UNIVERSITY OF IDAHO

SUBJECT

Doctor of Philosophy in Cybersecurity

APPLICABLE STATUTE, RULE, OR POLICY

Idaho State Board of Education Governing Policies & Procedures, III.G.

BACKGROUND/DISCUSSION

The Department of Computer Science at the University of Idaho is proposing the introduction of a Doctor of Philosophy (Ph.D.) program in Cybersecurity due to the significant growth and success of our existing Bachelor of Science (B.S.) and Master of Science (M.S.) programs in Cybersecurity. For example, over the past four years, the new B.S. program in cybersecurity has expanded from zero to 117 students, reflecting the increasing demand for cybersecurity educational opportunities.

Nationwide the rapid advancement of technology and the increasing frequency of cyber threats have created a critical need for highly trained cybersecurity professionals. Organizations across various sectors are seeking experts who can protect their digital assets and ensure the security of their information systems. The success of our B.S. and M.S. programs in Cybersecurity demonstrates the strong interest in our programs that can be leveraged to fulfill this need. The rapid growth in enrollment highlights our programs' relevance and the quality of education provided by our faculty.

A Ph.D. program in particular will foster advanced research and innovation in cybersecurity. Doctoral students will contribute to the development of new technologies and methodologies to combat emerging cyber threats. This will enhance the university's reputation as a leader in cybersecurity research. There is significant demand from Idaho industry and government for cybersecurity professionals and cybersecurity innovations. The Ph.D. program will help to meet those demands while strengthening our partnerships with industry leaders. Collaborations with companies and government agencies will provide students with practical experience and opportunities to work on real-world cybersecurity challenges. This will also facilitate the transfer of cutting-edge research into practical applications.

By producing highly skilled cybersecurity experts, the Ph.D. program will contribute to the economic development of the region and the nation. Graduates will be equipped to take on leadership roles in academia, industry, and government, addressing critical cybersecurity issues and enhancing national security.

The proposed Ph.D. program aligns with the University of Idaho's strategic goals of promoting research excellence, fostering innovation, and addressing societal

needs. It will attract top-tier students and faculty, further elevating the university's academic standing.

IMPACT

The proposed Ph.D. program in cybersecurity is a critical aspect of Idaho's overall strategy to address the critical demand for more cybersecurity professionals. In addition to directly recruiting students into the program it will improve recruitment into the existing M.S. and B.S. cybersecurity programs by creating a complete pathway for students who are planning on or interested in obtaining a Ph.D. It will raise the profile of all our cybersecurity programs, thereby increasing recruitment. The program and the resulting research will raise the profile of the University of Idaho and the State of Idaho in the cybersecurity community attracting business to the state.

Total expenditures ranges from $254,751 - $996,785 of new ongoing appropriated funds and $42,000 - $160,000 annually of one-time institution funds over a four-year period. House Bill 734, for fiscal year 2025, included $2,139,100 for Operational Capacity Enhancement, of which $800,200 was for the Cybersecurity Ph.D. Workforce Expansion. This new appropriation outlined the critical demand for Cybersecurity professionals due to the escalating threat of cyberattacks against critical infrastructure. The shortage of skilled cybersecurity professionals nationwide, and particularly in Idaho, necessitates immediate action. The Governor's Cybersecurity Task Force Report in March 2022 highlighted the urgency of addressing this issue. The United States experienced a staggering shortage of 3.5 million cybersecurity jobs in 2021. Idaho has seen a 28% increase in cybersecurity job openings, with over a thousand positions remaining unfilled. Industry leaders, including the Idaho National Laboratory, are actively seeking trained cybersecurity professionals. Investing in cybersecurity education is critical to supplying Idaho with skilled talent. Other states are heavily investing in cybersecurity research and education. For example, Dakota State University secured significant funding to expand cybersecurity programs, and neighboring states like Washington are investing heavily in cybersecurity degree programs. Idaho's higher education institutions need support to compete, attract faculty, and retain students. The funding received in response to this request will allow the University of Idaho to address Idaho's immediate and long-term workforce needs in cybersecurity. With the Cybersecurity Ph.D. program, we aim to ensure a steady supply of qualified professionals who can bolster cybersecurity defenses, and support Idaho's economic growth.

This funding will support recruiting new students into our cybersecurity program. Over the course of the next five years, it will allow an increase of up to 270 undergraduate students and 15 graduate students annually. This investment from the state will allow us to serve more students who are ready to learn and serve our state as they protect information and assets in the cybersecurity field. There will also be an increase in grant awards, ranging from $250,000-$350,000 annually, as faculty establish their research portfolios.

The original proposal included funding for three tenure track faculty and one clinical faculty member. This has been modified to one tenure track program director, one tenure track faculty, and two clinical faculty (see below). There are two reasons for the change. The current director of the Center for Secure and Dependable Systems (UI's cybersecurity research center) is stepping down, so we have the opportunity for an external search. This is a slightly more expensive position, so it required reducing one of the originally requested tenure track positions to a clinical faculty position. Additionally, the unexpectedly rapid growth of our cybersecurity programs has put additional pressure on our teaching bandwidth making a second clinical faculty hire more advantageous. Cybersecurity Workforce (requesting 6.00 FTP; $596,100 total salaries; $800,200 total General Fund PC funding with benefits):

- Tenure Track Professor/Program Director, $177,100, 12-month appointment, 1.00 FTP
- Tenure Track Professor, $105,000, 9-month appointment, 1.00 FTP
- Clinical Faculty (two), $94,500, 9-month appointments, 1.00 FTP each
- Information Technology Staff, $75,000, 12-month appointment, 1.00 FTP
- Program Manager, $50,000, 12-month appointment, 1.00 FTP

ATTACHMENTS

Attachment 1 – Doctor of Philosophy in Cybersecurity Proposal

BOARD STAFF COMMENTS AND RECOMMENDATIONS

University of Idaho anticipates six initial enrollments in FY25 and reaching 26 by FY29. Graduates will be realized starting in year three with one graduate and the program anticipates reaching four by year five. To keep the program viable, the university must regularly offer cybersecurity courses, some of which may be available to students in other majors. If the Ph.D. program does not reach at least six full-time students by its third year, U of I will reassess both the Ph.D. and MS programs in Cybersecurity. If the MS program has sufficient enrollment, the Ph.D. program can continue, as the courses will still be necessary for MS students and will not add teaching burdens. However, if both programs have low enrollment, the university will consider discontinuing them.

Consistent with Board Policy III.G, the proposed Ph.D. in Cybersecurity was reviewed by an external review panel consisting of Dr. Tyler Moore, the University of Tulsa and Dr. Indrakshi Ray, Colorado State University. Reviewers conducted their onsite review on November 26-28, 2023, and December 3-5, 2023, and provided observations and recommendations for program success. Due to scheduling conflicts, each reviewer could not be on campus for the on-site review at the same time.

