

SOUTH DAKOTA BOARD OF REGENTS

Academic and Student Affairs

AGENDA ITEM: 6 – I (5)

DATE: May 8-10, 2018

SUBJECT

Intent to Plan: MS in Security Policy & Management

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 Master of Science (MS) in Security Policy & Management. The program responds to increased demand for security policy leadership. Graduates would learn skills related to preparing and implementing cyber defense plans as well as gaining a foundation in practices, politics and cultures of terrorism, best practices to cope with related emergencies, and recovery processes. DSU points to studies indicating an estimated global shortage of two million cyber security professionals by 2019 as evidence of demand for graduates.

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 10 students per year after full implementation. 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(5):

I move to authorize DSU to develop a proposal for an MS in Security Policy & Management 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 – MS in Security Policy & Management



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:	Master of Science in Security Policy and Management
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. Gustafson

President of the University

4/2/2018

Date

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

The Master of Science in Security Policy and Management responds to the nation's growing security policy/leadership/management needs and issues. The proposed program provides graduates with a foundation in the security issues; practices, politics and cultures of terrorism; best practices to cope with a pending emergency; and operations during and recovery from an emergency.

Students will learn how to:

- Design and implement a comprehensive cybersecurity program
- Apply risk analysis concepts and models to a variety of organizations
- Create and establish cybersecurity frameworks in both the public and private sectors
- Understand multinational compliance requirements for cybersecurity
- Develop complete cybersecurity incident response plans
- Create an effective cybersecurity culture
- Apply ethical frameworks to security decisions
- Apply auditing concepts to the cybersecurity world
- Build models and metrics to measure the cybersecurity effectiveness in both public and private sector organizations

- Understand how cyber/physical systems converge
- Create more resilient organizations and systems through developing and implementing cybersecurity, security awareness, IT auditing, disaster recovery, business continuity, incident response and pandemic preparedness programs

The MS.SPM program will consist of 36 credits with 14 courses. While tracks are possible (CISO, Auditing, Emergency Preparedness, etc.), the program will launch without tracks/specializations. As the program builds enrollments, specializations may evolve.

To get started, students are provided introduction to technology (INFS 750) and security (INFA 701) courses. Thereafter, they take a sequence of cybersecurity leadership/management courses. They wrap up with more leadership and ethics material. Nine of the 14 courses are existing DSU courses and five of the courses are new:

- INFA 710 - Cybersecurity Program Design and Implementation 3 credits
- INFA 731 - Personnel Security 1 credit
- INFA 732 - Physical Security 1 credit
- INFA 733 - Vendor Management 1 credit
- INFA 758 - Cybersecurity Metrics 3 credits

Together these 14 courses (36 credits) provide a theoretical and practical foundation for managing security issues and addressing emergencies.

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 primary purpose for introducing this program is workforce development as the United States anticipates dramatic workforce growth in security leadership/management jobs, including but not limited to:

- Information Security Analysts
- Information Security Officers
- Chief Information Security Officers
- Information Security Consultants
- Cybersecurity Analysts
- Cybersecurity Officers
- Chief Cybersecurity Officers
- Cyber Security Consultants
- Cyber/Physical Security Specialists
- Security Management Practitioners
- Emergency Preparedness and Response Professionals
- IT Auditors

Graduates from this program will help fill critical workforce shortages nationally. 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 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

The federal workforce also benefits to gain from this program. For example, Department of Homeland Security (DHS) employs approximately 240,000 people, many in areas related to security policy and management, and in areas ranging from human resources to border control to the Secret Service.⁵

South Dakota currently does not produce security policy/management graduates. While state and national DHS locations have emerged since the establishment of DHS in 2002, South Dakota has not participated in producing Security Leadership graduates. Graduates are necessary to fill jobs at the federal, state, local and corporate levels:

Federal – On the federal level, the government’s law enforcement, military, and intelligence departments are the source of the guidelines which oversee our country’s various security leadership/management operations at both state and local levels. 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 security leadership/management and how they respond to terrorist attacks. The Security Management 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 security management department is to make sure that the government, at all levels, functions in an effective and coordinated manner.

Employees work throughout the country for the Department of Security Management and the agencies under its umbrella, including:

- 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

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)

⁵ U.S. Department of Homeland Security website: <https://www.dhs.gov/about-dhs>.

by U.S. citizens who meet specific guidelines. Median annual wages for security leadership/management professionals range from \$37,000 – \$39,680 for transportation security screeners to roughly \$60,000 – \$70,500 for emergency management directors, according to the Bureau of Labor Statistics.⁶

State – At the state level, security management agents are required to adopt federal policies and models of dealing with, and adapting to, various crises; then applying this to the security needs of their state. One of the biggest issues that security management faces at the state level is the federal government funds their department receives. A key metric that is used in calculating funding is the density of residents per state. Heavily populated states that have major metropolitan enclaves are given considerably more money to develop security management strategies and to implement said strategies. Since 2001 alone, about \$40 billion has been invested in both state and local sectors.

