SOUTH DAKOTA BOARD OF REGENTS

Academic and Student Affairs
Consent

AGENDA ITEM: 5 – C (1)
DATE: December 11-12, 2024

****

SUBJECT

New Graduate Certificate Request – DSU – Cyber Operations

CONTROLLING STATUTE, RULE, OR POLICY

BOR Policy 2.3.2 – New Programs, Program Modifications, and Inactivation/Termination

BACKGROUND / DISCUSSION

Dakota State University (DSU) requests authorization to offer a graduate certificate in Cyber Operations. The proposed certificate will provide students with essential knowledge of technical cyber operations including a deep dive into software reverse engineering, binary exploitation, and malware analysis. Furthermore, it will equip students with practical and theoretical knowledge and skills to analyze and apply technical cyber security concepts on modern systems.

IMPACT AND RECOMMENDATION

The proposed certificate will be offered on campus and online. DSU does not request new resources. No new courses will be required.

Board office staff recommends approval.

ATTACHMENTS

Attachment I – New Certificate Request Form: DSU – Cyber Operations

****

DRAFT MOTION 20241211_5-C(1):

I move to authorize DSU to offer a graduate certificate in Cyber Operations, as presented.

SOUTH DAKOTA BOARD OF REGENTS
ACADEMIC AFFAIRS FORMS

New Certificate

Use this form to propose a certificate program at either the undergraduate or graduate level. A certificate program is a sequence, pattern, or group of academic credit courses that focus upon an area of specialized knowledge or information and develop a specific skill set. Certificate programs typically are a subset of the curriculum offered in degree programs, include previously approved courses, and involve 9-12 credit hours including prerequisites. In some cases, standards for licensure will state explicit requirements leading to certificate programs requiring more than 12 credit hours (in such cases, exceptions to course or credit requirements must be justified and approved). 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 Certificate Form to the university website for review by other universities after approval by the Executive Director and Chief Academic Officer.

UNIVERSITY:	DSU
TITLE OF PROPOSED CERTIFICATE:	Cyber Operations
INTENDED DATE OF IMPLEMENTATION:	Spring 2025
PROPOSED CIP CODE:	11.0101
UNIVERSITY DEPARTMENT:	Beacom College of Computer and Cyber Sciences
BANNER DEPARTMENT CODE:	DCOC
UNIVERSITY DIVISION:	Computer Science
BANNER DIVISION CODE:	DSCI

☒ **Please check this box to confirm that:**

- The individual preparing this request has read AAC Guideline 2.3.2.2.C, which pertains to new certificate requests, and that this request meets the requirements outlined in the guidelines.
- This request will not be posted to the university website for review of the Academic Affairs Committee until it is approved by the Executive Director and Chief Academic Officer.

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.

Rebecca L. Hoey

Institutional Approval Signature
President or Chief Academic Officer of the University

10/30/2024
Date

Note: In the responses below, references to external sources, including data sources, should be documented with a footnote (including web addresses where applicable).

1. **Is this a graduate-level certificate or undergraduate-level certificate (*place an "X" in the appropriate box*)?**

   Undergraduate Certificate ☐ Graduate Certificate ☒

2. **What is the nature/ purpose of the proposed certificate? Please include a brief (1-2 sentence) description of the academic field in this certificate.**

   This graduate certificate provides students with essential knowledge of technical cyber operations including a deep dive into software reverse engineering, binary exploitation, and malware analysis. Furthermore, it equips students with practical and theoretical knowledge and skills to analyze and apply technical cyber security concepts on modern systems.

3. **If you do not have a major in this field, explain how the proposed certificate relates to your university mission and strategic plan, and to the current Board of Regents Strategic Plan 2014-2020.**
   Links to the applicable State statute, Board Policy, and the Board of Regents Strategic Plan are listed below for each campus.

