SOUTH DAKOTA BOARD OF REGENTS
ACADEMIC AFFAIRS FORMS

New Graduate Degree Program

Use this form to propose a new graduate degree program. The Board of Regents, Executive Director, and/or their designees may request additional information about the proposal. After the university President approves the proposal, submit a signed copy to the Executive Director through the system Chief Academic Officer. Only post the New Graduate Degree Program Form to the university website for review by other universities after approval by the Executive Director and Chief Academic Officer. The university should consult the "Campus Guide to the New Graduate Program Approval Process" for information on specific aspects of the approval process.

UNIVERSITY:	DSU
PROPOSED GRADUATE PROGRAM:	**Cyber Defense**
EXISTING OR NEW MAJOR(S):	**New**
DEGREE:	**Ph.D.**
EXISTING OR NEW DEGREE(S):	**Existing**
INTENDED DATE OF IMPLEMENTATION:	**Fall 2019**
PROPOSED CIP CODE:	**11.1003**
SPECIALIZATIONS:[1]	
IS A SPECIALIZATION REQUIRED (Y/N):	**No**
DATE OF INTENT TO PLAN APPROVAL:	**5/9/2018**
UNIVERSITY DEPARTMENT:	
UNIVERSITY DIVISION:	**Beacom College of Computing and Cyber Science**

University Approval

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

J. M. Gustafson — **3/15/2019**

President of the University — Date

Delete this box before submission

Doctor of Philosophy (Ph.D.) and the Doctor of Science (D.Sc.) programs prepare a student to become a scholar; that is, to discover, integrate, and apply knowledge, as well as communicate and disseminate it. A well-prepared doctoral graduate develops the ability to understand and critically evaluate the literature of the field and to apply appropriate principles and procedures to the recognition, evaluation, interpretation, and understanding of issues and problems at the frontiers of knowledge. The doctoral graduate will also have an appropriate awareness of and commitment to the ethical practices appropriate to the field.

[1] If the proposed new program includes specific specializations within it, complete and submit a New Specialization Form for each proposed specialization and attach it to this form. Since specializations appear on transcripts, they require Board of Regents approval.

A central purpose of scholarship is the extension of knowledge, and students in a doctoral program become scholars by choosing an area of specialization and a professor with whom to work. Individualized programs of study may then be developed and committee members selected cooperatively as course work is completed and research undertaken. When all courses are completed, the research finished, the dissertation written, and all examinations passed, the doctoral graduate should have acquired the knowledge and skills expected of a scholar who has made an original contribution to the field and has attained the necessary expertise to continue to do so.

The professional doctoral degree requires two or more years of professional study past the baccalaureate degree. This degree prepares an individual for entry into the practice of a recognized profession. Examples of professional doctorates are the M.D., Pharm. D., J.D., DVM, Ed.D., Au.D., and DPT degrees.

1. What is the nature/purpose of the proposed program?

Dakota State University requests permission to offer a Ph.D. program in Cyber Defense. The program will be offered on the Madison campus and online. It is responding to a nationwide need for professionals in cyber defense. Development of this new degree program is a university priority and strategic focus. A Ph.D. in Cyber Defense program is necessary to deal with our nation's growing cyber defense threats and workforce needs. The program addresses important technical aspects of cyber defense, yet infuses cyber defense leadership, ethics and management concepts to ensure well rounded graduates. The program can be completed on a full-time or part-time basis, with classes offered in three academic terms: fall, spring, and summer.

In the spring of 2016 Dakota State University was given permission by the SDBOR to offer a doctoral degree in Cyber Operations. In the fall of 2016 DSU admitted its first full cohort of program students. Three years of entry classes are summarized in Table 1.

Table 1. Three-year Growth in DSU's Ph.D. in Cyber Security

	Fall 2016	Fall 2017	Fall 2018
# Applicants	47	66	102
# Admissions	19	18	20
% Admitted	40.4%	27.2%	19.6%

The trajectory of interest in our doctoral program in Cyber Operations shows that over the short duration of the program applications have doubled, while the percentage of admissions are halved. The "yield" rate (proportion of students admitted to those enrolled) remains an enviable 90+%. These metrics speak to the quality of the program and consumer interest in the field. Other information of a more anecdotal note, reveals two interesting trends:

1. Less than half of the applicants have the technical skills needed to thrive in the Cyber Operations program. Without at least an MS degree in computer science, students will struggle with course concepts such as software exploitation, encryption, and reverse engineering.

2. Very few applications received by the university are from women. And even less are admitted to the program.

As we have studied our application and enrollment data, we see opportunities to create a path to a cyber-centric doctoral degree by distinguishing between the related domains of "Cyber

Operations" and "Cyber Defense." Our degree in cyber operations will remain technically oriented, while the proposed degree in cyber defense will allow students with related undergraduate and master's degrees (i.e., network and system administration, software engineering, and artificial intelligence) —not coincidentally, areas with larger proportions of women—to complete a doctoral degree in the Cyber Security field.

Specifically, the Cyber Defense doctoral program will provide graduates with a foundation in the security issues, practices, politics, risk analysis, and cultures of terrorism, as well as a foundation in research methodology and practice. The program provides in-depth cyber defense education for high-end cyber defense professionals capable of working in industry, government, the military, and academia.

