GROSSMONT COLLEGE

Feasibility Report Program Proposal

The Baccalaureate Degree Program (BDP)

Bachelor of Science in Strategic Cyber Defense Analysis

Program Feasibility Taskforce
5-19-2025

Table of Contents

1.0 Executive Summary

On October 6, 2021, California Governor Gavin Newsom signed the Assembly Bill (AB) 927, authorizing the expansion of the California Community Colleges Baccalaureate Degree Program [1][5]. This legislation allows the Board of Governors to approve up to 30 new baccalaureate degree programs annually, with the goal of increasing access to affordable four-year degrees and addressing workforce needs in high-demand fields, such as Healthcare; Biomanufacturing; Transportation Technology, and Cybersecurity [2]. The BDP is designed to provide students with affordable, local pathways to bachelor's degrees that do not duplicate programs offered by California State University (CSU) or University of California (UC) campuses. These degrees are tailored to regional labor market demands and focus on equity, economic mobility, and closing educational attainment gaps [4].

Grossmont College's Strategic Cyber Defense Analysis (GSCyber) bachelor's program is unique and different by its comprehensive curriculum, especially at the upper division level, which blends advanced technical skills - such as network defense, threat analysis, and ethical hacking - with training in policy, governance, risk management, and organizational leadership. The program is closely aligned with the Department of Defense (DoD) Cyber Workforce NICE (National Initiative for Cybersecurity Education) Framework and the Center of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units, ensuring graduates acquire nationally recognized competencies directly relevant to both public and private sector cybersecurity roles.

Grossmont College responded to this opportunity by developing a rigorous feasibility process to evaluate potential bachelor's degree offerings. The selection criteria included projected job growth, alignment with workforce needs, non-duplication with CSU and UC programs, and the feasibility of expanding from a two-year to a four-year degree structure. After careful review in May 2024, the feasibility workgroup selected a Bachelor of Science in Strategic Cyber Defense Analysis (GSCyber), proposed by the Division of Career Technical Education and Workforce Development.

Grossmont College's GSCyber exemplifies the BDP mission by offering a strategically designed, workforce-aligned program that fills a critical gap in the region. Grossmont's GSCyber program not only empowers students but also strengthens the local talent pipeline and supports California's broader economic and security objectives.

2.0 Program Differentiation

The proposed Grossmont College Bachelor of Science in Strategic Cyber Defense Analysis (GSCyber) aligns with recognized national frameworks, including the Department of Defense (DoD) Cyber Workforce Framework and the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework as shown below in Figure 1. These alignments ensure that the curriculum meets federal and industry expectations for workforce readiness.

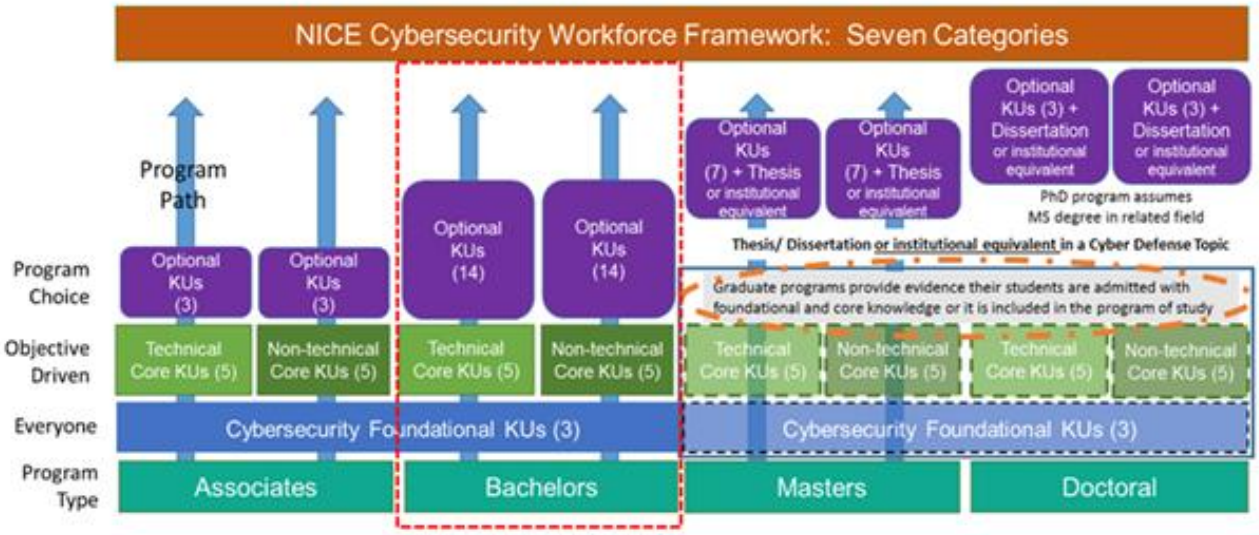


Figure 1. CAE-CD Knowledge Units Alignment Requirements

The program adheres to the standards outlined in the CAE-CD requirements document. Specifically, each academic program type—whether Associate, Bachelor's, Master's, or Doctoral—is required to integrate a specific combination of foundational content, core Knowledge Units (KUs), and a set number of elective KUs that are either technical or non-technical in nature. This structured approach guarantees that students develop the appropriate breadth and depth of cybersecurity expertise tailored to their educational level.