The reviewers view the Ph.D. in Cybersecurity as a strong program that addresses a clear need for cybersecurity expertise in Idaho, particularly for organizations like Schweitzer Engineering Laboratories and Idaho National Laboratory. They

highlight a significant shortage of cybersecurity research expertise in the state, which the program could help fill. Reviewers note that despite the university's relatively small size, it has a strong foundation in cybersecurity with experienced faculty and over 25 years of research and education in the field. Reviewers see the program as a natural progression of the university's offerings, well-aligned with the standards of the National Security Agency's Center of Academic Excellence-Cyber Defense program. Reviewers shared observations, potential challenges, and recommendations regarding graduate advising, admissions, resources, and the importance of providing a separate structure for the proposed Ph.D. This will help differentiate between the two Ph.D. programs (Cybersecurity and Computer Science) and avoid any confusion for students. While a written institution response to the external report is not required, the university amended their proposal to include information and clarification to address recommendations provided by the panel.

UI's request to offer a Ph.D. in Cybersecurity is consistent with their Service Region Program Responsibilities and their current institution plan for Delivery of Academic Programs in Region II. In accordance with State Board Policy III.Z responsibilities, no institution has statewide program responsibility specifically for cybersecurity programs. Currently there are no other doctoral programs in cybersecurity offered by Idaho's public postsecondary institutions. U of I currently offers a Ph.D. in Computer Science and Boise State University offers a Ph.D. in Computer Science with a Cybersecurity emphasis.

The proposal completed the program review process and was presented to the Council on Academic Affairs and Programs on November 7, 2024; and to the Instruction, Research, and Student Affairs Committee on December 5, 2024.

Board staff recommends approval.

BOARD ACTION

I move to approve the request by the University of Idaho to create a Ph.D. in Cybersecurity as presented by the full proposal presented in Attachment 1.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

Institutional Tracking No. _____

Idaho State Board of Education

FULL PROPOSAL FORM

Academic Programs

Date of Proposal Submission:	September 24, 2024			
Institution Submitting Proposal:	University of Idaho			
Name of College, School, or Division:	Engineering			
Name of Department(s) or Area(s):	Computer Science			
Official Name of the Program:	Cybersecurity			
Degree Information:	Degree Level: Graduate	Degree Type: PhD		
CIP code or Modification of CIP Code (consult IR /Registrar):	11.1003 Computer and Info. Systems Security/Information Assurance			
Method of Delivery: Indicate percentage of face-to-face, hybrid, distance delivery, etc.	70% Face-to-Face; 25% Hybrid; 5% distance			
Implementation Date:	Fall 2025			
Geographical Delivery:	Location(s)	Moscow, Coeur d'Alene	Region(s)	II
Indicate (X) if the program is/has: (Consistent with Board Policy V.R.)		Self-Support fee		Professional Fee		Online Program Fee
Indicate (X) if the program is: (Consistent with Board Policy III.Z.)	X	Regional Program Responsibility		Statewide Program Responsibility

Indicate those that apply to this request:

- [ ] Undergraduate Program
- [X] Graduate Program
- [ ] Undergraduate Certificate (30 credits or more)
- [ ] Graduate Certificate (30 credits or more)
- [ ] Specialized Certificate (above $250k/FY)

Proposed Action

- [X] New Program
- [ ] New branch campus or change in location
- [ ] Modification of Existing Academic Programs
  - [ ] Converting one program option to a stand-alone program
  - [ ] Consolidating two or more programs into one program
  - [ ] Splitting an existing program into two or more programs
  - [ ] Adding certificate or degrees to existing programs
  - [ ] Program expansion outside an institution's Designated Service Region except for programs for which institutions have statewide program responsibilities as defined in Board Policy III.Z.

College Dean	09/24/2024 Date	Vice President for Research (as applicable)	Date
Graduate Dean/other (as applicable)	9/24/2024 Date	Academic Affairs Program Manager, OSBE	Date
FVP/Chief Fiscal Officer	9/24/24 Date	Chief Financial Officer, OSBE	Date
Provost/VP for Instruction	09/24/24 Date	Chief Academic Officer, OSBE	Date
President	09/24/24 Date	SBOE/Executive Director or Designee 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 or expansion of each new program. All questions must be answered.

Rationale for Creation or Modification of the Program

1. **Describe the request and give an overview of the changes that will result.** 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.

   We are requesting adding a Ph.D. in Cybersecurity to the degrees offered by the Computer Science Department at UI. This program will complement the current degrees we offer: BS, MS, and Ph.D. in Computer Science and BS and MS in Cybersecurity. It will provide a terminal degree for our cybersecurity programs, which have seen explosive growth (Figure 1).

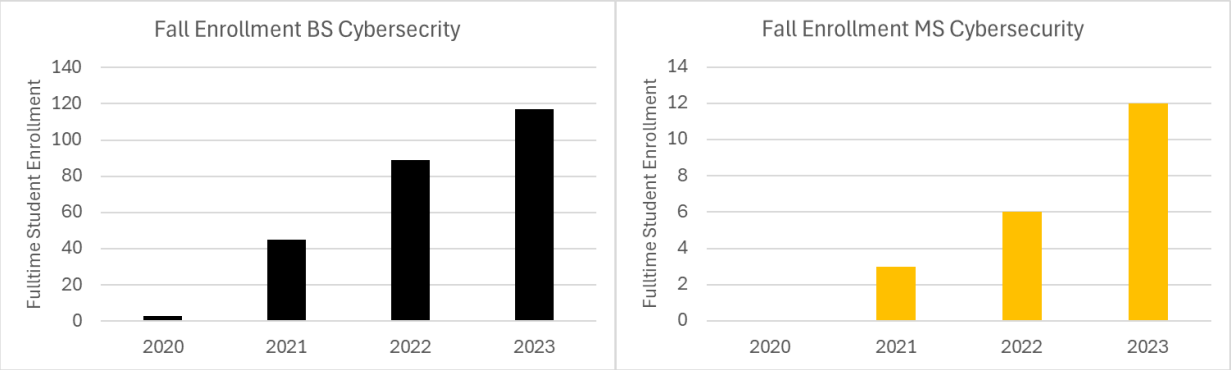

Figure 1: Growth in the BS Cybersecurity program (left) has grown from 3 students in 2020 (the first year the program was offered) to 117 students in 2023. Growth in the MS Cybersecurity program has doubled every year it's been offered (3 in 2021, 6 in 2022, 12 in 2203). During the same 4-year period enrollment in the BS Computer Science program grew by over 100 students.

The BS in Cybersecurity was introduced four years ago, in Fall 2020, it now has 117 majors. We introduced the MS in Cybersecurity in Fall 2021; it now has 12 majors. Of the 42 Ph.D. and 24 MS students pursuing Computer Science degrees roughly half are working on cybersecurity research projects. This rapid growth is driven by an enormous need for cybersecurity professionals of all levels, which this degree would help to fill.