Students will learn how to:

- Work in a variety of research methodologies to support innovation in technical careers
- Research and develop tools to advance the fields of: network defense, cyber and privacy risk management, software assurance, Internet of Things security (IoT), 5G network security, digital forensics, penetration testing, incident response, vulnerability scanning, network security monitoring and response, data privacy, multinational cybersecurity defense, IT governance and compliance, and privacy enhancing technologies.
- Research how cyber/physical systems converge
- Blend security and privacy to achieve maximum defense and flexibility
- Research and apply ethical frameworks to security decisions to integrate cyber ethics into their leadership and decision-making
- Research and develop models to measure cybersecurity and data privacy effectiveness in both public and private sector organizations

2. How does the proposed program relate to the university's mission and strategic plan, and to the current Board of Regents Strategic Plan 2014-2020?[2]

The statutory mission statement for Dakota State University is provided in SDCL 13-59-2.2: *The primary purpose of Dakota State University in Madison in Lake County is to provide instruction in computer management, computer information systems, electronic data processing and other related undergraduate and graduate programs . . .*

A STEM University

In pursuing this state mandated mission in computing and informational sciences, enrollment at DSU shows 1555 STEM students, or approximately 66.7% of student population[3]. Enrollment at DSU in STEM fields show just how committed the institution is to its mission and encourages us to maintain a steady focus on these fields in our mission-driven decision making. Our mission specificity and U.S. workforce data suggests large increases in workforce demand for cyber security professionals. We have responded through our DSU Rising Initiatives, which include but are not limited to:

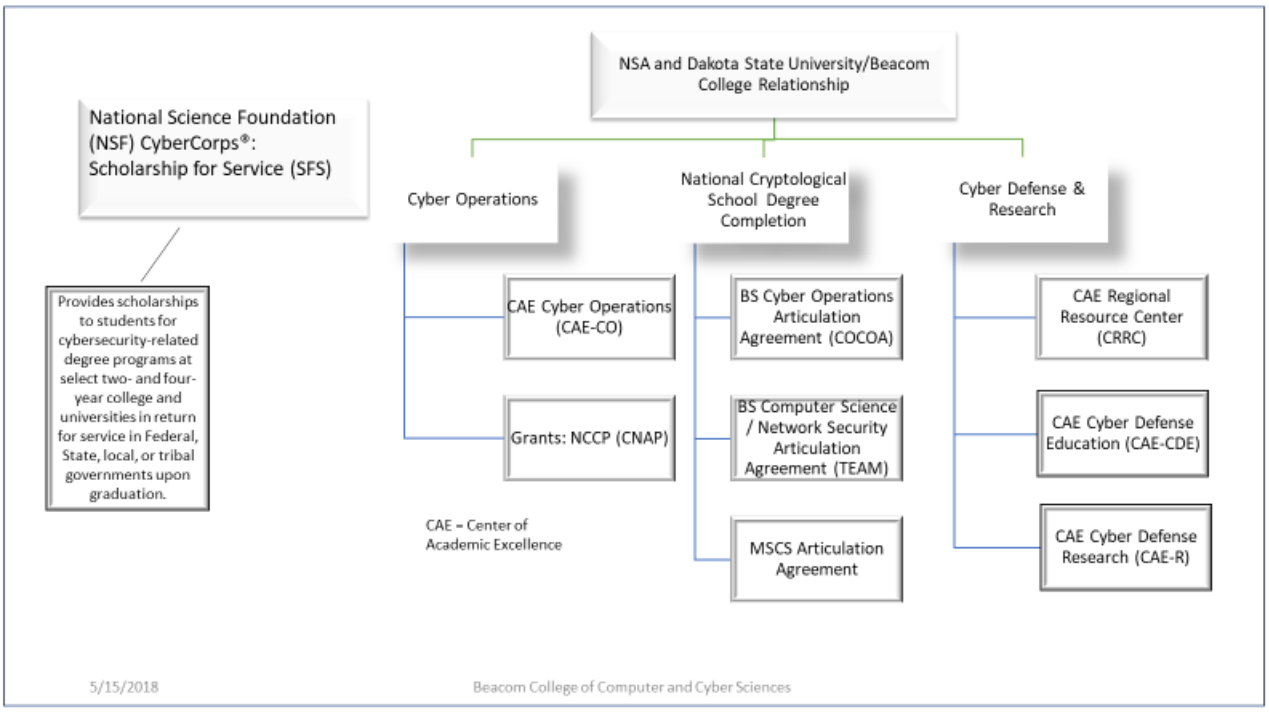
[2] South Dakota statutes regarding university mission are located in SDCL 13-57 through 13-60; Board of Regents policies regarding university mission are located in Board Policies 1:10:1 through 1:10:6. The Strategic Plan 2014-2020 is available from https://www.sdbor.edu/the-board/agendaitems/Documents/2014/October/16_BOR1014.pdf.

[3] US Department of Homeland Security, Fact Book SD Board of Regents, and the Consortium for Student Retention Data Exchange (2018).

1) The Aug. 20, 2017 opening of the Beacom Institute (the first LEED version 4 building in South Dakota) dedicated to computing and cyber sciences instruction including a Computer game design suite, Animation lab, Network and security administration lab all in its 31,000 Sq. ft. imprint.

2) The Fall 2019, opening of the Madison Cyber Labs, a research and development facility with hub of cybersecurity and cyber operations expertise, education, applied research and economic development.

3) Collaborations with prominent STEM-related federal agencies to promote cyber science education, research and workforce development. That collaboration is mapped below.



BOR Policy 1:10:5 authorizes Dakota State to offer graduate programs "that are technology-infused" and that provide service to state and the region. To date, the Board has approved seven master's programs and two doctoral programs for the University:

Doctoral Degrees

- Ph.D. in Information Systems (approved in 2005)
- Ph.D. in Cyber Security (approved in 2014)

Masters Degrees

- M.S. in Information Systems (approved in 1999)
- M.S.Ed. in Computer Education & Technology (approved in 1999)
- M.S. in Information Assurance (approved in 2003)
- M.S. in Health Informatics and Information Management (approved in 2009)
- Master of Business Administration (approved in 2010)
- M.S. in Computer Science (approved in 2012)

- M.S. in Analytics (approved in 2014)

This program clearly falls within the scope of DSU's expertise and more systemically defines the domain of service we are institutionally mandated to serve and is another step in fulfilling DSU's institutional mission.

The SDBOR Strategic Plan 2015-2020 includes the following vision statements:

- South Dakotans will have increased access to continuing education opportunities needed to upgrade their credentials while remaining in the workforce. Because the program will be offered online, this gives those who are full-time employed, the opportunity to complete the degree;

- South Dakota will have a working-age population with advanced levels of education needed to support our democracy and the modern, knowledge-based economy; and

- South Dakota will be a recognized national leader in the use of information technology to enhance its educational, economic, social, scientific, and political development.