By embedding these KUs into the curriculum, the program ensures that students acquire critical Knowledge, Skills, and Abilities (KSAs) that are directly mapped to real-world job functions and roles. These KSAs are not only academically rigorous but also industry-recognized, giving graduates a competitive edge when entering or advancing in the cybersecurity workforce [11].

In adhering to the NICE Framework, Grossmont College affirms its commitment to excellence in cybersecurity education, preparing students to meet the exacting standards of government agencies, defense contractors, and commercial enterprises. This strategic alignment enhances graduates' employability, supports workforce development, and contributes to national cybersecurity readiness.

While other institutions may offer programs based on the same NICE frameworks, Grossmont College's program differentiates itself by providing a comprehensive curriculum that balances technical instruction with coursework in strategic planning, management, business operations, and artificial intelligence. This dual-focus approach meets the growing demand for cybersecurity professionals capable of both implementing technical solutions and guiding organizational strategy.

Table 1. below shows the various cybersecurity degree programs in the San Diego region. There are limited bachelor degree programs in cybersecurity and the existing programs are at the Master's level, are online only, and do not provide the strategic focus beyond technical proficiency.

	Institution	Program Type	Status
1	San Diego City Cyber Defense	BDP program	First cohort 2024
2	California State University at San Diego SDSU	MS Cyber Management	No BS program
3	California State University at San Marcos CSUSM	BS Online Only	First cohort 2024
4	University of San Diego (Private)	Master Cyber	No BS program
5	National University (Private)	BS	On going

Table 1. San Diego Region Cybersecurity Programs

There are differences between the proposed Grossmont College Cybersecurity Program and other competitor programs. For example, comparing upper division San Diego City College courses with Grossmont College as shown below in Table 2., we can see that there are nine different Grossmont College courses that City College does not possess, which means that Grossmont College is 50% different from City College at the upper division. As an example, Grossmont College has a course on *Security Leadership Essentials for Managers* that reflects emphasis on leadership development that City College does not

have. In addition, the inclusion of emerging technologies, such as the artificial intelligence applications in cybersecurity course, positions the Grossmont College program at the forefront of industry trends and technological evolution.

	SANDIEGO CITY COLLEGE BS Cyber Defense and Analysis				Grossmont College BS Strategic Cyber Defense Analysis	
	Description	Unit			Description	Unit
1	**GE BUSE 440: Cyber Law and Ethics**	3	A	**CSIS 300**	**Emerging AI Technology and Cybersecurity**	3
2	**GE CISC 450: Security Analytics and Visualization**	3	B	**CSIS 305**	**Basic Cyber Operations**	3
3	**GE ENGL 402: Advanced Technical Writing**	3	C-5	**CSIS 310**	**Applied Cryptography**	3
4	**CYDA 400: Emerging Technology and Cybersecurity**	3	D-1	**CSIS 320**	**Cybersecurity Ethics**	3
5	**CYDA 410: Modern Cryptography**	3	E-3	**CSIS 325**	**Cybersecurity Writing**	3
6	**CYDA 420: Applied Network Security Monitoring**	3	F	**CSIS 330**	**Intrusion Detection and Analysis**	3
7	**CYDA 430: Applied Intrusion Detection and Analysis**	3	G	**CSIS 380**	**Wireless Security and Vulnerabilities**	3
8	**CYDA 440: Deconstructing Malware**	3	H-13	**CSIS 400**	**Cyber Intelligence & Incident**	3
9	**CYDA 450: Network Forensics**	3	I	**CSIS 410**	**Enterprise Operation Continuity (Cyber Response and Rec**	3
10	**CYDA 460: Digital Forensics**	3	J	**CSIS 427**	**Security Leadership Essentials for Managers**	3
11	**CYDA 500: Cyber Incident Response**	3	B-15	**CSIS 440**	**Infrastructure and Supply Chain Vulnabilities**	3
12	**CYDA 510: Disaster Response and Recovery**	3	C	**CSIS 450**	**Cloud Computing Security**	3
13	**CYDA 520: Cyber Threat Intelligence**	3	D-18	**CSIS 470**	**Strategic Cyber Defense and Analysis Capstone**	4
14	**CYDA 530: Advanced Security Implementation and Management**	3	E-17	**CSIS 460**	**Operational Security Architecture**	3
15	**CYDA 540: Critical Infrastructure and Supply Chain Protection**	3	F	**CSIS 465**	**Secure Programming Practices**	3
16	**CYDA 550: System and Network Auditing**	3	G	**CSIS 475**	**Mobile Device Security**	3
17	**CYDA 560: Operational Security Architecture**	3	H-10	**CSIS 480**	**Intro to Digital Forensics**	3
18	**CYDA 570: Cyber Defense and Analysis Capstone**	3	I-8	**CSIS 485**	**Intro to Malware Reverse Engineering**	3