During the same four-year period enrollment in the Computer Science BS also grew by over 100 students (over 40% growth). The addition of a Cybersecurity PhD and the associated increase in faculty and resources will support ongoing growth in the entire Cybersecurity/Computer Science ecosystem at UI.

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

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

This growth of standardized program content, along with the tremendous growth in job opportunities for our graduates, has led to the conclusion that we need to establish dedicated degree paths in cybersecurity. This degree will be focused on advanced cybersecurity concepts, building on the content of our undergraduate cybersecurity degree and creating pathways and synergy with both the MS in Cybersecurity and our research programs.

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.

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

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

1. *Information Security Analysts* – This is the DOL Job title for the following specialized cybersecurity work roles:
    a. System Security Analyst
    b. Cyber Defense Analyst
    c. Cyber Defense Infrastructure Support Specialist
    d. Vulnerability Assessment Analyst
    e. Cyber Defense Forensics Analyst
2. *Network Operations Specialist*
3. *Software Developer*
4. *System Administrator*
5. *Technical Support Specialist*

	State DOL data	Federal DOL data	Other data source: (describe)
Local (Service Area)			Projected increase in jobs over 8 years [Lightcast data] (see below).
State	11.4% to 13.3% increase in jobs over ten years depending on position (see below)	11.6% increase in jobs over ten years http://www.projectionscentral.com/Projections/LongTerm [uses DOL data]	
7 State Region (ID, CO, MN, OR, UT, WA, WY)			20.4% increase in wages 2019-2023(Lightcast data) 13,984 job postings for PhD level candidates in 2023requesting a PhD (compared to 13 PhD cybersecurity graduates from University of Utah in 2023, see below) [Lightcast data]
Nation		+32.7% in jobs over ten years U.S. Bureau of Statistics https://www.bls.gov/emp/tables/fastest-growing-occupations.htm (see below). +31.6% over ten years http://www.projectionscentral.com/Projections/LongTerm [uses DOL data]	

Our Lightcast analysis predicts a 37% increase in jobs in the region from 2022-2032 . The U.S. Bureau of Statistics lists Information Security Analysts as one of the fastest growing occupations in the nation, with an expected employment increase of 32.7% over the next decade. State DOL statistics project 11.4% growth for Computer System Analysts and 13.3% growth for Computer and Information Systems Managers by 2032. In summary, there will be strong workforce needs within the state, and nationally the need is much stronger. This suggests that a lack of available employees is slowing Idaho's growth in this sector.

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.*

We initiated the BS in Cybersecurity in the fall 2020. As of fall 2023 we have 117 Cybersecurity majors. This indicates the strong student interest in the field. We initiated the MS in Cybersecurity in the fall 2021 and we currently have 12 MS students in Cybersecurity.

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

Table 1: Past enrollments in the Cybersecurity (CYB) and in Computer Science (CS) courses that have cybersecurity as the focus (undergraduate/graduate). Note that with the introduction of the Cybersecurity Masters, many of the CS courses were redesignated as CYB courses, with new numbers. Note that there is steady growth at both the graduate and undergraduate levels.

Course	AY20-21	AY21-22	AY22-23	AY23-24	AY24-25 (Fall Data)
CYB110 (Undergraduates)	29	68	104	135	84 (Fall only, also offered Spring)
CS439/539 Applied Security		6/2			
CS447/547 Network Forensics	9/13	8/2			
CS438/CS538 Network Security	17/8	7/4			
CYB/CS536 Advanced Information Assurance Concepts	6	6	6	9	(Offered Spring)
CYB540 Advanced Networking & Security			8	7	15
CYB420/520 Digital Forensics			7/5	5/4	11/9

In addition to internal demand, we expect to see increases in new student enrollment due to the strong growth of cybersecurity jobs in the region, state, and nationally.

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

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

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

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 crosswalks 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.

Instructors will have the option of using inclusive access for textbooks. Courses will be available on-line and via videoconferencing between Moscow and Coeur d'Alene. This will reduce potential relocation costs. Students taking on-line courses from out of state will pay resident rates for courses. Pre-recorded courses will allow students to accelerate the program. New cybersecurity labs will allow students to use dedicated UI hardware and software rather than purchasing their own, reducing costs and giving them a uniform experience.

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)			
		FY21	FY22	FY23	FY24 (most recent)	FY21	FY22	FY23	FY24 (most recent)
UI	**PhD, CS**	45	47	46	42	2	7	9	7
BSU	**PhD, Computing w/ Cybersecurity Emphasis**	10	7	7	9	0	3	0	2

The proposed *PhD in Cybersecurity* degree will be the first PhD in Cybersecurity in the State of Idaho. It was designed from the ground-up to be exceedingly compliant with the criteria, knowledge, and skills detailed in the Center of Academic Excellence in Cyber-Defense (CAE-CD)

denomination by the U.S. National Security Agency and the U.S. Department of Homeland Security. The closest existing programs are the University of Idaho's PhD in Computer Science, many of whose students are doing research in cybersecurity. And Boise State University's PhD in Computing for students with an emphasis in cybersecurity.

Although both UI and Boise State have strong PhD programs, they are focused on computer science and students devote considerable time to Computer Science topics that are not relevant to cybersecurity. E.g. the core courses in Boise State's PhD degree, required of all PhD students, are:

CS 521 – Design and Analysis of Algorithms OR CS 561- Theory of Computation
CS 552 – Operating Systems
CS 573 – Advanced Software Engineering

These are core Computer Science, not Cybersecurity, courses. Students only learn the specific, relatively narrow, portions of cybersecurity that are required for their specific research topics, and these programs do not give graduates the breadth and depth of cybersecurity knowledge that is required by industry or necessary to broadly advance the field. A Cybersecurity PhD allows the entire program to be structured to maximize graduate's knowledge of the field.

(According to Lightcast data - as of 2023, in the 7 state regions (ID, WA, OR, UT, MN, WY, CO) only the University of Utah had a PhD program specifically in Cybersecurity. In 2023 the University of Utah program graduated 13 PhD students. Nationwide there are only 14 Cybersecurity PhD programs. Thus, there is an extreme need for Cybersecurity PhD programs in the region and the nation.)

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.

Not Applicable

This will be the first PhD in Cybersecurity in the state of Idaho. The only similar programs are PhD programs in Computing with an emphasis area or certificate in Cybersecurity. A PhD in Cybersecurity, as opposed to a PhD in another field with an emphasis or certificate, represents a much stronger focus on the field of cybersecurity, with a unique set of required core courses that guarantees graduates of the program will have the complete depth and breadth of cybersecurity required by industry.

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											
Projected Fall Term Headcount Enrollment in Program						**Projected Annual Number of Graduates from Program**					
FY25 (1st year)	FY26	FY27	FY28	FY29		FY25 (1st year)	FY26	FY27	FY28	FY29	
6	12	17	26	26		0	0	1	2	4	

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?