The DSU Strategic Plan also mentions the need to attract out-of-state students as high school enrollments in South Dakota are flat. This innovative program fits nicely with other DSU nationally recognized programs. The fact is that cyber defense is emerging as a profession and academic area of study. Dakota State is already an NSA and DHS National Center of Academic Excellence in Education, Research and Cyber Operations and this academic program fits nicely with an existing partner: DHS.

Adding a Ph.D. in Cyber Defense will provide an opportunity for either business or technology professionals to augment their skill set in cyber defense. It also deals with a real threat in our modern, knowledge-based economy and serves as another program which integrates technology across multiple disciplines. Cybersecurity Officers and Chief Cybersecurity Officers are being hired to take the lead on cyber defense in corporations and government agencies. This program provides the education to understand the threats and form a cybersecurity strategy to best protect the organization.

3. **Describe the workforce demand for graduates of the program, including national demand and demand within South Dakota.** *Provide data and examples; data sources may include but are not limited to the South Dakota Department of Labor, the US Bureau of Labor Statistics, Regental system dashboards, etc.*

Frankly, the vast majority of our applicants will be employed when they are accepted and enroll in the program. For them, enrollment in our program means filling a skill set that exists in their current organization, or providing job enhancement or transition potential aligned with their personal goals.

Cybersecurity roles rank among the most difficult to fill in the enterprise, with the talent gap in this field expected to reach 1.8 million jobs by 2022. Some studies are even more concerning such as one complete by ISACA, a non-profit information security advocacy group, which predicts there will be a global shortage of two million cyber security professionals by 2019. Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers

are struggling to fill 200,000 other cyber-security related roles, according to cyber security data tool CyberSeek. And for every ten cyber security job ads that appear on careers site Indeed, only seven people even click on one of the ads, let alone apply. Regarding the workforce, Table 1 outlines a brief list of jobs students would be eligible for:

Table 1 – Cyber Defense Jobs

• Penetration Tester - Technical cyber defense professional who identifies and communicates software and network vulnerabilities that are externally facing to the public. Findings are typically passed off to cyber security engineers to remediate. **This is the projected number one labor shortage in the cyber field.**
• Cyber Security Engineer - Cybersecurity engineers often come from a technical background within development, usually with knowledge of Python and Java. They can get behind the code and take a deep dive in to see what performance issues might occur from vulnerabilities, and what tweaks they can make. **This is the projected number two labor shortage in the cyber field.**
• Chief Information Security Officer (CISO) or Information Security Officer (ISO). Ultimately responsible for a company's cybersecurity strategies. They also make sure employees are up to date on security best practices. They typically hire and manage the network and software security professionals. **This is the projected number three labor shortage in the cyber field.**
• Security Analysts – This is the 16th fastest growing job between 2016 – 2016 (28%). It is also the 3rd highest paying job on this fastest growing list of jobs ($95,500 per year).
• Security Managers/Directors – Mid management who typically hire cyber defense professionals and implement/operationalize the cybersecurity strategy.
• Professor – Teach or research of one or more cyber defense disciplines.
• Cryptographer and Cryptanalyst – devise and implement encryption techniques to safely store or transmit sensitive information.
• Cyber Defense Researcher – Subject matter expert in one or more cyber defense disciplines who evolves or applies the science of cyber defense.
• Vulnerability Scanner – Technical cyber defense professional who identifies and communicates all levels of software and network vulnerabilities to cyber security engineers to remediate
• Cyber Security Consultants – Technical and managerial advisors who devise and/or implement cyber defense strategies.
• Cyber Defense Practitioners - Technical and managerial professionals who devise and/or implement cyber defense strategies.
• Information Technology Auditor - Technical and managerial professionals who test cyber defense strategies.

On the federal level government agencies, military, and intelligence departments are responsible for our country's various cyber defense operations. Various programs are utilized in these operations, like the National Incident Management System. This system is used as the standard operational procedure of all sectors of cyber defense and how they respond to terrorist attacks. The Cyber Defense Exercise and Evaluation Programs are also utilized, but they are typically used as federal template for training exercises. The main goal of the federal-level of the cyber defense department is to make sure that the government, at all levels, functions in an effective and coordinated manner. Cyber Defense graduates would be able to enter the federal workforce

and hit the ground running to assist in national cyber defense. Employees work throughout the country for the Department of Cyber Defense and the agencies under its umbrella, including:

- National Security Agency
- Department of Homeland Security
- Federal Emergency Management Agency
- U.S. Customs and Border Protection
- U.S. Citizenship and Immigration Services
- U.S. Immigration and Customs Enforcement
- Transportation Security Administration

All of these job fields are projecting growth over the next 10 years. For example, Cybersecurity Analysts who analyze threat data and write report/communicate results have a median pay of $90,120 per year and will grow 18% over the next 10 years (much faster than average). The federal workforce also benefits to gain from this program. For example, DHS employs approximately 240,000 people in areas ranging from human resources to border patrol to the Secret Service. Graduates from this program will help fill these critical workforce shortages. As a few examples, at least one organization predicts a global shortage of Security Analysts and Security Managers.[4] A second study indicates cyber security professionals are among the hardest tech jobs to fill in organizations with security professionals among the five most in-demand positions.[5] Specific occupations with expected growth related to this degree include Information Security Analysts who analyze threat data and communicate results; such positions have a median pay of $92,600 per year and expected growth of 28% over the next 10 years (much faster than average).[6] In South Dakota, there are currently 201 such positions and growing with an average wage of $79,000 - $88,000.[7] Table 1 identifies 12 critical cyber defense jobs, all with current and forecasted job shortages.

In addition, data privacy jobs (leaders, researchers, technicians, compliance professionals, engineers, lawyers, etc.) are beginning to boom as the issue becomes serious in corporations and governments. Chief Privacy Officers and Data Privacy Officers are senior executives in industry or government with both managerial and technical understanding of privacy to lead teams, agencies and organizations to the right privacy posture. According to payscale.com, average base salary is $147,362, with total compensation packages (with bonus, etc.) well over $200,000. Privacy Analysts identify and prevent current and future threats to user security and privacy. Process incoming samples and create detection policies for identifying them in the future. According to payscale.com, average base salary is $98,120. Privacy Engineers are the software developers researching and developing privacy enhancing technologies. Google, Square, Share,

[4] Jeff Kauflin, "The Fast-Growing Job With A Huge Skills Gap: Cyber Security," Forbes.com (March 16, 2017), available from https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#5ac09cf75163 (viewed March 30, 2018).

[5] Alison DeNisco Rayome, "These 5 Tech Jobs are the Hardest to Fill at Any Organization," techrepublic.com (July 12, 2017), available from https://www.techrepublic.com/article/these-5-tech-jobs-are-the-hardest-to-fill-at-any-organization/ (viewed March 30, 2018).

[6] Bureau of Labor Statistics, US Department of Labor, *Occupational Handbook*, Information Security Analysts https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm; (viewed January 30, 2018)

[7] Projections Central – State Occupational Projections, Short Term Occupational Projections, South Dakota, Information Security Analysts, at http://www.projectionscentral.com/Projections/ShortTerm (viewed January 30, 2018)

Facebook, Uber, AWS and many others currently have job openings posted on Indeed.com. The demand for privacy consultants, privacy auditors, incident handlers and privacy testers is emerging to develop privacy strategies, build governance strategies and ensure compliance. Five sample jobs listed on IAPP.ORG (The International Association of Privacy Professionals) that illustrates this growing need:

- Director, Information Governance Professional, Visa, Inc., Foster City, CA - A member of Visa's Global Privacy Office, you will assist in developing a long-term information governance strategy and be responsible for specific strategic and tactical technical and non-technical initiatives.

- Principal Customer Privacy Specialist, Pacific Gas & Electric, San Francisco, CA
  Provide technical subject-matter guidance and support to the enterprise to ensure the understanding of risks, threats, appropriate controls, effective business processes, and important strategies related to customer and employee privacy and data.

- Chief Privacy Officer, Meredith Corporation, Des Moines, Iowa
  Responsible for leading the privacy compliance, education, and protection strategy across all businesses and geographies for one of the nation's leading media companies whose content reaches nearly 200 million American consumers monthly.

- Senior Manager EMEA CoE Data Protection and Privacy Program, Medtronic, Heerlen, Limburg, Netherlands, UK, Brussels, Tolochenaz, île de France
  The Senior Manager, Data Protection and Privacy Program supports the Medtronic EMEA region (Europe, Middle East and Africa) Data Protection and Privacy Program Center of Excellence ("Global Program") and manages EU located team members

- Privacy Analyst 2, Nordstrom, Seattle, WA
  Demonstrated experience successfully working on privacy related projects, has experience investigating privacy/security incidents, deep technical skills, and is also able to bring excellent customer services skills to the job every day.

Federal - On the federal level government agencies, military, and intelligence departments are responsible for our country's various cyber defense operations. Various programs are utilized in these operations, like the National Incident Management System. This system is used as the standard operational procedure of all sectors of cyber defense and how they respond to terrorist attacks. The Cyber Defense Exercise and Evaluation Programs are also utilized, but they are typically used as federal template for training exercises. The main goal of the federal-level of the cyber defense department is to make sure that the government, at all levels, functions in an effective and coordinated manner. DS.CD graduate would be well-educated to enter the federal workforce and hit the ground running to help in national cyber defense. Employees work throughout the country for the Department of Cyber Defense and the agencies under its umbrella, including:

- National Security Agency
- Department of Homeland Security
- Federal Emergency Management Agency

- U.S. Customs and Border Protection
- U.S. Citizenship and Immigration Services
- U.S. Immigration and Customs Enforcement
- Transportation Security Administration

Working for these agencies often requires a security clearance, which can typically only be obtained by U.S. citizens who meet specific guidelines. Median annual wages for cyber defense professionals range from $37,000 for transportation security screeners to roughly $80,000 for some of the highly-technical, high demand cyber defense fields.

At the state level, DHS and other government agencies are looking to fill their workforce needs with high-end cyber talent. DSU has already placed two MSIA students do conduct reverse engineering and malware analysis in state government, and these DS.CD graduates would be even better prepared to secure the state's cyber infrastructure. At the state level, universities are looking to augment their traditional technology faculty and these graduates would be perfect for entry-level professorial positions.

Local –While the federal and state needs are obvious, the local needs are just as critical. For example, the Urban Areas Security Initiative has given significant funding to these following cities and their cyber defense departments:

- New York City – $1.4 billion
- Los Angeles – $644 million
- Washington D.C. – $568 million
- Chicago – $478 million
- San Francisco – $359 million

Private Sector – As technology expands in organizations, so do security risks and organizations are responding by hiring analysts, specialists and officers to enact cyber defense practices to augment the technical staff and keep organizations safe. The private sector needs more cyber defense researchers and high-end practitioners to keep up with the hackers, nation states and cyber armies coming into this domain. Information security officers, penetration testers and vulnerability scanners and three such jobs which require a deep understand of cyber technology and management concepts to protect organizations against the host of attacks of today and the sophistication and variety of the attacks on the horizon.

4. How will the proposed program benefit students?

The program offers a growing number of students an opportunity for specialized training in securing computer networked assets and addressing user information privacy. As tables 2 and 3 show, the number of students graduating from DSU and other regental schools in computer science-related majors has grown exponentially. This trend appears to also be mirrored regionally and nationally. This program offers an opportunity for highly specialized skills sets in a field requiring more specialized training.

