DAKOTA STATE UNIVERSITY

DOCTORATE OF PHILOSOPHY IN CYBER DEFENSE

Self-Study Report

March 2026

THE PURPOSE OF THIS SELF-STUDY IS TO EVALUATE THE STRUCTURE, GROWTH, AND SUSTAINABILITY OF THE PH.D. IN CYBER DEFENSE PROGRAM AT DAKOTA STATE UNIVERSITY. THE REPORT REVIEWS INSTITUTIONAL CONTEXT, PROGRAM CURRICULUM, FACULTY CAPACITY, RESEARCH INFRASTRUCTURE, STUDENT OUTCOMES, AND CONTINUOUS IMPROVEMENT PROCESSES.

The Beacom College of Computer and Cyber Sciences

Table of Contents

List of Tables

Executive Summary

The Ph.D. in Cyber Defense at Dakota State University prepares scholars and practitioners to conduct original research addressing complex cybersecurity challenges facing government, industry, and society. Since enrolling its first cohort in Fall 2019, the program has experienced steady growth in student interest and enrollment, reflecting both the national demand for advanced cybersecurity expertise and the university's established leadership in cyber education. The program serves both traditional doctoral students and experienced cybersecurity professionals seeking to advance research, policy, and technical innovation in the cyber domain.

Dakota State University has a long-standing mission in computing, cybersecurity, and information technologies. Since the state mission change in 1984, the university has developed nationally recognized programs focused on cyber operations, cyber defense, and applied research in computing disciplines. The university currently holds designations from the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Cyber Defense, Cyber Operations, and Cyber Research. These designations reflect the strength of DSU's programs and its contribution to the national cybersecurity workforce.

The Ph.D. in Cyber Defense is designed to produce graduates capable of conducting rigorous research, advancing cybersecurity knowledge, and leading organizations in addressing emerging cyber threats. The curriculum combines specialization coursework, a research methodology core, elective study, and dissertation research totaling 72 credit hours. Students may specialize in Technical Cyber Defense, Managerial Cyber Defense, or Data Privacy, allowing the program to serve professionals with diverse academic and professional backgrounds while maintaining a strong research foundation.

The program is supported by substantial institutional infrastructure and research resources. Facilities such as the PowerCyber Lab, Madison Cyber Labs (MadLabs®), and the MadLabs® Research Environment and Network (MADREN) provide advanced environments for experimentation, data analysis, and cybersecurity research. These resources enable students and faculty to conduct applied and interdisciplinary research aligned with national cyber defense priorities.

As a relatively young doctoral program, the Ph.D. in Cyber Defense continues to evolve through deliberate program evaluation and continuous improvement. The program monitors enrollment trends, dissertation progression, research output, and student outcomes to ensure that growth remains aligned with faculty mentorship capacity and research infrastructure. Strategic priorities include strengthening early-stage research mentoring, supporting doctoral student publication and conference participation, and maintaining sustainable faculty supervision loads.

This self-study evaluates the program's institutional context, curriculum structure, faculty capacity, research infrastructure, student support services, and assessment processes. The review demonstrates that the Ph.D. in Cyber Defense is aligned with Dakota State University's mission, supported by substantial research infrastructure, and positioned to contribute to the advancement of cybersecurity research and workforce development at the national level.

Part 1: Institutional History

1.1 Heritage: 1881 to 1982

Dakota State University (DSU) was established in 1881 as the first teacher education institution in Dakota Territory. Teacher education remained the primary mission of the institution through the 1950s. However, in response to the changing needs of South Dakota in the 1960s, the university began to expand its role to include degree programs in liberal arts and business. In 1980, South Dakota welcomed a major new industry into the state: the banking and credit card industry. The success and growth of this new industry, as well as the success of other information oriented, computer-based industries in the state, prompted the state's leadership to carefully examine the degree programs offered at the public institutions of higher education within the state.

Throughout its 143 years, DSU has had a proud heritage of preparing graduates to meet the needs of a changing society. Since 1881, the university has provided challenging academic programs in one of the best educational environments in the state. The continuation of this tradition of service is of prime importance to the faculty, students, staff, and administration of DSU.

1.2 Mission Change: 1983 to 1984

In 1984, the Legislature of the State of South Dakota (South Dakota Codified Law §13-59-2.2) assigned DSU the role and mission of developing technology-based degree programs in information systems, business, teacher education, and allied health care services at both the undergraduate and graduate levels. The Legislature provided $2.6 million in additional operating funds to support a three-year mission change at DSU.

During the initial phase of the transition, the academic programs of the institution were reviewed. Degree programs were phased out if they were duplicated at the other five regental institutions or if graduates would enter an over-supplied marketplace. The South Dakota Board of Regents (SDBoR) approved new information systems programs, computer equipment, and facilities for DSU. During the transition, special attention was given to ensure that all students in programs slated for phase out received a full opportunity to complete those programs. To ensure the continuation of education quality, when the number of students continuing in a program became exceedingly small, a special faculty mentoring program was developed.

The second phase of the transition began in August 1984, with the development of degree programs that integrated computers and information technologies into traditional academic subjects and added coursework specific to the computer and information systems areas. The University hired new faculty and retrained existing faculty.

Realizing that the innovative programs being developed at DSU were expensive, private industry and state government provided the University with additional financial resources. Consultants from state agencies and from national corporations also provided assistance and guidance that contributed greatly to the success of the mission change.

1.3 Statutory and Regents Mission Authority

1.3.1 Mission Statement by South Dakota Codified Law §13-59-2.2

The primary purpose of DSU is to provide instruction in computer management, computer information systems, electronic data processing, and other related undergraduate and graduate programs. The secondary purpose is to offer two-year, one-year and short courses for application and operator training in the areas authorized by this section.

This authorization includes the preparation of elementary and secondary teachers with emphasis in computer and information processing.

Except for degree programs in existence during the 1983-84 academic year, the unique baccalaureate programs authorized for DSU shall not be duplicated by the SDBoR.

1.3.2 Mission Statement by South Dakota Board of Regents (SDBoR)

The SDBoR regards the special focus universities of South Dakota as valuable contributors to the state's system of higher education. Special focus universities have a high concentration of degrees in a single field or set of related fields. Special focus universities offer master's and doctoral programs within their special focus area.

Universities operating within this sector are nationally recognized to promote research activities of their faculty, staff, and students. DSU's research is propelling the workforce, economy, and student experience. The SDBoR recognizes that special focus universities have unique characteristics and are critical to the success of the South Dakota system of higher education.

The principles outlined in this policy serve as overarching directions for special focus universities reflecting efficient and effective roles in scholarly research and economic development. In addition, special focus university functions align with the SDBoR strategies to advance student access, affordability, degree completion rates, and quality education.

1.4 Institutional Mission, Vision, and Strategic Plan

1.4.1 DSU Institution Mission, Vision, & Values

Mission. DSU's mission is to prepare cyber-savvy graduates who are lifelong learners, problem solvers, innovators, and leaders to live lives of positive purpose and consequence.

Vision. Innovative, entrepreneurial, and resilient since 1881, DSU will continue to rise through short - and long-term success of our students and graduates, increased strength in applied research and athletics, and deep engagement with our stakeholders, in an environment infused with quality improvement.

Values. DSU adheres to the following values:

- Distinguished and effective teaching

- Integrity
- Clear communication
- Innovation
- Inclusion
- Quality

1.4.2 Strategic Plan DSU ADVANCE 2027

DSU's strategic plan begins with its mission, vision, and values that create a framework for university strategic goals. The strategic plan is built on the university's strengths and focuses attention and commitment on the most pressing issues DSU is distinctively positioned to address while seeking to advance student success through highly engaged, high-impact educational practices.

The current Strategic Plan *DSU ADVANCE 2027* began in 2022 and will continue to evolve through 2027 and beyond. The Strategic Plan outlines a path to more direct scholarship, research, intellectual property, and economic development through solutions to all varieties of cyber threats to computing and information devices, networks, and their users. Both foundational goals and the five Pillars further frame actions, resources, and measures.

Foundational goals support strategic goal success:

- Ensure Financial Stability
- Strengthen Regional and National Relevance
- Enhance Ability to Recruit and Retain Talent
- Increase Student Enrollment
- Enhance Student Success
- Maintain Higher Learning Commission Accreditation
- Ensure Responsible Stewardship of State Resources
- Strengthen Risk Management Process

Five Pillars frame the focus of strategic goals and milestones (benchmarks):

- Pillar 1: Increase Student Success
- Pillar 2: Improve Engagement, Governance, & Communication
- Pillar 3: Grow Scholarship, Research, Intellectual Property, & Economic Development
- Pillar 4: Elevate Athletics
- Pillar 5: Increase Sustainability & Resilience

Mission and strategic plan alignment gave DSU its first graduate degree programs when authority was received from the SDBoR to offer a Master of Science in Information Systems (1998). A year later, the Master of Science in Educational Technology was offered on campus (1999). In 2004, DSU received authorization for its first doctoral program, offered in Information Systems. DSU now offers four doctoral degrees, nine master's degrees, and eleven graduate certificates. As the institution endeavors to articulate its mission in the fullest way, degree programs are scrutinized each year to ensure they remain on the forefront relative to technology to enhance and support instruction and address work force demands.

DSU currently holds three prestigious designations from the National Security Agency (NSA) and the Department of Homeland Security (DHS) as National Centers of Academic Excellence (CAE) in Cyber Defense, Cyber Operations, and Cyber Research. DSU received its first CAE distinction in Information Assurance Education in 2004, one of 50 programs recognized. DSU was named as a National Center of Academic Excellence in Cyber Operations (CAE-CO) in 2012, one of the first four schools to receive the CAE-CO designation for the 2012-2013 academic year. As of January 2026, there are currently 498 institutions with a designation, including CAE-CD, CAE-CO, and CAE-R from the National Security Agency. All 498 hold the CAE-CD designation, 21 institutions hold the CAE-CO designation, and 98 institutions hold the CAE-R designation. DSU is one of only nine universities in the U.S. that holds all three designations.

1.5 Accreditation History

DSU is accredited by the Higher Learning Commission (HLC), founded in 1895, and is one of several institutional accreditors in the United States. HLC accreditation indicates that DSU has the standards, processes, and assurance that it delivers quality educational experiences. DSU must meet 18 core components within the five HLC Criteria for Accreditation.

