**New Academic Degree Program**
**Full Proposal Application**
**South Dakota Board of Regents**
**Academic Affairs Forms**

**Internal Ticket ID:** 21467
**Created:** 12/6/2024
**Modified:** 7/16/2025

Use this form to propose a new degree program. The Board of Regents, Executive Director, and/or their designees may request additional information about the proposal. After the university President approves the proposal, submit a signed copy to the Executive Director through the System Academic Officer (through the online submission process).

*Note: Within the proposal, all references to external sources should be documented with a footnote (including web addresses where applicable).*

| | |
|---|---|
| **University** | DSU - Dakota State University |
| **Degree** | MS : Master of Science |
| **Name of Major** | X999 : New Major Requested **Cyber Operations** |
| **Specialization Required?** | No<br>*Note: If the new proposed program includes specific specializations within it, complete and submit a New Specialization Form for each proposed specialization and attach it to this form. Since specializations appear on transcripts, they require Board approval.* |
| **College/Department** | 8N : DSU Beacom Comp Cyber Sciences/DCSI : Computer Science |
| **Planned CIP Code** | 11.0101 |
| **WICHE WRRGP Eligibility** | Yes |

## Program Description

### 1. Provide the working program description that may appear in the university catalog.

The Master of Science (MS) in Cyber Operations is designed to provide specialized education and training in technical cybersecurity practices. The curriculum places a strong emphasis on deeply technical cyber operations skills such as reverse engineering, malware analysis, penetration testing, and software exploitation. These competencies are crucial for roles within intelligence, military, and law enforcement agencies, as well as for positions in data-driven industries that demand high-level security expertise.

### 2. Does the university request any exceptions to any Board policy for this program?

*Explain any requests for exceptions to Board Policy. If not requesting any exceptions, indicate **"None."***

None

**Strategic Impact**

**3. Describe how the program fits in with the institutional mission, strategic plan, existing institutional program array, and academic priorities.**

The proposed Master of Science in Cyber Operations (MSCO) directly aligns with Dakota State University's statutory mission under SDCL § 13-59-2.2 and BOR Policy 1.2.2, which designates DSU as a specialized institution for computer management, information systems, and cybersecurity. This mission underscores the university's focus on providing education in computer-related fields that meet the evolving demands of the industry, government, and national security sectors.

Alignment with Institutional Mission and Strategic Plan
DSU has strategically positioned itself as a national leader in cybersecurity education. The MSCO program further fulfills this mission by:

- Expanding DSU's program array to include a graduate-level pathway in Cyber Operations, filling a critical gap between the undergraduate (BS) and doctoral (PhD) degrees.
- Preparing graduates for advanced roles in offensive and defensive cyber operations, intelligence, and critical infrastructure protection.
- Supporting DSU's strategic initiatives to drive workforce development, cybersecurity research, and innovation at state, regional, and national levels.

Fit with Existing Programs
The MSCO enhances DSU's robust program offerings, which already include:

- Bachelor of Science in Cyber Operations (451 enrolled students as of Fall 2024).
- PhD in Cyber Operations (67 enrolled students).
- A Cyber Operations specialization within the MS in Computer Science (31 students).

The MSCO program will allow students to pursue a focused, technical, and applied graduate education in cyber operations, bridging the educational pathway between the undergraduate degree and the research-intensive PhD program. This addition aligns with the demand for mid-level professionals and supports DSU's efforts to provide industry-aligned, specialized education.

Contribution to Research and Economic Development
The MSCO will directly support DSU's research initiatives, particularly through the Applied Research Lab (ARL) and MadLabs®, which are focused on cutting-edge cybersecurity research.

Graduate students in the MSCO program will:

- Engage in applied research projects addressing real-world cyber challenges.
- Collaborate with faculty, government partners, and industry leaders to develop innovative solutions in reverse engineering, malware analysis, and software exploitation.
- Contribute to the lab's role as a hub for national cybersecurity innovation and workforce development.

The program aligns with DSU's strategic partnerships, including collaborations with organizations like the Johns Hopkins University Applied Physics Lab (JHUAPL) and Battelle, both of which have expressed the need for a master's-level Cyber Operations program.

Academic Priorities and Workforce Alignment
The MSCO program reinforces DSU's commitment to high-impact, research-based education, addressing critical cybersecurity workforce gaps identified in the South Dakota Board of Regents' Strategic Plan. It aligns with DSU's efforts to:

- Foster academic excellence through specialized, hands-on curriculum development.
- Support workforce development in high-demand fields such as cybersecurity, intelligence, and critical infrastructure protection.
- Enhance DSU's role as a leading institution in cybersecurity education and innovation, meeting both student aspirations and industry expectations.

**If the program does not align to the strategic plan, provide a compelling rationale for the institution to offer the program.**

Not required, it aligns.

