



GROSSMONT
COLLEGE



Career Technical Education
Workforce Development

Grossmont Cybersecurity (GSCyber) Program Overview Bachelor of Science Degree in Strategic Cyber Defense Analysis

Ahn Nuzen, Hau Nguyen, Philip Bell

Computer Science and Information Systems (CSIS) Department

BACKGROUND & GOAL

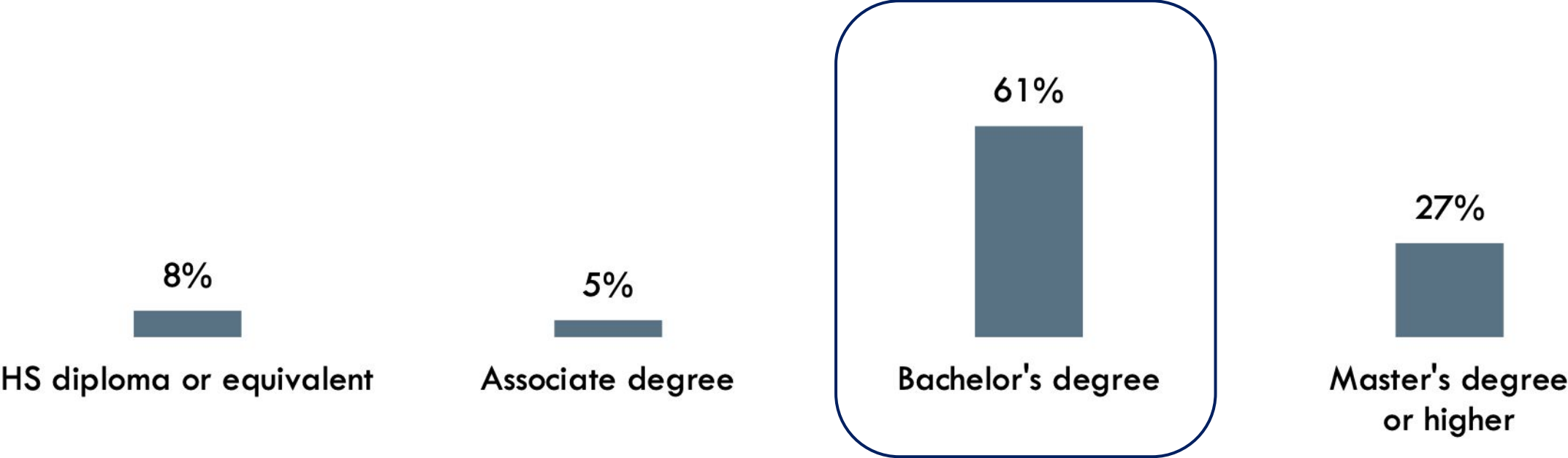
- California Governor Gavin Newsom signed AB 927 (Medina) authorizing the Community College Baccalaureate Degree program BDP.
- Accessible and affordable for community college students to obtain BS degrees and be eligible for a broader array of employment opportunities in Nursing, Biomanufacturing, Automotive technology, and Cybersecurity.
- Grossmont College's Committee approved the Cybersecurity program in May 2024. The committee considered job growth, duplication with existing institutions, and the feasibility of transitioning from a 2-year to a 4-year degree.

Labor Market Information and Analysis

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

Exhibit 9b: Educational Requirements for *Cybersecurity Occupations* in San Diego County²⁰



*May not total 100 percent due to rounding

Market Needs

	Institution	Program Type	Status
1	San Diego City Cyber Defense	BDP program	First cohort 2024
2	California State University at San Diego	MS Cyber Management	No BS program
3	California State University at San Marco	BS Online Only	First cohort 2025
4	University of San Diego (Private)	Master Cyber	No BS program
5	National University (Private)	BS	On going



GSCyber Program Highlights

1. Utilize DoD Cyber Workforce Framework Alignment: Ensure students possess the industry-recognized KSAs sought by employers in the field of defensive cyber operations.
2. Strategic Approach: Go beyond tactics to master the strategic planning and implementation of cybersecurity measures, inclusion of Business courses.
3. Comprehensive Curriculum: Focus on hands-on learning to prevent, detect, respond to, and recover from cyber incidents through a blend of policies, procedures, business, and cutting-edge technologies.

B.S. in Strategic Cyber Defense Analysis – Plan of Study

Course	Title	Units
	Year 1: Foundation Knowledge and skills	
CSIS 110	Principles of Information Systems	4
CSIS 113	Introduction to Linux	3
CSIS 120	Computer Maintenance and A+ Certification	3
CSIS 121	Introduction to Cybersecurity	3
CSIS 125	Network + Certification	2
CSIS 130	Windows Server: Installing & Configuring	2
CSIS 250	Introduction to Python Programming	3
English 120	College Composition and Reading	3
PSC-110	Introduction to Physical Sciences	3
PSC-111	PSC-110 LAB	1
PHIS 142	Ethics of Technology	3
		30
Course	Title	Units
	Year 2: Intermediate Cybersecurity Concepts	
CSIS 132	Intro to Web Development	3
CSIS 230	Windows Server: Administering	2
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
PHOS-180	Introduction to Public Policy	3
Math 160	Elementary Statistics	4
BUS-125	Business Law	3
		31