The university completes periodic reviews for reaffirmation of accreditation through HLC's Open Pathway, a ten-year cycle with an assurance review in year four and a comprehensive evaluation in year ten. The Open Pathway also includes an improvement component, the Quality Initiative, between years four and ten, that provides DSU the opportunity to pursue improvement projects that meet institutional needs.

The institution's most recent comprehensive visit, in October 2018, resulted in a positive review without any requirement for monitoring reports. In October 2022, DSU also met all 18 core components during its mid-cycle assurance review.

The Beacom College Computer Science Bachelor of Science program was granted ABET accreditation in fall of 2025.

1.6 University Structure and Academic Authority

1.6.1 Organizational Structure (Main Campus and National Presence)

1. Main Campus (Madison): The DSU's main campus located in Madison serves residential students in undergraduate, professional, and graduate programs. The campus includes the colleges of Arts and Sciences, Business and Information Systems, Education and Human Performance, and The Beacom College of Computer and Cyber Sciences.

2. National Presence: DSU offers specialized degrees to students from across the United States and beyond. DSU shall be the computing and information technologies and cyber security leader for the state of South Dakota, and a recognized leader across the United States.

1.6.2 Academic Curriculum and Credentials

DSU is statutorily authorized under SDCL § 13-59-2.2 to offer academic programs computer management, computer information technologies, cyber security, education with an emphasis in computer and technology systems, and other related undergraduate and graduate programs. Students who attend DSU pursue highly technical degrees with a broad focus in current and emerging computing and information technologies/cyber security that emphasize innovation, leadership, application, and research. DSU has the authority to credential certificates, associate degrees, baccalaureate degrees, master's degrees and doctoral degrees provided formal approval by the SDBoR. The SDBoR may authorize academic programs outside of the statutory mission as identified by the Regents due to workforce needs, strategic needs of the state, etc. All program requests must comply with BOR Policy 2.3.2 and 2.3.3.

1.6.3 Research and Economic Development

Special research focus universities in South Dakota perform a wide range of research initiatives. While DSU has an emphasis in the areas of Computer Sciences, DSU's educational and research activities address all aspects of current, emerging, and future Computer and Information Technologies/Cyber Security. DSU's research provides the maximum opportunity to students seeking to study with top researchers and pursue careers related to the technological fields. This is most important for those students pursuing graduate education. DSU conducts (3) three types of research increasing student growth which results in discovery, creativity, or innovation: ***f***aculty-driven discipline-specific research; collaborative, problem-driven applied research in all CIT/Cyber Security areas through the MadLabs®***.***

Regionally located in eastern South Dakota provides a unique hub where DSU and South Dakota State University (also regionally located in eastern South Dakota) complement each other in Agricultural Technological fields. Collaborative partnerships continue to evolve between the special focus universities and the research universities. This research pierces the boundaries in generating new innovative ideas. In addition to providing graduate student experience, research is a critical driver of both innovation and economic development.

Working together with business and industry in Madison, Sioux Falls, and all of South Dakota, DSU will foster continued research in South Dakota, economic development in South Dakota, and innovation throughout the United States. Specifically related, DSU offers highly specialized research in support of national security and defense through DSU's Applied Research Lab (ARL). The research activities of the MadLabs® and ARL drive innovation, workforce development, and economic development for South Dakota.

1.7 DSU Initiatives

1.7.1 DSU Rising Initiative

In 2017, DSU began a transformational five-year capital investment initiative called DSU Rising. The initiative was the result of a $30 million donation from philanthropists Miles and Lisa Beacom and Denny T. Sanford. The donation allowed for the construction of an $18 million, 40,000 square foot research and development building for the MadLabs®. The funds also provided for additional scholarships, new

program development, hiring of more faculty and staff, and support the university's intent to bring 5G network capabilities to Madison, the region, state, and eventually the nation.

1.7.2 DSU Rising II

The DSU Rising II project (2022) created a funding consortium to provide $90 million to fund new components to the cyber research and education environment: a 100,000 square feet facility to house the expanded DSU Applied Research Lab (ARL) in Sioux Falls, S.D., the support required to double the DSU cyber graduates, authority to expand DSU ARL Management and Security, to expand merit based student scholarships in cyber education, and to launch the Governors Cyber Academy (a statewide K-12 cyber education program).

1.8 University Profile

1.8.1 Student Demographics

The total headcount for Fall 2025 was 3,842, an 18.54% increase from 3,241 in Fall 2022. Graduate enrollment reached 757 students, representing an increase from 484 students in Fall 2022 of over 56.4%.

Of the Fall 2025 enrollment, 3,085 students were enrolled in undergraduate programs and 757 students were enrolled in graduate programs. DSU serves both residential and distributed learners through a combination of on-campus and online delivery. In Fall 2025, 1,319 students attended courses on campus, while 2,523 students were enrolled in online programs.

The university also maintains a significant international student presence. In Fall 2025, 317 students were international students, contributing to the diversity of the academic community and supporting DSU's engagement with the global cybersecurity and technology workforce.

Section 4.1 Enrollment Analysis, Retention, and Placement Review contains additional demographic information that includes a breakdown of students by gender and ethnicity for the Ph.D. in Cyber Defense program, The Beacom College of Computer and Cyber Sciences, and the university.

1.8.2 Technology and Computing Environment

Students at DSU enjoy unique access to technology. In 2005, all students were provided fully functional portable computers (tablets) that included digital inking capabilities and voice-to-text translation. Currently, DSU provides students with the latest Dell Latitude 7440, a 2-in-1 Laptop configured specifically for DSU academic programs.

For degree programs emphasizing information assurance, security issues, and digital design, additional lab facilities featuring computers with high end functionality have been added to the campus technology infrastructure.

1.9 College Mission

The mission of The Beacom College of Computer and Cyber Sciences is to educate and prepare students to be lifelong learners and professionals in Computer and Cyber Sciences. We seek to challenge students

to develop skills in computer and cyber sciences, to think logically, and to make sound decisions through our programs in Artificial Intelligence (B.S., M.S. and proposed Ph.D.), Computer Science (B.S., M.S., and Ph.D.), Cyber Defense (M.S. and Ph.D.), Cyber Operations (B.S., M.S., and Ph.D.), Data Privacy (M.S.), Computer Game Design (B.S.) and Network and Security Administration (B.S.).

In addition to course work in the academic setting, The Beacom College provides opportunities for students to learn through work and consulting experience. Internships and supervised professional practices are available in most programs.

1.10 History of the Ph.D. in Cyber Defense at DSU

The Cyber Defense program enrolled its first students in the Fall of 2019. The structure of the program required a core of various cybersecurity courses, both technical and managerial in focus:

INFA 702 - Data Privacy 3 credits

INFA 710 - Cybersecurity Program Design and Implementation 3 credits

INFA 713 - Managing Security Risks 3 credits

INFA 720 - Incident Response 3 credits

INFA 721 - Computer Forensics 3 credits

INFA 730 - Physical Security 3 credits

INFA 731 - Personal Security 3 credits

INFA 733 - Vendor Management 3 credits

INFA 754 - Intrusion Detection 3 Credits

INFA 758 - Security Metrics 3 credits

Over time and via continuous evaluation, it was determined that this inclusive approach proved to be a challenge for students depending on their background. While the admissions team strived to only admit well qualified students, it was found that students and faculty struggled due to the technical and managerial hybrid background required in the program. Students with a strong focus in cyber defense management were underprepared for technical coursework, such as Intrusion Detection. In a similar fashion, students that had strong technical backgrounds did not meet the expectations needed for concepts such as Personnel management.

This problem was studied in detail both with faculty and student stakeholders. It was determined after the assessment of the program that students would be better served through creating specializations within the program as opposed to having one size fits all. This led to the creation of three separate specializations within the program: Technical, Data Privacy, and Managerial. Upon application, students select which track they feel is the best fit for their background. These selections are taken into account by the admissions committee to evaluate that a student's background appropriately aligns to their preferred specialty.

1.11 Program Evolution and Strategic Context

Since enrolling its first cohort in Fall 2019, the Ph.D. in Cyber Defense has experienced sustained growth in both applications and enrollment. This growth reflects national demand for advanced cybersecurity expertise and DSU's expanding reputation in cyber defense education and research.

As a developing doctoral program, continued growth requires careful alignment between enrollment, faculty mentorship capacity, and research infrastructure. Doctoral education differs fundamentally from undergraduate and master's education in its reliance on individualized faculty supervision, intensive research mentoring, and dissertation committee engagement. The program therefore monitors enrollment trends, dissertation supervision loads, and faculty research alignment to ensure that program expansion remains sustainable.

The Ph.D. in Cyber Defense is housed within The Beacom College of Computer and Cyber Sciences, which provides a concentrated faculty base with expertise across technical cybersecurity, cyber operations, artificial intelligence, and data privacy. This structure allows the program to maintain strong alignment between doctoral coursework, faculty research expertise, and dissertation supervision.

As the program continues to mature, historical enrollment trends and program outcomes inform strategic priorities in faculty hiring, doctoral advising capacity, and research development. These priorities are intended to ensure that the program maintains rigorous academic standards while continuing to contribute to the national cybersecurity research workforce.

The Ph.D. in Cyber Defense at DSU is a research-focused doctoral program designed to prepare cybersecurity professionals and scholars to conduct original research, contribute to national cyber defense priorities, and assume leadership roles in academia, government, and industry.

Part 2: Trends in the Discipline of Cyber Defense

Cyber Defense continues to evolve rapidly in response to emerging threats, technological advances, and national cybersecurity policy shifts. Nationally, doctoral programs in cybersecurity are increasingly emphasizing interdisciplinary approaches that blend technical research with policy, ethics, and management. Key trends influencing DSU's Ph.D. in Cyber Defense include artificial intelligence and machine learning for threat detection, quantum security, federated learning, cyber resilience, and integration of privacy-preserving technologies. The program also tracks developments in national cyber workforce frameworks and aligns with the NSA CAE-R and NICE standards to ensure relevance and rigor.

Cybersecurity and cyber defense remain areas of sustained national and global urgency. The rapid evolution of threat environments, expansion of connected infrastructure, and increasing regulatory complexity have elevated the demand for advanced research expertise beyond entry-level workforce preparation. The discipline is shifting from reactive security practice toward proactive, research-driven defense strategies that integrate artificial intelligence, privacy engineering, policy analysis, and systems resilience.

At the doctoral level, this shift has several implications.

First, the demand for the Ph.D. in Cyber Defense is growing not only in academia, but also in federal agencies, national laboratories, defense contractors, and private industry. Doctoral graduates are increasingly expected to lead research initiatives, shape policy, and contribute original scholarship that influences national cyber strategy.