**4. How does the program connect to the Board of Regent's Strategic Plan?**

The proposed MSCO aligns with the goals of the South Dakota Board of Regents (BOR) Strategic Plan (2022-2027) by supporting workforce development, fostering academic excellence, and driving economic growth through advanced, specialized education in high-demand fields. The program is tailored to meet the needs of stakeholders, including government agencies and private sector leaders, who are actively seeking graduates with expertise in both cybersecurity and computer science to navigate the evolving technological landscape.

Governance, Access, and Affordability (Goals 1 and 2):

- The introduction of the MSCO supports the BOR's mission to make education accessible and responsive to state and regional needs. This specialized master's program broadens opportunities for students, including non-traditional and underserved populations, ensuring that they have pathways to advanced education and careers in high-demand fields.
- The focus on cybersecurity, a key area for economic growth and national security, exemplifies DSU's strategic approach to providing affordable, high-value education that supports South Dakota's long-term workforce development.

Academic Excellence, Student Success, and Educational Attainment (Goal 3):

- The MSCO emphasizes high-quality education through a rigorous, research-based curriculum that aligns with nationally recognized standards. This supports the BOR's goal of ensuring student success and improving educational outcomes by providing specialized programs that meet industry and academic standards.
- DSU's commitment to specialized accreditation and fostering student engagement through hands-on learning aligns with the BOR's focus on increasing the number of programs with high-impact practices. This enhances the university's ability to prepare students for success, thus contributing to higher degree attainment and retention rates.

Workforce and Economic Development (Goal 4):

- The MSCO directly responds to the BOR's strategic emphasis on aligning academic programming with workforce needs. This program educates graduates in advanced cybersecurity skills—such as reverse engineering, malware analysis, penetration testing, and software exploitation—that are critical for the intelligence, military, and private sectors. This ensures that DSU is contributing skilled professionals to the state's workforce, fulfilling projected needs for a more highly educated labor force.
- By addressing the national and regional demand for cybersecurity experts, the program helps meet the BOR's objective of aligning new academic programs with workforce gaps identified through initiatives like the Degree and Workforce Gap Analysis.
- This program would also enhance the capabilities and impact of DSU's ARL in Madison and Sioux Falls. The lab, set to become a hub for cutting-edge research in cyber operations, would benefit from highly trained master's students bringing both advanced theoretical knowledge and practical skills. These students would contribute to ongoing research projects, helping to solve real-world cyber challenges, develop new offensive and defensive technologies, and drive innovation in areas such as critical infrastructure protection and cybersecurity automation.
- By aligning the curriculum with the lab's focus on applied research, the master's program would foster collaboration among students, faculty, and industry partners. This collaboration would fuel the lab's mission to address emerging cyber threats and explore innovative solutions for businesses, government agencies, and the military. Graduates from the master's program would be well-equipped to assume leadership roles in these projects, ensuring that the lab remains at the forefront of cybersecurity advancements. Ultimately, this synergy between the master's program and the research lab would elevate DSU's reputation as a leader in cyber operations research, both regionally and nationally.

Strategic Investment in Higher Education (Goal 5):
The MSCO helps strengthen DSU's research and development initiatives, contributing to the broader goal of increasing South Dakota's competitiveness in the knowledge-based economy. Graduates from this program are not only prepared for employment but also positioned to participate in research-driven activities that promote technological advancement and innovation in the state.

Conclusion:
The MSCO at DSU aligns with the South Dakota BoR's Strategic Plan by fostering academic excellence, addressing workforce needs, enhancing student success, and supporting economic and research development. This program bolsters DSU's mission as a technology-focused institution, propelling it forward as a leader in cybersecurity education and contributing to the strategic vision of a stronger, more competitive public university system in South Dakota.

**Program Summary**

**5. If a new degree is proposed, what is the rationale?**

*This question refers to the type of degree, not the program. For example, if your university has authorization to offer the Bachelor of Science and the program requested is a Bachelor of Science, then the request is not for a new degree.*

**6. What modality/modalities will be used to offer the new program?**

*Note: The accreditation requirements of the Higher Learning Commission (HLC) require Board approval for a university to offer programs off-campus and through distance delivery.*

| | Yes/No | Intended Start Date |
|---|---|---|
| **On Campus** | Yes | Fall 2025 |

| | Yes/No | Location(s) | Intended Start Date |
|---|---|---|---|
| **Off Campus Location** | No | | |

| | Yes/No | Delivery Method(s) | Intended Start Date |
|---|---|---|---|
| **Distance Delivery** | Yes | Online Asynchronous | Fall 2025 |

| | Yes/No | Identify Institutions |
|---|---|---|
| **Does another BOR institution already have authorization to offer the program online?** | No | |

**7. If the program will be offered through distance delivery, identify the planned instructional modality:**

Asynchronous : Students are not required to attend the course at a specific time or location.

