eventually innovation grants
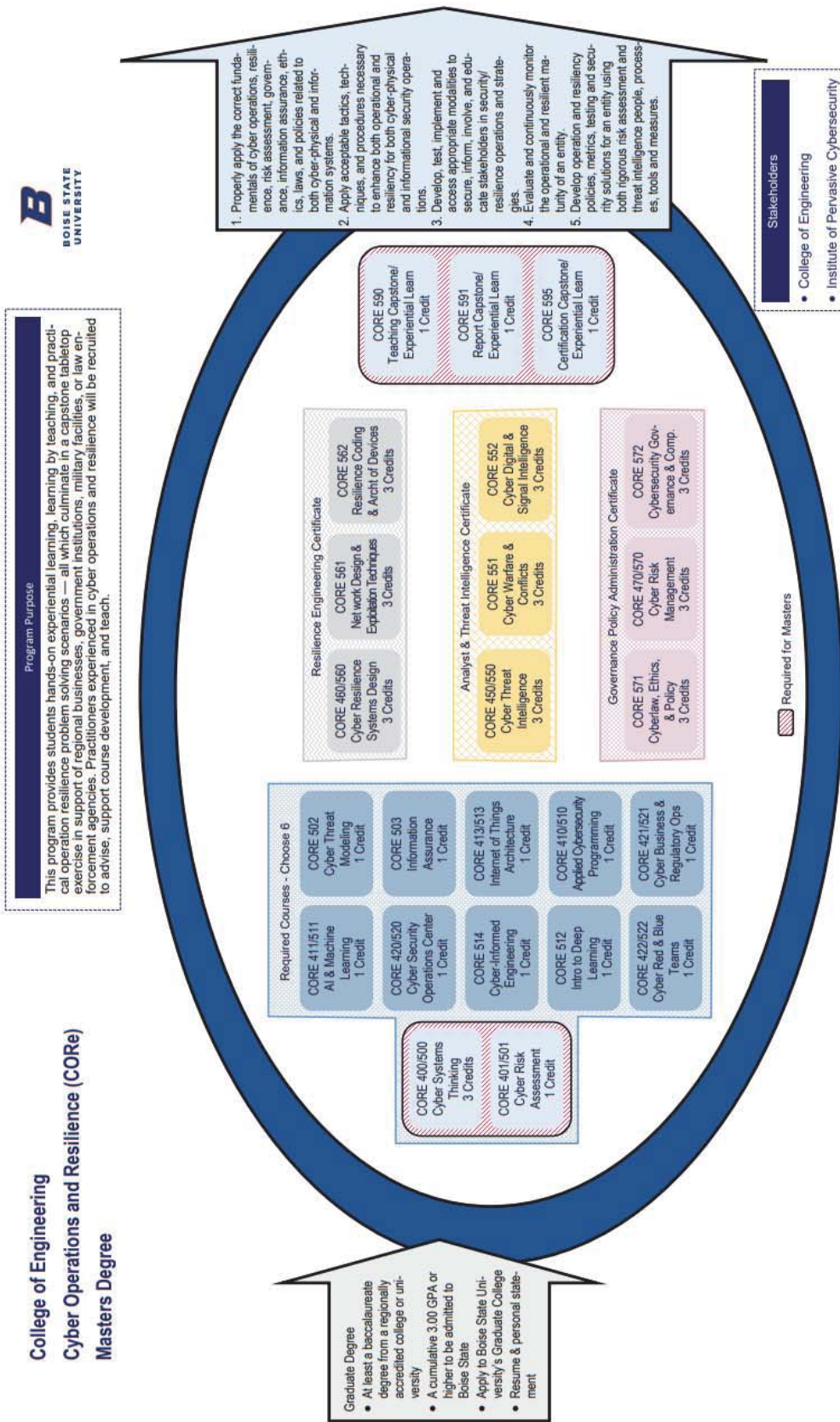
Boise State Online Marketing, Recruitment, Enrollment, Advising and Retention Fund (27.45% of revenue): A fund dedicated to marketing the program, recruiting students, enrolling qualified students, advising students and retaining students throughout the life of the program

