# SOUTH DAKOTA BOARD OF REGENTS

## Academic and Student Affairs

**AGENDA ITEM: 6 – I (4)**
**DATE: May 8-10, 2018**

**************************************************************************************

### SUBJECT

**Intent to Plan: DSU PhD in Cyber Defense**

### CONTROLLING STATUTE, RULE, OR POLICY

BOR Policy 2:23 – Program and Curriculum Approval

### BACKGROUND / DISCUSSION

Dakota State University (DSU) requests authorization to develop a proposal to offer a Doctor of Philosophy (PhD) in Cyber Defense. The program would provide graduates with high-level expertise in security issues, practices, politics and cultures of terrorism, as well as a foundation in research methodology and practice related to cyber defense. The program would prepare students for opportunities in critical areas of high workforce need, both in the private and public sector, while leveraging DSU's existing expertise in this field. DSU has not provided sample curriculum as is customary at this point in the planning process because comparable doctoral programs are rare. This provides DSU with an opportunity for an early entry to the marketplace in a growing field.

### IMPACT AND RECOMMENDATION

The proposed program is within the statutory and Board policy mission of DSU to provide programming in "computer management, computer information systems" and "technology-infused" areas. No related programs exist in the Regental system. DSU estimates graduating 8 students per year after full implementation and admitting 15 students per year. DSU does not anticipate asking for new state resources for the program.

Board office staff recommends approval the intent to plan with the following conditions:

1. The university will research existing curricula, consult with experts concerning the curriculum, and provide assurance in the proposal that the program is consistent with current national standards and with the needs of employers.

2. The proposal will define the specific knowledge, skills, and competencies to be acquired through the program, will outline how each will be obtained in the curriculum and will identify the specific measures to be used to determine

(Continued)

**************************************************************************************

### DRAFT MOTION 20180508_6-I(4):

I move to authorize DSU to develop a proposal for a PhD in Cyber Defense as presented.

whether individual students have attained the expected knowledge, skills, and competencies.

3. The university will not request new state resources without Board permission, and the program proposal will identify the sources and amounts of all funds needed to operate the program and the impact of reallocations on existing programs.

**ATTACHMENTS**

Attachment I – Intent to Plan Request Form: DSU – PhD in Cyber Defense

## SOUTH DAKOTA BOARD OF REGENTS

ACADEMIC AFFAIRS FORMS

# Intent to Plan for a New Program

Use this form to request authorization to plan a new baccalaureate major, associate degree program, or graduate program; formal approval or waiver of an Intent to Plan is required before a university may submit a related request for a new program. The Board of Regents, Executive Director, and/or their designees may request additional information. After the university President approves the Intent to Plan, submit a signed copy to the Executive Director through the system Chief Academic Officer. Only post the Intent to Plan to the university website for review by other universities after approval by the Executive Director and Chief Academic Officer.

| | |
|---|---|
| **UNIVERSITY:** | **DSU** |
| **DEGREE(S) AND TITLE OF PROGRAM:** | **Ph.D. Cyber Defense** |
| **INTENDED DATE OF IMPLEMENTATION:** | **Fall 2018** |

**University Approval**

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

J. M. Griffiths

President of the University

4/7/2018

Date

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

The Cyber Defense doctoral degree program is necessary to deal with our nation's growing cyber defense threats and workforce needs. The Ph.D. in Cyber Defense will provide graduates with a foundation in the security issues, practices, politics 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.

The doctoral degree in Cyber Defense will consist of 61 credits, which includes a literature review, professional research and theory, technical and managerial cyber defense courses, dissertation preparation, and other cyber defense topics. The program focuses on the 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.

**2. What is the need for the proposed program (e.g., Regental system need, institutional need, workforce need, etc.)? What is the expected demand for graduates nationally and in 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.)?**

The dual purpose for introducing this program includes: 1) workforce development as the United States anticipates dramatic workforce growth in cyber defense jobs; and 2) advance the science of cyber defense. Regarding the workforce, Table 1 outlines a brief list of jobs students would be eligible for:

Table 1 – Cyber Defense Jobs

| |
|---|
| Security Analysts |
| Security Managers |
| Professor |
| Cryptographer and Cryptanalyst |
| Cyber Defense Researcher |
| Vulnerability Scanner |
| Penetration Tester |
| Cyber Security Consultants |
| Cyber Defense Practitioners |
| Security Engineer or Architect |

Graduates from this program will help fill critical workforce shortages. As a few examples, at least one organization predicts a global shortage of two million cyber security professionals by 2019, specifically noting shortfalls for jobs as Security Analysts and Security Managers.[1] 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.[2] 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).[3] In South Dakota, there are currently 201 such positions and growing with an average wage of $79,000 - $88,000.[4]

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

[1] 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).

[2] 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).

[3] 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)

[4] 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)

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

***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.

## 3. How would the proposed program benefit students?

As noted earlier, the potential career opportunities with a cybersecurity degree are growing faster than other career areas. Positions include security officers, engineers/architects, and analysts.