Maximum capacity is determined by the size of the secure, computer equipped classrooms and the number of faculty to mentor PhD students. The secure computing classrooms can hold a total of ~20 students. Currently we only anticipate offering one section of each course, which limits us to no more than 20 students per cohort. Multiple sections of a class and/or expanded classrooms could increase this number. The number of PhD students a faculty can mentor (including additional faculty in the request) is a second limit on the maximum capacity, at approximately 30 PhD students.

Recruiting is primarily a function of the reputation of the University and of our faculty. Currently we recruit more Computer Science PhD students than we can accept and support. We anticipate the same situation for Cybersecurity PhD students and do not expect to need additional recruiting.
The numbers in the table are based on the number of students in and applying to the Computer Science PhD program whose research focus is cybersecurity. We expect a fair number of students in the first year due to pent-up demand followed by a lower, but steady, stream of incoming students.

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?

To maintain a viable program, we need to provide a regular offering of cybersecurity courses. Some of these courses can be taken by students in other majors.

If we have at least 10 students in the program, we will have roughly 5 cybersecurity PhDs in each course. The core courses and optional courses are the same as for the MS in cybersecurity so we anticipate another 5-7 MS students per class. Some Computer Science graduate students will also participate in these courses, bringing the numbers up to 12+ per course, which is a reasonable size for a graduate level course. For courses listed as 400/500 undergraduate Cybersecurity and Computer Science majors will also participate increasing the expected class sizes to 20+.

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

If we can't reach sustained enrollments of at least 6 full time PhD students by the third year we will need to reevaluate the program, along with the MS in Cybersecurity. If the MS is well populated, we can continue to offer the PhD because the required courses will still need to be offered for the MS students, thereby imposing no additional teaching burden. If both programs are under-populated, we will need to sunset them.

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

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

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**. With prior approval from the Board's Executive Director or designee, for programs that require specialized accreditation, external review for the accreditation process may supplant standard external peer review as provided in Board Policy III.G.[1]

See attached Appendix A

13. **Educator Endorsement/Certification Programs**. All new initial educator preparation programs that lead to an Idaho educator endorsement/certification require review and recommendation facilitated by the Office of the State Board of Education and approval from the Idaho State Board of Education.

Will this program include a new initial educator preparation program leading to an Idaho educator endorsement/certification?

Yes ____ No X

If yes, on what date was the new program application endorsement/certification submitted to the Office of the State Board of Education (Educator Effectiveness Program Manager)?

Date _____

[1] For programs that require specialized accreditation, external review for the accreditation process may supplant standard external peer review as in Board Policy III.G.a.i (2) a.i and may occur after approval of the program by the Board, if and only if receipt of initial accreditation is required before any student enrolls in the program. Institutions must receive from the Executive Director or designee approval to supplant external peer review with specialized accreditation review prior to submitting a doctoral program proposal. Institutions shall submit a copy of the specialized accreditation report to the Board Office within 30 days of completion of the review.

All new program applications for endorsement/certification are submitted via CANVAS by the educator preparation provider dean, assistant dean, or director.

14. Three-Year Plan: If this is a new proposed program, is it on your institution's Board 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:

	The 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.
	We failed to include it when we had the opportunity.
	Other:

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.	15 in required courses 18 in additional courses 45 in research credits
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	78

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

Required PhD courses:
3 credits - CYB 501 -- Cybersecurity Seminar - 1 credit. Taken three times. This seminar will cover issues related to modern cybersecurity. Research papers, ethical hacking, etc. This will be distinct from the Computer Science graduate seminar.

3 credits - CYB507/CS507 -- Research Methods

3 credits - CYB520 -- Digital Forensics

3 credits - CYB536 -- Advanced Information Assurance

3 credits - CYB540 – Advanced Network Security

15 credits - Subtotal

18 credits - Electives as agreed with Major Professor

45 credits - CYB 600 - Doctoral Research and Dissertation – as part of the study plan.

78 credits Total: 15 credits of required courses + 18 credits of electives + 45 credits Research

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

The student must pass a qualifying examination which is a written and/or oral examination, administered by the student's graduate committee and an examination of a student's proposed dissertation research, including both a written proposal and an oral public presentation covering related research, preliminary results, and a research plan.

The student must produce a dissertation, presenting an original, significant contribution to Cybersecurity. The dissertation should be publishable, in whole or in part, and should demonstrate the ability of the candidate to successfully initiate and pursue a significant, original research project. A public presentation and defense of the final dissertation is required. It is expected that all PhD students will publish the results of their research before completion of their degree.

Students must spend at least one year on a UI campus or show, to the satisfaction of their committee, that they have received a research experience equivalent to being on a UI campus at their location of study.

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.

Graduates of the program will have:

1. The ability to clearly present, in oral form, research results and the broader implications of that research for both the field of cybersecurity and for society.
2. The ability to clearly present, in written form, research results and the broader implications of that research for both the field of cybersecurity and for society.
3. The ability to do original research in cybersecurity and to appropriately and accurately analyze the results.
4. An in-depth knowledge of cybersecurity and the ability to apply that knowledge, integrating and building upon the foundation provided by a relevant undergraduate degree.
5. Be able to demonstrate an understanding of the broader implications of research for cybersecurity and for society.

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.

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

1. Student Work from: CYB536 Advanced Information Assurance, CYB540 Network Security, and CYB520 Computer and Network Forensics. Direct measure of knowledge of content material and skills.
2. Student Work from: CYB501 Cybersecurity Seminar. Direct measure of knowledge of the societal impact of cybersecurity and professional ethics.
3. Rubrics completed by each students' major professor and committee members at the time of their project presentation or thesis defense.

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

Student Work

Faculty select representative material from the courses, potentially including assignments, projects, quizzes, exams, presentations, etc., with which to assess the student outcomes.

Committee Rubrics

The following rubric is completed by each student's major professor and committee at both the proposal defense and the final dissertation defense:

Category	Exceeds Requirements (4)	Meets Requirements (3)	Partially Meets Requirements (2)	Does Not Meet Requirements (1)
U of I Outcome: Learn and Integrate				
Students work shows an in-depth knowledge of the degree subject matter.				
U of I Outcome: Think and Create				
Student has demonstrated the ability to do original research and to appropriately and accurately analyze the results.				
U of I Outcome: Communicate				
Written Communication: has produced a clear, meaningful document.				
Oral Communication: has produced a clear, meaningful presentation and responded well to questions.				
U of I Outcome: Clarify purpose and perspective; Citizenship				
Student has demonstrated an understanding of the broader implications of that research for both the field and society.				

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

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.[2]

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 full program will be offered in Moscow and Coeur d'Alene (CdA)

RADICL Labs, these are specially designed, secure computing lab used to teach advanced cybersecurity courses that include attack and defense. In Moscow this lab is in JEB6. In Coeur d'Alene this lab is in the Hedlands building. However, with the expected increase in class size it is unlikely that these labs will continue to be of sufficient size for courses that are listed as 400/500 – e.g. the RADICL in JEB6 only holds 14 students.