APPENDIX A – Program Map

College of Engineering
Cyber Operations and Resilience (CORe)
Masters Degree

BOISE STATE UNIVERSITY

Program Purpose

This program provides students hands-on experiential learning, learning by teaching, and practical cyber operation resilience problem solving scenarios — all which culminate in a capstone tabletop exercise in support of regional businesses, government institutions, military facilities, or law enforcement agencies. Practitioners experienced in cyber operations and resilience will be recruited to advise, support course development, and teach.

1. Properly apply the correct fundamentals of cyber operations, resilience, risk assessment, governance, information assurance, ethics, laws, and policies related to both cyber-physical and information systems.
2. Apply acceptable tactics, techniques, and procedures necessary to enhance both operational and resiliency for both cyber-physical and informational security operations.
3. Develop, test, implement and access appropriate modalities to secure, inform, involve, and educate stakeholders in security/resilience operations and strategies.
4. Evaluate and continuously monitor the operational and resilient maturity of an entity.
5. Develop operation and resiliency policies, metrics, testing and security solutions for an entity using both rigorous risk assessment and threat intelligence people, processes, tools and measures.

Stakeholders
- College of Engineering
- Institute of Pervasive Cybersecurity

Graduate Degree
- At least a baccalaureate degree from a regionally accredited college or university
- A cumulative 3.00 GPA or higher to be admitted to Boise State
- Apply to Boise State University's Graduate College
- Resume & personal statement

Required Courses - Choose 6

CORE 411/511 AI & Machine Learning 1 Credit	CORE 502 Cyber Threat Modeling 1 Credit
CORE 420/520 Cyber Security Operations Center 1 Credit	CORE 503 Information Assurance 1 Credit
CORE 514 Cyber-Informed Engineering 1 Credit	CORE 413/513 Internet of Things Architecture 1 Credit
CORE 512 Intro to Deep Learning 1 Credit	CORE 410/510 Applied Cybersecurity Programming 1 Credit
CORE 422/522 Cyber Red & Blue Teams 1 Credit	CORE 421/521 Cyber Business & Regulatory Ops 1 Credit

CORE 400/500 Cyber Systems Thinking 3 Credits
CORE 401/501 Cyber Risk Assessment 1 Credit

Resilience Engineering Certificate

| CORE 460/560 Cyber Resilience Systems Design 3 Credits | CORE 561 Network Design & Exploitation Techniques 3 Credits | CORE 562 Resilience Coding & Archit of Devices 3 Credits |

Analyst & Threat Intelligence Certificate

| CORE 450/550 Cyber Threat Intelligence 3 Credits | CORE 551 Cyber Warfare & Conflicts 3 Credits | CORE 552 Cyber Digital & Signal Intelligence 3 Credits |

Governance Policy Administration Certificate

| CORE 571 Cyberlaw, Ethics, & Policy 3 Credits | CORE 470/570 Cyber Risk Management 3 Credits | CORE 572 Cybersecurity Governance & Comp. 3 Credits |

CORE 590 Teaching Capstone/Experiential Learn 1 Credit
CORE 591 Report Capstone/Experiential Learn 1 Credit
CORE 595 Certification Capstone Experiential Learn 1 Credit

Required for Masters

23

APPENDIX B – Letters of Support

Idaho National Laboratory – Scott Cramer, Director Cybercore Integration Center

State of Idaho, Information Technology Services – Keith Tresh, Chief Information Security Officer

Ursus Security, LLC – Kim L. Jones, Founder and Managing Director

Johnny Security Seed, LLC – Richard W. Owen, CEO and Chief Evangelist

MUFG Union Bank, N.A. – Stanley R. Jarocki, Vice President

Idaho National Laboratory **INL**

October 13, 2020   CCN 248073

Idaho State Board of Education
650 West State St.
Suite 307
Boise, ID 83720

Subject: Letter of Support Regarding Boise State Course Offerings in Cyber Operations and Resilience

Dear Board Members,

As part of our continued collaboration with Boise State University (BSU) and in support of the Cybercore Integration Center (CIC) mission at Idaho National Laboratory (INL), this letter expresses our strong endorsement of the proposed Cyber Operations and Resilience course offerings.