Local – Although many cities in the United States do not require extensive counter-terrorism strategy to function, a lot of cities on the local level have mimicked the proactive policy exhibited on the federal level. Major metropolitan areas such as New York, Los Angeles, and Boston have already fallen victim to terrorism. These cities are still considered major targets because they have some of the largest populations of people living near each other. To thwart such attacks in the future, the government has invested funding, training, and equipment in various forms in these high profile metropolitan areas. The Urban Areas Security Initiative has given significant funding to these following cities and their security management 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 – Although saving American lives is the most important goal of security leadership/management, protecting American enterprise is also viewed as an imperative component of American society to protect. The private sector of American society (i.e. corporations, organizations, etc.) provide extensive services for the American public such as manufacturing, transportation, telecommunications, utilities, food, healthcare, banking and defense projects. Homeland security agents and the private sector are each working to protect this portion of our society and provide knowledge and a range of expertise that are essentially utilized to combat issues of cybersecurity and business continuity planning. As technology expands in organizations, so do security risks and organizations are responding by hiring analysts, specialists and officers to enact security leadership/management practices to augment the technical staff and keep organizations safe.

3. How would the proposed program benefit students?

The program focuses on the leadership/management and policy aspects of cyber defense, including to identify, detect, protect, respond and recover from security incidents, disasters and emergencies. More importantly, the program focuses on developing well-rounded cybersecurity decision-makers with a background in leadership and ethics. The program prepares well-rounded graduates to work

⁶ The Occupational Information Network (O*NET) developed under the sponsorship of the U.S. Department of Labor/Employment and Training Administration, Transportation Security Screeners, <https://www.onetonline.org/link/summary/33-9093.00>; and Emergency Management Directors, <https://www.onetonline.org/link/summary/11-9161.00>; (viewed January 30, 2018)

in a variety of security leadership/management and emergency preparedness capacities such as cyber defense, land borders, seaports and airports, threat assessment, disaster management, and crisis response planning and management. The goal of the program is to develop both the critical acumen and theoretical outcomes before, during, and after cyber emergencies, and build sustainable Cybersecurity Management Systems (ISMS) to protect organizations of all kinds. Graduates will develop the ability to write, implement and manage a variety of cyber defense plans, including cybersecurity programs, business continuity plans, incident response plans, emergency preparedness plans, auditing programs, security awareness programs and physical security plans. The program will provide students with a broad understanding of safety and security issues, as well as focus on critical components in the field of Security Policy and Management:

- Current Issues in Cybersecurity
- Cybersecurity Law and Regulation
- Data Privacy
- Cybersecurity Risk Management
- Cybersecurity Program Design and Implementation
- Creating a Culture of Cybersecurity
- Cybersecurity Auditing
- Emergency Preparedness
 - Incident Response
 - Business Continuity
 - Disaster Recovery
 - Pandemic Preparedness
- Cybersecurity Metrics
- Cybersecurity Ethics
- Intelligence Sharing and Analysis
- Securing Thru Technology
- Personnel Security
- Physical Security
- Vendor Management
- Cybersecurity Management Tools and Best Practices
- Cybersecurity Research
- Leadership

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?⁷

Security Policy/Management often 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.

⁷ 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.

The proposed programs align with multiple action steps related to graduate education in the SDBOR Strategic Plan 2014-2020. These include growing the number of graduate degrees awarded, growing the number of new graduate programs, and increasing the number of graduate STEM programs. In addition, 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;
- 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.

Adding a MS in Security Policy/Management will provide an opportunity for either business or technology professionals to augment their skill set in security leadership/management. 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.

The 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 security leadership/management is emerging as a profession and academic area of study. Dakota State is already a 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.

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?

South Dakota currently has no security policy/management degree offerings from public universities in South Dakota at either the undergraduate or graduate level.

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.⁸

⁸ 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.

	Institution	Program Title
<i>Minnesota</i>	None	None
<i>Montana</i>	None	None
<i>Wyoming</i>	None	None
<i>North Dakota</i>	None	None
<i>South Dakota</i>	None	None
<i>Nebraska</i>	Bellevue University	Master of Science in Security Management

Large online universities such as the University of Phoenix, Kaplan University and Capella University can reach into South Dakota and offer Cybersecurity Policy and Management programs. Many other traditional universities already offer online security management degrees, such as Penn State University, Northeastern University, Tulane University, Arizona State University, and Colorado Technical University.