Table 2. Upper Division Course Comparison Between City College and Grossmont College

Grossmont College's comprehensive and interdisciplinary structure provides a clear competitive advantage over programs that focus exclusively on technical skillsets. Grossmont College's approach ensures graduates are adaptable, future-ready, and equipped to contribute to cybersecurity resilience across public and private sectors.

Grossmont College's Cybersecurity program is also in the process of be certified by the NSA as a Center of Academic Excellence in Cyber Defense. The program has achieved the first phase of certification with an approved Plan of Study. No other community college in the San Diego region has achieved this yet. Grossmont College's Cybersecurity program also provides more of a strategic and holistic approach that cultivates professionals who are not only technically proficient but also capable of becoming leaders and making informed business decisions.

3.0 Comprehensive and Interdisciplinary Curriculum

The curriculum is thoughtfully designed to provide a well-rounded and rigorous educational experience that goes beyond traditional technical instruction. While students receive in-depth training in core cybersecurity concepts—such as network security, cryptography, and threat analysis, they also engage with a broad range of interdisciplinary subjects that are critical in today's multifaceted cybersecurity landscape. These include policy development, regulatory compliance, risk management, and organizational behavior.

Shown below in Table 3 is Year 1 and Year 2 of the bachelor's curriculum. The new bachelor's degree courses begin at 300-400 level in Year 3 and year 4 in Table 4. Program-level SLOs are listed in Section 7.0.

	Grossmont BS Strategic Cyber Defense Analysis (GSCyber)	
	Bridging Theory to Practice	
Course	**Title**	**Units**
	Year 1: Foundation Knowledge and skills	
CSIS 113	Introduction to Linux	3
CSIS 121	Introduction to Cybersecurity	3
CSIS 122	Cloud + Certification	3
CSIS 125	Network + Certification	3
CSIS 250	Introduction to Python Programming	3
ENGL 120 *	College Composition and Reading	3
PSC 110 *	Introduction to Physical Sciences	3
PSC 111 *	PSC-110 LAB	1
PHIl 142 *	Ethics of Technology	3
COMM 122 *	Public Speaking	3
BIO B2 *	Biological Sciences	3
		31
Course	**Title**	**Units**
	Year 2: Intermediate Cybersecurity Concepts	
CSIS 252	Cyber Security & AI with Python	4
CSIS 263	Security + Certification	3
CSIS 264	Ethical Cybersecurity Hacking	3
CSIS 265	Computer Forensics Fundamentals	3
CSIS 267	Cyber Security Analyst (CySA+)	3
PHSC 180 *	Introduction to Public Policy	3
MATH 160 *	Elementary Statistics	4
BUS 125 *	Business Law	3
C Humanities *	Arts & Humanities	3
		29

Table 3. Year 1 and Year 2 Curriculum

*Recommended Lower Division General Education

	Grossmont BS Strategic Cyber Defense Analysis (GSCyber)	
	Bridging Theory to Practice	
Course	**Title**	**Units**
	Year 3: Advanced Cybersecurity Techniques and Applications	
CSIS 300	Emerging AI Technology and Cybersecurity	3
CSIS 305	Basic Cyber Operations	3
CSIS 310	Applied Cryptography	3
CSIS 320 **	Cybersecurity Ethics	3
CSIS 325 **	Cybersecurity Writing	3
CSIS 330	Intrusion Detection and Analysis	3
CSIS 380	Wireless Security and Vulnerabilities	3
CSIS 400	Cyber Intelligence & Incident	3
CSIS 410	Enterprise Operation Continuity (Cyber Response and Recovery)	3
		27
Course	**Title**	**Units**
	Year 4: Professional Development and Specialization	
CSIS 427 **	Security Leadership Essentials for Managers	3
CSIS 440	Infrastructure and Supply Chain Vulnerabilities	3
CSIS 450	Cloud Computing Security	3
CSIS 470	Strategic Cyber Defense and Analysis Capstone	3
CSIS 460	Operational Security Architecture	3
CSIS 475	Mobile Device Security	3
CSIS 480	Intro to Digital Forensics	3
CSIS 485	Intro to Malware Reverse Engineering	3
CSIS 465	Secure Programming Practices	3
	General Education	44
	Major	76
	Total	120

Table 4. Year 3 and Year 4 Curriculum

** Upper Division General Education

The integration of business principles equips students with essential skills in strategic thinking, project management, and communication, enabling them to align cybersecurity initiatives with broader organizational goals. Courses on governance, legal frameworks, and ethical considerations further enrich students' understanding of the societal and institutional implications of cybersecurity.