INL is a world leader in research and technologies for securing and protecting the critical infrastructure of the United States and is focused on fundamental challenges with greatest impact. Building on the current success of BSU and CIC collaborations, these competency-based learning models will help to reach additional students while addressing outstanding needs in the current workforce.

INL has been observing the cybersecurity security curriculum development across the state of Idaho. University of Idaho offers a BS in Cybersecurity, a degree focused on computer science and programming. Idaho State University is now offering a BAS in Cyber-Physical Systems Engineering Technology, concentrated on industrial cybersecurity. There is another identified need for cyber operations, which targets frontline workers who continually face security concerns and address challenges across the enterprise. We are delighted that BSU has taken the appropriate steps to address this gap, at both the BS and MS level, and are prepared to make course offerings available as soon as next fall.

The fact that the courses will be available as an asynchronous online program, opens the instruction to much broader audiences across the state and affords full-time workers and remote learners the ability to build skills outside of the traditional classroom setting. This progressive and flexible platform offers broad reach and greater access to a variety of students, from diverse backgrounds and skill sets, to advance education and workforce development efforts necessary to meet cybersecurity needs now, and in the future.

In short, we see these programs as beneficial to industry, local governments, counties, and state entities in training cybersecurity frontline workers to protect and defend, enhance critical thinking skills and provide more resilience within our cyber environments, which addresses elements currently in short supply and which will only grow in demand. Increasing the number

of people capable of cyber operations and accelerating their development, is core to our mission and vital to both our state and the nation.

We applaud BSU efforts and continued contributions in supporting the Idaho cyber-education ecosystem and willingness to advance offerings designed to provide access to a wide range of students, while addressing identified needs is the workforce.

We believe these efforts will be of benefit to the community, the state and the region, as well as INL, and strongly support the proposed offerings being put into practice and made available.

Sincerely,

Scott Cramer, Director Cybercore Integration Center
National & Homeland Security

SC:KL

Distribution:
Sin Ming Loo, Boise State University

cc: Z.D. Tudor, MS 3750
        W.C. Kiestler, MS 3750
        S.F. McAraw, MS 1444
        E.J. Taylor, MS 1444
        M.T. Bingham, MS 3605

26

State of Idaho

Information Technology Services
Office of the Governor

BRAD LITTLE
Governor
JEFF WEAK
Administrator
GREG ZICKAU
Deputy Administrator/
Chief Information Officer

11331 W. Chinden Blvd, Suite B201
P.O. Box 83720
Boise, ID 83720-0042
Telephone (208) 605-4000 or FAX (208) 605-4093
http://its.idaho.gov

September 23, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear Board Members,

I am writing this letter in support of Boise State University's proposed Bachelor of Science and Master of Science Degree in Cyber Operations and Resilience (CORe).

Given the importance of cybersecurity in every aspect of modern life and the shortage of trained cybersecurity professionals nationwide, this program and the graduates it produces will benefit the public and private sectors inside Idaho and the nation a whole. The proposed Cyber Operations and Resilience programs will build a pathway for professionals to change careers and help existing cybersecurity professionals deepen their expertise. This program will also help cybersecurity professionals progress into management level positions and will feed some of the PhD programs statewide if these same professionals choose to continue their education by pursuing a doctorate degree.