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

We expect the students to be new students but there could be some students in the MS in Information Assurance (MSIA) who want the leadership/management side of cybersecurity so may change degree programs. See the anticipated enrollment numbers documented in Question 8. Note that “transfer” students could be students moving from MSIA to the MS Security Policy and Management.

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.

We anticipate this program mirroring the current MSIA program at DSU which had an average enrollment of 40 students over the past five years. The MSIA has graduated 21 students in each of the last three years. Once this program is mature, it is likely we would admit 15-20 students annually. Because this M.S. degree requires 36 credits, students will take longer to graduate depending upon credits per term (fall, spring, summer). We also anticipate this program will be completed by those working full-time which again will influence the number of graduates per year. Ramp up enrollment numbers for the program include:

Year	Enrollment Expectations	Number of Graduates
Year 1	8	0
Year 2	15	3
Year 3	20	5
Year 4	25	8
Year 5 and up	30	10

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)?⁹

	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 just as other online graduate courses 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 ¹⁰	No	No
Ask Board to approve a new or increased student fee	No	No

The Beacom College of Computer and Cyber Sciences is adding one full-time equivalent to augment the existing DSU faculty who will teach in the program.

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.

See Appendix A – pages 9 and 10.

⁹ The accreditation requirements of the Higher Learning Commission (HLC) require Board approval for a university to offer programs off-campus and through distance delivery.

¹⁰ 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.

APPENDIX A

University of Maryland-University College Master's in Cybersecurity Management & Policy

<http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity-management-policy-ms.cfm>.

The Master of Science in cybersecurity management and policy at University of Maryland University College can help you gain the tools you need to join the management track in cyber security so that you can establish, implement, and oversee a cyber security policy structure for an organization. Learn how to create a security approach that combines technology, governance, and compliance perspectives. Gain advanced knowledge in organizational structures, communication, operational business processes, and the legal framework for cyber security policy.

Career Preparation

This program is designed to help IT professionals prepare to join the management team in a public- or private-sector cyber security organization and develop and oversee cyber security policy. Potential career fields include cybersecurity and policy, data protection, and information security.

Learning Objectives

Through your coursework, you will learn how to

- Understand multinational compliance requirements for cyber security
- Apply risk analysis concepts and models to a variety of organizations
- Incorporate cyber security into healthcare and financial services organizations
- Create and establish cyber security frameworks in both the public and private sectors
- Develop complete cyber security incident response plans

Core Courses (2017-18 Catalog)

Course Number	Course Name	Credit Hours
CBR 600	Communicating, Problem Solving, and Leading in Cybersecurity	6
CMP 610	Foundations in Cybersecurity Management	6
CMP 620	Cybersecurity Governance	6
CMP 630	Risk Management and Organizational Resilience	6
CMP640	Cybersecurity Program Development	6
CYB 670	Capstone in Cybersecurity	6

All courses must be taken in the order listed. All courses are available online. Select courses may be available in a hybrid format.

You must complete each course with a grade of B or better to advance to the next course. The grade of C is not available for these courses.

APPENDIX A – PAGE 2

Coursework Examples

In past projects, students have had the opportunity to

- Develop a cyber security program for a government entity private-sector organization
- Create cyber security policies for a government entity or private-sector organization
- Perform a cyber security threat analysis, including a vulnerability assessment, and develop a risk management approach for a government entity or private-sector organization
- Develop and determine cyber incident response procedures based on management best practices

Experience Recommended for Success in the Program

If you do not have work experience in information technology, an IT academic background, or IT certifications, we strongly recommend you take Basic Information Technology (0 Credits, ASC 605), Essentials of Computer Programming (0 Credits, ASC 609), and Structure of Computer Programming (0 Credits, ASC 611). These courses will give you a foundation that will help you succeed in the program. We recommend Graduate Writing Skills (0 Credits, ASC 601) if you'd like to improve your graduate writing skills.

Industry Certification

This program can help prepare you for the following certification exams:

- [Certified Information Systems Security Professional \(CISSP\)](#)
- [CompTIA Security+](#)
- [Disaster Recovery Institute \(DRI\)](#)
- [Global Information Assurance Certification \(GIAC\)](#)
- [Project Management Professional \(PMP\)](#)

Graduation Requirements

- You must maintain a GPA of 3.0 or higher at all times.
- All degree requirements must be fulfilled within five consecutive years.
- Any transfer credits must have been earned within the five-year time frame to be applied toward a graduate degree.