This holistic approach cultivates professionals who are not only technically proficient but also capable of making informed decisions within the context of business operations, legal constraints, and human factors. As a result, graduates are uniquely prepared to assume leadership roles and effectively contribute to cybersecurity efforts in a variety of sectors, including government, healthcare, finance, and critical infrastructure.

4.0 Strategic Focus Beyond Technical Proficiency

While many cybersecurity programs focus heavily on developing tactical, hands-on skills such as configuring firewalls, conducting penetration tests, or managing incident response, Grossmont College's program distinguishes itself by incorporating a strategic breadth into its curriculum. This approach recognizes that technical proficiency alone is not sufficient in today's complex and evolving threat landscape.

Students are taught not only how to execute cybersecurity tasks, but also how to think critically and strategically about security across the entire enterprise. The curriculum emphasizes the design and implementation of comprehensive security frameworks, the alignment of cybersecurity initiatives with organizational objectives, and the anticipation of future threats in the context of business continuity and risk management. Key topics include cybersecurity governance, long-term planning, budgeting for security investments, and measuring the effectiveness of security controls in achieving operational goals.

Through this strategic emphasis, students gain a deep understanding of how cybersecurity functions as a core component of organizational resilience and success. They learn to evaluate and influence policies, lead cross-functional teams, and make informed decisions that balance security, usability, and cost. These capabilities prepare graduates to take on leadership roles such as cybersecurity analysts, risk managers, compliance officers, and security architects—positions that require a vision beyond immediate technical challenges.

By cultivating both technical skills and strategic insight, Grossmont College ensures its graduates are not just implementers of security solutions but also architects of

organizational defense strategies who can shape the cybersecurity posture of an enterprise from the top down.

Grossmont College Computer Science and Cybersecurity Organization was also established to provide leadership opportunities, and a space for tech hobbyists and other career-oriented computer science and cybersecurity majors to come together, to collaborate, and to have a place where they felt they belonged. They compete in cyber competitions, work on technical group projects, and have industry guest speakers. For example, they have competed in the SoCal Cyber Cup and have succeeded in beating all Southern California Community Colleges in the cyber competition, bringing home the 1st place trophy and $5,500 award to Grossmont College.

5.0 Strong Regional Demand and Workforce Alignment

Grossmont College's cybersecurity program is uniquely positioned to respond to robust and growing regional workforce needs. The San Diego County area has emerged as a key hub for cybersecurity activity, fueled by a concentration of defense contractors, technology firms, healthcare organizations, and research institutions—all of which require sophisticated cybersecurity measures to protect critical data and infrastructure. Labor market analytics as shown below in Exhibit 1, consistently project a strong and sustained demand for skilled cybersecurity professionals throughout the region, making the program not only timely but strategically vital.

Exhibit 1: Number of Jobs for *Cybersecurity Occupations* in San Diego County (2022-2027)[2]

Occupational Title	2022 Jobs	2027 Jobs	2022 - 2027 Net Jobs Change	2022-2027 % Net Jobs Change	Annual Job Openings (Demand)
Computer Occupations, All Other	8,906	9,493	587	7%	769
Network and Computer Systems Administrators	3,867	4,083	216	6%	310
Information Security Analysts	1,503	1,793	290	19%	176
Computer Network Support Specialists	1,536	1,654	118	8%	146
Computer Network Architects	1,542	1,645	103	7%	120
Total	17,354	18,668	1,314	8%	1,521

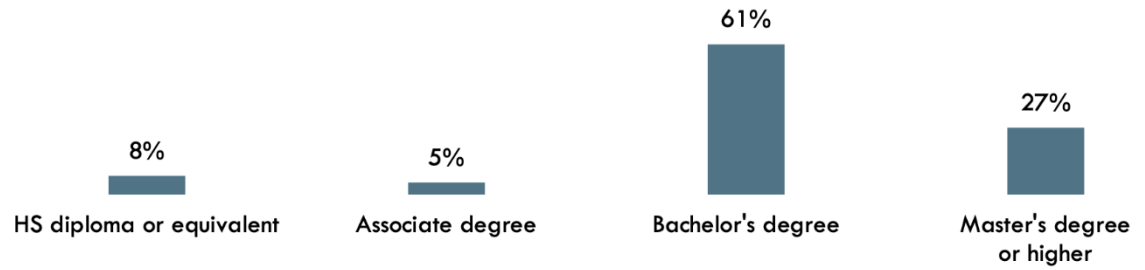
In addition to the above occupational titles with high annual job openings, other related occupational titles are included below that require a bachelor's degree.

