Program Contacts: Please provide the name and email address for each individual requested below

Primary contact name
Nicole Kontak

Primary contact email address
nicoler@arizona.edu

Person who will serve in role of Director of Undergraduate Studies (DUS) for the certificate (This is not always the same as the DUS for affiliated programs or head of managing academic unit)
-

Email address
-

If known, list the members of the certificate oversight committee for this certificate. Note: undergraduate certificate oversight committees shall consist of a minimum of 3 members, 2 of which are faculty and at least one of the 2 is participating faculty in the certificate program. The oversight committee is responsible for 1) qualifications of participating faculty, 2) coordination of admissions recommendations with the Office of Admissions, and 3) curricular changes.
-

Name of Admissions contact
-

Email address
-

Name of Graduate Program Coordinator
-

Email address
-

Name of Director of Graduate Studies
-

Email address
-

Name of Graduate College Degree Counselor
-

Email address
-

Plan Administration

Offering College
College of Information Science

Offering Department(s) (If multiple offering departments, list each one)	Department Ownership Percent	Is the Academic Owner the same as the Budget Owner?
Applied Science	Applied Science - 100%	Yes

Budget Office Owner & Percent Ownership - CUSTOM

-

College Rationale: In consultation with proposing unit's college-level administration, describe how the proposed academic program fits within the mix of programs currently offered by the college, and how it advances the overall mission of the college and university.

Prior to Fall 2022, all BAS degrees offered by CAST had general education, foundation, and upper division requirements distinct from the curriculum of all other bachelor's degrees at the University of Arizona. Starting in Spring 2022, when the university updated the general education requirements, the BAS degrees followed, and curricular changes were made to reduce the upper division requirements of the BAS degrees from 60 to 42, in alignment with BA and BS degree requirements. Now, BAS degrees are consistent
with the curricular requirements of other BA and BS degrees across the university, including the acceptance of transfer credit.

Year 1	Year 2	Year 3
716	895	1119

What concrete evidence/data was used to arrive at the numbers?

Current enrollment in the Engineering emphasis area of BAS Cyber Operations was used as a starting point and the percentage student enrollment increase from Spring 2024 to Spring 2025 for the BAS Cyber Operations was estimated at 25%.

Print On Transcript	Transcript Description	Transcript Indent (New)
Yes	Major in Cyber Operations	-

Print On Diploma	Diploma Description	Diploma Indent (NEW)
Yes	Cyber Operations	-

CIP Code (required)

Refer to The National Center for Education Statistics to determine appropriate 6-digit CIP code

29.0207

NSC Classification

-

Program Length Type
Years

Program Length in Years
4

If Program Length is not 2, 4, or 6 years, please explain:
-

SULA Special Program
-

Evidence of Market Demand

Please provide an estimate of the future state-wide and national demand for graduates of the proposed academic program. Please specify the source (e.g., Lightcast; Jobs EQ; US Department of Labor) of workforce demand data and detail the assumptions that underpin these projections. Curricular Affairs can provide a job posting/demand report (from O*NET) by skills/keywords/CIP code of the proposed program; contact curricular_affairs@list.arizona.edu to request the report if needed for your proposal. If job market data is unavailable or not applicable, please explain why and elaborate another justification for the proposed program.

Based on Lightcast data for CIP 29.0207 Cyber-Security

National: Demand for graduates is likely to increase 20–30% over the next decade in specialized cyber warfare roles.

This is a specialized, high-value niche within cybersecurity.

Although the current undergraduate pipeline is small, national defense trends point to strong, sustained growth in demand for these graduates—especially in defense-centric states (e.g. Virginia, Maryland, California, Texas, Arizona, Florida, South Carolina, Colorado and Washington, based on the presence of federal installations, defense-related, industries, contracting, etc).

Being a niche specialization, few undergrad programs exist—creating higher demand per graduate.

Government roles (DoD, US Cyber Command, NSA, FBI), defense contractors, and private sector threat teams are tapping these graduates.

Institutions that launch or scale Cyber/Electronic Operations programs stand to fill a critical skills gap and align with long-term workforce needs.

Similar Programs Offered at Arizona Public Universities

Are there similar programs at the University of Arizona?	List all similar programs at the same academic level currently offered at this institution	Number of Students	Accredited
Yes	BAS, Cyber Operations	1651	Yes
Are there similar programs at Arizona State University?	**List all similar programs at the same academic level currently offered at this institution**	**Number of Students**	**Accredited**
Yes	BS, Info Technology-Cybersecurity	700	Yes

Are there similar programs at Northern Arizona University?
No

Peer Comparison

Select three peers (if possible/applicable) for completing the comparison chart from ABOR-approved institutions, AAU members, and/or other relevant institutions recognized in the field.

Use Peer Comparison Chart from the Curricular Affairs website. The comparison programs are not required to have the same degree type and/or title as the proposed UA program. Information for the proposed UA program must be consistent throughout the proposal documents. Minors and Certificates may opt to include only 2 peer comparisons.

Peer_comparison_Cyber_Ops_(2) (1).docx

Budget Projection

Complete and upload the budget projection form found here.

Contact your department / college finance manager for more information.

Budget_projection_Cyber_Ops_(2) (1).xlsx

Campus

Campus

Campus
University of Arizona - Main

Sub Plan Required
No

Locations

Location
Tucson

First Admit Term	Last Admit Term	Teach Out Term
-	-	-

Campus
Arizona Online

Sub Plan Required
No

Locations

Location
Online

First Admit Term	Last Admit Term	Teach Out Term
-	-	-

Learning Outcomes (Required three minimum)

Name
Students will evaluate and apply legal and ethical principles to make informed and responsible decisions in complex cybersecurity scenarios.

Tags
-

Concepts

1. Professional ethics codes in cybersecurity 2. Legal frameworks governing cybersecurity activities such as CFAA, wiretapping laws, and international regulations 3. Digital rights and privacy principles 4. Jurisdictional considerations in cyber investigations 5. Chain of custody and evidence handling procedures 6. Whistleblower protections and reporting obligations 7. Conflict of interest identification and management 8. Cultural sensitivity in global cybersecurity operations 9. Responsible disclosure practices 10. Professional boundaries and scope of authority

Assessment

1. Ethics case study analysis addressing real-world cybersecurity dilemmas 2. Role-playing simulation of ethical decision-making in crisis situations 3. Professional code of conduct development project 4. Student exit survey

Competencies

1. Evaluate ethical implications of cybersecurity decisions and actions
2. Apply legal constraints to cybersecurity investigation and response activities
3. Assess potential conflicts between security needs and individual rights
4. Analyze jurisdictional requirements for cross-border security operations
5. Synthesize ethical principles with practical security requirements
6. Critique cybersecurity practices for legal and ethical compliance
7. Construct ethical decision-making frameworks for complex scenarios

Measures

1. Rubric scores on case study analysis measuring ethical reasoning quality, legal compliance awareness, stakeholder consideration 2. Behavioral observation checklist during role-playing exercises 3. Completeness and quality assessment of professional code development 4. Responses to student exit survey

Name

Students will evaluate network architectures, functions, and protocol implementations to assess security risks.

Tags

-

Concepts

1. Network protocol stacks and layered models 2. Network topologies and infrastructure components 3. Routing and switching principles 4. Network security protocols and implementations 5. Virtualization and containerization technologies 6. Distributed systems architecture 7. Network services and applications

Assessment

1. Technical architecture diagram creation with detailed component explanations 2. System analysis report examining network security implications 3. Hands-on lab exercises configuring and documenting network components 4. Student exit survey

Measures

1. Rubric scores on architecture diagrams measuring technical accuracy, completeness, security consideration integration 2. Rubric scores of highly technical programming lab assignments 3. Quality assessment of system analysis reports using technical writing criteria 4. Lab completion rates and accuracy of system configuration tasks 5. Responses to student exit survey

Competencies

1. Evaluate network architecture designs for security vulnerabilities
2. Assess network protocol implementations for security weaknesses
3. Synthesize understanding of system architecture with cybersecurity requirements
4. Construct detailed technical documentation of network architectures

Name

Students will analyze the motivations, methods, and goals of cyber threat actors to develop defensive strategies.

Tags

-

Concepts
1. Threat actor typologies such as nation-state, criminal, hacktivist, insider, and script kiddie 2. Motivational frameworks such as financial gain, political objectives, espionage, ideology, and personal grievances 3. Attack methodologies and techniques such as MITRE ATT&CK framework 4. Threat intelligence and attribution analysis 5. Social engineering and psychological manipulation tactics 6. Advanced Persistent Threat campaign structures 7. Cybercriminal ecosystem and underground markets 8. Geopolitical influences on cyber operations 9. Threat actor evolution and adaptation patterns 10. Supply chain and third-party attack vectors

Measures
1. Rubric scores on case study analysis (measuring accuracy of motivation assessment, method identification, goal articulation) 2. Quality ratings of threat intelligence reports using industry standards 3. Performance assessment during tabletop exercises (decision-making accuracy, strategic thinking) 4. Responses to student exit survey

Assessment
1. Threat actor case study analysis examining real-world attack campaigns 2. Threat intelligence report creation profiling specific actor groups 3. Tabletop exercise simulating threat actor decision-making processes 4. Student exit survey

Competencies
1. Analyze threat actor behavior patterns and motivations
2. Evaluate different attack methodologies for their strategic purposes
3. Apply threat intelligence to predict likely threat actor actions
4. Assess organizational vulnerabilities from threat actor perspectives
5. Synthesize motivational analysis with defensive strategy development
6. Compare threat actor capabilities and resource limitations
7. Construct threat actor profiles based on observable behaviors and techniques

Program Requirements

Total units required to complete degree
120

Upper-division units required to complete degree
42

Foundation courses: Second language
2nd semester proficiency

General education requirements: 32 units

Pre-admission expectations (i.e. academic training to be completed prior to admission)
-

Graduate non-degree status units permitted?
No

If yes, list how many
-

List any special requirements to declare or gain access to this major (completion of specific coursework, minimum GPA, interview, application, etc.)
N/A

Major units required (includes core and required electives; excludes supporting coursework)
48

Upper-division units required in the major
42

Residency units to be completed in the major
30

Minimum total units required
-

Minimum upper-division units required
-

Total transfer units that may apply to minor
-

Minimum total units required
-

Minimum upper division units
-

Total transfer units that may apply to the certificate
-

List any special requirements to declare/admission to this minor (completion of specific coursework, minimum GPA, interview, application, etc.)
-

Required supporting coursework
Courses that do not count towards major units and major GPA, but are required for the major. Courses listed must include prefix, number, units, and title. Include any limits/restrictions needed (house number limit, etc.). Provide course use form from home department for courses not owned by your department

CYBV 101 Principles of Cyber Operations I (3) (New)

CYBV 102 Principles of Cyber Operations II (3) (New)

CYBV 103 Scripting for Cyber Operations I (3) (New)

CYBV 104 Scripting for Cyber Operations II (3) (New)

MATH XXX (3) *Course being identified with the math department

Major requirements

List all major requirements including core and electives. If applicable, list the emphasis requirements for each proposed emphasis*. Courses listed count towards major units and major GPA. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.). Provide course use form from home department for courses not owned by your department.

CORE (18 CREDITS)

CYBV226 Networking Fundamentals Networking for Cyber Operations I (3) (MOD)

CYBV 228 Networking for Cyber Operations II (3) (New)

CYBV329 Cyber Ethics Cyber Ethics (3)

CYBV 333 Cryptography for Cyber Operations (3) (New)

NETV379 Cloud Computing Cloud Computing (3)

CYBV 400 Active Cyber Defense (3)

CAPSTONE (3 CREDITS)

CYBV 498 Capstone (3)

EMPHASIS: ARTIFICIAL INTELLIGENCE (27 CREDITS)

APCV 302 Statistics in Information Age (3)

APCV 361 Data Analysis and Visualization (3)

APCV 371 Artificial Intelligence in Cyber Operations I (3) (MOD)

APCV 471 Artificial Intelligence in Cyber Operations II (3) (MOD)

APCV 483 Machine Learning in Cyber (3)

APCV 485 Deep Learning in Cyber (3)

CYBV 473 Violent Python (3)

CYBV 474 Advanced Analytics for Security Operations (3)

ISTA 322 Data Engineering (3)

EMPHASIS: SECURITY (27 CREDITS)

CYBV 310 Intro to Sec Prog 1 (3)

CYBV 311 Intro to Sec Prog 2 (3)

CYBV 470 C Programming (3)

CYBV 479 Wireless Networking (3)

CYBV 388 Cyber Investigation and Forensics (3)

CYBV 454 Malware Threat and Analysis (3)

CYBV 480 Cyber Warfare (3)

CYBV 489 OS for Security Professionals (3)

CYBV 471 Assembly (3)

Major requirements

List all major requirements including core and electives/selectives. If applicable, list the emphasis requirements for each proposed emphasis*. Thesis and non thesis options should be listed as separate emphases. Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.). Provide course use form from home department for courses not owned by your department.

Minor requirements

List all required minor requirements including core and electives. Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.). Provide course use form from home department for courses not owned by your department.

Certificate requirements

List all certificate requirements including core and electives. Courses listed must include **course prefix, number, units, and title**. **Mark new coursework (New)**. Include any limits/restrictions needed. Provide course use form from home department for courses not owned by your department.

Research methods, data analysis, and methodology requirements?
No

If yes, provide description
-

Internship, practicum, applied course requirements
No

If yes, provide description
-

Senior thesis or senior project required
No

If yes, provide description
-

Master thesis or dissertation required?
No

If yes, provide description
-

Is substitution of required or elective courses permitted at advisor's discretion?
No

If yes, provide description
-

May units earned for the certificate be applied to affiliated graduate programs?
Note: There is no University maximum on the number of units from a certificate program that may also apply toward a UA degree program, subject to time limitations for degree programs.

If yes, list how many
-

Minor: Optional or Required?
Optional

Can students earning a second degree or major use the second degree/major to satisfy the required minor for this major?
No

Will this major offer a minor with the same name?
No

Minor requirements
-

Minimum total units required for minor
-

Any restrictions on multiple use of courses?
No

If yes, provide description
-

Additional requirements (provide description and/or attach file)
n/a

Admissions (Applicable to Undergraduate Majors and Certificates only)

Add to undergraduate admissions application?
Yes

Add to Next Steps Center for orientation major changes?
Yes

Admit Type
First-Year, Transfer, Readmission

Admissions Criteria
General UA admisisons

If selective criteria, please elaborate
-

Emphases/Subplans (Applicable to Majors only)

Emphasis in Artificial Intelligence

Code
-

Name
AI

Long Name
Artificial Intelligence

Transcript Level
Print on Official

Evaluate Subplan
No

Transcript Description (e.g. Major in Public Relations)
Emphasis in Artificial Intelligence

Print On Transcript
Yes

Diploma Description (e.g. Public Relations)
Artificial Intelligence

Print On Diploma
Yes

Emphasis in Security

Code
-

Name
Security

Long Name
Security

Transcript Level
Print on Official

Evaluate Subplan
No

Transcript Description (e.g. Major in Public Relations)
Emphasis in Security

Print On Transcript
Yes

Diploma Description (e.g. Public Relations)
Security

Print On Diploma
Yes

Subplan Campus & Locations (Applicable to Majors only)

Subplan Campuses

Subplan
AI

Subplan Campus
University of Arizona - Main

Subplan Locations

Subplan Location
Tucson

Subplan
AI

Subplan Campus
Arizona Online

Subplan Locations

Subplan Location
Online

Subplan
Security

Subplan Campus
University of Arizona - Main

Subplan Locations

Subplan Location
Tucson

Subplan
Security

Subplan Campus
Arizona Online

Subplan Locations

Subplan Location
Online

Dependencies

Instructional Modality

Select all that apply
In Person, Fully Online

New Administrative Use

Short Title
CYBROPSBS

Online campus
Yes

Status
Active

Display Plan in Public Catalog
No

Catalog Short Description
-

Catalog Display Name
-

Field Of Study
-

HEGIS Code
-

Plan Type (Admin)
-

First Term Valid
-

Learning Outcomes UA - CUSTOM
-

Catalog Image

-

Catalog Display Notifications

-

Allow Integration Sync To SIS
Yes

Additional Information

If necessary, provide any additional information that has not already been captured in the proposal. This could include the course use/collaboration form, addendum explaining/supporting the budget projection, other helpful information you did not already include in the proposal but that CA and faculty governance committees should be aware of.

-

THE UNIVERSITY OF ARIZONA

BUDGET PROJECTION FORM

Name of Proposed Program or Unit: BS Cyber Operations

	Projected		
	1st Year 2026 - 2027	2nd Year 2027- 2028	3rd Year 2028- 2029
METRICS			
Net increase in annual college enrollment UG	322	403	504
Net increase in college SCH UG	9,669	12,087	15,108
Net increase in annual college enrollment Grad			
Net increase in college SCH Grad			
Number of enrollments being charged a Program Fee			
New Sponsored Activity (MTDC)			
Number of Faculty FTE	3	6	9
FUNDING SOURCES			
Continuing Sources			
UG Revenue (online) 60% of growth	3,045,853	3,807,316	4,759,146
UG Revenue (main) 30% in-state; 10% out-of-state	433,188	541,485	676,856
Program Fee Revenue (net of revenue sharing)			
F and A Revenues			
Reallocation from existing College funds (attach description)			
Other Items (attach description)			
Total Continuing	**$ 3,479,041**	**$ 4,348,801**	**$ 5,436,002**
One-time Sources			
College fund balances			
Institutional Strategic Investment			
Gift Funding			
Other Items (attach description)			
Total One-time	**$ -**	**$ -**	**$ -**
TOTAL SOURCES	**$ 3,479,041**	**$ 4,348,801**	**$ 5,436,002**
EXPENDITURE ITEMS			
Continuing Expenditures			
Faculty	495,000	1,039,500	1,559,250
Other Personnel (advisors, program directors, etc.)			
Employee Related Expense (2-year start-up per faculty)	30,000	60,000	60,000
Graduate Assistantships			
Other Graduate Aid			
Operations (materials, supplies, phones, etc.)	6,000	12,000	18,000
Additional Space Cost			
Other Items (attach description)			
Total Continuing	**$ 531,000**	**$ 1,111,500**	**$ 1,637,250**
One-time Expenditures			
Construction or Renovation			
Start-up Equipment			
Replace Equipment			
Library Resources			
Other Items (attach description)			
Total One-time	**$ -**	**$ -**	**$ -**
TOTAL EXPENDITURES	**$ 531,000**	**$ 1,111,500**	**$ 1,637,250**
Net Projected Fiscal Effect	**$ 2,948,041**	**$ 3,237,301**	**$ 3,798,752**

THE UNIVERSITY OF ARIZONA

New Academic Program
PEER COMPARISON

Select two peers (if possible/applicable) from 4-year AAU members, and/or other relevant institutions recognized in the field. The comparison programs may have a different degree type and/or title as the proposed UA program. Details of the proposed UA program must be consistent throughout all proposal documents.

