Intent to Plan for a New Program
South Dakota Board of Regents
Academic Affairs Forms

Internal Ticket ID: 21467
Created: 12/6/2024
Modified: 1/2/2025

Use this form to request authorization to plan a new baccalaureate major, associate degree program, or graduate program; formal approval or waiver of an Intent to Plan is required before a university may submit a related full proposal request for a new program. The Executive Director and/or their designees may request additional information. After the university President approves the Intent to Plan, submit a signed copy to the Executive Director through the System Academic Officer through the proper process. Only post the Intent to Plan to the university website for review by other universities after approval by the Executive Director, System Academic Officer or designee. This form is meant to capture critical elements for stakeholders to review prior to a full proposal.

University	DSU - Dakota State University
Degree	MS : Master of Science
Name of Major	X999 : New Major Requested **Cyber Operations**
Specialization Required?	*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
Intended Date of Full Proposal	Fall 2025
Planned CIP Code	11.0101

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 be a technical program firmly grounded in computer science and will emphasize applied research in cybersecurity. Students enrolled in the program will become a vital resource for research engineers, as well as for regional and national employers. The program aims to produce graduates with advanced technical expertise in cyber operations, applied research in cybersecurity, and innovation within computer science, emphasizing high-demand skills like malware analysis and software exploitation.

The curriculum places a strong emphasis on specialized 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. With the rapid growth of cyber threats and the increasing demand for specialized skills, there is a clear need for Dakota State University (DSU) to establish a MSCO. While DSU already offers a strong foundation through its bachelor's and Ph.D. programs in Cyber Operations, the absence of a master's level program limits opportunities for students seeking advanced, hands-on training. A master's program would bridge the gap between undergraduate education and the research-intensive Ph.D. pathway. It would not only benefit current students looking to deepen their expertise but also provide a direct pathway for professionals seeking to enhance their skills in areas such as offensive and defensive cyber operations, critical infrastructure protection, and advanced cybersecurity techniques.

At the state and national level, the proposed master's program aligns with South Dakota's growing cybersecurity needs and the increasing demand for mid-level cyber experts across the country. The program would prepare graduates to fill critical positions in government, defense, healthcare, and the private sector, addressing workforce shortages identified by industry leaders. By offering this program, DSU would contribute to positioning South Dakota as a leader in cybersecurity education, while providing a direct pipeline of highly skilled professionals capable of addressing evolving cyber threats and advancing both state and national security interests.

This program would also enhance the capabilities and impact of DSU's Applied Research Lab in 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 MSCO 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 MSCO and the research lab would elevate DSU's reputation as a leader in cyber operations research, both regionally and nationally.
Recently, the Johns Hopkins University Applied Physics Lab expressed the need for a MSCO at DSU. According to the director of a key lab, their engineers often lack the necessary expertise unless they are DSU graduates. The lab specializes in operations requiring deep knowledge of cyber operations techniques, and there is a significant gap in educational opportunities for its engineers. DSU is actively working to address this gap.

Battelle Energy Alliance also expressed interest in a MSCO at DSU. Between JHUAPL and Battelle, they have hundreds of research engineers who could benefit from this degree program.

Justification for Establishing the "Cyber Operations" Program as a Separate Academic Offering
The proposal to establish a distinct "Cyber Operations" academic program alongside the existing "Computer Science with a Specialization in Cyber Operations" is driven by critical differences in program focus, market demand, student needs, and alignment with industry expectations. Below are the key reasons supporting the necessity of offering two separate programs.

Distinct Educational Objectives
This program is designed to provide highly specialized, hands-on training in technical cybersecurity practices. It is tailored for students seeking cybersecurity specific roles with practical, operational skills as the primary focus. In the existing Computer Science degree with a Specialization in Cyber Operations integrates cybersecurity concepts, its core curriculum emphasizes foundational computer science principles such as algorithms, software development, and systems design. The cybersecurity specialization supplements this broad base but does not deliver the depth of technical, tactical, and strategic training found in the standalone Cyber Operations program.

Alignment with Workforce Demands
Industry and government organizations increasingly seek candidates with specialized expertise in cyber operations to address the growing threats in cyberspace. Roles such as cybersecurity analysts, penetration testers, and cyber operators require focused training that a general computer science degree with a specialization cannot fully provide.

Targeted Student Recruitment
The standalone Cyber Operations program appeals to students who are specifically interested in cybersecurity careers, this is particularly relevant for government employees and contractors.

By contrast, the existing program is better suited for students who wish to build a foundation in computer science while exploring cybersecurity as a complementary discipline.

Market Differentiation and Institutional Prestige
Offering a dedicated Cyber Operations program enhances DSU's ability to attract top-tier students and faculty interested in deeply technical cybersecurity. It differentiates the university as a leader in addressing the critical shortage of skilled cybersecurity professionals.

Maintaining both programs ensures that the university can simultaneously appeal to students seeking general computing expertise and those pursuing specialized, career-ready training in cybersecurity.

Strategic Impact

2. 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.

3. 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

4. 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.

5. 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	

6. 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.

Academic Quality

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

8. 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.

9. 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.

Duplication and Competition

10. 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?

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

Within a 100-mile radius of DSU, there are no non-Regental colleges or universities offering master's programs in cyber operations.

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

12. 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 industry is undergoing unprecedented growth, both nationally and within South Dakota, fueled by escalating cyber threats and increasing reliance on digital infrastructure. Although this expertise is not specifically recognized in research on labor, it aligns with other programs that project the need for this expertise. The most closely related fields that have data about them are the Information Security Analyst and Information Security Engineers.

National Outlook:

- O-NET OnLine identifies roles such as Information Security Analysts and Information Security Engineers as having a "Bright Outlook," indicating rapid growth and numerous job openings. https://www.onetonline.org/link/summary/15-1212.00?redir=15-1122.00

- Projections Central projects a 35% increase in employment for Information Security Analysts from 2022 to 2032, significantly higher than the average for all occupations. https://projectionscentral.org/Projections/LongTerm

South Dakota Perspective:

- South Dakota Department of Labor & Regulation (https://dlr.sd.gov/lmic/lb/2024/lbart_sept2024_occ_projections_fastest_growing.aspx) projects a 7.7% growth in occupational employment from 2022 to 2032, outpacing the national average.
- While specific projections for cybersecurity roles in South Dakota are not detailed, the state's overall employment growth suggests a positive trend for technology-related fields.

Workforce and Degree Gap Analysis:

- The South Dakota Board of Regents' Workforce and Degree Gap Analysis Report (https://sdbor.edu/wp-content/uploads/2023/11/8_F1_BOR0623.pdf) highlights a need for advanced degrees in technical fields, including cybersecurity, to meet the state's evolving workforce demands.

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

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

National Outlook:

- Job Openings: As of 2023, there are approximately 700,000 unfilled cybersecurity positions across the United States. https://cset.georgetown.edu/publication/introducing-the-cyber-jobs-dataset/
- 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.

South Dakota Outlook:

- Job Openings: The state has around 1,200 cybersecurity job openings. https://www.freedomworkshere.com/cybersecurity
- 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.

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.

14. 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.

15. 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

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

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	7080	150
University of Texas at San Antonio	TX : Texas	MS Cyber Operations	60	175

17. 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 academic area at DSU, with a total Fall 2024 enrollment of 544 students across the Bachelor of Science in Cyber Operations, the Master of Science in Computer Science (MSCS) with a Cyber Operations specialization, and the Ph.D. in Cyber Operations. The Bachelor of Science in Cyber Operations leads the way with 451 enrolled students.

For those seeking to advance their education beyond the bachelor's level, current options are limited to the MSCS with specializations in Cyber Operations or Cyber Defense. Establishing a dedicated MSCO program will provide a direct pathway for students to deepen their expertise in Cyber Operations, eliminating the need to choose between broader specializations. This targeted program is expected to attract both current students and professionals from partner organizations, further solidifying DSU's leadership in the field.

Fall 2024 Enrollment by Cyber Operations Programs

Program Students	Enrolled Fall 2024
BS in Cyber Operations	451
MSCS with Cyber Operations specialization	31
Ph.D. in Cyber Operations	67
Total	544

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	Enrolled Fall 2022	Students Enrolled Fall 2023	Students Enrolled Fall 2024
MSCS	39	30	23
MSCS with AI specialization	3	7	16
MSCS with Cyber Operations specialization	27	25	31
Total	69	62	70

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

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

Include the number of openings, as well as the percentage of growth when possible.

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.

19. Narrative Description of the preliminary estimates on annual enrollment in this program by year six

Include all students within the program, not just those new to the program.

Based on preliminary estimates and DSU's established reputation in cybersecurity education, the projected annual enrollment for the MSCO program by year six reflects consistent growth. This projection accounts for both new enrollees and continuing students within the program, showcasing DSU's ability to attract and retain talent in a field with high demand.

Year 1 to Year 6 Enrollment Trajectory: In the first year of the program, we estimate the enrollment of 15-20 students, consisting of new enrollments and students transitioning from related master's programs. The university's reputation, existing infrastructure, and strong ties to government and industry partners will help drive initial interest and enrollment.
Growth Over the First Three Years: We anticipate the enrollment to grow by approximately 10% annually during the initial three years, supported by DSU's active recruitment efforts, partnerships with regional and national organizations, and the appeal of the program's technical focus. By year three, total enrollment could reach 30-45 students, combining first-year and continuing participants.

Expansion by Year Six: By year six, the program is expected to achieve steady growth with 15-20 new annual enrollees and a retention rate of 85-90%, resulting in 30-45 total students actively participating in the MSCO.

The university's continued investment in resources, faculty, and collaborations with entities such as DARC will play a pivotal role in sustaining and promoting this growth. The program's success is fueled by the demand for technical expertise in cyber operations, leveraging DSU's existing strengths in cybersecurity and computer science.

Strategic Relevance to DSU: This projection aligns with DSU's mission to provide cutting-edge education in computer science and cybersecurity, meeting workforce demands outlined in the South Dakota Board of Regents' strategic plan. The growth trajectory positions DSU as a significant contributor to the regional and national pool of highly skilled cybersecurity professionals, cementing its status as a leader in this crucial academic and professional domain.