Second, competition among institutions offering doctoral education in cybersecurity is increasing. Institutions designated as National Centers of Academic Excellence are expanding graduate offerings, and several universities have launched online or hybrid doctoral models. While DSU's accessibility to practitioner learners is a strength, the program must continuously ensure that rigor, research productivity, and scholarly engagement meet or exceed national expectations for doctoral education.

Third, the discipline itself is becoming more interdisciplinary. Effective cyber defense research now requires integration of technical security mechanisms, data privacy considerations, human factors, governance structures, and economic impact analysis. The interdisciplinary structure of the Ph.D. in Cyber Defense program aligns well with this evolution; however, it requires ongoing curricular review to maintain coherence and depth across domains.

In response to these disciplinary trends, the Ph.D. in Cyber Defense program emphasizes:

- Sustained emphasis on original, publishable research contributions
- Strategic alignment of faculty expertise with emerging research domains such as AI-enabled security, critical infrastructure protection, and privacy-enhancing technologies
- Participation of doctoral students in externally funded research initiatives
- Continuous evaluation of curriculum relevance relative to national cybersecurity priorities

The discipline of cyber defense will continue to evolve rapidly. The program's responsibility is not only to respond to change, but to contribute meaningfully to shaping the field through research, innovation, and doctoral leadership development.

Part 3: Academic Program and Curriculum

The Ph.D. in Cyber Defense program is designed to prepare students for leadership roles and advanced research careers in cybersecurity. It emphasizes the development of research methodologies, ethical decision-making, and advanced technical expertise.

3.1 Program Curriculum

The curriculum is structured in five components: prerequisite knowledge courses when required, specialization coursework, research core coursework, elective coursework, and dissertation research.

The Ph.D. in Cyber Defense requires 72 total credit hours, distributed across specialization coursework, research core courses, electives, and dissertation research summarized in Table 1.

Table 1. Ph.D. in Cyber Defense Program Credit Structure

Component	Credits
Specialization Coursework	15
Research Core	12
Electives	18
Dissertation Preparation and Research	27
Total Program Credits	**72**

The detailed course requirements for each component of the curriculum are described in the sections that follow. Students may specialize in Data Privacy, Managerial Cyber Defense, or Technical Cyber Defense. Each specialization focuses on distinct skill areas - from privacy management to network security monitoring and offensive security.

3.1.1 Knowledge Courses (6 Credits)

Individuals who do not meet prerequisite knowledge requirements may be required to take up to six additional credits. These courses are required for students who cannot demonstrate sufficient background knowledge in cybersecurity or related technical fields. The prerequisite courses are summarized in Table 2.

Table 2. Knowledge Prerequisite Courses

Course	Title	Credits
CSC 609	Operating Environments	3
INFA 701	Principles of Information Assurance	3

These courses do not count toward the 72-credit program requirement and are assigned only when prerequisite knowledge is insufficient.

3.1.2 Required Specialization Courses (15 Credits)

Students select one of three specializations at the time of application. Each specialization requires completion of 15 credit hours of required coursework as summarized in Tables 3–5.

Table 3. Data Privacy Specialization Required Courses

Course	Title	Credits
INFA 702	Introduction to Data Privacy	*3*
INFA 713	Managing Security Risks	*3*
INFA 722	Data Privacy Management	*3*
INFA 726	Data Privacy Technology	*3*
INFA 742	Ethics and Information Technology	*3*
	Total Credits	***15***

Table 4. Managerial Specialization Required Courses

Course	Title	Credits
INFA 702	Introduction to Data Privacy	*3*
INFA 713	Managing Security Risks	*3*
INFA 720	Incident Response	3
INFA 730	Physical Security	1
INFA 731	Personnel Security	1
INFA 733	Vendor Management	1
INFA 758	Security Metrics	3
	Total Credits	**15**

Table 5. Technical Specialization Required Courses

Course	Title	Credits
INFA 735	Offensive Security	3
INFA 751	Wireless Security	3
INFA 754	Network Security Monitoring and Intrusion Detection	3
INFA 720	Incident Response	3
INFA 721	Digital Forensics	3
	Total Credits	**15**

Completion of one specialization is required for all students in the Ph.D. in Cyber Defense program. The specialization coursework provides advanced technical, managerial, or data privacy foundations that support subsequent doctoral research preparation.

3.1.3 Research Core (12 Credits)

The research core of the program, shown in Table 6, is structured for students to learn appropriate applications of research methodologies, academic writing styles, and preparation for dissertation work.

Table 6. Research Core Courses

Course	Title	Credits
CSC 803	An Introduction to Research	3
CSC 804	Computer and Cyber Security Research Methodology	3
CSC 807	Computer and Cyber Security Research Design and Implementation	3
CSC 808	Mixed Research Methods for Computer and Cyber Sciences: Design and Implementation	3
	Total Credits	**12**

3.1.4 Dissertation (27 Credits)

Dissertation credits account for the faculty and student time devoted to dissertation research and supervision. The dissertation phase combines structured research preparation, doctoral seminars, and supervised dissertation research totaling 27 credit hours as shown in Table 7.

Table 7. Dissertation Credit Requirements

Course	Title	Credits
CSC 809	Dissertation Preparation	3
CSC 890	Doctoral Research Seminar	3
CSC 890	Residency Research Seminar	3
CSC 898D	Dissertation	18
	Total Credits	**27**

Students must complete three on-site residency research seminars (CSC 890, one credit each) held in a face-to-face format on the Madison, South Dakota campus. Residencies are offered each semester and typically last three to five days. These seminars provide opportunities for students to engage with faculty and peers, discuss contemporary cybersecurity research, present research ideas, identify dissertation advisors, and complete major doctoral milestones including proposal defense, oral comprehensive examination, and final dissertation defense. Completion of these components results in the required 72 credit hours for the Ph.D. in Cyber Defense.

3.1.5 Electives (18 Credits)

Any CSC/INFA 700-800 course, except INFA 701.

The research core provides a foundation in advanced research methods, mixed-methods design, and cybersecurity-specific methodologies. The dissertation phase culminates in original research contributing to the discipline, supported by in-person research residencies in Madison, South Dakota.

3.2 Oral Comprehensive Exams

The purpose of the oral comprehensive examination is for the faculty to assess the student's synthesis of knowledge in the areas of the discipline and research core of the Ph.D. Cyber Defense program. The comprehensive exam is a significant milestone towards determining the student's readiness to undertake independent research in the cyber defense field.

All Ph.D. in Cyber Defense students must demonstrate a minimum level of disciplinary and research competence. The oral comprehensive examination assesses students' mastery of core disciplinary knowledge and research preparation.

3.2.1 Selection of the Oral Examination Committee and Chair

The oral examination committee is composed of two (or more) faculty members who participate in the graduate cyber defense program and who hold current graduate faculty status at DSU.

- Two members of the committee must be faculty members from the Beacom College of Computer and Cyber Sciences

- Additional members, as observers, may teach in the program but may not hold doctoral degrees.

3.2.2 Eligibility

The student must successfully complete (B or better), or currently be enrolled in, all core discipline and research courses. They must be in good academic standing with DSU.

3.2.3 Process

The oral comprehensive examination is approximately 2 hours in length. The oral exam is a closed book exam, i.e., the use of any material (books, articles, notes, etc.) is not allowed during the exam.

The procedure for the oral examination is as follows:

1. The committee chair introduces the student.
2. A recording of the oral exam is started for an official record.
3. The student summarizes his/her experiences as a Ph.D. student.
4. Discipline-specific and research methods questions from core Ph.D. CD courses are the subjects to be covered in the examination.
5. An approximate time frame for oral examination is up to 10 minutes per course. All 10 minutes are not required. Committee members will use their judgement on timing but should keep questions per class/topic to 10 minutes or less.
6. The committee will direct questions to the student in order to assess the student's competency in the selected field of study and the student's ability to synthesize knowledge gained while in the program.
7. Throughout the exam, the committee will assess student performance.
8. After the examination has been completed, the student will be asked to leave the room. At this time the committee members evaluate the student's understanding of the selected field of cyber defense and research knowledge.
9. The student is brought back into the room to receive the committee's pass/fail decision.

3.2.4 Grading

Students passing both components (discipline and research) of the comprehensive exam will be considered as an overall pass. There will be a maximum of 2 attempts for any of the components. Only components failed will be retested. Upon the failure of two attempts, the student may not continue in the program.

3.2.5 Appealing Academic and Administrative Decisions

All appeals are made to the Graduate Dean's office and all decisions based on appeal are voted on by Graduate Council.

3.2.6 Timeline

The exam can be scheduled after the midpoint of the semester or towards the end of the academic semester. Ideally, students would schedule their oral comps in the last few weeks of the semester before they plan to begin formally supervised dissertation work.

Note that summers can be unpredictable, and students are not guaranteed summer availability of faculty.

3.3 Ph.D. Residency

Collaboration is an essential part of DSU's Ph.D. program. All Ph.D. programs within The Beacom College at DSU are available online; this online nature requires intentional design to build scholarly community in an online format. To alleviate some of these concerns yet allow the program to remain available to practitioner learners, students collaborate via three residencies on the campus in Madison, SD. Students are required to complete three residency sessions, though additional participation is encouraged. The core requirements of each are:

- First residency: meet program faculty and student cohorts, begin exploration of research topics as well as seeing the dissertation process in action. Attend dissertation proposals and defenses and partake in in-depth research experiences
- Second residency: the student will propose their dissertation topic and seek feedback from faculty and peers. In addition, the students will partake in the research experience of other peers, providing feedback and insight from their experiences to other students' dissertations.
- Third residency: the student will complete their final dissertation defense. In addition, the students will partake in the research experience of other peers, providing feedback and insight from their experiences to other students' dissertations.

3.4 Dissertation

It is the doctoral student's responsibility to make sure that dissertation preparation meets the specified formatting requirements. The style, format, content and layout standards technically ensure dissertation research can be appropriately submitted and easily catalogued for future consumer access.

DSU's growing research program has traditionally allowed the dissertation standards and formatting to be determined by the dissertation chair. As the programs have grown and matured, a more standardized approach is required. After engagement with appropriate stakeholders, an initiative to create college-specific dissertation guidelines was launched. In order to meet the unique needs of each college, it was determined that The Beacom College of Computer and Cyber Science would establish a college-specific set of dissertation standards. The dissertation standards are available for review but are not included in this document for the sake of brevity.