BHSU:	*SDCL § 13-59*	*BOR Policy 1.2.1*
DSU:	*SDCL § 13-59*	*BOR Policy 1.2.2*
NSU:	*SDCL § 13-59*	*BOR Policy 1.2.3*
SDSMT:	*SDCL § 13-60*	*BOR Policy 1.2.4*
SDSU:	*SDCL § 13-58*	*BOR Policy 1.2.5*
USD:	*SDCL § 13-57*	*BOR Policy 1.2.6*

Board of Regents Strategic Plan

   As the science behind cyber security concepts advances, DSU must continue to respond to workforce development needs. This program is designed to serve working professionals who currently hold a master's degree in computer science with two years of workforce experience and are interested in exploring the technical nature and science of Cyber Operations. Related degrees will be approved on a case-by-case basis. This certificate specifically supports the DSU Strategic Plan and the stated goals of workforce development.

4. **Provide justification for the certificate program, including the potential benefits to students and potential workforce demand for those who graduate with the credential.** *For workforce related information, please provide data and examples. Data may include, but are not limited to the South Dakota Department of Labor, the US Bureau of Labor Statistics, Regental system dashboards, etc. Please cite any sources in a footnote.*

   This graduate certificate program in Cyber Operations offers students a range of benefits while addressing the increasing workforce demand in this critical field.

   According to the 2023 (ISC)² Cybersecurity Workforce Study, the global cybersecurity workforce gap grew to an all-time high of 5.5 million. Workforce demands in the United States alone were up 11.3% (to nearly 1.5 million) in 2023. ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap.

   The continued demand for cybersecurity professionals in the U.S. is accelerating. Employment for information security analysts is projected to grow by 33% between 2023 and 2033, according to the U.S. Bureau of Labor Statistics. This is much faster than the average growth

rate for other occupations, which is projected at around 5% Information Security Analysts : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics (bls.gov)

5. **Who is the intended audience for the certificate program (including but not limited to the majors/degree programs from which students are expected)?**

   Working cyber professionals currently serving in a cyber-operator role or individuals who have already completed a master's in computer science and are interested in a post-Masters certificate but not interested in pursuing a full Ph.D.

6. **Certificate Design**
   A. **Is the certificate designed as a stand-alone education credential option for students not seeking additional credentials (i.e., a bachelor's or master's degree)? If so, what areas of high workforce demand or specialized body of knowledge will be addressed through this certificate?**

      Dakota State University programs are recognized for their high degree of practical experience and hands on curriculum along with a deep theoretical foundation. This certificate is the result of requests from industry partners who would like additional credentials but not a full Ph.D. This certificate is specifically aimed at technical cyber security professionals whose work includes Software Reverse Engineering, Binary Exploitation, and Malware Analysis. This certificate also complements DSU's existing master and Ph.D. programs.

   B. **Is the certificate a value added credential that supplements a student's major field of study? If so, list the majors/programs from which students would most benefit from adding the certificate.**

      Yes.
      Master: Computer Science, Cyber Operations Specialization
      Ph.D.: Cyber Operations
      This certificate is aimed at working professionals who have completed a computer science master's degree and have directly related work experience. Given the hands-on nature of the courses along with validation from our previous external program reviews, these courses will serve to increase the workforce's needs in technical cyber security.

   C. **Is the certificate a stackable credential with credits that apply to a higher level credential (i.e., associate, bachelor's, or master's degree)? If so, indicate the program(s) to which the certificate stacks and the number of credits from the certificate that can be applied to the program.**

      The Cyber Operations Graduate Certificate consists of five core courses from the Ph.D. program in Cyber Operations. Students who wish to pursue the Ph.D. after completing the certificate must submit a full application and undergo the standard review process for admission. If admitted, these courses will count towards the Ph.D. requirements. Due to the interactive and complimentary nature of these five core courses, DSU requests permission to exceed the standard credit hour certificate limit and offer the Cyber Operations Graduate Certificate as a 15-credit hour student experience.