- Security Analyst
- Network Security Engineer
- Incident Response Specialist
- Penetration Tester
- Security Consultant
- Cybersecurity Architect
- Cybersecurity Manager
- Cybersecurity Policy Advisor

The Grossmont College GSCyber program is designed to produce graduates who are not only technically proficient but also capable of filling leadership roles within cybersecurity teams, departments, and organizations. By addressing both operational and strategic competencies, the program prepares students for a wide range of career pathways, from security analysts and network defenders to cybersecurity managers and policy advisors.

Current data indicates that approximately 61% of cybersecurity-related job postings in San Diego County require candidates to possess at least a bachelor's degree as shown below in Exhibit 9b. This statistic highlights the increasing complexity of cybersecurity roles and the need for higher education pathways that prepare students with advanced knowledge, practical experience, and leadership capabilities. Grossmont College's program directly supports this need by offering a rigorous curriculum that aligns with both academic standards and employer expectations.

Exhibit 9b: Educational Requirements for *Cybersecurity Occupations* in San Diego County[20]



*May not total 100 percent due to rounding

Importantly, the current regional supply of graduates with a bachelor's degree in cybersecurity significantly lags employer demand. The current graduate rate of cybersecurity bachelor degrees is less than the number of jobs needing to be filled. In addition, a bachelor's degree is needed for a lot of federal government cybersecurity jobs.

This shortage underscores a critical workforce gap and presents a strategic opportunity for Grossmont College to emerge as a leading pipeline for qualified cybersecurity talent. By preparing students to meet these in-demand qualifications, the program not only enhances individual career prospects but also strengthens the region's cybersecurity infrastructure and economic resilience.

San Diego City College is the only community college to currently offer a bachelor's degree in cybersecurity in the San Diego region. For Fall 2025 semester admission, San Diego City College Bachelor's Degree in Cybersecurity had around 90 applications. They extended offers to only 55 students. As a result, there is significant demand for students to pursue a Bachelor's Degree in Cybersecurity. San Diego City College cannot meet this demand to produce cybersecurity professionals at the bachelor's level.

In partnership with local employers, industry advisory boards, and workforce development agencies, Grossmont College ensures that its program remains responsive to evolving industry needs. This close alignment between education and employment fosters a dynamic talent ecosystem where students can transition seamlessly from academic preparation to impactful careers in a high-growth, high-stakes field.

Members of the Grossmont College Cybersecurity Industry Advisory Board that approved the proposed curriculum are noted in Table 5 below.

Name	Company	Title
Huy Ly	Mejun	CEO
Keith Fernandez	San Diego Sheriff Dept	Network/CSS Manager
Daniel Najor	Big Watt Digital	Founder/Director/VP
MD Rana	Army Futures Command	Lead/SME Cyber/AI Innovation/R&D

Table 5. Grossmont College Cybersecurity Industry Advisory Board

6.0 Supportive Regulatory Environment

The launch of Grossmont College's cybersecurity bachelor's degree program is both timely and strategically aligned with recent developments in California's higher education policy. A pivotal milestone came with the passage and signing of Assembly Bill 927 (AB 927) by Governor Gavin Newsom, which grants California community colleges the authority to offer bachelor's degrees in high-need, workforce-aligned fields. This landmark legislation represents a major shift in the state's approach to public higher education, expanding access to four-year degrees and helping to close persistent gaps in workforce development.

By authorizing community colleges to confer bachelor's degrees, AB 927 addresses longstanding barriers related to affordability, capacity, and geographic accessibility—especially for students who are place-bound or financially constrained. Grossmont College's entry into this new academic tier is not only fully legitimized under this legal framework but is also directly supported by the intent of the legislation: to meet regional labor market needs through locally delivered, high-quality education.

For students, this means they can now pursue a bachelor's degree in cybersecurity, one of the most in-demand and fastest-growing fields—without incurring the high costs typically associated with four-year universities and especially, private institutions. For the region, it means a new, scalable talent pipeline that aligns with both state and national cybersecurity priorities.

Moreover, this regulatory shift positions Grossmont College as an innovator and leader within the California Community Colleges system. By leveraging the legislative framework provided by AB 927, the college is helping to redefine what accessible, career-focused higher education looks like in the 21st century—delivering programs that are affordable, responsive to industry needs, and designed to empower students to thrive in a rapidly evolving digital economy.