**8. What are the student learning outcomes for this program?**

Upon completion of the MSCO program, students will demonstrate the following competencies:

a. Demonstrate the procedures of reverse engineering
b. Evaluate various types of cyber vulnerabilities, both internal and external, to reduce organizational risk.
c. Execute constructed attacks against computer systems to take advantage of discovered vulnerabilities.

## 9. For associate's and bachelor's degree proposals, identify the 3-5 AAC&U Essential Learning Outcomes that have been selected for this program.

*Use the chart below to indicate the student learning outcomes that align to the selected ELOs (See BOR Policy 2.11 and Guideline 8.5).*

| **Essential Learning Outcomes (AAC&U)** | **Student Learning Outcomes** |
|---|---|
| Inquiry and Analysis | |
| Critical and Creative Thinking | |
| Information Literacy | |
| Teamwork | |
| Problem Solving | |
| Civic Knowledge and Engagement | |
| Intercultural Knowledge | |
| Ethical Reasoning | |
| Foundational Lifelong Learning Skills | |
| Integrative Learning | |

## 10. Enter the number of credit hours required to graduate

| Credit Hours |
|---|
| |

**11.Complete the following tables to provide a degree program curriculum summary.**

A. Table 1 –Total Program Degree Credit Hours

| | Credit Hours In Program | |
|---|---|---|
| | **Hours Per Requirement** | **%Total Hours** |
| **System General Education Requirements** | 0 | |
| *Subtotal - Gen Ed Requirements* | 0 | % |
| **Program Requirements** | | |
| Required Support Courses | 30 | |
| Major Requirements | 24 | |
| Major Electives | 6 | |
| *Subtotal - Program Requirements* | 30 | % |
| **Free Electives** | 0 | |
| *Subtotal - Free Electives* | 0 | % |
| **Degree Total** | 30 | % |

**Board Policy 2:29 requires each baccalaureate level degree program to require 120 credit hours and each associate degree program to require 60 credit hours. Exceptions to this policy require documentation that programs must comply with specific standards established by external accreditation, licensure, or regulatory bodies or for other compelling reasons, and must receive approval by the Executive Director in consultation with the President of the Board of Regents.*

B. Table 2 – Insert Required Program Support Courses Impacting Other Programs (outside department). Do not include General Education courses.

*The individual curriculum tables should be included as a word document* ***attached*** *to the TDX ticket.*

C. Table 3 – Insert Major Requirements (within department)

*The individual curriculum tables should be included as a word document* ***attached*** *to the TDX ticket.*

D. Table 4 – Insert Major Electives

*The individual curriculum tables should be included as a word document* ***attached*** *to the TDX ticket.*

**12. New Course Approval**

*New courses required to implement the new degree program may receive approval in conjunction with program approval or receive approval separately. Please check the appropriate statement:*

Yes

**Academic Quality**

**13. What peer institutions and current national standards will be referenced to develop the curriculum for this program?**

*Peer Institution: Regional and Competitive institutions. Include links to at least 3 comparable programs at peer institutions and links to national or accreditation standards, if any.*

DSU is recognized as one of the foremost experts in the cybersecurity field. Peer institutions are those with an NSA Center of Academic Excellence designation in Cyber Operations (CAE-CO). The inclusion of the colleges and universities below provides critical context for developing a robust curriculum for the new MSCO program at DSU.

Why These Institutions Were Selected:

- Peer Excellence in Cybersecurity Education

Each institution highlighted demonstrates a strong commitment to cybersecurity and cyber operations education, either through CAE-CO designation or by offering programs that closely align with DSU's goals. By benchmarking against these programs, DSU ensures its curriculum will be competitive, comprehensive, and aligned with national and global industry demands.

- Diverse Program Offerings and Models

The selected institutions represent a variety of program types, including graduate-level programs and specialized government-supported institutions. This diversity provides a well-rounded perspective on best practices in curriculum design, student engagement, and pathways for professional advancement.

- Alignment with National Standards

The programs at these institutions adhere to the high standards set by the NSA for Centers of Academic Excellence. This ensures that graduates are prepared to meet the challenges of the cybersecurity workforce. Referencing these programs helps DSU align its curriculum with these national benchmarks and ensures its continued leadership in the field.