[2] 2 Financial Impact shall mean the total financial expenditures, regardless of funding source, needed to support personnel costs, operating expenditures, capital outlay, capital facilities construction or major renovation, and indirect costs that are incurred as a direct result of establishing, modifying, or discontinuing a new instructional program, instructional unit, or administrative unit. *Revised per Board Policy III.G, June 2024.*

General Computing Lab, this is a standard computing lab designed to teach programming and defense-oriented cybersecurity. In Moscow this lab is in JEB321. In Coeur d'Alene this lab is currently in HC240B. Again, this lab holds 20 students, which is likely to be insufficient if the program grows as anticipated.

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

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

There will be increased use of the secure laboratory classrooms at both campuses and the size of the existing class will likely increase beyond current classroom capacity.

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.

Videoconference equipped teaching laboratory for 40+ students (alternatively additional teaching resources to separate larger courses into multiple sections to accommodate current teaching laboratory capabilities, but that would be more expensive). This is needed to accommodate the growth in the existing BS programs in both Computer Science and Cybersecurity. The addition of a Ph.D. in cybersecurity only increases an existing need.

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.

Library resources are sufficient.

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

None.

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 program will require:

- Two additional tenure track faculty, one of whom will replace the former director of the Center for Secure and Dependable Systems (UI's cybersecurity research center), who recently stepped down.
- Two additional clinical faculty.
- Two additional IT staff.
- Four graduate teaching assistants.

We will need at least 2 additional sections of CYB600 and CYB500 the graduate research courses. This will support the research of the new PhD students. We anticipate needing one additional section of CS/CYB507 the research methods course – it is currently offered Fall only and a Spring offering will be needed to support the increase in students.

The additional faculty will offer new courses, to be developed, in their specific research areas, we anticipate one new course for each faculty member. The new courses are not strictly necessary to the degree, but new hires are necessary, and they will need to teach courses in their areas to recruit and give graduate students the foundational knowledge to start research.

The additional IT support staff are necessary to maintain the high security teaching and research environments necessary to offer a cutting-edge cybersecurity curriculum and research environment.

The teaching assistants are necessary to recruit and retain the highest quality PhD students.

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.

The Department of Computer Science, the College of Engineering, and the University of Idaho have outstanding instructional, support, and administrative resources that currently support our PhD in Computer Science as well as multiple other graduate programs across the college and campus. This includes The Center for Excellence in Teaching and Learning (CETL), which provides instructional support; the Office of Information Technology, which provides technology support, and has its own branch dedicated to the College of Engineering; and multiple research institutes, most notably the Center for Secure and Dependable Systems, to support research. Thus, no new support structures or units are required, although some additional resources (e.g. two additional IT staff) need to be added to existing units to support the program's growth and the general Computer Science/Cybersecurity ecosystem.

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?

This proposed program will *strengthen* several existing programs. The BS and MS programs in

Cybersecurity will be improved by the addition of more faculty with expertise in cybersecurity. It will improve the diversity of courses available, increase opportunities for undergraduate research, and expand the existing cybersecurity ecosystem at UI. Having a PhD program in cybersecurity will increase the attractiveness of the BS and MS programs in both Cybersecurity and Computer Science.

The increased breadth of research will improve cross campus collaborations, allowing the cybersecurity faculty to better support and integrate with other disciplines that include cybersecurity aspects such as business, law, and political science. Overall, the synergies created by the program will improve the quality and productivity of 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.

Four faculty total:
2 Tenure Track faculty – ideally two on the Moscow campus and one on the Coeur d'Alene campus
2 Clinical faculty

Additional staff support:
2 IT support staff – ideally one each on the Moscow and Coeur d'Alene campuses.
4 Teaching Assistant positions.

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?

Not Applicable

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.

House Bill 734, for fiscal year 2025, included $2,139,100 for Operational Capacity Enhancement, of which $800,200 was for the Cybersecurity Ph.D. Workforce Expansion.

The justification for this new appropriation outlined the critical demand for Cybersecurity professionals due to the escalating threat of cyberattacks against critical infrastructure. The shortage of skilled cybersecurity professionals nationwide, and particularly in Idaho, necessitates immediate action. The Governor's Cybersecurity Task Force Report in March 2022 highlighted the urgency of addressing this issue. The United States experienced a staggering shortage of 3.5 million cybersecurity jobs in 2021. Idaho has seen a 28% increase in cybersecurity job openings, with over a thousand positions remaining unfilled. Industry leaders, including the Idaho National Laboratory, are actively seeking trained cybersecurity professionals. Investing in cybersecurity education is critical to supplying Idaho with skilled talent. Other states are heavily investing in cybersecurity research and education. For example, Dakota State University secured significant funding to expand cybersecurity programs, and neighboring states like Washington are investing heavily in cybersecurity degree programs. Idaho's higher education institutions need support to

compete, attract faculty, and retain students. The funding received in response to this request will allow the University of Idaho to address Idaho's immediate and long-term workforce needs in cybersecurity. With the Cybersecurity Ph.D. program, we aim to ensure a steady supply of qualified professionals who can bolster cybersecurity defenses, and support Idaho's economic growth.

This funding will support recruiting new students into our cybersecurity program. Over the course of the next five years, it will allow an increase of up to 270 undergraduate students and 15 graduate students annually. This investment from the state will allow us to serve more students who are ready to learn and serve our state as they protect information and assets in the cybersecurity field. There will also be an increase in grant awards, ranging from $250,000-$350,000 annually, as faculty establish their research portfolios.

Cybersecurity Workforce (requesting 6.00 FTP; $596,100 total salaries; $800,200 total General Fund PC funding with benefits):

- Tenure Track Professor/Program Director, $177,100, 12-month appointment, 1.00 FTP
- Tenure Track Professor, $105,000, 9-month appointment, 1.00 FTP
- Clinical Faculty (two), $94,500, 9-month appointments, 1.00 FTP each
- Information Technology Staff, $75,000, 12-month appointment, 1.00 FTP
- Program Manager, $50,000, 12-month appointment, 1.00 FTP

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?

Some of the initial start-up costs of computer servers have already been supplied through grants. These are one-time costs to purchase hardware, so do not require sustained funds.

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?

Not Applicable

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.

Some courses will include minimal (~$20) course fees to support the on-going maintenance and replacement of computing resources used by students in the courses in accordance with Board Policy V.R., 3.b.

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.

Not Applicable

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

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

See attached budget.

SUBJECT

Board Resolutions on DEI Ideology; Governance; and Freedom of Expression in Higher Education

REFERENCE

November 2024	Board members discussed initial drafts of three resolutions related to diversity, equity, and inclusion; governance; and freedom of expression in higher education.

APPLICABLE STATUTE, RULE, OR POLICY

Idaho State Board of Education Governing Policies and Procedures, Sections I.E., II.L., II.P., and III.B.