7.0 Program Proposal Checklist

In compliance with the Grossmont College Feasibility Review of Instructional Programs policy, the following elements are included in the Bachelor of Science in Strategic Cyber Defense Analysis (GSCyber) Program Proposal:

1. A letter from the area dean stating their support for the development of the new program.
    a. Completed and attached.

2. Title and description of the proposed program:
    a. List of planned awards in the program
        1. Bachelor of Science in Strategic Cyber Defense Analysis
    b. Program description summary
        1. At Grossmont College, the Bachelor of Science in Strategic Cyber Defense Analysis program is designed to be more accessible and affordable for community college students. It equips our graduates with a robust foundation in theoretical knowledge and practical skills that are directly applicable to the modern cybersecurity landscape. The comprehensive curriculum seamlessly integrates hands-on experience, industry-recognized certifications, and real-world scenario-based learning to prepare students for success in this rapidly evolving field.
    c. Program-level SLOs
        1. Develop proficiency in implementing and managing secure networks, systems, and software.
        2. Gain practical experience through lab work, internships, and real-world cybersecurity projects.
        3. Identify, analyze, and resolve cybersecurity threats and vulnerabilities.
        4. Prepare for key cybersecurity certifications such as CompTIA Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP).
        5. Understand legal, ethical, and regulatory aspects of cybersecurity.
        6. Effectively communicate cybersecurity concepts to both technical and non-technical audiences.
    d. Faculty assigned to the program
        1. Full time faculty: Hau Nguyen, Philip Bell.
        2. Part time faculty: Ahn Nuzen.

3. Fit with Institutional Strategic Plan and Mission:
    a. The program supports Grossmont's mission to provide workforce-aligned education and addresses a critical employment gap in cybersecurity at the bachelor's level.
    b. A baccalaureate degree program, specifically a Strategic Cyber Defense Analysis (GSCyber) program, aligns well with both Grossmont College's mission and its institutional strategic plan. The college's mission is to "create clear and accessible pathways to degrees and jobs leading to social and economic mobility for our students". A baccalaureate degree program, particularly in a field like cybersecurity, directly contributes to this mission by offering advanced educational and career opportunities. Furthermore, the college's primary strategic goal is to strive for educational excellence, and a well-designed baccalaureate program would align with this goal by providing higher-level learning and completing students' educational goals.
    c. Per Vision 2030: A Roadmap for California Community Colleges.
        1. Outcome 2: Baccalaureate attainment. Increase with equity, the number of California community college students attaining a baccalaureate degree.
        2. Outcome 2a: Increase with equity, the number of California community college students who ultimately earn a bachelor's degree.
        3. Benchmark: Use the new data sharing agreements with the University of California (UC) and California State University (CSU) systems to build this metric and set initial benchmark.
        4. Outcome 2c: Increase with equity the number of California community college students who earn a community college baccalaureate.
        5. Benchmark: By 2030, the number of California community college students who earn a community college baccalaureate will increase by 30%.

4. Proposed implementation date:
    a. Fall 2026.

5. Explanation of the resources available to support the program:
    a. Funding and Financial Aid:
        1. Federal Student Aid (FAFSA)
    b. State and Institutional Funding:
        1. Potential state funding to support baccalaureate programs.
        2. May also allocate internal funding.
    c. Academic Support Services:

1. Robust Computer Science and Information Systems (CSIS) Department Tutoring program.
2. Library
3. CS and Cyber Club

d. Technology Support:
    1. Technology support, including distance education support; online and hybrid programs.
e. Advising and Counseling:
    1. Academic advising and counseling services
f. Simulation Laboratories:
    1. Current simulation labs provide a safe and controlled environment for students to practice cybersecurity skills.
g. Student Support Services:
    1. Career Services. Career counseling and job placement services to help students find employment after graduation.
h. Disability Services:
    1. Accommodations for students with disabilities
i. Mental Health Services:
    1. Mental health support services, including counseling and crisis support, to help students manage stress and well-being.
j. Military and Veteran Services
k. Curriculum Development
l. Admissions and Records
m. Faculty Development:
    1. Provide faculty with professional development opportunities to help them stay up to date on best practices and research.

6. Anticipated new cost:
    a. New Faculty
        1. First year: additional 2 full-time CSIS faculty, 1 full-time Counselor, and 4 Adjunct part-time faculty.
            i. Existing Faculty: 1 full-time faculty and 4 Adjunct part-time faculty.
        2. Second year: an additional 1 full-time faculty and 3 Adjunct part-time faculty.
    b. Infrastructure Needs
        1. 20% hardware expansion of computer labs, especially in the ability to create virtual environment for students to practice in virtual sandboxes.
    c. Curriculum development and refinement process.
    d. State application submission process.

e. Administrative costs to prepare two-year college to become four-year college: student financial aid, staff, facilities, etc.