Table 2. DSU Undergraduate Enrollments in Computer Science-Related Technology Majors

Fall Enrollments	2012	2013	2014	2015	2016	2017	2018
B.S. Computer Science	168	182	217	291	348	339	350
B.S. Computer and Network Security (Cyber Operations)	173	209	245	255	313	403	464
B.S. Computer Game Design	103	116	110	112	98	102	99
B.S. Network and Security Admin	41	79	107	138	158	146	147
*Annual Fall Enrollment Totals	484	586	679	796	917	990	1,060

Source: DSU 20012-2018 Fall Enrollment Reports. B.S. in Computer Game Design was approved in 2008; B.S. in Network and System Administration was approved in 2009.
* A student may be counted more than once in a program due to specializations.

Table 3. SD Public University Graduates in Computer Science and Information Systems

Baccalaureate Degrees Conferred	BHSU	DSU	NSU	SDSMT	SDSU	USD	System
2012 Graduates	0	92	3	20	12	7	134
2013 Graduates	0	95	5	19	22	5	146
2014 Graduates	0	112	3	13	24	9	161
2015 Graduates	0	110	1	21	24	8	164
2016 Graduates	0	124	5	30	17	11	187
2017 Graduates	0	151	2	18	31	10	212
2018 Graduates	FY19 Factbook – Not available						
Total Graduates	0	684	19	121	130	50	1004

From the 2013-2018 SDBOR Fact Books

On average, about 16 percent of DSU's baccalaureate graduates enroll in graduate school. That number is slightly higher for DSU's baccalaureate graduates in the computer science-based degree programs, with an average of 22 percent of that group going on to graduate school. Majors included computer science, computer and network security, and computer information systems.

Opportunities for funded and disciplinary research. The proposed program is intended to attract and retain high-quality faculty members with active research agendas in cyber defense and security. Dakota State University has been successful in attracting external support for research and additional graduate students are needed to assist DSU faculty with grant-supported projects (see appendix). Students enrolled in this proposed program would have opportunities to participate in that research which would shape their own emerging research agenda.

5. Program Proposal Rationale:

A. If a new degree is proposed, what is the rationale[8]

A new degree is not being proposed. DSU currently offers a Ph.D. degree in Information Systems and Cyber Defense.

[8] "New Degree" means new to the university. Thus if a campus has degree granting authority for a Ph.D. program and the request is for a new Ph.D. program, a new degree is not proposed.

B. What is the rationale for the curriculum?

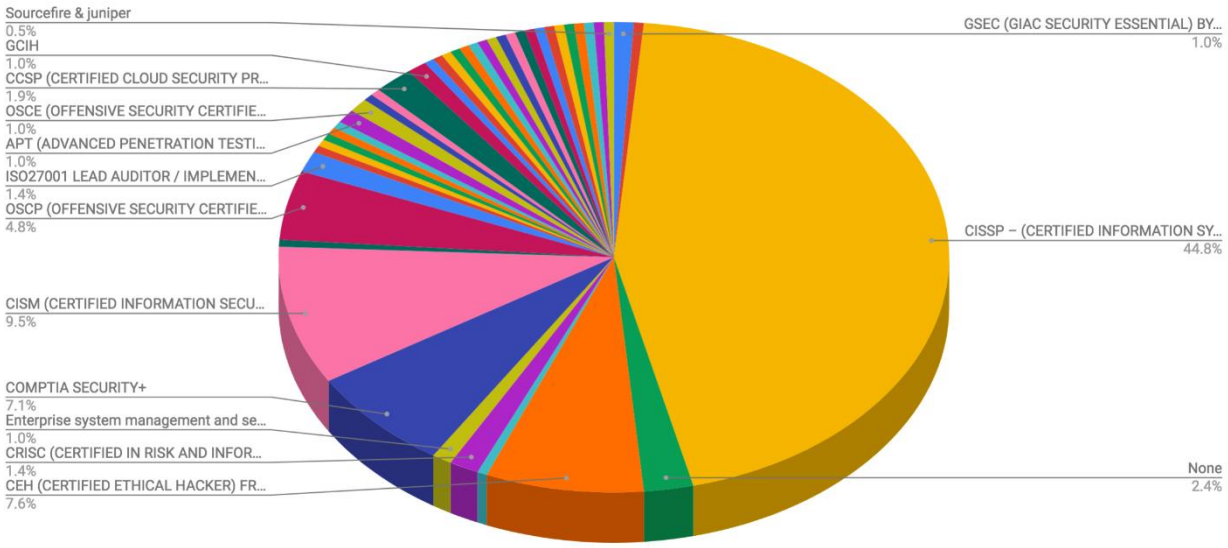
The curriculum is designed to address the need for high-end security experts with technical, managerial and leadership skills. The PhD curriculum is mapped to the top 3 security certifications according to Job Board Search Results.

Certification	Simply Hired	Indeed	LinkedIn	TechCareers	Total
CISSP	9,760	12,967	20,129	6,875	**49,731**
CISM	3,088	4,049	6,663	6,409	**20,209**
CEH	2,100	2,849	4,471	1,360	**10,780**

CISSP = Certified Information Security Systems Professional
CISSM = Certified Information Security Manager
CEH = Certified Ethical Hacker

C. Demonstrate/provide evidence that the curriculum is consistent with current national standards. *Complete the tables below and explain any unusual aspects of the proposed curriculum?*

A recent survey of cybersecurity professionals outlined the top security certifications in the field:



These certifications speak to industry and government needs for content consistent with the CISSP, CISM and CEH. DSU has mapped its proposed coursework to the content of each of these certifications.

Domain	Name	DSU Course(s)
1	Information Security Governance and Risk Management	INFA713 INFA745
2	Access Control	INFA701 INFA713
3	Cryptography	INFA723
4	Security Architecture and Design	INFA701 INFA710
5	Telecommunications and Network Security	INFS754 INFA754
6	Software Development Security	CSC748 INFA735
7	Business Continuity and Disaster Recover Planning	INFA701 INFA713
8	Legal, Regulations, Investigations, and Compliance	INFA710 INFA758
9	Physical Security	INFA732
10	Operations Security	INFA731 INFA732 INFA733

The CISM certification has 6 domains and is most focused on cyber security management concepts. Courses INFA701, INFA710, INFA713, INFA715, INFA731, INFA732, and INFA733 map directly to these six domains.

D. Summary of the degree program (complete the following tables):

[Insert title of proposed program]	**Credit Hours**	**Percent**
Required courses, all students	24	36%
Research Core	9	14%
Dissertation	11-21	32%
Electives	12	18%
Total Required for the Degree Total	56-66	100%

Required Courses

Prefix	**Number**	**Course Title** *(add or delete rows as needed)*	**Credit Hours**	**New (yes, no)**
INFA	702	Data Privacy	3	Yes
INFA	710	Cybersecurity Program Design and Implementation	3	Yes
INFA	713	Managing Security Risks	3	No
INFA	720	Incident Response	3	No
INFA	721	Computer Forensics	3	No
INFA	731	Personnel Security	1	Yes
INFA	732	Physical Security	1	Yes
INFA	733	Vendor Management	1	Yes

INFA	754	Intrusion Detection	3	No
INFA	758	Security Metrics	3	Yes
		Subtotal	24	

Required Research Core

Prefix	Number	Course Title *(add or delete rows as needed)*	Credit Hours	New (yes, no)
CSC	803	An Introduction to Cyber Security Research	3	No
CSC	804	Cyber Security Research Methodologies	3	No
CSC	807	Cyber Security Research	3	No

Dissertation

Prefix	Number	Course Title *(add or delete rows as needed)*	Credit Hours	New (yes, no)
CSC	809	Dissertation Preparation	3	No
CSC	890	Dissertation Seminar 1	3	No
CSC	898D	Dissertation	11-21	No

Students will be required to complete three on-site research seminars (CSC 890, 1 credit each, taken 3 separate times) in a face-to-face setting at the Madison, SD campus. These research seminars will be held annually and take place from 3-5 days. The research seminars are intended to acquaint students with contemporary cyber security research issues, allow students to report, present, and discuss articles pertinent to cyber defense research and provide students an opportunity to meet faculty, identify a dissertation advisor, present their dissertation proposal defense, as well as completing the final dissertation defense and oral comprehensive exam.

Elective Courses: List courses available as electives in the program. Indicate any proposed new courses added specifically for the program. (12 credits required)

Prefix	Number	Course Title *(add or delete rows as needed)*	Credit Hours	New (yes, no)
CSC	748	Software Exploitation	3	No
INFA	716	Privacy Technologies	3	Yes
INFA	717	Privacy Enhancing Technologies	3	Yes
INFA	718	Privacy Management	3	Yes
INFA	723	Cryptography	3	No
INFA	735	Offensive Security	3	No
INFA	742	Ethics and Information Technology	3	no
INFA	745	Compliance and Audit	3	no
INFA	751	Wireless Security	3	no
BADM	765	Management and Leadership	3	no
CSC	791	IS: Collab Cyber Sec Research	3	No
INFA	792	Topics	3	No
INFA	794	Internship	3	No

It is anticipated that applicants will be security technicians or in security management. The program accommodates these focus areas whereby technicians can take electives which are highly technical while security managers/information security officers can opt to security management and leadership courses.

6. Student Outcomes and Demonstration of Individual Achievement

A. What specific knowledge and competencies, including technology competencies, will all students demonstrate before graduation? *The knowledge and competencies should be specific to the program and not routinely expected of all university graduates.* **Complete Appendix A – Outcomes using the system form.** *Outcomes discussed below should be the same as those in Appendix A.*

Students will learn to:

- Work with a variety of research methodologies
- Research and develop tools to advance the fields of:
    - Network defense
    - Software assurance
    - Data privacy
    - The Internet of Things security (IoT)
    - 5G network security
    - Digital forensics
    - Penetration testing
    - Vulnerability scanning
    - Network security monitoring and response
    - Multinational cybersecurity defense
    - Cyber/physical systems converge
    - Cyber risk management
    - Cyber incident response plans
    - IT auditing universe
    - Privacy enhancing technologies
    - Measure cybersecurity effectiveness in both public and private sector organizations
- Apply ethical frameworks to security decisions
- Provide leadership in cyber defense

B. Are national instruments (i.e., examinations) available to measure individual student achievement in this field? If so, list them.

There are no national instruments to measure this innovative academic program. This said, the program is mapped to the CISSP, CISM and CEH security certifications and students would be able to sit for and pass these certification examinations. The university has begun early discussions with ISC2 (the organization who awards the CISSP) to become a testing center and bake the CISSP examination into the assessment process.

C. How will individual students demonstrate mastery? Describe the specific examinations and/or processes used, including any external measures.[9] What are the consequences for students who do not demonstrate mastery?

Program exit requirements of students include: qualifying portfolio and dissertation defense.

Qualifying Portfolio: The portfolio is intended to assess the student's potential for completing the doctoral program and pursuing a successful career in teaching, research or corporate management. The portfolio will be assessed prior to the end of the fourth semester of student enrollment. Artifacts that demonstrate the student's ability to contribute to the advancement of cyber security and practice through high-quality research and teaching will be evaluated by the student's research committee. Artifacts that might be included in the portfolio include:

- Research papers co-authored with a faculty member and submitted for publication in a peer-reviewed conference or journal;
- Teaching evaluations from cyber security undergraduate courses;
- Grant proposals co-authored with a faculty member and submitted for funding to an appropriate agency.

Original Research and Dissertation: Doctoral students are expected to conduct original research leading to completion of a dissertation which describes the results of that research. The dissertation is intended to assess the student's ability to conceive and perform independent research. An oral defense of the dissertation proposal will occur at the commencement of the dissertation work and an oral defense of the dissertation will occur upon completion of the original research and the written dissertation. The successful defense of the student's dissertation is the final test of the student's ability to perform independent research and communicate research results to others. The quality of the student's independent research will also be evaluated based on the student's publication and presentation record.

DSU graduate policies require that the program submit an annual assessment report on achievement of student learning outcomes. Once the program is approved, program faculty will meet to ensure a common set of policies, guidelines, and expectations are in place.

7. What instructional approaches and technologies will instructors use to teach courses in the program? *This refers to the instructional technologies and approaches used to teach courses and NOT the technology applications and approaches expected of students.*

In 1989, DSU's Dr. Eric Johnson Dean of the College of Arts and Humanities offered South Dakota's first ever internet delivered course. Dakota State University has experienced solid growth in online enrollments since then. Using the latest available data, 37% of the fall 2017 student credit hours at DSU were generated online. Our courses not only conveniently serve South Dakotans but draw students from across the country and many parts of the world. This is especially true of our graduate programs which have developed a reputation for offering high quality, nationally recognized courses and programs.

[9] What national examination, externally evaluated portfolio or student activity, etc., will verify that individuals have attained a high level of competence and identify those who need additional work?

The proposed Ph.D. in Cyber Defense will be offered entirely online (with exception of CSC 890 residency events). As with our other online graduate programs, we will use a number of instructional approaches which capitalize on the use of distributed technologies. Those strategies include, video lectorate's and vignettes appropriately chunked to and sequenced to acknowledge what cognitive science has taught us about online delivery of instruction. Strategies also include seminars, laboratory technologies, and guided research in the student's specialization. Courses will be delivered with D2L courseware for virtual networking, submitting assignments, and class discussion. Other applications and tools will encourage small group collaborations, virtual information sessions, online chats and discourse. Special tools will support synchronous dissertation committee work, and point-to-point and multi-user video platforms will also be used.

DSU has invested heavily in a virtualized infrastructure to allow for technical, hands-on experiences for students on campus and at a distance. This VMware environment has been instrumental in the online delivery of the undergraduate computer science and computer and network security majors as well as the graduate degrees in Cyber Operations and Cyber Defense. Educational experiences for students are greatly enhanced through these applied, hands-one technology-based activities.

Students will be required to complete the three on-sight research seminars (CSC 890) in a face-to-face setting at the Madison, SD campus. These research seminars will be held annually and take place over multiple days.

The DSU Office of Graduate Studies and the Office of Online Education will support the Beacom College of Computing and Cyber Sciences in delivery of the online program, courses, and student services. We will also comply with ADA Accessibility standards to offer students with special needs the best in barrier free learning.

8. Did the University engage any developmental consultants to assist with the development of the curriculum?[10] Did the University consult any professional or accrediting associations during the development of the curriculum? What were the contributions of the consultants and associations to the development of curriculum?

Developmental consultation is DSU internal.

9. Are students enrolling in the program expected to be new to the university or redirected from other existing programs at the university? Complete the table below and explain the methodology used in developing the estimates (*replace "XX" in the table with the appropriate year*)? *If question 12 includes a request for authorization for off-campus or distance delivery, add lines to the table for off-campus/distance students, credit hours, and graduates.*

Students are expected to matriculate from either a DSU computer or cyber sciences program (MSCD, MSCS) or from another universities computer science or cyber sciences programs. Dakota State University seeks highly motivated individuals with education and professional credentials that will enable them to be successful doctoral students. Students must have a bachelors or master's degree in computer science to apply.

[10] Developmental consultants are experts in the discipline hired by the university to assist with the development of a new program (content, courses, experiences, etc.). Universities are encouraged to discuss the selection of developmental consultants with Board staff.

DSU understands that students will come from a variety of computing programs with diverse backgrounds and academic preparation. This said, we have established five our program prerequisites:

- Introduction to Cyber Security
- Identity Management
- Network Security
- Software Development
- Cryptography

The Program Admission Committee will review these program prerequisites form each application to facilitate determination of program readiness.

Both bachelor-prepared and masters-prepared students are invited to apply to the PhD in Cyber Defense. DSU aims to attract high-potential bachelor-prepared students who will complete the Masters in Cyber Defense coursework along the way as they work towards the PhD in Cyber Defense. DSU is also targeting masters-prepared students and will follow SDBOR and DSU policies with regard to transfer credits for required and elective courses.

	Fiscal Years*			
	1st	**2nd**	**3rd**	**4th**
Estimates	FY 2019	FY 2020	FY 2021	FY 2022
Students new to the university	10	11	12	12
Students from other university programs	2	1	0	0
Continuing students				
=Total students in the program (fall)	12	24	36	48
Program credit hours (major courses)**	?	?	?	?
Graduates	0	0	4	8

*Do not include current fiscal year.

**This is the total number of credit hours generated by students in the program in the required or elective program courses. Use the same numbers in Appendix B – Budget.

Because the average time spent completing a degree requiring a dissertation is 4-7 years, the estimates for the number of graduates per year is calculated using that information. However, based on the success of other DSU graduate programs, we believe we will meet and exceed the BOR's requirement for five graduates in five years after the program is created, marketed, and established.

10. Is program accreditation available? If so, identify the accrediting organization and explain whether accreditation is required or optional, the resources required, and the University's plans concerning the accreditation of this program.

The university plans on approaching the National Security Agency to designate this PhD as a certified program (in accordance to NSA cyber defense standards). The program needs to run for several years to have a track record before the NSA will designate the program. Currently, the NSA has designated the MSCD program as meeting their requirements.

11. Does the University request any exceptions to any Board policy for this program? Explain any requests for exceptions to Board Policy. *If not requesting any exceptions, enter "None."*

No policy exceptions requested.

12. Delivery Location[11]

A. Complete the following charts to indicate if the university seeks authorization to deliver the entire program on campus, at any off campus location (e.g., UC Sioux Falls, Capital University Center, Black Hills State University-Rapid City, etc.) or deliver the entire program through distance technology (e.g., as an online program)?

	Yes/No	***Intended Start Date***
On campus	No	Choose an item. Choose an item.

	Yes/No	***If Yes, list location(s)***	***Intended Start Date***
Off campus	No		Choose an item. Choose an item.

	Yes/No	***If Yes, identify delivery methods[12]***	***Intended Start Date***
Distance Delivery (online/other distance delivery methods)	Yes	This program will be online only and delivered the same as other online graduate degree programs at DSU.	**Fall 2019**

The program can be completed on a full-time or part-time basis, with classes offered in three academic terms: fall, spring, and summer. As per BOR policy regarding Ph.D. students, students will be required to complete the program within 7 years of the semester of the student's admission.

B. Complete the following chart to indicate if the university seeks authorization to deliver more than 50% but less than 100% of the certificate through distance learning (e.g., as an online program)? [13]

	Yes/No	***If Yes, identify delivery methods***	***Intended Start Date***
Distance Delivery (online/other distance delivery methods)	Yes	Online	**Fall 2019**

13. Cost, Budget, and Resources: Explain the amount and source(s) of any one-time and continuing investments in personnel, professional development, release time, time redirected from other assignments, instructional technology & software, other operations and maintenance, facilities, etc., needed to implement the proposed major. Address off-

[11] The accreditation requirements of the Higher Learning Commission (HLC) require Board approval for a university to offer programs off-campus and through distance delivery.
[12] Delivery methods are defined in AAC Guideline 5.5.
[13] This question responds to HLC definitions for distance delivery.

campus or distance delivery separately. *Complete Appendix B – Budget and briefly summarize to support Board staff analysis.*

The Beacom College of Computer and Cyber Sciences will add one full-time equivalent faculty to augment the existing DSU faculty teaching in the program.

14. **Board Policy 2:1 states: "*Independent external consultants retained by the Board shall evaluate proposals for new graduate programs unless waived by the Executive Director.*" Identify five potential consultants (including contact information and short 1-2 page CVs) and provide to the System Chief Academic Officer (the list of potential consultants may be provided as an appendix). In addition, provide names and contact information (phone numbers, e-mail addresses, URLs, etc.) for accrediting bodies and/or journal editors who may be able to assist the Board staff with the identification of consultants.**

Ph.D.CD External Reviewer Candidates

Rayford Vaughn, University of Alabama Huntsville (retired). Former Vice President for Research and Economic Development, The University of Alabama in Huntsville. Also UA Huntsville; Head of the Department of Computer Science and Engineering, Director, Critical Infrastructure Protection Center (CIPC), and Director, Center for Computer Security Research (CCSR). MS and Ph.D. in computer Science from Kansas State University. Numerous honors and recognitions in Software Engineering and Cyber Security. Previously reviewed emerging program in Cyber Operations for DSU.

Cynthia Irvine, **Naval Postgraduate School.** Distinguished Professor of Computer Science and Director of the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School. Her research centers on the design and construction of high assurance systems and multilevel security. A new interest is cyber systems and operations, which led to her being the first Chair of the recently formed NPS Cyber Academic Group from 2011 through 2015. She is an author on over 160 papers and reports and has supervised the research of over 140 Masters and PhD students. From 2005 through 2009, she served as Vice-Chair and subsequently as Chair of the IEEE TC on Security and Privacy. In October 2015, she was inducted into the National Cybersecurity Hall of Fame.

Jean Kamp, Indiana University. Director of Center for Security and Privacy in Informatics, Computing, and Engineering. She spent the year after earning her doctorate from Carnegie Mellon (1996) as a Senior Member of the Technical Staff at Sandia National Laboratories. She began her career as an engineer at Catawba Nuclear Station with a MSEE at University of North Carolina at Charlotte. Her research focuses on the intersection of human and technical trust, leveraging economic models and human-centered design to create safe, secure systems. Her early contributions in the interdisciplines of economics of security, user-centered security, risk communication, and online trust underlie her applied research in the domains of IoT, authentication, secure networking, ecrime, public policy, ethics in computer science, and a few works on applied cryptography.

Mark Gondree, Sonoma State Univeristy. Assistant Professor in the Computer Science Department. Previously, Gondree was a Research Associate Professor in the Computer Science Dept at the Naval Postgraduate School in Monterey, CA, where he taught, advised students and

did research related to computer security and computer security education. His sponsors include the National Science Foundation, the US Navy, the National Reconnaissance Office and the Department of Homeland Security. Gondree received his PhD from the Computer Science Dept. at UC Davis in 2009. While at UCD, Gondree was a researcher in the CS theory lab, and a member of the cryptography research group and the electronic voting research group. Gondree received his master's in computer science from Case Western Reserve University in 2003.

15. Is the university requesting or intending to request permission for a new fee or to attach an existing fee to the program (*place an "X" in the appropriate box*)? *If yes, explain.*

[ ]	[X]
Yes	No

Explanation (if applicable):

16. New Course Approval: New courses required to implement the new graduate program may receive approval in conjunction with program approval or receive approval separately. Please check the appropriate statement:

[X] YES,
the university is seeking approval of new courses related to the proposed program in conjunction with program approval. All New Course Request forms are included as Appendix C and match those described in section 5D.

[ ] NO,
the university is not seeking approval of all new courses related to the proposed program in conjunction with program approval; the institution will submit new course approval requests separately or at a later date in accordance with Academic Affairs Guidelines.

17. Additional Information: *Additional information is optional. Use this space to provide pertinent information not requested above. Limit the number and length of additional attachments. Identify all attachments with capital letters. Letters of support are not necessary and are rarely included with Board materials. The University may include responses to questions from the Board or the Executive Director as appendices to the original proposal where applicable. Delete this item if not used.*

Program management

Policy and procedure oversight (including admissions eligibility, probation, suspensions, and certification for graduation) will be administered by the DSU Graduate Office. A graduate program committee, led by the program coordinator, will be responsible for recommending curriculum changes, course scheduling, admission decisions, and other program management tasks. All changes to the program will be subject to the approval of DSU's Graduate Council and will follow DSU graduate policies. Students will be assigned a faculty advisor.

Currently, there are no other Cyber Defense programs offered at the doctoral level at public or private universities. Nor do related programs exist at public colleges and universities in the region (MN, ND, MT, WY or NE). However, large for-profit online universities are reaching into South Dakota to offer Cyber Defense academic programs. Examples include Fairfax University and Capella University.

DSU's proposed Master of Science (MS) in Security and Policy Management is proposed as a stackable with the Ph.D. in Cyber Defense.