The dissertation must represent original work. Proper attribution is required for all sources, including text, data, figures, tables, and visual materials.

The use of generative AI tools (e.g., ChatGPT, image generators, code generators) in dissertation research or writing must be disclosed and is subject to the approval of the dissertation chair and committee. Any content produced or substantially shaped by AI must be clearly documented and attributed. Undisclosed or inappropriate use of AI will be treated as an academic integrity violation, as is the falsification of data, research results, citations, or other scholarly material. Students are encouraged to review DSU's statement on Academic Integrity.

The SDBoR has established expectations of student behavior including acts of Academic Misconduct or Dishonesty. Students can read SDBoR Policy 3.4.1 Student Code of Conduct policies specific to Acts of Academic Misconduct and Dishonesty.

3.4.1 Dissertation Ethics

Conducting sound, responsible research is more than simply following rules and regulations. Responsible researchers consider the impact of their work on participants in their research, students and mentees, advisors and other faculty, their program and university, and of course, humanity.

All doctoral students are required to complete training on Responsible Conduct of Research addressing issues of authorship, peer review, plagiarism, and research misconduct. This online training can be done through DSU's Office of Research and Economic Development (RED) who manage these offerings through the Collaborative Institutional Training Initiative (CITI). IRB (Institutional Review Board) approval is required for any research involving human subjects, including surveys, interviews, and observational studies. Compliance with these policies is critical and must be done before any data is collected. Students would also do well to review DSU Policies on Human Subjects Research (6.6), Data Retention and Destruction (6.5), and Research-Based Data Collection and Release Policy (01-20-00).

3.4.2 Publication and Archival

Archiving of Master's Theses and Doctoral Dissertations have enduring value as records of scholarship at DSU. They serve as the final reports of research conducted at the institution, by students of the institution, under the direction of the faculty of the institution. Therefore, the University preserves and makes available these theses to scholars and the public by maintaining an archival collection and a circulating collection.

All masters theses and doctoral dissertations require an electronic submission through ProQuest, which fills orders for paper or digital copies of the dissertation and makes a digital version available online via their subscription database, ProQuest Dissertations & Theses. ProQuest provides worldwide distribution of your work from the master copy. Students retain control over their dissertation and are free to grant publishing rights as they see fit.

Copies of doctoral dissertations and master's theses are also uploaded in PDF format to DSU's Beadle Scholar. A print and bound copy of each master's thesis or doctoral dissertation is submitted to DSU's Karl Mundt Library by ProQuest. Students can also order print and bound copies for themselves, dissertation chairs or others.

Students are strongly encouraged to maintain their dissertation-related development work (e.g., code, scripts, and technical resources) on GitHub. Doing so provides a secure, version-controlled record of progress; supports transparency and reproducibility of research; and creates a professional portfolio that can be shared with faculty, peers, and future employers. Hosting work on GitHub also aligns with best practices in open science.

3.4.3 Publication Embargo

DSU is committed to the dissemination of scholarly work while also recognizing that, in certain circumstances, immediate public release of a dissertation may not be in the best interest of the student or their research.

Doctoral students may request an embargo on their dissertation at the time of submission for archiving. An embargo delays public access to the full text of the dissertation in the university's repository and other distribution channels.

- Students may request an embargo of up to six (6) months with written justification. Conditions for embargo may include pending publication, intellectual property (IP) or patent considerations, or contractual obligations with external sponsors.
- In the case of IP or patent considerations, the student must have informed and coordinated with DSU's Technology Transfer Chair.
- All embargo requests must be supported by the students' dissertation chair and submitted with the final dissertation materials.
- Requests to extend an embargo beyond six months must again include written justification and a single extension of no more than 6 months can be approved. Total embargo is limited to one-year.

The Graduate Dean reviews and adjudicates all embargo requests. This policy balances the University's mission to share scholarly research with the academic community and public while respecting the legitimate needs of students to delay access for professional or legal reasons.

3.5 Transfer Credits

Academic courses will be transferred as meeting graduation requirements if the courses parallel the scope and depth requirements for the degree or if the courses meet electives required for the degree.

The following minimum conditions must be met before graduate-level credit can be accepted:

- The institution from which credit is transferred is regionally accredited at the Master's level.
- The student must have been in good standing at the institution from where the credit is transferred.
- The grades in courses transferred are "B" or better.
- The transfer credits must have been completed no more than five years prior to commencement of the DSU graduate degree program.
- No more than 29 credits may be applied to another master's degree. The program committee for each degree program may establish specific program level processes and criteria for course evaluation.

3.6 Curriculum Evaluation and Ongoing Review

The Ph.D. in Cyber Defense curriculum is designed to balance advanced disciplinary knowledge, research methodology, and independent scholarly contribution. Milestones such as the oral comprehensive examination, structured residency experiences, and formal dissertation standards provide clear progression benchmarks for doctoral candidates.

As the program has matured, faculty have engaged in ongoing evaluation of the curriculum to ensure alignment with national doctoral standards and disciplinary evolution. Several areas require continuous monitoring:

3.6.1 Online Delivery and Scholarly Culture

All Ph.D. programs within The Beacom College are delivered online, supplemented by required in-person residencies. While this model increases accessibility for practitioner learners, it differs from traditional residential doctoral programs in its opportunities for spontaneous scholarly exchange and research immersion.

Faculty continue to assess whether:

- Residency frequency and duration sufficiently support research community development.
- Online research seminars provide adequate intellectual rigor and engagement.
- Additional structured research colloquia or dissertation workshops would strengthen scholarly cohesion.

3.6.2 Comprehensive Examination Structure

The oral comprehensive examination is intended to assess synthesis of disciplinary and research knowledge. Faculty periodically review examination outcomes to determine:

- Whether exam structure appropriately evaluates research readiness.
- Whether time-to-completion of core coursework aligns with expected candidacy timelines.
- Whether additional formative assessments would better support dissertation preparation.

3.6.3 Dissertation Preparation and Research Readiness

The dissertation phase represents the culminating scholarly contribution of the program. As enrollment has increased, faculty are placing increased emphasis on early research engagement within coursework to accelerate topic refinement and proposal development.

Ongoing curricular priorities include:

- Encouraging early identification of research interests.
- Strengthening integration between research methods courses and dissertation design.
- Monitoring time-to-candidacy and time-to-defense trends.

- Expanding opportunities for doctoral students to co-author publications with faculty.

3.6.4 Continuous Improvement Process

Curriculum review occurs through regular faculty discussion, assessment of student performance data, and evaluation of emerging cybersecurity research priorities. Adjustments to course sequencing, elective offerings, and research seminar content are made as necessary to ensure relevance, rigor, and sustainability.

As the Ph.D. in Cyber Defense continues to grow, curricular decisions will remain closely aligned with faculty capacity, research productivity, and national expectations for doctoral scholarship.

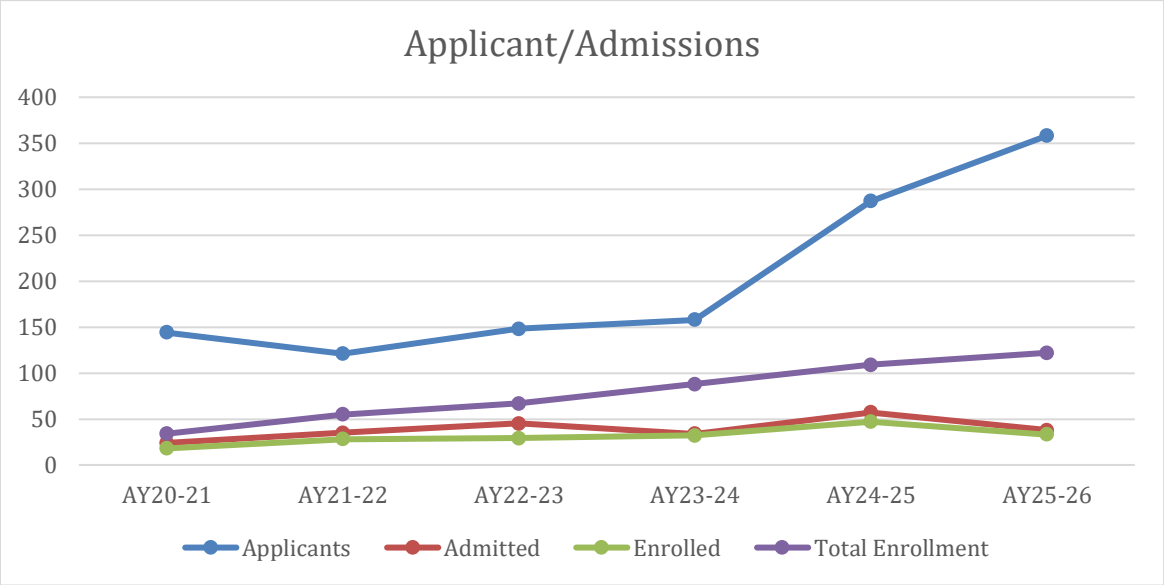
Part 4: Program Enrollments and Student Placement

Since its inception, the Ph.D. in Cyber Defense program has attracted students from diverse professional backgrounds, including federal service, military organizations, private industry, and academia. Graduates pursue careers in cybersecurity research, higher education, defense analysis, and leadership roles across both public and private sectors.

The program has experienced steady growth while maintaining admission limits aligned with faculty advising capacity and dissertation supervision resources. Applicant demand consistently exceeds available cohort capacity, as reflected in the data summarized below.

Tables 1–3 summarize application trends, enrollment patterns, and retention outcomes for the program. Table 8 summarizes applicant volume, admissions decisions, yield, and total program enrollment.