- Institutional Scale and Focus

The enrollment sizes and institutional missions of these programs vary widely, from large public universities like Mississippi State University (23,000 students) to highly specialized institutions like the Air Force Institute of Technology (approximately 1,050 students). This range reflects the ability to serve diverse populations while maintaining program excellence.

a. Mississippi State University: Offers a Master of Science in Cyber Security and Operations, with options for thesis, professional project, or coursework-only tracks. They are one of the ten universities, like DSU, that hold all three CAE designations of CAE-CD (since 2001), CAE-CO (since 2013), and CAE-R (since 2024). The student population is approximately 23,000 students.

b. University of Nebraska at Omaha (UNO): Offers a Master of Science in Cybersecurity with pathways emphasizing cyber operations, secure software engineering, and critical infrastructure. UNO is a CAE-CO-designated university with a student population of approximately 15,000.

c. Air Force Institute of Technology (AFIT): Located at Wright-Patterson Air Force Base in Ohio, AFIT serves as the Air Force's graduate school of engineering and management. It offers advanced degrees in cyber operations and related fields and is designated as a CAE-CO institution. The institution enrolls over 650 in-residence students and approximately 400 in distance learning and non-resident programs.

d. Naval Postgraduate School (NPS): Situated in Monterey, California, NPS provides graduate education in Cyber Systems and Operations with a focus on national defense applications. Designated as a CAE-CO institution, NPS has an enrollment of 2,670 students, with 1,445 full-time and 1,225 part-time.

The programs highlighted provide a strategic foundation for designing DSU's MSCO curriculum by showcasing successful models of cyber operations education. The diverse approaches and standards upheld by these institutions enable DSU to integrate proven best practices while maintaining its distinct leadership in the field. This ensures that DSU's MSCO program will address the evolving demands of both students and industry partners, solidifying its position as a trailblazer in cybersecurity education.

**14. What program accreditation is available, if any?**

There is no program accreditation, but DSU already holds the NSA National Center of Academic Excellence in the field of Cyber Operations (CAE-CO). DSU is one of only 22 universities in the US that holds this very elite designation.

**15. Will the proposed program pursue accreditation or certifications?**

No

**If no, why has the department elected not to pursue accreditation for the program?**

We already hold the only designation.

**16. Did the university engage any developmental consultants to assist with the development of the curriculum? Did the university consult any professional or accrediting associations during the development of the curriculum? What were the contributions of the consultants and associations to the development of the curriculum?**

*Developmental consultants are experts in the discipline hired by the university to assist with the development of a new program, including content, courses, and experiences, etc. Universities are encouraged to discuss the selection of developmental consultants with Board staff.*

No

**17. Inclusion of High Impact Practices (HIP) across all undergraduate programs is a strategic priority of the Board of Regents to enhance academic quality and increase student engagement. For associate's and bachelor's degree proposals, which HIPs will faculty embed into the program?**

*Mark all that apply. To be considered as a HIP program, two or more should be selected and required in the program.*

| High Impact Practices | Included |
|---|---|
| Capstone courses and projects | |
| Collaborative assignments and projects | |
| Common intellectual experiences | |
| Diversity/global learning | |
| ePortfolios | |
| First year experiences | |
| Internships | |
| Learning communities | |
| Service learning, community-based learning | |
| Writing intensive courses | |
| Undergraduate research | |

**18. For associate's and bachelor's degree proposals, discuss how HIPs will be embedded into the program**

*Your discussion should provide examples and include whether the HIP is required or an optional component. It should also indicate at what point the experience is offered or required. (eg "students will be required to participate in an internship during their third year of enrollment in order to develop skills in…").*

**Student Success**

This section outlines the university's plan to assess student achievement of the program learning outcomes.

**19. Complete the table below to provide evidence of a preliminary assessment plan. Place an asterisk next to assessments that are national or state-level instruments.**

*Note: It is only necessary to indicate the summative assessment for each outcome, not the formative assessments used throughout the program.*

| Program Learning Outcome | Course | Summative Assessment |
|---|---|---|
| Demonstrate the procedures of reverse engineering | - CSC 732: Assembly Language - CSC 774: Reverse Engineering - CSC 776: Reverse Engineering Malware | Students complete hands-on labs and a capstone reverse engineering project where they analyze compiled binaries, identify software behaviors, and produce comprehensive technical reports using static and dynamic analysis techniques. |
| Evaluate various types of cyber vulnerabilities, both internal and external, to reduce organizational risk. | - INFA 723: Cryptography - CSC 773: Mobile Communication and Advanced Network Security - CSC 748: Software Exploitation | Students conduct security evaluations of real-world systems, identify vulnerabilities through audits or tools (e.g., fuzzing, protocol analysis), and produce risk mitigation reports including cryptographic assessments and network defense strategies. |
| Execute constructed attacks against computer systems to take advantage of discovered vulnerabilities. | - CSC 748: Software Exploitation - CSC 774: Reverse Engineering - CSC 737: Embedded Systems | Students perform attack simulations in lab environments, successfully constructing and executing exploits against vulnerable binaries or embedded systems, documenting the process and demonstrating impact through controlled penetration tests and red team-style exercises. |

**20. How will outcomes for graduates of the program be assessed?**

*Outcomes may include employment and placement rates, licensure examination pass rates, acceptance rates to graduate school, student or employer surveys, or other assessments of graduate outcomes.*

- Percentage of graduates of the program who secure employment within 6 months of graduation in program related positions.
- The percentage of employed graduate students who assume additional data privacy related job responsibilities in current positions or in positions to which they are promoted.
- Percentage of program graduates who pursue a discipline-related Ph.D. within 5 years of program completion.
- Graduate feedback (surveys, interview, focus groups) on graduates' career progression and how well the program prepared them for professional roles.
- Regular faculty review of course and program assessment data to identify trends in student performance.
- Employer surveys will identify strengths and weaknesses of data privacy job-related performance of graduates.
- Identify peer disciplinary programs to benchmark performance on key indicators (IPEDs) to identify best practices and areas for improvement.

**Duplication and Competition**

**21. Do any related programs exist at other public universities in South Dakota?**
*A list of existing programs is available through the university websites and the RIS Reporting: Academic Reports Database. If there are no related programs within the Regental system, indicate* ***none.***

No. Within South Dakota's public university system, no other institutions offer a master's program specifically focused on cyber defense or cyber operations.

**A. If yes, defend the need for an additional program within the state, Include IPEDS enrollment data and additional data as needed.**

**B. If yes, would this program be a candidate for Regental system collaboration?**

**22. Do any related programs exist at any non-Regental college or university within 150 miles of the university?**
*List those programs here:*

DSU offers an MS in Cyber Defense, which prepares students with knowledge and skills to prevent cyber attacks -- a different skillset than cyber operations (offensive cybersecurity.) Within a 150-mile radius of DSU, there are no non-Regental colleges or universities offering master's programs in cyber operations. Southwest Minnesota State University in Marshall, MN recently indicated the launch of an MS in Cybersecurity, which is not equivalent to DSU's MS in Cyber Operations or its MS in Cyber Defense. SMSU's program does not require a bachelor's degree in a computer science-related field, and their website notes "To prepare for this program, students should familiarize themselves with fundamental programming and computer networking concepts using readily available online educational resources." Minnesota State University, Moorhead offers an MS in Cybersecurity offered through a mix of online and on campus courses. The curriculum leans to cyber defense, with no specific coursework in software exploitation, malware analysis, or reverse engineering. Neither option is specific to cyber operations and both lack the technical rigor of the proposed program. Neither university offers a doctoral program in cyber operations, as DSU does.

**A. If yes, use IPEDS to identify the enrollment in those programs.**

**B. What evidence suggests there is unmet student demand for the proposed program, or that the proposed program would attract students away from the existing program?**

## Market Demand

This section establishes the market demand for the proposed program (eg Regental system need, institutional need, workforce need). Use the following sources for your data:

- South Dakota Department of Labor & Regulation
- O-Net
- US Department of Labor Projections Central
- SDBOR Workforce and Degree Gap Analysis Report

**23. What is the expected growth of the industry or occupation in South Dakota and nationally?**
*Include the number of openings, as well as the percentage of growth when possible.*

The cybersecurity field is experiencing significant growth both nationally and within South Dakota.

National Outlook:
According to the U.S. Bureau of Labor Statistics (BLS), employment of information security analysts, which is the most closely related area to cyber operations, is projected to grow 33% from 2023 to 2033, a rate much faster than the average for all occupations. This growth is expected to result in approximately 17,300 job openings annually over the decade, stemming from both new positions and the need to replace workers transitioning to other roles or exiting the workforce.
https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

South Dakota Outlook:
While specific projections for cyber operations analysts in South Dakota are not readily available, the state's overall occupational growth is anticipated to be robust. The South Dakota Department of Labor and Regulation projects a 7.7% increase in occupational employment from 2022 to 2032, outpacing the national average of 2.8% for the same period.
https://dlr.sd.gov/lmic/lb/2024/lbart_sept2024_occ_projections_fastest_growing.aspx

Given the nationwide demand for cybersecurity professionals, it is reasonable to infer that South Dakota will also experience growth in this sector, though exact figures are not available. The cybersecurity industry is poised for substantial expansion both nationally and within South Dakota, offering numerous opportunities for professionals in the field.

**24. What evidence, if any, suggests there are unfilled openings in South Dakota or nationally?**

National Outlook:
- Job Openings: As of 2023, there are approximately 700,000 unfilled cybersecurity positions across the United States.
- Growth Projections: The U.S. Bureau of Labor Statistics projects a 35% increase in employment for Information Security Analysts from 2021 to 2031, significantly outpacing the average growth rate for all occupations. https://cset.georgetown.edu/publication/introducing-the-cyber-jobs-dataset/

South Dakota Outlook:
- Job Openings: The state has around 1,200 cybersecurity job openings.
- Growth Projections: While specific percentage growth data for South Dakota is limited, the state's commitment to cybersecurity education and infrastructure suggests a positive trend.

https://www.freedomworkshere.com/cybersecurity

DSU Applied Research Corporation (DARC): DSU is expanding its cybersecurity research capabilities through the Dakota State University Applied Research Corporation (DARC). A new 100,000-square-foot facility in Sioux Falls is set to open in 2026, aiming to house approximately 400 cyber research professionals. This is in addition to DSU's initiative to scale up its Applied Research Lab capacity to 125 full time positions (DSU Cyber 2027).
https://www.siouxfalls.business/with-groundbreaking-dsu-applied-research-building-hits-critical-milestone/
https://dsu.edu/news/2022/01/dakota-state-90-million-initiative.html

This expansion is expected to create numerous job opportunities and contribute to addressing the cybersecurity workforce gap in South Dakota.

Both nationally and within South Dakota, the cybersecurity sector is poised for substantial growth, with a significant number of unfilled positions indicating strong demand for qualified professionals. Initiatives like DSU's DARC are instrumental in bridging this gap by providing specialized training and research opportunities. By offering this degree program, DSU can help close this gap.

**25. What salaries can program graduates expect to earn in South Dakota and nationally?**

Graduates with a Master of Science in Cyber Operations can anticipate competitive salaries both nationally and within South Dakota.

National Salary Expectations:

- Average Salary: According to a UC Berkeley survey, individuals holding a master's degree in cybersecurity earn an average salary of $214,000, with a median of $200,000, excluding bonuses. https://fortune.com/education/articles/cybersecurity-masters-grads-are-landing-200k-plus-pay-packages/

- Median Advertised Salary: Between January and October 2022, the median advertised salary for cybersecurity professionals with a master's degree was $110,000. https://www.franklin.edu/blog/masters-in-cybersecurity-salary

South Dakota Salary Expectations:

- Average Salary: As of September 14, 2024, the average annual pay for cybersecurity roles in South Dakota is $123,771. https://www.ziprecruiter.com/Salaries/Cyber-Security-Salary--in-South-Dakota

- Cybersecurity Engineer Salary: The average salary for a Cybersecurity Engineer in South Dakota is $120,907, with a typical range between $108,035 and $134,030. https://www.salary.com/research/salary/listing/cyber-security-engineer-salary/sd

These figures indicate that while South Dakota's salaries are slightly below the national average, they remain competitive, especially considering the state's cost of living. Graduates can expect to earn substantial incomes, with opportunities for higher earnings as they gain experience and advance in their careers.

**26. Optional: Provide any additional evidence of regional demand for the program.**
*e.g. prospective student interest survey data, letters of support from employers, community needs...*

**Student Demand**

**27. Provide evidence of student completers/graduates at that degree level at peer institutions that offer the same/similar program using data obtained from IPEDS.**

*Peer Institution: Regional and Competitive institutions. Choose programs not already listed in question 11. Use the most recent year available.*

| University Name | State | Program Name | Number of Degrees Conferred in Program | Total Number of Conferrals at Level (Undergrad or Grad) |
|---|---|---|---|---|
| University of Maryland Global Campus | MD : Maryland | MS Cyber Operations | 120 | 350 |
| Naval Postgraduate School | CA : California | MS Cyber Operations | 70 | 150 |
| University of Texas at San Antonio | TX : Texas | MS Cyber Operations | 60 | 175 |

**28. What evidence suggests there is interest from prospective students for this program at the university?**

We anticipate that the majority of students enrolling in the new MSCO program will be new to DSU. Industry partners such as Johns Hopkins University Applied Physics Laboratory and Battelle have expressed significant interest, stating that their employees are eager to enroll if this program becomes available.

Cyber Operations is the most heavily enrolled degree program at DSU, with a total of 543 students across the Bachelor of Science in Cyber Operations, the Master of Science in Computer Science (MSCS) with a Cyber Operations specialization, and the PhD in Cyber Operations. Currently, 451 students are enrolled in the Bachelor of Science in Cyber Operations. For those wishing to continue to a master's degree, their current options are limited to programs such as the Master of Science in Computer Science with a Cyber Operations specialization or Cyber Defense. Establishing this new program will eliminate the need for students to make this difficult choice by providing a direct path to advance their studies in Cyber Operations.

There are currently 23 students enrolled in the MSCS degree program, and 31 students enrolled in the MSCS degree program with the Cyber Operations specialization. It is likely that students from the specialization will change to the MSCO, but the enrollment in the MSCS with specializations is holding steady with 69 students in Fall 2022, 62 students in Fall 2023, and 70 students in Fall 2024. We believe the MSCS may initially see a drop in enrollment, but it is strong enough to stand on its own and will continue to grow.

Fall 2024 Enrollment by Cyber Operations Programs

BS in Cyber Operations - 451 students
MSCS with Cyber Operations specialization - 31 students
Ph.D. in Cyber Operations - 67 students
Total - 544 students

MSCS Enrollment Trends
In Fall 2024, the MSCS program includes 23 students without a declared specialization, 16 students in the Artificial Intelligence (AI) specialization, and 31 students in the Cyber Operations specialization. Overall, enrollment in the MSCS program, including all specializations, has remained steady, as shown below:
Program Students
MSCS - 39 (FA22), 30 (FA23), 23 (FA24)
MSCS with AI specialization - 3 (FA22), 7 (FA23), 16 (FA24)
MSCS with Cyber Operations specialization - 27 (FA22), 25 (FA23), 31 (FA24)
Total - 69 (FA22), 62 (FA23), 70 (FA24)

These enrollment trends demonstrate strong and consistent interest in specialized graduate education at DSU. By introducing the MSCO program, DSU will not only meet the growing demand for advanced studies in Cyber Operations but also reinforce its position as a leader in the field.

**Enrollment**

**29. Are students enrolling in this program expected to be new to the university or redirected from existing programs at the university?**

We expect there to be mostly new students enrolled, although it is realistic that some of the students currently enrolled in the Master of Computer Science with the Cyber Operations specialization will change majors to this program. We do not see this hindering other degree programs. Enrollment is strong enough in the Computer Science program for it to remain viable and even flourish.

**30. Complete the enrollment worksheet to provide an enrollment projection for the next six academic years**

| | |
|---|---|
| Worksheet Completed | Yes |

**31. What is the minimum number of students required in this program to break even, with respect to the budget?**

Since we are not hiring any new instructors nor do we have additional costs to create this program, we can have zero students enrolled and still break even.

**32. Discuss the assumptions informing your enrollment estimates.**
*(e.g. current enrollment and trends in similar programs, IPEDS data, recruitment strategies, partnerships)*

Enrollment projections for the MSCO program are grounded in several key assumptions. First, we anticipate strong interest from new students based on DSU's national reputation in cybersecurity education and industry-aligned curriculum. Demand is supported by significant interest from strategic partners such as Johns Hopkins University Applied Physics Lab and Battelle, whose employees have expressed readiness to enroll. We also expect internal transfers from the current MS in Computer Science (MSCS) with a Cyber Operations specialization, as students seek a more focused and technically intensive degree. Historical stability in MSCS enrollment trends (69 in 2022, 62 in 2023, 70 in 2024) suggests a solid baseline of interest in graduate-level cyber education. We assume approximately 10% annual growth in enrollment during the first three years due to DSU's established cybersecurity infrastructure, including the Applied Research Lab and DARC, which offer hands-on research opportunities and career pipelines. These factors, combined with a nationwide shortage of skilled cyber professionals, inform our expectation of 20 initial enrollees and sustained growth to 49 students by year six.

**33. If projected program enrollment is not realized in year two, what actions is the university prepared to take?**

If program enrollment is not realized by year two, the university is prepared to either change the marketing strategy or cease offering the program.

**34. Discuss the marketing and recruitment plan for the program**
*Include information on partnerships and pipelines (e.g. articulation agreements with BOTE, collaboration with partner university, community partnerships).*

The MSCO joins a highly regarded portfolio of graduate programs at Dakota State University—an institution nationally recognized for excellence in computer and cyber sciences. Cyber Operations is a cornerstone of DSU's academic identity, supported by elite designations such as the NSA Center of Academic Excellence in Cyber Operations. Recruitment for the MSCO program builds upon this reputation and leverages a strong existing base of undergraduate and doctoral programs, offering a clear and compelling pathway for both new students and professionals seeking technical advancement. Our enrollment strategy emphasizes five key dimensions:

1) On Campus Recruitment: DSU's undergraduate programs, particularly the BS in Cyber Operations, serve as the most direct pipeline into the MSCO. The university will implement a 4+1 Accelerated Pathway allowing eligible BSCO students to complete up to three graduate-level MSCO courses (9 credits) during their senior year. This not only shortens time-to-degree but also reduces overall cost and creates a seamless transition into

graduate education.

Additional recruitment efforts will target undergraduate students in technically aligned majors such as Computer Science and Network and Security Administration, emphasizing the tactical and hands-on nature of the MSCO. Marketing materials will highlight how the program bridges the gap between foundational and advanced offensive and defensive cyber skills—including reverse engineering, malware analysis, and software exploitation.

2) Alumni Engagement: Outreach will focus on DSU alumni with bachelor's degrees in Cyber Operations, Network and Security Administration, and Computer Science, showcasing the MSCO as a natural next step for career progression. Messaging will emphasize the program's alignment with real-world cybersecurity challenges and the unique opportunity for alumni to deepen their skill sets in a technical, operations-focused graduate program. Additionally, alumni currently holding positions in defense, intelligence, and security roles will be encouraged to refer colleagues or pursue the MSCO themselves as part of continuing professional development.

3) Partnerships and Collaborations: Strategic collaboration with organizations such as Johns Hopkins University Applied Physics Lab (JHUAPL), Battelle Energy Alliance, and the Dakota State University Applied Research Corporation (DARC) will drive enrollment by targeting their engineering and cybersecurity personnel who need advanced, operations-oriented education. DSU's involvement in WICHE/WRGP and MHEC ensures regional affordability and access.

4) Targeted Recruitment: The university will deploy targeted outreach using Educational Testing Services (ETS) lists and graduate search tools to identify students with interests in offensive cybersecurity, reverse engineering, and critical infrastructure protection. Digital campaigns will be distributed through professional organizations such as the Information Systems Security Association (ISSA), InfraGard, and SANS Institute, as well as cybersecurity subgroups within AFCEA and IEEE. Industry-specific messaging will target sectors such as defense, healthcare, and financial services—highlighting the MSCO's relevance to their security needs.

5) Social Media and Digital Campaigns: Recruitment will be amplified through professional platforms such as LinkedIn, Google Ads, Facebook, and Instagram, with campaigns emphasizing career growth in high-demand roles like penetration tester, reverse engineer, and cyber operations analyst. Testimonials from DSU alumni and industry partners will be spotlighted to reinforce the program's practical impact and strong career outcomes. All social content will direct viewers to the MSCO application portal and program overview.

**Financial Health**

**35. Complete the budget worksheet to provide a budget projection for the next six academic years.**

| | |
|---|---|
| Worksheet Completed | Yes |

| Financial Health Summary | | | | | | |
|---|---|---|---|---|---|---|
| | 1st FYxx | 2nd FYxx | 3rd FYxx | 4th FYxx | 5th FYxx | 6th FYxx |
| Tuition & Fee Revenues | 75975 | 182339 | 265912 | 296301 | 349484 | 349484 |
| Program Expenses | 17055 | 21319 | 21320 | 127605 | 125106 | 125106 |
| **NET** | 58920 | 161020 | 244592 | 168696 | 224378 | 224378 |
| Other Supporting Revenues | | | | | | |
| **NET (Other)** | 58920 | 161020 | 244592 | 168696 | 224378 | 224378 |

**36.Explain the amount and source(s) of any one-time and continuing investments in personnel, professional development, release time, time redirected from other assignments, instructional technology and software, other operation and maintenance expenses, facilities, etc., needed to implement the proposed major.**

*Address off-campus or distance delivery separately.*

We are not requesting one-time or continuing investments in personal, professional development, release time, or time redirected from other assignments, instructional technology and software. There are no other operational maintenance expenses to implement the proposed program.

**37. If new faculty are not requested, describe how existing faculty will be utilized and indicate whether this action will impact other existing programs.**

No new faculty are requested. We will use current faculty or adjuncts to cover new courses. We have budgeted to hire one additional faculty member in year 4, dependent upon enrollment and budget.

**38. Is the university requesting or intending to request permission for a new fee or to attach an existing fee to the program?.**

| | |
|---|---|
| Requesting Permission for Fee? | Yes, existing fee |
| Explanation | Yes, the university requests approval to apply the on campus Computer Science discipline fee to on campus graduate courses, and the Non-Resident Online Computer Science, Cyber Operations, and Network & Security Administration fee to online graduate courses in this program. |

**39. Use the table below to describe potential risks to the program's implementation over the next four years.**

*For each risk, identify the severity (low, medium, high), probability of occurrence (low, medium, high) and the institution's mitigation strategy for each risk.*

| Risk | Severity | Probability | Mitigation Strategy |
|---|---|---|---|
| **Low Enrollment** | Medium | Low | Increase marketing to regional, national, and global sectors. Encourage graduates of the BSCO program through the accelerated 4+1 program. |

## External Review

**40. If this proposal is for a graduate program, provide information below for at least five potential consultants who may be considered to conduct the external review.**

| Reviewer Name | Title | Institution |
|---|---|---|
| / | | |
| / | | |
| / | | |
| / | | |
| / | | |

## Additional Information

**41. (Optional) Use this space to provide pertinent information not requested above that may assist the Board in understanding the proposal.**

None

## Approvals

### University Approval

**To the Board of Regents and the Executive Director:** *I certify that I have read this proposal, that I believe it to be accurate, and that it has been evaluated and approved as provided by university policy.*

| President of the University | Date |
|---|---|
| Dr. Jose Marie Griffiths | 4/23/2025 |

| Academic Affairs, Provost | Date |
|---|---|
| Dr. Rebecca Hoey | 4/23/2025 |

| Finance and Administration, Vice President | Date |
|---|---|
| Stacy Krusemark | 6/5/2025 |

| Enrollment Management, Vice President | Date |
|---|---|
| Amy Crissinger | 4/23/2025 |