7. List of all comparable or closely related programs:
   a. San Diego City College: BDP in Cyber Defense
   b. CSU San Marcos: Online only BS in Cybersecurity
   c. National University: BS in Cybersecurity (private)
   d. No BDP program at University of San Diego; only a master's program (private)
   e. No BDP program available at San Diego State University or UC San Diego

8. Justification of need for the new program (support university transfer to a particular major, labor market demand, etc.)
   a. Career options and/or transfer information
      1. Information Security Analyst
      2. Network Security Engineer
      3. Incident Response Specialist
      4. Penetration Tester
      5. Security Consultant
      6. Cybersecurity Architect
   b. Transfer support to Master's and PhD program in Cybersecurity
      1. Program meets Master's and PhD program articulation
   c. High regional demand: 1,521 new jobs annually in San Diego County in cybersecurity.
   d. High educational requirements: 61% of bachelor's degree needed for Cybersecurity Occupations in San Diego County.
   e. Lack of comparable in-person BDP programs at public universities.
   f. Career pathway support for cybersecurity.

9. A request for the formation of a Program Feasibility Taskforce to review the program proposal and make their recommendation.
   a. Completed.

10. Based upon the recommendation of the Program Feasibility Taskforce, the newly proposed program will move forward in the established curriculum review process.
    1) In-progress. Bachelor of Science in Strategic Cyber Defense Analysis (GSCyber) curriculum already has been developed and submitted to the curriculum committee.

8.0 Baccalaureate Degree Program Application Checklist

1) **What is the name of your proposed baccalaureate degree program?**
   Bachelor of Science in Strategic Cyber Defense Analysis

2) **What is the CIP Code of your proposed baccalaureate degree program?**
   11.0101 Computer and Information Sciences, General

3) **What is the name of your current associate degree program?**
   Associate of Science in Cybersecurity and Networking

4) **What is the primary TOP code for your current associate baccalaureate degree program? List no more than two.**
   0701.00 Information Technology, General

5) **ACCJC Substantial Change Approval**. Our district has applied for or received substantive change approval to offer the proposed baccalaureate degree program through the Accrediting Commission for Community and Junior Colleges (Ed. Code § 78042(a).) Note: While an application may be submitted prior to receiving ACCJC approval, the Chancellor's Office will only provide provisional approval until evidence of ACCJC approval is received. If you have already received approval from ACCJC, please provide your substantive change letter. – Not yet

6) **Review Category.**
   Full Review: New programs being considered for the first time.

7) **Non-Duplication Analysis Form**. – In Progress

8) **Evidence of Workforce Need and Demand.** Please complete the attached *Summary of* W*orkforce Need and Demand Template* to support the necessity for a four-year degree for your proposed program. – In Progress

9) **Labor Market Assessment.** Upload the required BDP Labor Market Assessment Report produced by your regional Center of Excellence. The assessment should document relevant workforce data and information about the occupations your program will prepare students to enter. The report must be submitted in its original form as an attachment. The report must include the following: - In Progress

a. **State Data Analysis**

- **Educational Requirements and Certifications:** Summarize the educational requirements, licensing, or third-party certifications needed for up to five identified occupations that the program targets as entry-level positions.

- **Work Experience:** Detail the typical work experience preferred for these occupations.

- **Degree Alignment:** Analyze whether the proposed degree aligns with educational requirements for the target occupations.

- **Preference for Bachelor's Degree Holders:** Evidence that employers prefer entry-level workers who hold a bachelor's degree in the proposed field.

- **Salary Differentials:** Evidence that employers offer higher salaries to entry-level workers with a bachelor's degree compared to those with an associate degree or no degree.

- **Outlook:** Provide projected 10-year and annual average job openings for the target occupations in California.

b. **Regional Data Analysis**

- **Historical Employment Trends:** Analyze historical employment trends for the target occupations in the region.
- **Projected Demand:** Detail projected 10-year and annual average job openings to establish demand for workers in the region.
- **Projected Supply:** Include historical and projected annual average graduates from similar higher education programs in the region, factoring in the anticipated completions from your new program.
- **Occupational Wages:** Compare entry-level wages (25th percentile) for the target occupations against the living wage requirement for a single adult and a single parent with one child in the region.

c. Center of Excellence Director Letter of Certification

- The report must include a signed letter of certification from the Center of Excellence director that this labor market assessment was conducted specifically for the proposed baccalaureate degree program using the Center of Excellence Baccalaureate Degree Program Labor Market Assessment protocols.

10) Evidence of Regional Consultation. – Completed

11) Optional Attachments:

a. Letters from Partners or Employers
b. Committee meeting minutes or recommendations. – Completed
c. Other evidence to support the need for your proposal

12) Program Description. – Completed.