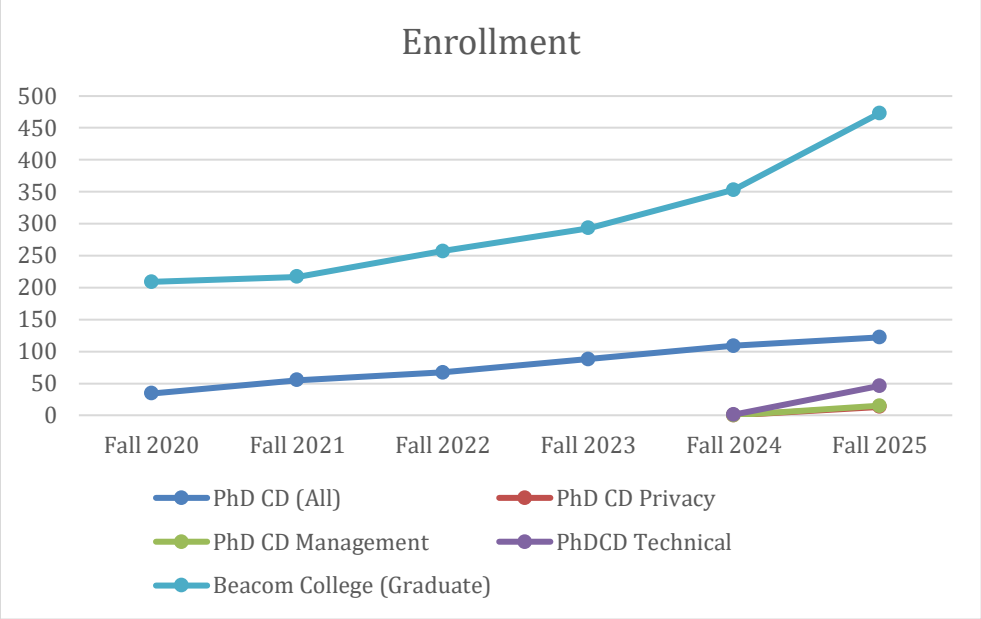
Table 8. Applicants, Admissions, Matriculation, and Total Program Enrollment



Note: Applicant, admission, and enrollment figures reflect the annual admissions cycle for the Ph.D. in Cyber Defense program.

Aside from admissions, the program has maintained overall steady growth along with the college's graduate programs. Table 9 presents total program enrollment by year and includes specialization distribution beginning in Fall 2024, alongside overall Beacom College graduate enrollment.

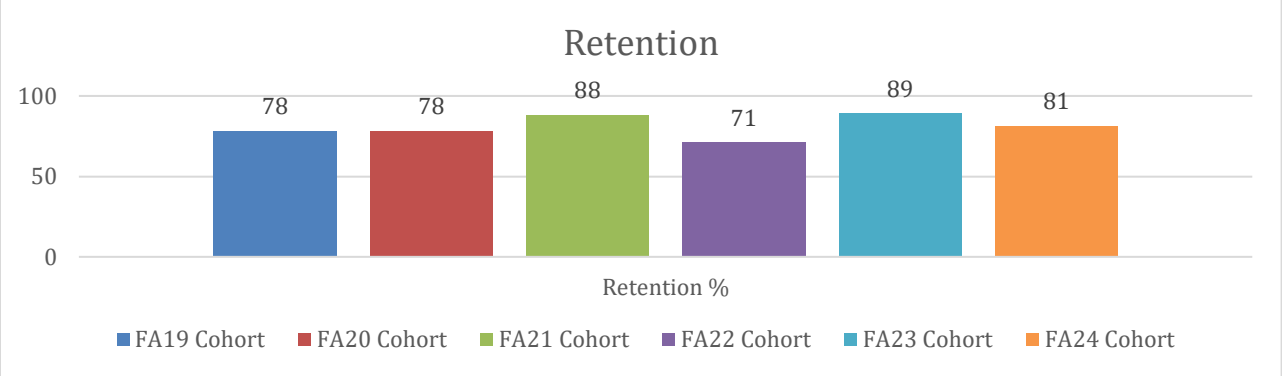
Table 9. Ph.D. in Cyber Defense Enrollment by Specialization (Introduced Fall 2024) and Beacom College Graduate Enrollment



Note: Enrollment figures reflect fall census enrollment. Specializations were introduced in Fall 2024.

The program has maintained retention rates above 80% for first-time admitted cohorts, as shown in Table 10**.**

Table 10. Program Retention by Year



Note: Retention is calculated based on first-time admitted doctoral cohorts.

Applicant demand consistently exceeds available capacity. Managing this demand while maintaining sustainable faculty advising workloads remains an central program management priority.

4.1 Enrollment Analysis, Retention, and Placement Review

Since its inception, the Ph.D. in Cyber Defense has experienced substantial growth in applicant volume and total enrollment. This sustained interest reflects strong national demand for advanced cybersecurity expertise and the program's growing visibility.

While growth reflects strong program reputation and national workforce demand, doctoral enrollment must remain aligned with faculty capacity and research mentorship availability. The program monitors admission selectivity and cohort size to ensure that growth does not outpace dissertation supervision resources.

4.1.1 Admission and Yield Trends

Applicant volume has increased significantly over recent academic years. Admission decisions are guided by:

- Academic preparation
- Research potential
- Professional experience
- Alignment with faculty expertise

As demand increases, maintaining selectivity remains essential to preserving doctoral rigor and ensuring student success.

4.1.2 Retention and Cohort Progression

Retention data by cohort are tracked and reviewed regularly. Faculty examine patterns in:

- Persistence through core coursework
- Successful completion of comprehensive examinations
- Progression to dissertation proposal
- Time-to-defense

Doctoral attrition may result from professional obligations, research misalignment, or personal circumstances. The program continues to evaluate whether additional early-stage research mentoring, proposal workshops, or structured advising checkpoints would improve persistence.

Table 11. Ph.D. in Cyber Defense Admissions and Progression Summary

Metric	Value
Applications Reviewed	967
Applications Accepted	182
Acceptance Rate	18.4%
Students Completing Coursework	128
Dissertation Defenses Completed	25

Admission data reflect strong applicant demand and a selective admissions process. Progression data indicate that a substantial proportion of admitted students complete doctoral coursework and advance toward dissertation research. As a relatively young program, the number of completed dissertations

continues to grow as cohorts progress through the program. The program maintains a highly selective admissions process, with an acceptance rate of 18.4%, ensuring alignment between student preparation, research potential, and faculty mentorship capacity.

4.1.3 Time-to-Degree Monitoring

As a relatively young doctoral program, longitudinal time-to-degree data continue to mature. However, monitoring candidacy timelines and dissertation duration remains a strategic priority. Faculty review:

- Time from admission to comprehensive exam
- Time from candidacy to dissertation defense
- Factors influencing delays

The goal is to balance flexibility for practitioner learners with expectations consistent with national doctoral standards.

4.1.4 Comprehensive Examination Outcomes

The oral comprehensive examination represents the primary academic milestone confirming readiness to advance to doctoral candidacy. As of Spring 2026, thirty-nine oral comprehensive examinations have been administered in the Ph.D. in Cyber Defense program. The first-attempt pass rate is 84.6%. Six students required a second attempt; all successfully passed on the second attempt, resulting in an overall pass rate of 100%.

These outcomes indicate strong alignment between program admissions standards, doctoral coursework preparation, and the expectations of the comprehensive examination process. Students who require a second attempt receive targeted faculty guidance to address identified gaps prior to retesting.

Students who do not pass on the first attempt receive targeted remediation from their doctoral committee and typically retest within the following academic term. To date, all students who have taken a second attempt have successfully passed the examination.

Comprehensive examinations are evaluated by two to three doctoral faculty examiners with additional faculty observers to ensure consistency and academic rigor. Comprehensive examination outcomes for the program are summarized in Table 12.

Table 12. Ph.D. in Cyber Defense Oral Comprehensive Examination Outcomes (2023-2026)

Metric	Value
Total Oral Comprehensive Exams Administered	39
First-Attempt Pass Rate	84.6%
Students Requiring Second Attempt	6
Second-Attempt Pass Rate	100%
Overall Pass Rate	100%

Note: Outcomes represent all comprehensive examinations administered during the reporting period.

Comprehensive examinations are administered by a core group of doctoral faculty with experience supervising doctoral research, ensuring consistency in expectations, evaluation standards, and academic rigor across examination cycles.

Successful completion of the comprehensive examination advances students to doctoral candidacy and the dissertation research phase.

4.1.5 Graduate Placement

Doctoral graduates are prepared for leadership roles in academia, government, defense, and industry. As the number of graduates increases, the program is formalizing processes to track:

- Sector placement distribution
- Research versus practitioner leadership roles
- Continued publication and professional engagement
- Alumni contributions to cybersecurity policy and innovation

Systematic placement tracking will inform future curricular adjustments and strategic partnerships.

4.1.6 Enrollment Sustainability

The program recognizes that strong applicant demand must be balanced with responsible growth. Sustainable doctoral education requires alignment among:

- Faculty chair availability
- Research infrastructure capacity
- Advising workload
- Institutional support services

Annual enrollment targets will continue to be evaluated relative to faculty capacity and dissertation supervision commitments.

Enrollment planning is directly tied to documented dissertation supervision capacity. The Ph.D. in Cyber Defense program enforces a maximum cap of six active dissertation chair assignments per faculty member across all doctoral programs. Admission targets are reviewed annually relative to current chair load distribution to ensure that no faculty member exceeds this threshold. This capacity-based enrollment model ensures that program growth remains deliberate, sustainable, and aligned with individualized doctoral mentorship standards.

Part 5: Faculty Credentials

The Ph.D. in Cyber Defense is supported by faculty in The Beacom College of Computer and Cyber Sciences who hold terminal degrees in computer science, cyber operations, and related disciplines. Faculty contribute to doctoral instruction, research mentorship, and dissertation supervision while maintaining active research agendas and professional engagement within the cybersecurity community.

Core faculty supporting the program include Dr. Kyle Cronin (Department Chair), Dr. Cody Welu, Dr. Chad Fenner, Dr. Kyle Korman, Jason Jenkins, Quentin Covert, Kanthi Narukonda, and additional faculty who contribute expertise in cybersecurity, artificial intelligence, and data privacy research.

Additionally, faculty from related departments including Computer Science, Cyber Operations, and Emerging Technologies support the program through course instruction, elective offerings, and dissertation supervision. Table 13 summarizes the faculty members who support the program and identifies their academic credentials and roles within the program, including doctoral instruction, dissertation supervision, and elective course support.

Table 13. Faculty Supporting the Ph.D. in Cyber Defense Program

Faculty	Degree	Ph.D. in Cyber Defense Program Role
Ahmad Al-Hammouri	Ph.D.	Chairs & supports dissertations
Andrew Kramer	Ph.D.	Teaches support/elective courses
Austin O'Brien	Ph.D.	Chairs & supports dissertations
Chad Fenner	Ph.D.	Teaches program core courses, chairs & supports dissertations
Cody Welu	Ph.D.	Teaches program core courses, chairs & supports dissertations
Jihene Kaabi	Ph.D.	Teaches program research courses, chairs & supports dissertations
John Hastings	Ph.D.	Teaches program research courses, chairs & supports dissertations
Kanthi Narukonda	M.S., Ph.D ABD	Teaches program core courses
Kyle Cronin	D.Sc.	Department Chair, supports dissertations
Mark Spanier	Ph.D.	Chairs & supports dissertations
Michael Ham	D.Sc.	Teaches support/elective courses
Pat Engebretson	D.Sc.	Chairs & supports dissertations
Quentin Covert	Ph.D. ABD	Teaches program core courses
Shawn Zwach	Ph.D.	Teaches support/elective courses
Tyler Flaagan	Ph.D.	Teaches program core courses, chairs & supports dissertations
Varghese Vaidyan	Ph.D.	Teaches program research courses, chairs & supports dissertations
Youssef Harrath	Ph.D.	Teaches program research courses, chairs & supports dissertations

5.1 Workload

DSU's current faculty workload policy became effective May 1, 2025. While the standard workload is 30 workload units per academic year, time is allocated to faculty members who hold professorial rank and who actively engage in research, scholarship, or creative artistic activity or who actively pursue professional service activities related to their disciplines. Ordinarily, reasonable allocated time is equivalent to six workload units of instruction, or its equivalent per academic year and, if assigned, the faculty member must be actively engaged in productive scholarship. The institution may adjust this workload requirement to ensure faculty members have adequate time for research and scholarship or service or as deemed necessary by the institution.

The typical full time teaching load for tenured or tenure track faculty is 24 semester credit hours for each academic year (fall and spring). Faculty whose teaching load exceeds that requirement (and who are actively engaged in research, scholarship, or creative artistic activity and who actively pursue professional service activities related to their disciplines) may qualify for overload pay when the teaching load exceeds the 24-credit requirement in any given academic year. Faculty holding professorial rank but located off campus are required to provide service to the university, service to the discipline, and to actively engage in research, scholarship, or creative artistic activity.

Academic advising is recognized as part of a faculty member's teaching workload and generally will not exceed an assignment as primary adviser of more than 50 students for faculty members with professorial rank and more than 30 students for faculty members with lecturer rank. An unusually heavy advising load can be offset by a reduction in the faculty member's committee or other college assignments and/or a reduction in teaching load for faculty members holding lecturer rank.

5.2 Faculty Development

In July 2018 DSU established its Center for Teaching and Learning (CTL) to serve as the university hub of teaching support and innovation. Prior to the establishment of the CTL, a single university committee was charged with identifying instructional development topics and implementing faculty workshops/events. That committee is now an advisory group to the CTL, which is directed by a senior faculty (1/2 time, by application) and includes an instructional design and technology specialist (full time) and clerical support. The CTL is also assisted by four faculty associates (one from each of the four colleges at DSU) who are among the university's most accomplished instructors with strengths in course development, learner engagement, and assessment. The CTL faculty associates provide mentoring and consultation with individual faculty when time permits. Additionally, the CTL identifies, coordinates, and provides professional and academic development activities for faculty and staff. The CTL works with academic administrators and faculty to identify instructional priorities and develop programming to address those priorities.

The CTL not only supports teaching and learning traditional classroom environments but is especially focused on providing pedagogical and technology development in online environments. This support has included the creation of instructional aids, materials, and media that are accessible online to assist faculty in improving teaching and student interaction skills.

The CTL has also initiated peer review of all online courses using the state mandated Quality Assurance (rubric). For graduate students, the CTL provides expertise to support the goals of the university, including assisting in the production of quality thesis, dissertations, presentation, grant writing, and understanding of compliance issues. For undergraduates, engagement objectives include topics on mentored research, integrity (plagiarism, and copyright), and student service/government.

5.3 Funding for Faculty Research and Professional Development

Examples of funds available for faculty research and travel include:

- DSU supports a Faculty Research Initiative (FRI) intended to encourage and facilitate faculty research and creative activity. The competitive grants offer up to $3,000 for individual faculty or up to $5,000 for collaborative teams.
- The Supporting Talent for Research Trajectories (START) internal funding program was launched in 2018. This seed fund offers faculty support for preliminary work on research that will result in proposals for externally funded research grants.
- DSU also routinely sets aside significant funding for instructional and professional travel and for faculty training. Individual faculty can qualify for up to $1,200 for travel and training at qualifying events.

5.4 Faculty Capacity, Research Productivity, and Sustainability

The Ph.D. in Cyber Defense is supported by a diverse group of faculty who contribute to core instruction, research mentorship, and dissertation supervision. Institutional workload policy provides for research engagement and scholarly activity, recognizing the central role of scholarship in doctoral education.

As the program has grown, faculty capacity and dissertation supervision availability has become an increasingly important strategic consideration.

5.4.1 Dissertation Supervision Load

Doctoral education relies heavily on sustained faculty mentorship. Faculty members serve as dissertation chairs and committee members across multiple cohorts. To maintain research quality and timely student progress, the program monitors:

- Active dissertation chair assignments per faculty member
- Committee participation load
- Alignment between faculty research expertise and student dissertation topics
- Cross-program supervision demands

Annual review of dissertation assignments helps ensure that faculty workload remains sustainable and that students receive appropriate mentorship depth.

As of Spring 2026, fifteen faculty members serve as active dissertation chairs within the Ph.D. in Cyber Defense program. Doctoral dissertation supervision occurs across multiple doctoral programs within The

Beacom College of Computer and Cyber Sciences. Because faculty frequently serve as chairs and committee members across programs, dissertation supervision load is monitored collectively to ensure that faculty mentoring responsibilities remain sustainable and aligned with institutional policy. Table 14 summarizes current dissertation chair assignments across Beacom doctoral programs.

Table 14. Doctoral Dissertation Supervision Overview (Beacom Faculty Only, Spring 2026)

Metric	Value
Beacom faculty eligible to chair dissertations	23
Total active dissertation chair assignments	56
PhD Cyber Defense dissertations	24
PhD Computer Science dissertations	6
PhD Cyber Operations dissertations	31
PhD Information Systems dissertations (by Beacom)	1
Maximum allowed per faculty (policy cap)	6

Note: Dissertation chair assignments include all doctoral programs within The Beacom College of Computer and Cyber Sciences. Faculty supervision load is monitored across programs to ensure compliance with the institutional cap of six active dissertations per chair.

Active Ph.D. in Cyber Defense chair assignments total 24 dissertations and are distributed across faculty within The Beacom College and select approved interdisciplinary faculty.

To maintain doctoral mentorship quality, the program enforces a maximum cap of six active dissertation chair assignments per faculty member across all doctoral programs. Faculty supervision load is formally categorized as low, medium, or high based on total cross-program chair commitments. Faculty who reach the six-dissertation cap are not assigned additional doctoral students until load decreases.

Enrollment targets and admission decisions are reviewed annually in alignment with documented chair capacity to ensure that doctoral growth does not exceed sustainable faculty supervision limits. This structured oversight process supports timely student progression and preserves the integrity of individualized doctoral mentorship.

5.4.2 Research Productivity and Scholarly Engagement

Faculty supporting the Ph.D. in Cyber Defense maintain active research agendas, publish in peer-reviewed venues, and present at national conferences. Continued emphasis on scholarly productivity is essential to sustaining doctoral rigor.

Strategic priorities include:

- Increasing co-authorship between faculty and doctoral students
- Expanding participation in externally funded research initiatives
- Strengthening publication output in high-impact cybersecurity venues
- Aligning faculty hiring and development with emerging research areas

Doctoral programs are strengthened when faculty scholarship and student research trajectories are closely integrated.

5.4.3 Hiring and Future Capacity Planning

Given sustained enrollment growth, future hiring decisions must account for:

- Emerging specialization needs
- Dissertation supervision capacity
- Research funding opportunities
- Interdisciplinary collaboration demands

Strategic hiring of research-active faculty in high-demand cybersecurity domains will remain a priority to ensure program sustainability.

5.4.4 Faculty Development and Support

Institutional support structures such as the Center for Teaching and Learning provide ongoing instructional development. At the doctoral level, faculty development also includes:

- Support for grant proposal development
- Conference travel and research dissemination
- Mentorship for junior faculty engaged in dissertation supervision
- Structured review of research expectations

Maintaining a strong faculty cohort requires not only credentialed expertise but also sustained institutional investment in scholarly growth.

5.4.5 Sustainability Considerations

The program recognizes that doctoral growth must be aligned with faculty availability and research infrastructure. Continuous monitoring of:

- Teaching load distribution
- Advising assignments
- Dissertation chair commitments
- Research productivity benchmarks

ensures that the Ph.D. in Cyber Defense maintains both academic rigor and operational sustainability.

Part 6: Academic and Financial Support

The Ph.D. in Cyber Defense program is supported by institutional resources that provide academic advising, research support, and professional development opportunities for doctoral students. These resources are coordinated through the Office of Graduate Studies and The Beacom College of Computer and Cyber Sciences. Available support includes graduate assistantships, internal research funding through the START and Faculty Research Initiative (FRI) programs, and instructional development through the Center for Teaching and Learning. Research facilities such as MadLabs® and the Applied Research Lab provide additional opportunities for funded research and industry collaboration.

6.1 Advising

DSU employs a two-tier advising model for Ph.D. in Cyber Defense students. After hearing from the Graduate Dean on their acceptance to the program, graduate enrollment counselors reach out to new students to coordinate student onboarding activities including admissions, orientation, and academic advising. The graduate enrollment counselors support graduate students in every stage of their graduate program, helping to provide information, access resources, register for classes, alleviate administrative and technological barriers, and promote student success. Other key roles for graduate enrollment counselors include:

- Advising and assisting students with the development of their Plan of Study and recommending it to the respective department chair for approval.
- Completing course substitutions and credit transfer forms.
- Maintaining up-to-date, accurate and detailed documentation on student interactions, progress, and meetings.
- Recommending appropriate resources for students who need additional academic support to improve student success.
- Collaborating with appropriate departments (Registrar, Financial Aid, Cashier, Disabilities Services, Counseling Services, Veterans Services, etc.) to resolve individual student issues and ensure positive student experiences.

New doctoral students are also assigned a graduate faculty advisor. Upon entry to the program, the Cyber Defense Department Chair, Dr. Kyle Cronin, serves as the initial academic advisor for all doctoral students.