Students will learn to:

- Work with a variety of research methodologies
- Research and develop tools to advance the fields of:
    - Network defense
    - Software assurance
    - 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
    - Measure cybersecurity effectiveness in both public and private sector organizations
- Apply ethical frameworks to security decisions
- Provide leadership in cyber defense

4. **How does the proposed program relate to the university's mission as provided in South Dakota Statute and Board of Regents Policy, and to the current Board of Regents Strategic Plan 2014-2020?**[5]

Cyber Defense involves technology, either directly or indirectly. Dakota State University's mission includes integrating technology into various disciplines, and this unique program is another step in fulfilling DSU's mission. The university's statutory mission includes a specialization in "computer management, computer information systems, electronic data processing, and other related undergraduate and graduate programs" (SDCL § 13-59-2.2). 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. This program would grow the number of graduate degrees awarded, growing the number of new graduate programs, and increasing the number of graduate STEM programs.

The SDBOR Strategic Plan 2014-2020 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.

5. **Do any related programs exist at other public universities in South Dakota? If a related program already exists, explain the key differences between the existing programs and the proposed program, as well as the perceived need for adding the proposed new program. Would approval of the proposed new program create opportunities to collaborate with other South Dakota public universities**

[5] 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.

South Dakota currently has no doctoral cyber defense degree offerings from public or private universities.

6. **Do related programs exist at public colleges and universities in Minnesota, North Dakota, Montana, and/or Wyoming?** *If a related program exists, enter the name of the institution and the title of the program; if no related program exists, enter "None" for that state. Add additional lines if there are more than two such programs in a state listed.*[6]

| | Institution | Program Title |
|---|---|---|
| ***Minnesota*** | None | None |
| ***Montana*** | None | None |
| ***Wyoming*** | None | None |
| ***North Dakota*** | None | None |
| ***South Dakota*** | None | None |

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

We anticipate most students will be new to the university. Students could matriculate from either a DSU computer or cyber sciences program (MS in Information Assurance or MS in Computer Science) or from another universities computer science or cyber sciences programs.

8. **What are the university's expectations/estimates for enrollment in the program through the first five years? What are the university's expectations/estimates for the annual number of graduates from the program after the first five years? Provide an explanation of the methodology the university used in developing these estimates.**

According to the SDBOR Dashboard[7], DSU graduates in the MS for Computer Science and MS for Information Assurance for the years 2013-17 totaled 123 students.

The program anticipates enrollments from 50-60 students when the program becomes established. Once this occurs, it is likely we would admit approximately 15 students annually. Initial enrollment numbers for the program include:

| Year | Enrollment Expectations | Number of Graduates |
|---|---|---|
| Year 1 | 10 | 0 |
| Year 2 | 15 | 0 |
| Year 3 | 20 | 0 |
| Year 4 | 25 | 4 |
| About | 30 | 8 |

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

[6] This question addresses opportunities available through Minnesota Reciprocity and WICHE programs such as the Western Undergraduate Exchange and Western Regional Graduate Program in adjacent states. List only programs at the same degree level as the proposed program. For example, if the proposed program is a baccalaureate major, then list only related baccalaureate majors in the other states and do not include associate or graduate programs.

[7] https://www.sdbor.edu/dashboards/Pages/Graduate-Production.aspx

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.

**9. Complete the following charts to indicate if the university intends to seek authorization to deliver the entire program at any off-campus location (e.g., UC Sioux Falls, Capital University Center, Black Hills State University-Rapid City, etc.) or intends to seek authorization to deliver the entire program through distance technology (e.g., as an on-line program)?**[7]

| | 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* | *Intended Start Date* |
|---|---|---|---|
| **Distance Delivery** | Yes | This program will be online only and delivered the same as other online graduate degree programs at DSU. | **Fall 2018** |

**10. What are the university's plans for obtaining the resources needed to implement the program?** *Indicate "yes" or "no" in the columns below.*

| | Development / Start-up | Long-term Operation |
|---|---|---|
| Reallocate existing resources | Yes | Yes |
| Apply for external resources | No | No |
| Ask Board to seek new State resources[8] | No | No |
| Ask Board to approve a new or increased student fee | No | No |

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. Additional funding for faculty is available through the gift DSU received in August.

**11. Curriculum Example: Provide (as Appendix A) the curriculum of a similar program at another college or university.** *The Appendix should include required and elective courses in the program. Catalog pages or web materials are acceptable for inclusion.* **Identify the college or university and explain why the selected program is a model for the program under development**.

In our search for similar programs, we have not found a program with the same title we are proposing. I have asked the two faculty members most involved with this request if they know of a comparable program, even though the title may be different, and I'm waiting for their reply.

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

[8] Note that requesting the Board to seek new State resources may require additional planning and is dependent upon the Board taking action to make the funding request part of their budget priorities. Universities intending to ask the Board for new State resources for a program should contact the Board office prior to submitting the intent to plan.