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 330	Intrusion Detection and Analysis	3
CSIS 380	Wireless Security and Vulnerabilities	3
		18
Course	Title	Units
	Year 4: Professional Development and Specialization	
CSIS 470	Strategic Cyber Defense and Analysis Capstone	3
	15 elective units below	15
CSIS 400	Cyber Intelligence & Incident	3
CSIS 410	Enterprise Operation Continuity (Cyber Response and Recovery)	3
CSIS 430	Cyber Security Project Management	3
CSIS 440	Infrastructure and Supply Chain Vulnerabilities	3
CSIS 450	Cloud Computing Security	3
CSIS 460	Operational Security Architecture	3
CSIS 465	Secure Programming Practices	3
CSIS 475	Mobile Device Security	3
CSIS 480	Intro to Digital Forensics	3
CSIS 485	Intro to Malware Reverse Engineering	3
	General Education	23
	Major	97
	Total	120

DOD Cyber Workforce Framework

CAE Cyber Defense (CAE-CD) Program Guidance - 2024

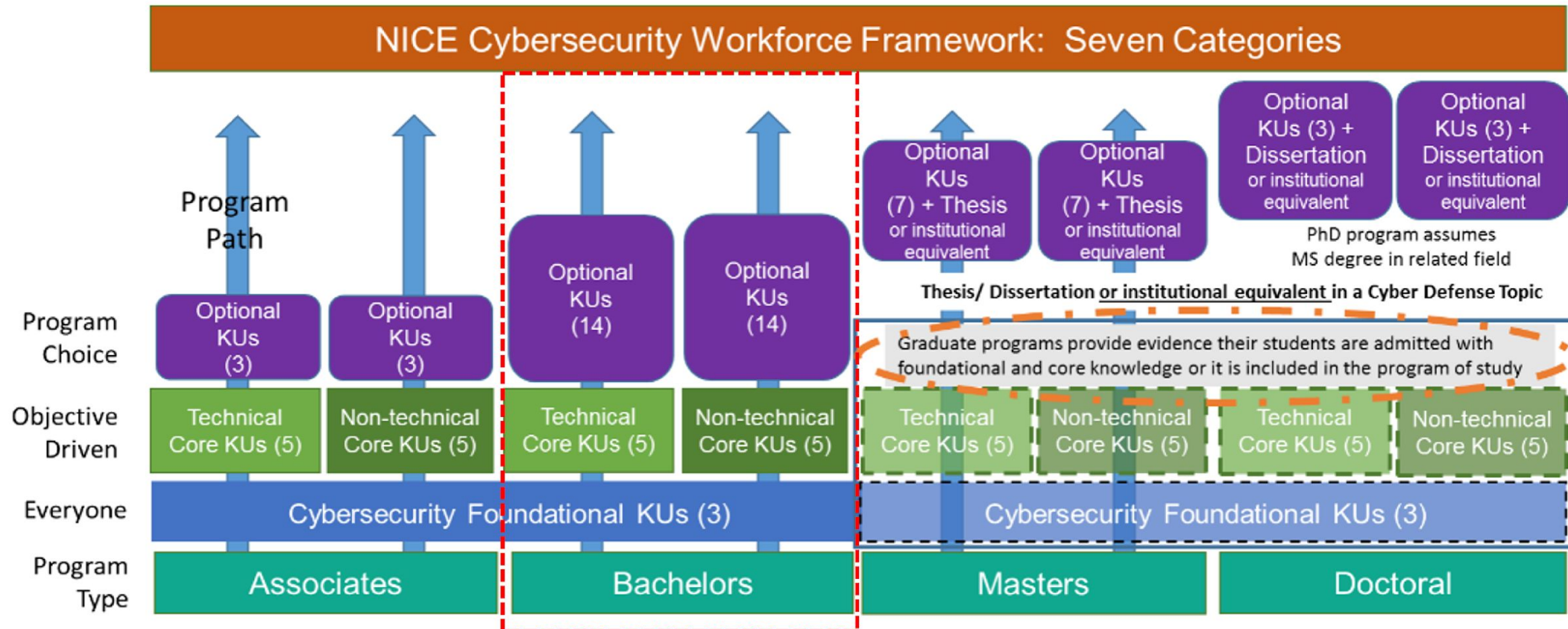


Figure 4. CAE-CD Knowledge Units Alignment Requirements
https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf
Academic Senate Nov 18, 2024

Task Descriptions and Percent Completion

For Grossmont BS Cyber to be ready for review and approval in Cycle 3 Jan 2025, the following preliminary tasks need to be completed before Jan 2025:

1. Preliminary Research and information a) gathering, Team, structure, b) understanding regulations regarding Assembly Bill No. 927, what we are allowed to do and not Todo, and c) an approach to our BS Cyber curriculum that aligns with the goal of the program – **95%**
2. Program Prerequisite coursework for potential students, course #, name, units, brief descriptions. Including upper-division courses that we don't offer now – **95%**
3. Complete course outlines submittable to the curriculum GBSCyber program – **95%**
4. Grossmont College Curriculum process – **Ready waiting for submission window.**

GROSSMONT
COLLEGE



Career Technical Education
Workforce Development



Thank you Questions?