Peers chosen based on Center for Academic Excellence (CAE) CAE-CO (Cyber Operations) by the National Security Agency

Program name, degree, and institution	BS in Cyber Operations	Cyber Security (BBA), UTSA	Cyber Operations (BS), Dakota State
Completions for last two years, MAJORS only (can be found on market data report)	[redacted]	Not published	50–100/year (part of ~200 total overall tech grads annually)
Program Description	The Bachelor of Science in Cyber Operations at The University of Arizona is elite preparation for the next generation of cyber professionals. You'll learn to think like both attacker and defender, mastering skills like reverse engineering malware, network analysis, penetration testing, and low-level programming to fully understand how modern computer systems and network operate.	The UTSA BBA in Cyber Security is offered by the College of Business (in-person or 100 % online). It blends business acumen with cyber defense techniques, teaching students to design secure infrastructures that support organizational goals. Courses cover areas like intrusion detection, incident response, digital forensics, secure network and software design, policy, and governance—all within a business framework.	The BS in Cyber Operations is a traditional 4-year degree, offered on campus and online, focused on defending high-value digital information through study of confidentiality, integrity, and availability. It emphasizes computer forensics, network and software security, malware reverse-engineering, and practical labs analyzing real threats, breaches, and vulnerabilities
Target Careers from Market Data Report	Information Security Analyst, Computer Network Architect, Computer Forensics Analyst, Cyber Operations Specialist, Systems	Information Security Analyst, Computer Network Architect, Computer Forensics Analyst, Cyber Operations Specialist, Systems	Information Security Analyst, Computer Network Architect, Computer Forensics Analyst, Cyber Operations Specialist, Systems

	Security Engineer, Cyber Threat Analyst	Security Engineer, Cyber Threat Analyst	Security Engineer, Cyber Threat Analyst
Emphases? (Yes/No) List, if applicable. For majors only.	Yes	Not required	Not required
Minimum # of units required	120, 42 upper division	120, 39 upper division	120, 54 upper division
Special requirements to gain admission to program? (i.e. pre-requisites, GPA, application, etc.)	Programming and Networking Supporting Coursework	Complete IS 2053 Programming I and IS 3413 Telecommunications and Networking with a C or better	None
UG - Level of Math required (if applicable)	Cryptography	MAT 1053 Mathematics for Business (TCCN: MATH 1324) or higher with a C or better	MATH 201 Discrete Math (3)
UG - Level of Second Language required (if applicable)	Second semester proficiency	Second Language not specifically required. Requirement is 3 credits of Language, Philosophy and Culture (options include elementary language courses)	None
Internship, practicum, or applied/experiential requirements? If yes, describe.	Capstone	IS 4893: Cyber Security Capstone (3 credits)	None
Additional requirements			

Additional questions:

1. How does the proposed program align with peer programs? Briefly summarize the similarities between the proposed program and peers, which could include curriculum, overall themes, faculty expertise, intended audience, etc. See table below.
2. How does the proposed program stand out or differ from peer programs? Briefly summarize the differences between the proposed program and peers, which could include curriculum, overall themes, faculty expertise, intended audience, etc. See table below.

Feature	UA BS Cyber Ops	DSU BS Cyber Ops	UTSA BBA Cyber Security
Degree Type	Proposed: BS (Science)	BS (Science)	BBA (Business Admin)
Hands-On Focus	High – capstone, internships	High – malware, RE, labs	Moderate – labs + business
Academic Tracks	Emphasis areas	No tracks, but deep technical	Business-focused, broad cyber
NSA CAE Status	CAE-CO	CAE-CO & other CAE	CAE-E, CAE-O, CAE-R (all 3)
Career Path	Technical – analysts, defense, offense	Technical – cyber operations	Managerial – security admin
Faculty expertise	Security research, analytics, malware/forensics expertise	Tool-based labs, ethical hacking, cyber forensics	Business-informed cybersecurity, digital forensics & secure design, policy/business integration
Target Student	Post-traditional and traditional, transfer, adult learners, currently employed	Traditional, cyber competitors, tech-driven learners	Business focused, first generation, aspiring CISOs

3. How do these differences make this program more applicable to the target student population and/or a better fit for the University of Arizona?

   The proposed BS in Cyber Operations degree will continue to be accessible to post traditional and transfer populations, by design. However, the newly scaffolded BS program will also allow traditional students to engage in research and hands on experiences.