Idaho Code §67-5909B

BACKGROUND/DISCUSSION

The Idaho State Board of Education has long affirmed its interest in promoting an environment of belonging and success for all students at the public postsecondary institutions it governs. Administrators, faculty, and staff are responsible for creating a welcoming and dynamic learning environment for all students, as an outgrowth of their investment in student success.

In April 2023, the Board adopted a resolution prohibiting the institutions from requiring diversity statements in hiring. This was followed by amendments to Board policy II.P. to codify the resolution language. The following spring, the Legislature adopted legislation prohibiting diversity statements in hiring and admissions at the institutions.

In addition to its newer policy related specifically to diversity statements, the Board has long-standing policies related to governance, presidential power, review of tenured faculty, academic freedom, academic responsibility, and freedom of expression in higher education (Board policies I.E., II.L, II.P. and III.B).

In November 2024, the Board members discussed draft versions of three resolutions: A Resolution on Diversity, Equity, and Inclusion in Higher Education; A Resolution on Governance in Higher Education; and A Resolution on Freedom of Expression in Higher Education.

The Board sought and has received feedback from institutional leaders, students, and the general public about the draft resolutions. This feedback has informed revisions to each of the resolutions.

IMPACT

The three updated resolutions affirm the Board's existing policies and institutional practices related to governance, tenure, academic freedom and freedom of expression, but also extend these policies through directives that aim to better support all students regardless of their identifying characteristics, establish clear criteria for evaluating presidents, require reporting on post-tenure review actions, ensure political neutrality of the institutions, and provide curricular transparency.

ATTACHMENTS

Attachment 1 – A Summary of the Resolutions
Attachment 2 – A Resolution on DEI Ideology in Higher Education
Attachment 3 – A Resolution on Governance in Higher Education
Attachment 4 – A Resolution on Freedom of Expression in Higher Education
Attachment 5 – Guidance on the Resolution on DEI Ideology in Higher Education

BOARD STAFF COMMENTS AND RECOMMENDATIONS

Some of the language of these resolutions is drawn from or inspired by recent legislation in Utah, particularly House Bill 261. Portions of the Resolution on Freedom of Expression in Higher Education borrow verbatim from a recent resolution adopted by the Utah Board of Higher Education on the same topic. If the Board approves these resolutions, staff recommends the directives be codified in Board policy.

BOARD ACTION

I move to approve the Resolution set forth in Attachment 2, the title of which is as follows:

A Resolution on DEI Ideology in Higher Education

Moved by _____ Seconded by _____ Carried Yes _____ No _____

AND

I move to approve the Resolution set forth in Attachment 3, the title of which is as follows:

A Resolution on Governance in Higher Education

Moved by _____ Seconded by _____ Carried Yes _____ No _____

I move to approve the Resolution set forth in Attachment 4, the title of which is as follows:

A Resolution on Freedom of Expression in Higher Education

Moved by _____ Seconded by _____ Carried Yes _____ No _____

AND

I move to direct staff to develop proposed amendments to Board policy codifying the principles of each adopted resolution, where applicable, and bring the amendments forward for first readings not later than the August 2025 Board meeting.

Moved by _____ Seconded by _____ Carried Yes _____ No _____

A Summary of Three Resolutions of the Idaho State Board of Education

Three resolutions of the Idaho State Board of Education affirm the Board's existing policies and provide directives to ensure the success of all students.

Resolution on Diversity, Equity, and Inclusion

This resolution affirms Board policy and Idaho code prohibiting diversity statements in hiring and admissions decisions and confirms that Idaho's institutional accreditor does not require specific structures or activities related to DEI at Idaho's public postsecondary institutions. The resolution defines "DEI Ideology" and makes the following directives:

- Institutions shall establish and maintain equality of opportunity for all students regardless of personal identity characteristics;
- Institutions shall ensure that no central offices, policies, procedures, or initiatives are dedicated to DEI ideology;
- Institutions shall ensure that no employee or student is required to declare gender identity or preferred pronouns.

Resolution on Governance

This resolution affirms Board policy that establishes presidential power at the public postsecondary institutions, including that final decisions at the institutional level rest with the Presidents, and affirms that the Board is responsible to hold the Presidents accountable for their performance. It also affirms that institutions are required by Board policy to conduct regular reviews of tenured faculty and that Presidents may terminate tenured faculty members for "adequate cause." The resolution makes the following directives:

- The Board shall establish clear criteria for evaluating the presidents;
- Institutions shall report to the Board on post-tenure review actions;
- Institutions shall develop faculty codes of conduct.

Resolution on Freedom of Expression

This resolution affirms Board policies and principles related to academic freedom and academic responsibility for faculty, students, and institutions, including the limits to academic freedom. The resolution makes the following directives:

- Institutions shall maintain political neutrality, protect speakers' rights to free expression, protect the safety of those participating in constitutionally protected speech, introduce campus communities to diverse viewpoints, and establish programs designed to educate students and faculty about the institutions' role as the marketplace of ideas;

- Institutions shall provide curricular transparency by making course information available to the public.

Idaho State Board of Education

650 W. State Street ● Suite 307 ● Boise, ID ● 83702
P.O. Box 83720 ● Boise, ID ● 83720-0037

A RESOLUTION ON DEI IDEOLOGY

WHEREAS, the general supervision of the state educational institutions of the state of Idaho is vested in the State Board of Education pursuant to Article IX, §2 of the Idaho Constitution and Idaho Code § 33-101; and

WHEREAS, the State Board of Education serves as the Board of Regents of the University of Idaho (Article IX, §10 of the Idaho Constitution; Idaho Code § 33-2802), and the Board of Trustees of Idaho State University (Idaho Code § 33-3003), Boise State University (Idaho Code § 33-4002), and Lewis-Clark State College (Idaho Code § 33-3102); and

WHEREAS, the Board requires the postsecondary institutions to "create a welcoming and dynamic learning environment of belonging by administrators, faculty, and staff who are invested in the success of every student" (Board Policy II.P Human Resources Policies and Procedures); and

WHEREAS, the Board recognizes and values the unique diversity of Idahoans and expects the postsecondary institutions to foster a campus culture that appreciates and reflects this diversity; and;

WHEREAS, the institutions are prohibited from requiring diversity statements in hiring (Board Policy II.P) and in hiring and admissions (Idaho Code § 67-5909B); and

WHEREAS, the Board affirms that Idaho's institutional accreditor does not require institutions to establish or maintain central offices, policies, procedures or initiatives dedicated to diversity, equity, or inclusion beyond general efforts to address existing achievement gaps; and

WHEREAS, the Board affirms that Idaho's institutional accreditor provides general standards of quality assurance but the Board maintains authority over the specific actions the institutions shall take to meet these broad accreditation standards.

NOW, THEREFORE, BE IT RESOLVED that diversity, equity, and inclusion ideology ("DEI ideology") is any approach that prioritizes "personal identity characteristics" (race, color, sex, sexual orientation, national origin, religion, or gender identity) over individual merit; and

BE IT FURTHER RESOLVED that the institutions shall establish and maintain equality of opportunity so that all students may succeed regardless of personal identity characteristics.