Boise State University already offers a Bachelor of Science in Computer Science with a Cybersecurity emphasis and a PhD in Computing with Cybersecurity emphasis, so these proposed programs fill a missing level that would be attractive to many potential students. Idaho employers need multiple universities inside our state to offer programs that specialize in all aspects of cybersecurity to satisfy the demand and need for trained cybersecurity professionals. To that end, Boise State University is participating in conversations within our state to codify an agreement for all major universities to share courses, curriculum and resources within the cybersecurity area of concentration.
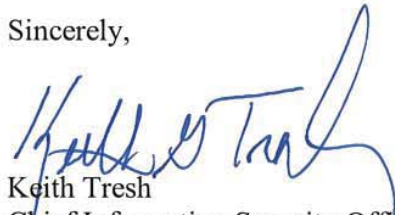
I also want to highlight the fact that Boise State University hired several faculty members with operational cybersecurity experience in the last five years. They have also worked hard to seek and maintain many key industry/government relationships within the cybersecurity field including the State of Idaho, Information Technology Services as well as the Idaho National Lab.

27

As an example, and a matter of fact, I was hired in August of 2019 to teach in their current baccalaureate program. I also participate in all of their Cybersecurity planning and sit on the Board of Boise State's up-and-coming Institute for Pervasive Cybersecurity.

In closing, I would like to add that as a public servant with over 25 years of information technology and cybersecurity operational experience, I feel these programs can and will dramatically increase the available number of trained cybersecurity professionals within Idaho and nationwide. I wholeheartedly support the creation and implementation of both the Bachelor of Science and Master of Science degrees in Cyber Operations and Resilience!

If you have questions or need more information, please feel free to contact me at (208) 605-4054 or keith.tresh@its.idaho.gov.

Sincerely,

Keith Tresh
Chief Information Security Officer
Office of Information Technology Services
Office of the Governor
Keith.Tresh@its.idaho.gov
Office: (208) 605-4054
Cell: (208) 407-8509

Ursus Security LLC
"Standing in the Gap"

October 8th, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Esteemed Board Members:

I am writing this letter to express my strongest possible support for Boise State University's Cyber Operations and Resilience (CORe) degree programs.

As a senior cybersecurity profession and former senior cyber executive, I have long struggled with the challenge of finding skilled professionals to fill the ranks of my supported organizations. As the cyber talent gap widened and universities took up the call for support, I was disappointed at the caliber of students produced by our institutes of higher learning. In far too many cases "cyber graduates" had only theoretical knowledge of cybersecurity principles across a narrow portion of the career field; they were inadequately prepared to face the fluid (and often non-standard) real-world dilemmas faced by today's cyber warriors.

When I was asked to evaluate Boise State University's CORe program and approach, I entered the process with a high degree of skepticism. I am pleased to say that I left the process more excited and impressed than I have been with a university-led program in a long time. Boise State's curricula (at both the Bachelors and Masters levels) remains entrenched in a real world, practical approach which prepares students to meet the challenges of a cybersecurity career head on. Further, the modular approach is extremely well suited for those looking to transition careers – something which must be embraced if we are ever to close the cyber job-talent gap. Boise State's commitment to hiring top tier cyber talent – including senior cyber executives and not just educational professionals – gives me an extremely high degree of confidence around the caliber of graduates these programs will produce. I look forward to introducing Boise State's first crop of graduates into the companies I advise and support.

Boise State University is to be commended for taking a proactive, thought-leading approach to solving one of our nation's most vexing problems. I urge you to support these efforts wholeheartedly.

29

Ursus Security LLC
"Standing in the Gap"

Please feel free to contact me if you have questions.

Sincerely,

Kim L. Jones CISM, CISSP, CDGSE, M.Sc.
Founder and Managing Director
Ursus Security LLC
(480) 253-9120
Kim.Jones@UrsusWorldwide.com
https://www.linkedin.com/in/kimjones-cism/

30

Johnny Security Seed, LLC.
4412 E la Estancia Cir
Cave Creek, AZ 85331
www.JohnnySecuritySeed.com

September 30, 2020

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear Board Members,

I am writing this letter in support of Boise State University's Bachelor of Science (BS) and Master of Science (MS) Degree programs in Cyber Operations and Resiliency (CORe). I understand that Boise State and other universities offer degrees in Computer Science with an emphasis in Cyber Security, but Cyber Security can no longer be just an extra area of study.