Other roles for graduate faculty advisors include:

- Discussing skill development and specializations
- Career planning
- Transitioning students to dissertation chair and committees
- Guide students through the program assessment process (comprehensive exams, dissertation)
- Addressing challenges that may occur with student preparedness

Each student also has a dissertation advisor who helps the student with research and dissertation. A doctoral dissertation committee is formed when a student is ready to conduct proposal defense and

dissertation defense. The committee includes a chair or co-chairs, at least one program faculty representative, and one Graduate Council representative.

All dissertation/theses project committees are comprised of a chair (or two co-chairs) and additional members of no less than three or more than four members. The chair must be a full member of the DSU Graduate Faculty and a member of the students' degree program faculty. With the Department Chair's permission, the student may also select a chair outside the program committee who possesses expertise in the student's chosen topic. An exception to dissertation chair service may be made in the case of inter-institutional collaborations and under the structure of an MOU signed by the University Provost. A dissertation chair or committee member from a collaborating university may be recommended by the Program Chair and approved by the College Dean and Dean of Graduate Studies. At least one committee member must be a tenure-track faculty member within the DSU program.

In addition to the chair or co-chairs, the dissertation committee must include at least two additional members who hold terminal degrees. And may be selected from the following groups:

- Program faculty: Graduate Faculty from the student's program of study.
- College or University Faculty: Full-time or adjunct faculty with Graduate Faculty status having expertise in the student's area of research or methodological application. Faculty without Graduate Faculty status can also be considered.
- External to the university: From industry, business, government, other institutions of higher education, doctoral candidates may submit a prospective committee members vitae/resume and a inclusion justification to the Dissertation Chair for consideration. The Chair forwards the recommendation to the Dean of Graduate Studies for approval. There is no monetary compensation provided for the service of external dissertation committee members.

6.2 Karl Mundt Library

The mission of the Karl E. Mundt Library is to support the curriculum of DSU. The Mundt Library provides a wide range of services and a diverse collection of reference and informational materials for the use of the faculty and staff of DSU. The library exists to serve as an archive of accumulated knowledge, a gateway to scholarship, and a catalyst for the discovery and advancement of new ideas. In fulfilling its obligation to provide knowledge to the University and the scholarly community at large, the library collects, organizes, and provides access to recorded knowledge in all formats. The library faculty initiates discussions and proposes creative solutions to the information challenges facing the University and the scholarly community. The library's faculty and staff actively participate in providing quality service, access, instruction, and management of scholarly information.

Since DSU received its current focused mission in the 1980s, the Mundt Library's mission has been to expand its collection of materials on computers, technology, and information systems. To that end, the library has subscribed to an ever-widening number of databases and eBooks that support this emphasis. The physical and electronic collections continue to expand through faculty recommendations and requests, as well as from librarian selection based upon their knowledge of the curriculum and its needs.

The journal collection is also based on faculty requests and is fine-tuned by means of an annual analysis of journal use. This analysis helps the library focus its expenditures (and finite budget) on those journals that are regularly needed and used by the institution's students. The collections have been enriched with digital information. The library subscribes to numerous online databases including the Association for Computing Machinery (ACM) Digital Library, ProQuest Research Library, ABI Inform, IEEE, Lexis-Nexis and over 100 others. Most of the material indexed in these databases includes direct access to the full text of the articles indexed. For those articles not available in full text, the library provides speedy interlibrary loan service at no extra cost to all DSU students, faculty, and staff.

The library holds an extensive collection of electronic books on computer security and information assurance, which are discoverable via the library catalog. In addition, the library subscribes to O'Reilly for Higher Ed, which provides access to 150 titles that provide hands on training in many areas of technology. The library also provides access to LinkedIn Learning, which provides digital tutorials in almost every area of technology, marketing, education, and career planning.

The Karl E. Mundt Library is a member of several library consortiums and maintains borrowing and lending agreements with academic libraries across the country and around the world. As such, the library can attain materials in digital and/or physical formats for any scholarly need.

In addition to the collections, systems and services offered, Library staff also provide assistance and instruction to faculty and students through workshops, classroom instruction, online tutorials, and one-to-one assistance and training. Library faculty collaborates with course faculty to ensure students have the research background necessary to complete course assignments.

Library faculty develops tutorials, subject guides, and other instructional materials to support classroom learning on campus and online. It is also the library's goal to graduate students who are able to find, evaluate, and use information to solve problems and to make decisions effectively. Graduates should have the knowledge and skills to function successfully as continuous learners in a continuously changing information world. To successfully meet its goals, the library provides excellent collections, information systems, services, instruction, and staff.

6.3 Graduate Programs and Research Support Services

The Office of Graduate Studies was established to promote and support graduate education at DSU. The Dean of Graduate Studies collaborates with and supports the functions and responsibilities of the Graduate Council and the graduate program committees within each college and serves as the advocate for graduate education and graduate student support at DSU. The day-to-day operations of the Office of Graduate Studies are student centered. The office offers guidance and help to students from the first inquiry to graduation. This includes providing accurate and timely program information and maintaining the graduate programs website with current information for degree seeking students (https://dsu.edu/admissions/graduate/). The office also facilitates the recruitment of prospective students, the application process, assisting in setting up interactive audio video for remote sites in South Dakota and online for distance students. Other services provided by the Office of Graduate Studies include assisting with course scheduling and course rotations; making students aware of changes in

schedules, rotations, and graduate policies; assisting with registration; supporting the assistantship committees; monitoring student progress toward graduation; and serving as a liaison among other support staff, faculty, and administrators

6.4 Doctoral Student Support and Research Development

The Ph.D. in Cyber Defense benefits from established institutional support structures, including advising services, library access, and graduate program assistance. As a doctoral program, however, student support extends beyond administrative and financial processes to include research development, scholarly mentoring, and professional preparation.

6.4.1 Research Advising and Mentorship

Doctoral advising includes both academic progression monitoring and research mentorship. Students engage faculty early in the program to identify potential research directions and align with dissertation chairs. Because the program serves practitioner learners in an online format, structured advising checkpoints are essential to maintain research momentum.

The program continues to evaluate:

- Frequency and structure of advising interactions
- Early identification of dissertation topics
- Faculty-student research alignment
- Proposal development support mechanisms

Strengthening early-stage research mentoring remains a priority to reduce delays between coursework completion and candidacy.

6.4.2 Library and Research Infrastructure Support

The Karl Mundt Library and graduate research services provide access to digital databases, interlibrary loan services, citation support, and research consultations. For doctoral students, these services are particularly important in:

- Literature review development
- Research design refinement
- Data management planning
- Publication preparation

The program encourages doctoral students to engage library faculty early in the dissertation process to ensure methodological rigor and comprehensive literature coverage.

6.4.3 Financial and Professional Support

Institutional financial aid processes are established and compliant with national standards. While many doctoral students are working professionals, financial support structures remain important in facilitating:

- Conference travel
- Professional memberships
- Research dissemination
- Residency participation

As the number of doctoral students increases, the program will continue to evaluate the availability of travel funds, research stipends, and grant opportunities that directly support doctoral scholarship.

6.4.4 Residency Experience as Scholarly Support

The required in-person residencies function not only as academic milestones but also as structured research immersion experiences. Residencies provide:

- Direct faculty interaction
- Peer feedback on research ideas
- Exposure to dissertation proposals and defenses
- Opportunities for collaborative dialogue

The program continues to assess whether additional structured research workshops or writing intensives during residency periods would further strengthen dissertation completion rates.

6.4.5 Continuous Improvement in Student Support

Doctoral student support is evaluated through:

- Retention data
- Comprehensive examination outcomes
- Dissertation progression timelines
- Alumni feedback

As the program matures, support structures will continue evolving to ensure alignment between enrollment growth and doctoral success. Program leadership conducts annual reviews of enrollment trends, faculty supervision capacity, student progression milestones, and research outcomes to ensure the Ph.D. in Cyber Defense program maintains alignment with national doctoral education standards and institutional resources.

Part 7: Facilities and Equipment

The program leverages DSU's advanced research infrastructure, including the PowerCyber℠ Lab, Madison Cyber Labs (MadLabs®), and the MADREN research network. These facilities provide secure, virtualized environments for experimentation and data analysis in cyber defense, artificial intelligence, and digital forensics.

Because the Ph.D. in Cyber Defense program is delivered primarily online, laboratory resources are made accessible through secure remote access, virtualization, and structured residency engagement.

7.1 PowerCyber℠ Lab

Technology education is inherently hands-on by nature; it is a major component of constructivist learning. Much like a biology or chemistry lab, a great deal of setup goes into creating a hands-on lab for technology labs. Multiple computers are required, plus networking gear to connect them together, plus any additional accessories such as a firewall, router, cellular telephones, etc. Once all of these are properly configured, the hardware setup must be duplicated several times for utility by multiple students. This process is effective but is very time consuming and outright prevents online students from participating on hands-on labs.

Several needs exist for an effective lab implementation that has a focus on technology education. The lab must give students the ability to practice what they learn; this is what sets students apart when they enter the workforce. Several challenges exist that must be overcome:

Challenge 1, Extensibility: The need within the technology program is a system that can provide the same user experience to students, online or on campus. The default tends to be that online students are second-class students, unable to participate in physical labs.

Challenge 2, Efficiency: The creation of labs can be considerably time-consuming for a single online class, upwards of 8-10 hours per lab. Couple this time requirement with having to replicate the lab many times over for both on-campus and online populations, it simply isn't possible for a single faculty member to manage their own labs with courses of 40-90 students.

Challenge 3, Versatility: Any lab environment for use in the technology area needs to support all areas of technology. Being restricted to a single platform (such as Microsoft Windows) creates restrictions that are impossible to overcome. The lab solution needs to support any/all technology platforms.

Challenge 4, Safety: Teaching cybersecurity fundamentals can have grave consequences for beginners. A simple typo can make the difference between a basic lab exercise and launching a real-world cyber attack against another organization. Any lab environment used must protect the learners from themselves.

DSU's PCL is our custom designed solution to the problems of technological education. Our lab was designed and implemented in 2009, and its use has continually grown ever since with the additions of new classes plus growing enrollment.

The lab allows an instructor to focus their time on creating and testing their lab. Once their lab is created, it can be cloned for testing in a matter of minutes. Once the lab is finalized, the lab administrator can copy unique instances of the lab to all students within the class. This process takes approximately 20 minutes total, depending on the size of the class.

The lab has the ability to run any x86 platform (namely Windows, MacOS, FreeBSD, or Linux), ARM (Linux and embedded operating systems), in addition to popular firewall and router platforms as well as cellular base stations. These labs are all safely contained so that students are safe when practicing any cybersecurity concepts.

Due to the self-service nature of our lab implementation, it can be used for projects far beyond the classroom. The lab hosts research projects for undergraduate and graduate students, in addition to housing research projects for faculty members. Due to the safe/secure nature of the lab, it also houses DSU's GPU environment.

The labs users vary from semester to semester but largely include students from all technology programs at DSU.

To facilitate the large lab environment, enterprise grade hardware is required. This is the type of hardware that would be found in any large-scale corporate IT environment and includes:

- Virtualization software/scripts that are both custom created for our unique needs coupled with software from VMWare
- Wireless/Cellular/Mobile modules to create live cellular base stations leveraging software defined radios
- Enterprise servers
    - Approximately 150 hosts
    - Large memory capacity per server, in excess of 128 GB
    - High network throughput, in excess of 4X gigabit interfaces
    - Storage Area Network connectivity, dual 10GB iSCSI
- Large-scale networking equipment (from Juniper Networks)
- Large storage capacity for storing student/staff labs and research from HP/3PAR
- Overall, the raw capacity of the lab is approximately:
    - 15TB RAM
    - 1100 CPU Cores

- 700TB of storage

7.2 Madison Cyber Labs

On Jan. 31, 2018, Governor Dennis Daugaard signed House Bill 1057 into legislation which permitted the demolition of DSU's Lowry Hall and construction of the Madison Cyber Labs, or MadLabs®. The Madison Cyber Labs build on DSU's expanding capabilities and strengths to establish a hub of cybersecurity and cyber operations expertise, research, and economic development in South Dakota. As of December 2023, DSU faculty has established sixteen MadLabs. Construction of the $18 million, 40,000 square foot MadLabs® building, located on the southwestern edge of campus, was completed in Fall 2019. It is the first research facility of its kind in the Upper Great Plains region.

There are five components to MadLabs® game-changing plan to reshape the cyber field in South Dakota, including:

- **Resources**: a winning combination of laboratory research space, state-of-the-art hardware and software, faculty expertise, and growing institutional relationships with a wide variety of public and private agencies
- **People**: undergraduate and graduate students, faculty, researchers, interns, and other collaborators
- **Programs**: nationally recognized cyber degrees from the associate to doctoral level, along with other professional development opportunities
- **Research areas and institutes**: focus areas in defined interdisciplinary and multidisciplinary regions, that draw from every college on campus
- **REED Connection**: DSU is connected to the South Dakota Research, Education, and Economic Development Network (REED) via a 100 Gbps connection. Providing the campus with connectivity to Internet2, the Great Plains Network, and other research networks.

MadLabs® drives innovation and ideas from DSU into the South Dakota economy, the Great Plains, and the nation. At the same time, it draws new talent to the state and the region. The facility and its programs attract elite scholars, researchers, professionals, and partnerships with government, businesses, nonprofits, and other higher education institutions. 25 Researchers within MadLabs® primarily focus on projects exploring and advancing technology application, information and quality assurance, business adverse event planning, economic growth, and policy improvement across multiple disciplines and fields. MadLabs® focus areas include cybersecurity, digital forensics, cyber defense, Artificial Intelligence (AI) and machine learning, reverse engineering, and malicious digital artifacts. MadLabs® also fosters partnerships with the public and private sectors to cultivate ideas and transform their research to make a difference in the world.

MadLabs® currently includes 16 labs:

- AdapT Lab
- AI Lab
- CAHIT

- CBAR Lab
- CLASSICS Institute
- Cyber Education and Professional Development Lab
- CybHER® Security Institute
- Deep Red Lab
- DigForCE Lab
- IT Living Lab
- MADRID Lab
- PATRIOT Lab
- Pri Lab
- Smart Home Lab
- Success Lab
- VERONA Lab

7.3 MADREN

The computing resources are available through the MadLabs® Research Environment and Network (MADREN) at DSU. MADREN is an extensive technology infrastructure dedicated to cybersecurity research. The MADREN includes 10 Lenovo SR630s servers, each with dual Intel Xeon Gold 5118 Processors, for a total of 240 cores @ 2.3 GHz. This is supported by 2.56TB of TruDDR4 @ 2666MHz RAM available and a 126TB HPE Nimble Storage Adaptive Flash Array. These resources are accessible through virtualization via VMware Director. The MADREN also contains a large GPU cluster accessible through VMware View. It includes 5 Lenovo SR670s servers, each with dual Intel Xeon Gold 6242 Processors, for a total of 160 Cores @ 2.8 GHz each, and 1.92TB of TruDDR4 Performance+ RAM @ 2933MHz. The cluster has 40 NVIDIA Tesla T4 16GB cards, with 12,800 Turing Tensor Cores and 102,400 CUDA Cores. The total GPU capacity represents 324 Teraflops, 2.6 Petaflops, 5,200 TOPS (INT8), or 10,400 TOPS (INT4). All MADREN resources have access to Internet2, with a max data transfer of 100 Gbps.

7.4 Infrastructure Utilization and Sustainability

The Ph.D. in Cyber Defense program benefits from significant research infrastructure, including the Power Cyber Lab, MadLabs® research facilities, and advanced high-performance computing and GPU resources. These assets provide a strong foundation for applied and interdisciplinary cybersecurity research.

As the doctoral program grows, infrastructure evaluation focuses on utilization, accessibility, and long-term sustainability.

7.4.1 Doctoral Research Utilization

Doctoral students utilize laboratory and computing resources for:

- Network security experimentation
- Intrusion detection modeling

- AI-enabled cybersecurity research
- Privacy-preserving data analysis
- Large-scale simulation and performance testing

Faculty actively align dissertation topics with available infrastructure to ensure that research questions are both rigorous and technically feasible.

The program continues to assess whether:

- GPU and HPC capacity remain sufficient for growing enrollment.
- Remote access tools adequately support online doctoral learners.
- Lab scheduling and support services scale with dissertation demand.

7.4.2 Alignment with Emerging Research Domains

Cyber defense research increasingly intersects with artificial intelligence, critical infrastructure protection, cloud security, and privacy engineering. Infrastructure investments must anticipate evolving research needs.

Strategic priorities include:

- Monitoring hardware upgrade cycles.
- Expanding support for AI and data-intensive research.
- Strengthening integration between MadLabs® initiatives and doctoral dissertations.
- Ensuring infrastructure remains competitive relative to peer institutions.

7.4.3 Sustainability and Funding

Advanced computing infrastructure requires sustained financial investment. The program works in coordination with college and institutional leadership to:

- Plan for hardware refresh cycles.
- Maintain external research partnerships that support infrastructure development.
- Align grant activity with lab expansion and maintenance.
- Ensure continued access to high-bandwidth research networks.

Long-term infrastructure sustainability is essential to preserving doctoral research quality.

7.4.4 Facilities as a Strategic Asset

MadLabs® was designed as a hub for cybersecurity research, innovation, and economic development. For doctoral students, these facilities provide more than physical space; they represent opportunities for:

- Faculty collaboration
- Interdisciplinary engagement
- Industry and government partnership development
- Research dissemination and visibility

As the program matures, increased integration between doctoral research projects and MadLabs® initiatives will remain a priority.

Part 8: Program Learning Outcomes and Assessments

Upon completion of the Ph.D. in Cyber Defense, graduates will be able to:

- Author research within the cyber defense realm to aid the industry in better protecting itself.
- Create new mechanisms for the active defense of an organization.
- Select appropriate strategies for proactively protecting an organization's electronic infrastructure.

Program learning outcomes are assessed through comprehensive examinations, dissertation defenses, peer-reviewed research dissemination, conference participation, and alumni career outcomes. Faculty committees review dissertations for rigor, originality, and contribution to the field. The program engages in continuous improvement through faculty evaluation, feedback, and graduate outcomes analysis.

8.1 Assessment Results and Continuous Improvement

The Ph.D. in Cyber Defense defines learning outcomes centered on original research contribution, development of advanced defensive mechanisms, and strategic cybersecurity leadership. Assessment mechanisms include dissertation evaluation, research dissemination, conference participation, and alumni feedback.

As the program matures, emphasis has shifted from defining assessment processes to evaluating outcomes and using findings to guide improvement.

8.1.1 Dissertation Quality and Research Contribution

Dissertation defenses serve as the primary summative assessment of doctoral achievement. Faculty committees evaluate:

- Originality of contribution
- Methodological rigor
- Technical depth
- Relevance to contemporary cyber defense challenges

As enrollment grows, faculty continue to examine whether dissertation topics reflect emerging national cybersecurity priorities and whether students are sufficiently prepared for publication-level scholarship.

A strategic priority moving forward is increasing the rate at which dissertation research results in peer-reviewed publication or formal dissemination in professional venues.

8.1.2 Comprehensive Examination Outcomes

The oral comprehensive examination functions as a readiness benchmark for independent research. Faculty review pass rates, retest frequency, and qualitative performance patterns to identify:

- Areas of curricular strength

- Gaps in disciplinary synthesis
- Opportunities for earlier formative feedback

Where patterns indicate recurring weaknesses, course sequencing and instructional emphasis are adjusted accordingly.

8.1.3 Retention and Completion Monitoring

Retention data are reviewed annually to evaluate persistence across coursework and dissertation phases. As a relatively young doctoral program, longitudinal completion data are still developing; however, the program has prioritized:

- Monitoring time-to-candidacy
- Monitoring time-to-defense
- Identifying barriers to dissertation progression
- Strengthening structured advising checkpoints

These metrics inform adjustments to research mentoring, residency structure, and advising practices.

8.1.4 Alumni and Placement Feedback

Graduate outcomes provide critical insight into program effectiveness. As the number of graduates increases, the program is formalizing alumni tracking to assess:

- Placement sector distribution
- Leadership roles attained
- Continued research productivity
- Contribution to national cybersecurity initiatives

Feedback from graduates and employers will increasingly inform curriculum refinement and partnership development.

8.1.5 Continuous Improvement Process

Assessment findings are discussed in faculty meetings and incorporated into program planning. Improvements implemented or under active consideration include:

- Strengthening early research engagement within coursework
- Expanding opportunities for doctoral student publication
- Enhancing dissertation proposal development support
- Aligning enrollment targets with faculty supervision capacity

The Ph.D. in Cyber Defense recognizes that doctoral education requires ongoing evaluation and adaptation. Continuous improvement remains central to maintaining rigor, sustainability, and national relevance. Assessment results are reviewed annually by program faculty to guide curriculum refinement, research mentoring practices, and enrollment planning.