BE IT FURTHER RESOLVED that the institutions shall not use personal identity characteristics in decisions affecting the employment or education of any employee or student.

BE IT FURTHER RESOLVED that institutions shall not establish or maintain a central office, policy, procedure, or initiative that promotes DEI ideology.

BE IT FURTHER RESOLVED that institutions shall ensure that no student resource or student success center serves students based on DEI ideology.

BE IT FURTHER RESOLVED that no institution employee or student shall be required to declare gender identity or preferred pronouns in any form of communication.

BE IT FURTHER RESOLVED that nothing herein shall prevent institutions from complying with federal and state laws, external regulatory requirements, or from following other specific guidance provided by the Office of the State Board of Education related to this resolution.

BE IT FURTHER RESOLVED that the resolutions contained herein shall be implemented by June 30, 2025.

ADOPTED and APPROVED by the Idaho State Board of Education, December 18, 2024.

_____
Linda Clark, President

Idaho State Board of Education

650 W. State Street ● Suite 307 ● Boise, ID ● 83702
P.O. Box 83720 ● Boise, ID ● 83720-0037

A RESOLUTION ON GOVERNANCE IN HIGHER EDUCATION

WHEREAS, the general supervision of the state educational institutions of the state of Idaho is vested in the State Board of Education pursuant to Article IX, §2 of the Idaho Constitution and Idaho Code § 33-101; and

WHEREAS, the State Board of Education serves as the Board of Regents of the University of Idaho (Article IX, §10 of the Idaho Constitution; Idaho Code § 33-2802), and the Board of Trustees of Idaho State University (Idaho Code § 33-3003), Boise State University (Idaho Code § 33-4002), and Lewis-Clark State College (Idaho Code § 33-3102); and

WHEREAS, the Board affirms through established policy that presidents of the institutions have "full power and responsibility within the framework of the Board's Governing Policies and Procedures for the organization, management, direction, and supervision of the institutions" (Board Policy I.E.); and

WHEREAS, the Presidents are "held accountable by the Board for the successful functioning of the institution in all of its units, divisions, and services" (Board Policy I.E.); and

WHEREAS, the Board "expects the Presidents to obtain the necessary input from faculty, classified and exempt employees, and students," often through participatory or shared governance, but "holds the Presidents ultimately responsible for the well-being of the institutions" (Board Policy I.E.); and

WHEREAS, the Board understands the principle of "shared governance" to mean a practice of participatory governance that ensures the voices of faculty, employees, and students are considered in administrative and governance decisions made by the Presidents but not to mean a practice whereby faculty, employees, and students share equal power with the Presidents; and

WHEREAS, the Board affirms that "final decisions at the institutional level rest with the Presidents" (Board Policy I.E); and

WHEREAS, the Board confers to the Presidents of the institutions the authority to terminate the employment of any tenured faculty member for "adequate cause," which is defined by the Board

to mean "performance…judged to have been unsatisfactory or less than adequate during the period under review" (Board Policies I.E. and II.L); and

WHEREAS, the Board affirms its policy related to post-tenure review requiring all faculty who receive tenure to receive both annual performance reviews as required of all employees of the state, as well as distinct "periodic performance review[s]…conducted in terms of the tenured faculty member's continuing performance in the following general categories: teaching effectiveness, research or creative activities, professional related services, other assigned responsibilities, and overall contributions to the department" (Board Policy II.G); and

NOW, THEREFORE, BE IT RESOLVED that the Board shall establish clear criteria for evaluating the performance of the Presidents in their duties to ensure successful functioning of the institution in all its units, divisions and services.

BE IT FURTHER RESOLVED that each institution shall submit an annual report related to post-tenure review outcomes, including the number of reviews conducted, the number of performance improvement plans resulting from the post-tenure review process, and the justification for not dismissing faculty who fail to meet the requirements of a post-tenure performance improvement plan.

BE IT FURTHER RESOLVED that each institution establish and maintain a faculty code of conduct that defines the faculty rights, responsibilities, and conduct to foster and sustain an environment conducive to sharing, supporting, and critically examining knowledge and values, and to create an ethical educational climate that strives for effective teaching and learning without prejudice or favor toward any student.

BE IT FURTHER RESOLVED that the resolutions contained herein shall be implemented by June 30, 2025.

ADOPTED and APPROVED by the Idaho State Board of Education, December 18, 2024.

_____
Linda Clark, President

Idaho State Board of Education

650 W. State Street ● Suite 307 ● Boise, ID ● 83702
P.O. Box 83720 ● Boise, ID ● 83720-0037

A RESOLUTION ON FREEDOM OF EXPRESSION IN HIGHER EDUCATION

WHEREAS, the general supervision of the state educational institutions of the state of Idaho is vested in the State Board of Education pursuant to Article IX, §2 of the Idaho Constitution and Idaho Code § 33-101; and

WHEREAS, the State Board of Education serves as the Board of Regents of the University of Idaho (Article IX, §10 of the Idaho Constitution; Idaho Code § 33-2802), and the Board of Trustees of Idaho State University (Idaho Code § 33-3003), Boise State University (Idaho Code § 33-4002), and Lewis-Clark State College (Idaho Code § 33-3102); and

WHEREAS, the Board affirms that "in addition to constitutionally protected freedoms of speech, assembly, and religion, students and faculty have the right to engage in free inquiry, intellectual debate, and freedom of scholarship both on and off campus" (Board Policy III.B.); and

WHEREAS, the Board affirms that "students and faculty have the right to express opinions and provide feedback concerning institutional governance and administration without fear of censorship or retaliation" (Board Policy III.B.); and

WHEREAS, the Board affirms that "students have the right to express personal opinions about concepts and theories presented in their courses and to disagree with opinions expressed by faculty and fellow students" (Board Policy III.B.); and

WHEREAS, the Board affirms that "students may not be directed or otherwise compelled to personally affirm, adopt or adhere to any particular political, religious or philosophical tenet or ideology " (Board Policy III.B.); and

WHEREAS, the Board affirms that faculty, students, and the institutions each enjoy certain tenets of academic freedom but are also bound to equally important tenets of academic responsibility (Board Policy III.B.); and

WHEREAS, the Board affirms the rights and responsibilities of faculty to determine what and how to teach in their courses free from administrative or political influence, but within the bounds of academic freedom and academic responsibility, institutional policies, and relevant state and federal laws; and

WHEREAS, the Board affirms that academic freedom does not protect faculty from student challenges to, or disagreement with, instructional methods and content choices; does not protect faculty or students from penalties for violating the law; does not confer the right to faculty or students to violate institutional policies; does not protect faculty or students from disciplinary action consistent with institutional and Board policies; does not protect faculty or students from sanctions or dismissal for professional misconduct or poor performance; and does not protect faculty or students from investigations into allegations of or discipline for scientific misconduct or other violations of institutional or Board policy (Board Policy III.B); and

WHEREAS, the Board values curricular transparency to ensure students have full self-determination in making academic choices, and affirms that all educational content produced by faculty in the course of their duties as public employees of the state of Idaho are public documents (Board Policy V.M.); and

WHEREAS, the Board desires to set expectations for how institutions will implement the broad principles of free expression and academic responsibility operationally through specific policies, practices, and procedures;

NOW, THEREFORE, BE IT RESOLVED that the Board establishes the following expectations and directives to further its commitment to promoting and preserving free expression within the postsecondary institutions it governs and cultivating a thriving marketplace of ideas:

Institutions shall establish and maintain policies, practices and procedures that will

- Maintain political neutrality. Institutions, as governmental entities, or employees acting in their official capacities as representatives of the institution must refrain from taking public positions on political, social, or unsettled issues that do not directly relate to the institution's mission, role, or pedagogical objectives. This does not mean faculty, staff, or students must remain neutral; indeed, institutions should promote a culture that encourages and celebrates forums in which faculty, students, staff, and community members may express conflicting, controversial, or unpopular viewpoints. A fundamental mission of higher education is to promote the exchange of knowledge and ideas through teaching, research, critical evaluation, civil discourse, and debate. Neutrality as an entity allows the institution to protect this mission by supporting those who engage in open, rigorous debate without disaffecting segments of its faculty, staff, and students whose sincerely held beliefs conflict with others. The institution can thereby fulfill its responsibility to be an impartial steward of the marketplace of ideas in which sincerely held viewpoints are subject to rigorous scrutiny and must withstand the challenge of open debate and critical examination on their own merits, not the institution's endorsement.

- Protect a speaker's right to free expression, including controversial, unpopular, or offensive expression. This includes prohibiting individuals or groups from substantially

disrupting others' protected expression. Institutions have a solemn responsibility not only to promote the freedom to debate and scrutinize all ideas in appropriate forums but also to protect that freedom when others attempt to restrict it.

- Protect the educational, research, service, housing and other legitimate functions of the institution by implementing limited and reasonable restrictions on the time, place, and manner of speech to avoid disruption or materially interfering with the normal operation of the institution.

- Protect the safety of campus and the institution's property by prohibiting conduct that violates fire and safety regulations, impedes the normal flow of pedestrian or vehicular traffic, or violates laws or regulations.

- Protect the safety of those participating in constitutionally protected speech on campus by working with security personnel and campus or local law enforcement to establish procedures and criteria for determining when and how it is appropriate for the institution to intervene in a forum for free expression for the sake of public safety.

- Provide processes for reserving spaces, hosting events, and for addressing disputes that may arise over free expression.

- Provide a process for an institution to address, condemn, or prohibit expression that is not constitutionally protected such as that which causes physical harm, damages property, incites violence or illegal activity, constitutes a genuine threat, discriminates, harasses, or otherwise violates the law or institutional policy.

- Protect and cultivate academic freedom and academic responsibility. Faculty must be free to investigate, research, discuss, publish, and teach within their academic expertise and on topics relevant to course curricula without interference from institutional administrators, elected officials, governing boards, or other entities. Institutional neutrality should not be interpreted to allow for restrictions on curriculum, research, expression germane to research or curriculum or to otherwise restrain academic exploration within the bounds of traditional academic freedom and academic responsibility.

- Introduce campus communities to diverse viewpoints, including inviting speakers, sponsoring symposiums and lectures, or presenting other opportunities to hear differing perspectives and ideas. To provide these opportunities policies shall be developed that include criteria to avoid making decisions related to speakers or events on the basis of

opposition to the viewpoint(s) being expressed or that a viewpoint is controversial, and criteria to avoid prohibiting a speaker's presence or an event on campus because it may generate concerns about security and public safety. These policies and procedures should include clear, objective, narrow, and content-neutral criteria for determining security costs charged to a speaker, event organizer, or a sponsoring entity.

- Establish a program designed to educate new students, faculty, and staff about the institution's role as the marketplace of ideas; what constitutes protected speech and what does not; when the institution may intervene in free expression activities, such as when they involve direct threats, violence, illegal harassment or discrimination; how to appropriately express viewpoints through events, such as protests, parades, or other events, including an explanation of the institution's time, place and manner restrictions; and the institution's policies prohibiting the disruption of others' rights to free expression, including shouting down speakers or blocking speakers' access to a forum. The scope and medium in which the institution delivers this program may be tailored to the institution's mission and role.

BE IT FURTHER RESOLVED that each institution shall make curricular information about each course available to the public digitally in a manner that shall be defined in Board policy.

BE IT FURTHER RESOLVED that the resolutions contained herein shall be implemented by June 30, 2025.

ADOPTED and APPROVED by the Idaho State Board of Education, December 18, 2024.

_____
Linda Clark, President

The Office of the State Board of Education provides the following guidance related to the Resolution on DEI Ideology in Higher Education adopted by the Board on December 18, 2024.

Nothing in the resolution prohibits the institutions from taking any of the following actions:

- **Undertaking non-discriminatory activities, policies, and procedures to support student success, including students at higher risk of not completing a program or degree;**
    - Examples include
        - Supporting first generation college students, veterans, students with disabilities, international students, PELL eligible students, and transfer students, including establishing or maintaining designated centers for such students
        - Pursuing recruitment, enrollment, retention, completion, and graduation goals based on objective demographic and institutional data, especially for compliance with program-specific accreditation
        - Addressing cultural education, celebration, engagement, or awareness without the promotion of differential treatment

- **Supporting citizens of federally recognized American Indian tribes;**
    - Examples include
        - Establishing and maintaining a designated center for American Indian students
        - Supporting American Indian cultural events
        - Offering or facilitating scholarships for American Indian students

- **Complying with athletic requirements;**
    - Examples include
        - Complying with Title IX requirements of the federal Higher Education Act as they relate to athletics
        - Complying with NCAA, NAIA and athletic conference requirements

- **Complying with academic program-specific accreditation requirements;**
    - Examples include
        - Adhering to accreditation standards for certain health professions programs

- **Supporting student clubs and employee affinity groups;**
    - Examples include
        - Allowing students to establish clubs focused on political or social issues
        - Allowing faculty and staff to establish groups for themselves based on specific interests or personal identity characteristics

- **Maintaining eligibility for grants and federal programs;**
    - Examples include

        - Complying with National Science Foundation grant requirements like recruiting or mentoring students from underrepresented groups, creating opportunities for individuals from diverse backgrounds, or developing inclusive research environments

- **Offering scholarships**
    - Examples include
        - Offering scholarships to American Indian students, first-generation students, or students from historically underserved communities

- **Complying with federal and state laws and regulations**
    - Examples include
        - Complying with the Americans with Disabilities Act (ADA)
        - Establishing and maintaining a disability center
        - Complying with the Higher Education Act, including meeting requirements for designation as a Hispanic Serving Institution (HSI)