7. List the courses required for completion of the certificate in the table below (if any new courses are proposed for the certificate, please attach the new course requests to this form). *Certificate programs by design are limited in the number of credit hours required for completion. Certificate programs consist of nine (9) to twelve (12) credit hours, including prerequisite courses. In addition, certificates typically involve existing courses. If the curriculum consists of more than twelve (12) credit hours (including prerequisites) or includes new courses, please provide explanation and justification below.*

Prefix	**Number**	**Course Title** *(add or delete rows as needed)*	**Prerequisites for Course** *Include credits for prerequisites in subtotal below.*	**Credit Hours**	**New (yes, no)**
CSC	840	Cyber Operations I	None	3	No
CSC	841	Cyber Operations II	None	3	No
CSC	844	Advanced Reverse Engineering	None	3	No
CSC	846	Advanced Malware Analysis	None	3	No
CSC	848	Advanced Software Exploitation	None	3	No
			Subtotal	15	

8. Student Outcome and Demonstration of Individual Achievement.
Board Policy 2:23 requires certificate programs to "have specifically defined student learning outcomes.

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.*

1) Be able to utilize reverse engineering tools and procedures to conduct static and dynamic analysis on unknown binaries to understand their behavior and purpose.
2) Be able to utilize reverse engineering tools and procedures to conduct static and dynamic analysis on unknown binaries to understand their behavior and purpose.
3) Be able to develop an in-depth understanding of cyber operations content focusing on mitigating cyber threats and anticipation of a cyber-attack.
4) Be able to use automated exploitation tools, understand manual exploitation process in a Windows and Linux environment, and create shell code using software exploitation techniques including but not limited to heap and RP exploitation.

B. Complete the table below to list specific learning outcomes – knowledge and competencies – for courses in the proposed program in each row. *Label each column heading with a course prefix and number. Indicate required courses with an asterisk (*). Indicate with an X in the corresponding table cell for any student outcomes that will be met by the courses included. All students should acquire the program knowledge and competencies regardless of the electives selected. Modify the table as necessary to provide the requested information for the proposed program.*

Individual Student Outcome (Same as in the text of the proposal)	CSC 844	CSC 846	CSC 840	CSC 841	CSC 848
Utilize reverse engineering tools and procedures to conduct static and dynamic analysis on unknown binaries to understand their behavior and purpose.	X				
Utilize reverse engineering tools and procedures to conduct static and dynamic analysis on unknown binaries to understand their behavior and purpose.		X			
Develop an in-depth understanding of cyber operations content focusing on mitigating cyber threats and anticipation of a cyber-attack.			X	X	
Use automated exploitation tools, understand manual exploitation process in a Windows and Linux environment, and create shell code using software exploitation techniques including but not limited to heap and RP exploitation.					X

9. Delivery Location.

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

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., USD Community College for Sioux Falls, Black Hills State University-Rapid City, Capital City Campus, etc.) or deliver the entire program through distance technology (e.g., as an on-line program)?

	Yes/No	***Intended Start Date***
On campus	Yes	

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

	Yes/No	***If Yes, identify delivery methods*** *Delivery methods are defined in AAC Guideline 2.4.3.B.*	***Intended Start Date***
Distance Delivery (online/other distance delivery methods)	Yes	X15 Online Asynchronous – Term Based Instruction	**Spring 2025**
Does another BOR institution already have authorization to offer the program online?	No	**If yes, identify institutions:**	

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 on-line program)? *This question responds to HLC definitions for distance delivery.*

	Yes/No	***If Yes, identify delivery methods***	***Intended Start Date***

Distance Delivery (online/other distance delivery methods)	No		Choose an item. Choose an item.

10. 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.*

Items of note:

1) This certificate is in response to federal partners' request for specific workforce development needs. As a result of conversations, five total classes are requested in this certificate.
2) Application to this certificate will require a master's in computer science or an undergraduate degree in computer science and a related masters with a minimum of two years of direct work experience in software reverse engineering, technical malware analysis, or binary exploitation.