In today's world we continue to collect, process and store more information and base many decisions on this ever-growing collection of data. This simply adds greater importance and risk to those systems and data. However, we have a nation-wide shortage of skilled and educated people who can provide the protection that we require. The Cybersecurity Industry is in a need of not only more qualified people, but those who are trained to think and address rapidly changing threats.

I applaud Boise State University for creating programs that start first with the high school student. Johnny Security Seed has a similar effort and approach. As one who has significant technical training and many certifications stacked on top of my formal college education, I have found that the combination has been a key element in my success. I see these programs as vital to creating professionals who can address ever-changing operational issues to ensure the resiliency of critical data and systems. I also support the program's experiential learning credit approach. Hackers follow no formal education road map and to respond we need to create a workforce capable of accomplishing the mission, oftentimes in a less structured fashion. I believe that the proposed curriculums would provide my current and prior businesses a more capable employee to help in this ongoing fight.

As a point of reference, I have spent over 50 years protecting information of which over 30 years was focused on creating and managing cyber security programs. I created the Information Security Program for Mission Operations at Johnson Space Center, NASA. While there, I was awarded a "Silver Snoopy" by the astronauts for the program and a Continuous Improvement Award by the NASA Administrator for avoiding over $25M in costs. After that, I created four other very successful security programs across various industries. I am a past International President of the Information Systems Security Association (ISSA) and a member of the Information Security Hall of Fame. Most recently I was honored with Fellow status of the world renowned Ponemom Institute (https://www.ponemon.org).

Should you have any questions of if I may be of other assistance, I can be contacted at Rich@JohnnySecuritySeed.com or on my cell at 480-686-5527.

1

31

Sincerely,

Richard W. Owen, Jr.
CEO and Chief Evangelist

32

⊙ **MUFG**

MUFG Union Bank, N.A.
Information Risk Management
Risk Management Division for the
Americas
6802 E Bobwhite Way
Scottsdale, AZ 85266
T: +1-480-381-0887

Stanley.Jarocki@unionbank.com

Idaho State Board of Education
650 West State Street, 3rd Floor
Boise, ID 83702

Dear State Board Members:

I am writing this letter in full support of the proposed Cybersecurity Bachelor and Master programs at Boise State. These programs incorporate fundamental aspects of Cybersecurity that are needed to maintain a key core element – Cyber Operations and Resiliency – that are so desperately needed and which require trained individuals to cover all critical infrastructure sectors today and in the future.

Today, as a veteran of many attacks that I have experienced in the Federal Government sector, the critical infrastructure sectors – financial, healthcare, retail – and having lived through 911 at ground zero, I speak from experience. Cyber resources that drive the systems of our environment must be secure, auditable, compliant, and resilient. Knowledgeable talent is needed at the entry level and senior executive level to promote the proper planning, testing and execution to keep these systems running. Just imagine what would happen if hospital cyber system went down and doctors, nurses and staff had to resort to pen and pencil. Today in the time of the pandemic huge numbers of lives would be lost, treatment would have to stop and those needing care would not be able to get it. And it could be your family members or yourself. Sounds farfetched? Well, it is happening as they are being attacked not only by natural disasters but by Bad Actors using Ransomware, DDoS attacks and other extortion attempts. Cyber is the nervous system, communications paths, and knowledge repositories upon which our lives are built and depend. Therefore, the need for Cyber professionals and cyber warriors to support and build strong infrastructure is needed. Where are they going to get this knowledge? They will be able to get this critical knowledge base from Boise State's Bachelor and Master's programs in Cyber Operations and Resiliency.

The key to these powerful new programs - the Cyber Operations and Resilience (CORe) Bachelor of Science (BS) and Master of Science (MS) programs – lies in their ability to develop focused curriculum that provide needed skill sets that they can use day one. These programs are geared to instruct and produce Cybersecurity professionals focused on operational tools, methodologies, and efficiencies, as well as ensuring system resiliency for maximum risk reduction coverage using risk appropriate costs. The goal of the CORe curriculums is to prepare learners at the beginning levels to view and think of systems as holistic models while determining how resiliency can be achieved. CORe presents the interdependencies infrastructure has between cyber and physical to achieve operational effectiveness. In short, CORe is about business, real life and the world of cybersecurity and their interrelationships and how strengthening the bonds of dependency can lead to a more robust and resilient system/network/society.

A holistic system level thinking approach is at the heart of the CORe program. The asynchronous online curriculum provides for a challenging set of achievement modalities:

1. Pathways for high school students (traditional and career & technical education), community college graduates, and working professionals with an undergraduate degree in any field,
2. Stackable certification pathways for learners to achieve career alignment without the need for long-term program commitments,
3. A curriculum that awards experiential learning credits in an affordable manner,
4. A potential for strong internship with local and national industries and critical infrastructure sectors, and
5. Accelerated BS/MS curriculum for learners looking to achieve maximum career opportunity in the shortest time frame possible.

As an early practitioner in the field of Cybersecurity I had to boot strap my knowledge with a lot of "OJT" (On the Job Training) to get the job done. Adding needed skills such as audit, risk management and executive leadership was not easy. Holding CISO positions in a variety of industries and major companies in the financial, healthcare and retail sectors. - I can attest that finding individuals with these skills is extremely hard. Nationally, there is estimated to be over 3 million job openings creating a dire shortage of talent. This is exasperated even more due to the increased attacks by bad actors and nation states who feel we are too preoccupied with the "Pandemic." Trained people are desperately needed with practical operational skills who can contribute day one.

As the editor / contributor of the USA National Security Plan for the financial sector and chief architect of the Financial Services Information Sharing and Analysis Center and presently as a VP of Information Risk Management for the 5th largest bank in the World – MUFG – I can attest that quality trained talent is desperately needed. Additionally, as an advisor to higher education intern programs, it is extremely important that Cybersecurity needs to start with K-12 to show that diversity and excitement does exist in the world of Cybersecurity. I believe the curriculum that I have reviewed is the right start in our battle to cultivate passionate and talented individuals who will be practically trained to jump in and defend the cyber world of today and, more importantly, tomorrow.

I also believe local Boise Headquartered companies such as Albertsons is another example of an organization that requires cybersecurity and resiliency as we have observed in recent disasters and the Pandemic. Food supplies are critical and the supply chain systems that support operations and get the goods to the stores and people is critical to humanity's survival.

So it is extremely important that support for the ability to produce learners with the caliber of talent needed for the state of Idaho, the nation, and worldwide, be provided at the highest level of state government – through the governor's office, and through approval of these programs through the state board of education.

Sincerely,

Stanley R. Jarocki

Stanley R. Jarocki

Vice President

34

Cybersecurity Education Opportunities Fall 2021 and Beyond

Knowledge (y-axis)

PhD in Computing, Cybersecurity Emphasis - Now / In-person

*MS, Cyber Operations & Resilience - Fall 2021 / Online
*MS, Cybersecurity - Fall 2021 / In-person

Certificate in Cryptography and Cryptanalysis - Fall 2021 / Online

BS, Computer Science w/ Cybersecurity Emphasis - Now / In-person

*BS, Cyber Operations & Resilience - Fall 2021 / Online
BS, Computer Systems Engineering - Fall 2021 / In-person

Cybersecurity Minor - Now / In-person

Four Cyber/Physical Certificates for STEM Students - Now / Hybrid
(Power, Process, Software, Hardware)

Cryptography and Cryptanalysis Certificate - Fall 2021 / Online

Cyber Operations Certificate and Certification - Now / Online

Cybersecurity For All Certificate - Now / Online

Legend:
- Graduate Degrees
- Graduate Certs
- Undergrad Minors or Degrees
- Undergrad Certs
- Certifications

*Under Review. Forthcoming subject to the Board approval.

IRSA

Student Involvement (not to scale) (x-axis)

TAB 6 Page 1