13) Program Quality and Curriculum Design. – In Progress

14) Administrative and Funding Plans. Please complete and upload the *Administrative and Funding Plan template*. This document asks what led to the development of the proposed degree, how it fits in with the higher education master plan, faculty qualifications, student support services, impacts to resources (physical, technological, equipment, and financial), and a budget showing the institution's capacity to start and maintain the proposed program. - To be completed.

15) The Chancellor's Office recommends that districts adopt policies and practices consistent with the Budgeting Best Practices published by the Government Finance Officers Association (GFOA). Foremost among these best practices is consideration of financial reserves. The Chancellor's Office recommends that districts adopt formal policies to maintain sufficient unrestricted reserves with a suggested minimum of two months of total general fund operating expenditures. See Memo FS 22-03 Fiscal Forward Portfolio and Budget Architecture and Development Recommendations. Please provide a copy of your district's formal policy to maintain unrestricted reserves. – To be completed.

9.0 Dean Letter of Support

GROSSMONT COLLEGE

Office of the Dean of Career Technical Education/Workforce Development
8800 Grossmont College Drive, El Cajon, CA 92020-1799
Phone: 619-644-7158 Fax 619-644-7970

May 1, 2025

I am pleased to offer my strong support for Grossmont College's proposal to establish the Bachelor of Science in Strategic Cyber Defense Analysis (GSCyber) under the California Community Colleges Baccalaureate Degree Program (BDP).

Grossmont College has committed substantial time and resources toward the development of this program. My office has secured funding to support the duration of the development phase, and we have already deployed multiple personnel to advance efforts related to the bachelor's degree initiative over the past year. As a result, we are well-positioned to launch and sustain this program successfully.

Since Governor Gavin Newsom signed Assembly Bill 927 on October 6, 2021, the BDP has authorized the California Community Colleges Board of Governors to approve up to 30 new baccalaureate degree programs annually. This legislation aims to expand affordable access to four-year degrees that are uniquely tailored to meet regional workforce demands without duplicating programs offered by the California State University or University of California systems. The BDP emphasizes equity, economic mobility, and closing educational attainment gaps by providing local pathways to bachelor's degrees in high-demand fields such as cybersecurity.

Grossmont College has responded to this opportunity with a rigorous feasibility process that evaluated potential bachelor's degree offerings based on projected job growth, workforce alignment, and program feasibility. After thorough review, the college selected the GSCyber program in May 2024, proposed by the Division of Career Technical Education and Workforce Development.

The GSCyber program is distinguished by its comprehensive curriculum that integrates advanced technical skills—such as network defense, threat analysis, and ethical hacking—with critical training in policy, governance, risk management, and organizational leadership. It aligns closely with the Department of Defense Cyber Workforce Framework (NICE) and the CAE-CD Knowledge Units, ensuring graduates gain nationally recognized competencies relevant to both public and private sector cybersecurity roles.

This program exemplifies the mission of the BDP by strategically addressing a critical regional workforce gap, empowering students with high-demand skills, and strengthening the local talent pipeline. It supports California's broader economic and security objectives by preparing graduates to meet the evolving challenges in cybersecurity.

I fully endorse Grossmont College's GSCyber Bachelor of Science degree as a vital addition to the California Community Colleges Baccalaureate Degree Program and a significant step forward in expanding equitable, affordable, and workforce-aligned higher education opportunities in our region.

Sincerely,

Javier Ayala, Ph.D.

Dean of Career Education & Workforce Development
Grossmont College

10.0 Citations

[1] https://www.cccco.edu/About-Us/Chancellors-Office/Divisions/Educational-Services-and-Support/What-we-do/Curriculum-and-Instruction-Unit/Curriculum/Baccalaureate-Degree-Program

[2] https://www.cccbachelordegrees.org

[3] https://www.cccco.edu/About-Us/News-and-Media/Press-Releases/2024-six-new-bachelors-degree-progams

[4] https://icangotocollege.com/bachelors-degree-program

[5] https://www.cccco.edu/-/media/CCCCO-Website/About-Us/Board-of-Governors/Meeting-schedule-and-agenda/January-2016-Agenda/Files/Attachment32BAHandbook2.ashx?la=en&hash=9E55D7280D8F060E8DE2FCDC3A9DE02E1BCCB381

[6] https://trackbill.com/s3/bills/CA/2021/AB/927/analyses/senate-education.pdf

[7] https://mysdccd.atlassian.net/wiki/spaces/SBDM/overview

[8] https://www.ccleague.org/advocacy/baccalaureate-degree-programs/

[9]https://ahed.assembly.ca.gov/sites/ahed.assembly.ca.gov/files/hearings/13.%20AB%20927%20Analysis%202021.pdf

[10] https://www.insidehighered.com/news/2021/10/18/california-community-colleges-expand-baccalaureate-programs

[11] https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf