THE UNIVERSITY OF ARIZONA

New Academic Program Workflow Form

General

Proposed Name: Cyber Defense

Transaction Nbr: 00000000000076

Plan Type: Specialization

Academic Career: Undergraduate

Degree Offered: Undergraduate Certificate

Do you want to offer a minor? N

Anticipated 1st Admission Term: Sprg 2021

Details

Department(s):

UAZS

DEPTMNT ID	DEPARTMENT NAME	HOST
2910	College of Applied Science and Technology	Y

Campus(es):

DIST

LOCATION	DESCRIPTION
CHANDLER	Chandler
YUMA	Yuma

ONLN

LOCATION	DESCRIPTION
ONLN	Online

SOUTH

LOCATION	DESCRIPTION
DOUGLAS	Douglas
MESA	Mesa
NOGALES	Nogales

LOCATION	DESCRIPTION
SIERRAVSTA	Sierra Vista

Admission application terms for this plan: Spring: Y Summer: Y Fall: Y

Plan admission types:

Freshman: N Transfer: N Readmit: N Graduate: Y

Non Degree Certificate (UCRT only): N

Other (For Community Campus specifics): N

Plan Taxonomy: 29.0207, Cyber/Electronic Operations and Warfare.

Program Length Type: Program Length Value: 0.00

Report as NSC Program:

SULA Special Program:

Print Option:

Diploma: Y Undergraduate Certificate, Cyber Defense

Transcript: Y Undergraduate Certificate, Cyber Defense

Conditions for Admission/Declaration for this Major:

-Minimum 2.5 GPA
-Complete all pre-requisite coursework

Requirements for Accreditation:

n/a

Program Comparisons

University Appropriateness

The Cyber Defense Certificate is designed to provide students in related fields with the opportunity to earn a certificate in a fast-growing and highly desired career field. Currently, the only undergraduate degree in the area of cybersecurity offered at the University of Arizona is the BAS in Cyber Operations (BAS-CO) offered by the College of Applied Science & Technology (CAST). Students who take this certificate may decide to pursue an advanced degree in cybersecurity, such as the MS in Cybersecurity that is being jointly offered by MIS and ENGR or may pursue the graduate certificates in MIS or ENGR, or ¿ thus benefiting other units on campus. Moreover, degree and non-degree seeking students could earn the certificate by taking the six required CYBV courses. UA is expanding its corporate partnerships and this certificate is

appropriately designed to support their needs as well as the needs of the Department of Justice (DOJ), Department of Defense (DoD), and other governmental and non-governmental partners.

Arizona University System

NBR	PROGRAM	DEGREE	#STDNTS	LOCATION	ACCRDT

Peer Comparison

see attached

Faculty & Resources

Faculty

Current Faculty:

INSTR ID	NAME	DEPT	RANK	DEGREE	FCLTY/%
22071416	Jason Denno	2910	Instructor	Master of Science	1.00
22074078	Thomas Jewkes	2910	Assit. Prof. Pract.	Master of Science	1.00
22078226	Paul Wagner	2910	Assit. Prof. Pract.	Master of Science	1.00
22081465	Harry Cooper	2910	Adj. Assit. Prof	Master of Science	1.00
22081483	Troy Ward	2910	Adj. Assit. Prof	Master of Science	1.00
22081494	Jordan Vanhoy	2910	Assit. Prof. Pract.	Master of Science	1.00
22083351	Chester Hosmer	2910	Assit. Prof. Pract.	Bachelor of Science	1.00
22086398	Steven Wood	2910	Adj. Assit. Prof	Master of Science	1.00
22086399	Colin Brooks	2910	Adj. Assit. Prof	Master of Science	1.00
22086411	Michael Galde	2910	Assit. Prof. Pract.	Master of Science	1.00
22088393	Jonathan Martinez	2910	Adj. Assit. Prof	Master of Science	1.00
22088394	Michael Duren	2910	Adj. Assit. Prof	Master of Science	1.00

Additional Faculty:

none

Current Student & Faculty FTE

DEPARTMENT	UGRD HEAD COUNT	GRAD HEAD COUNT	FACULTY FTE
2910	1081	0	12.00

Projected Student & Faculty FTE

	UGRD HEAD COUNT			GRAD HEAD COUNT			FACULTY FTE		
DEPT	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3
2910	35	65	100	0	0	0	12.00	12.00	12.00

Library

Acquisitions Needed:

none

Physical Facilities & Equipment

Existing Physical Facilities:

none

Additional Facilities Required & Anticipated:

none

Other Support

Other Support Currently Available:

CAST Cyber Operations program will directly support this certificate

Other Support Needed over the Next Three Years:

none

Comments During Approval Process

9/11/2020 9:53 AM

PAULEWAGNER

Comments
Approved.

9/11/2020 12:03 PM

LDENNO

Comments
Approved.

9/14/2020 11:25 AM

SWIELAND

Comments
Approved for Online and Distance locations. Mesa is not approved as it is on a teach out plan and per Paul Wagner should be replaced with PimaCCEast location.

THE UNIVERSITY OF ARIZONA.

UNDERGRADUATE CERTIFICATE – ADDITIONAL INFORMATION FORM

Note: Certificate programs offered at the University of Arizona, at the undergraduate or graduate level, are not approved as eligible programs for federal student financial aid. Although students enrolled in certificate programs are not eligible for any federal student aid programs, students may be eligible for private loans, outside scholarships, and University of Arizona department funding. For more information, please see Federal Student Financial Aid Eligibility for Programs.

General Information

Proposed Title of Certificate: Cyber Defense Certificate -- Undergraduate

CIP Code: 29.0207, Cyber/Electronic Operations and Warfare

Anticipated first admission term: Spring 2021

Requested by: The College of Applied Science & Technology

Program Affiliation – specify whether the UA offers an affiliated undergraduate program – the affiliated program may or may not have the same name as the proposed certificate.

Undergraduate Major in Cyber Operations

Certificate Description: The 18-credit hour Undergraduate Certificate in Cyber Defense will provide students the skills necessary to design defensible network architectures; employ active and passive defensive technologies; arm those defensive technologies with tactical Cyber Threat Intelligence (CTI); conduct Network Security Monitoring (NSM) and Threat Hunting operations; respond to security incidents; and how to manipulate network environments in order to defend against advanced cyber threats. Students will conduct interactive exercises to secure Linux and Windows operating systems; conduct network traffic flow analysis and forensics; conduct anomaly/intrusion detection and identification; identify and block command and control operations; conduct Incident Response (IR) activities; and how to implement and manage Zero Trust Networks (ZTN) within on-premises and cloud-based environments. Upon completion of the certificate, students will have a sound understanding of the technologies and methods utilized to defend systems and networks. They will be able to describe, evaluate, and operate a defensive network architecture; employing multiple layers of protection using technologies appropriate to meet mission security goals.

Purpose

The Cyber Defense Certificate is designed to provide students in related fields with the opportunity to earn a certificate in a fast-growing and highly desired career field. Currently, the only undergraduate degree in the area of cybersecurity offered at the University of Arizona is the BAS in Cyber Operations (BAS-CO) offered by the College of Applied Science & Technology (CAST). Students who take this certificate may decide to pursue an advanced degree in cybersecurity, such as the MS in Cybersecurity that is being jointly offered by MIS and ENGR or may pursue the graduate certificates in MIS or ENGR, or – thus benefitting other units on campus. Moreover, degree and non-degree seeking students could earn the certificate by taking the six required CYBV courses. UA is expanding its corporate partnerships and this certificate is appropriately designed to support their needs as well as the needs of the Department of Justice (DOJ), Department of Defense (DoD), and other governmental and non-governmental partners.

Target Audience(s)

This program serves students from across the university, and specifically those without the technical background necessary to be successful in the field of cybersecurity. The required courses are designed to build the requisite knowledge, skills, and abilities in the area of Cyber Defense. Due to the pervasive cybersecurity demands in every field, this certificate is an excellent complement to any UA technical or non-technical degree program.

This certificate meets the needs of our: industry partners (ranging from multi-billion-dollar companies to local small business startups); the Department of Defense; Federal, State, and Local government agencies; and non-governmental organizations.

If a student chooses to do so, they might major in any of the degrees housed in the College of Applied Science & Technology at the University of Arizona – the certificate provides and introductory pathway into any of these degrees:

Undergraduate Major in Cyber Operations
Undergraduate Major in Applied Computing / Informatics / Network Operations
Undergraduate Major in Intelligence and Information Operations

Certificate Requirements - complete the table below to list the certificate requirements, including number of credit hours required and any special requirements for completion. Certificate requirements should include sufficient units to provide a substantive program and an appropriate level of academic rigor and in no case be less than 12 units of credit.

Minimum total units required *minimum 12 units	18
Minimum upper-division units required *minimum 6 units of credit must be upper division UA coursework	18
Total transfer units that may apply to the certificate.	0
List any special requirements to declare/admission to this certificate	-Minimum 2.5 GPA -Complete all pre-requisite coursework
Certificate requirements. List all required 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 (house number limit, etc.). Provide email(s)/letter(s) of support from home department head(s) for courses not owned by your department.	Core: Complete 6 courses (18 units): - CYBV302 Linux Security Essentials (3) - CYBV303 Windows Security Essentials (3) - CYBV326 Introductory Methods of Network Analysis (3) - CYBV400 Active Cyber Defense (3) - CYBV435 Cyber Threat Intelligence (3) - CYBV460 Principles of Zero Trust Networks (3)

Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	none
Additional requirements (provide description)	none
Any double-dipping restrictions (Yes/No)? If yes, provide description. *A maximum of 6 units may double-dip with a degree requirement (major, minor, General Education) or second certificate.	None distinct or beyond the University max of 6 units.

Current Courses–using the table below, list all existing courses included in the proposed certificate. You can find information to complete the table using the UA course catalog or UAnalytics (Catalog and Schedule Dashboard> "Printable Course Descriptions by Department" On Demand Report; right side of screen). If the courses listed belong to a department that is not a signed party to this implementation request, upload the department head's permission to include the courses in the proposed certificate and information regarding accessibility to and frequency of offerings for the course(s). Upload letters of support/emails from department heads to the "Letter(s) of Support" field on the UAccess workflow form. Add rows to the table, as needed.

Course prefix and number (include cross-listings)	Units	Title	Course Description	Pre-requisites	Modes of delivery (online, in-person, hybrid)	Typically Offered (F, W, Sp, Su)	Dept signed party to proposal? (Yes/No)
CYBV302	3	Linux Security Essentials	Provides students with an in-depth analysis of Linux and Unix security issues. This includes configuration guidance using industry standards and benchmarks and implementation through practical, real world examples. The course will examine how to mitigate or eliminate general problems that apply to Nix like OSs, including vulnerabilities in passwords and password authentication systems, virtual memory system, and	None	Online, In-person, Hybrid	F, Sp	Yes

			applications most commonly run.				
CYBV303	3	Windows Security Essentials	Provides students with the foundational knowledge of the Windows Operating System and securing Windows environments including; learning PowerShell scripting, host hardening and active directory scripting, smart tokens and Public Key Infrastructure (PKI), protecting admin credentials, and thwarting hackers inside the network. Students will use hands-on labs and exercises to secure Windows systems, networks, applications, and data.	None	Online, In-person, Hybrid	F, Sp	Yes
CYBV326	3	Introductory Methods of Network Analysis	Provides a methodology for analyzing networks by examining the network at its infrastructure, network and applications layers; exploring how they transfer data; investigating how network protocols work to enable communication; and probing and analyzing how the lower-level network layers support the upper ones. Students will use hands-on labs and exercises to investigate and analyze network fundamentals.	None	Online, In-person, Hybrid	F, Sp, Su	Yes
CYBV400	3	Active Cyber Defense	Provides students with an introduction to the policies, techniques, and operational capabilities and limitations of implementing an Active Cyber Defense program. A broad survey of development of defensible network architectures; integration of passive defensive technologies; consumption and production of Cyber Threat Intelligence (CTI)	APCV320 and CYBV385 or Consent of Instructor	Online, In-person, Hybrid	F	Yes

			products; implementation of Network Security Monitoring (NSM) and Hunt Teaming (HT) operations; employment of Incident Response (IR) plans; and Threat and Environment Manipulation techniques (TEM) will be presented, and students will use hands-on activities to practice and implement active defense methodologies.				
CYBV435	3	Cyber Threat Intelligence	An investigation of threat actors and the techniques they employ to attack networks. Students will research threat capabilities and objectives. Formal ethical hacking methodology including reconnaissance, scanning and enumeration, gaining access, escalation of privilege, maintain access and reporting is examined.	APCV 320 and CYBV 385 or Consent of Instructor	Online, In-person, Hybrid	F	Yes
CYBV460	3	Principles of Zero Trust Networks	Provides students with an overview of the fundamentals of Zero Trust Networks (ZTN). Students will be presented with the most effective methodologies used by leading companies and cyber professionals to design and implement ZTN. Students will use interactive exercises to become familiar with the design concepts including Software Defined Networks (SDN) and how to leverage SDN and mutual TLS authentication to create a scalable and robust ZTN.	CYBV301 or CYBV385, CYBV400 or Consent of Instructor	Online, In-person, Hybrid	F, Sp	Yes

New Courses Needed – using the table below, list any new courses that must be created for the proposed program. If the specific course number is undetermined, please provide level (ie CHEM 4**). Add rows as needed. Is a new prefix needed? If so, provide the subject description so Curricular Affairs can generate proposed prefix options.

None

Faculty & Resources

Current Faculty - complete the table below. If UA Vitae link is not provided/available, attach a short CV (2-3 pages) to the end of the proposal or upload to the workflow form. UA Vitae profiles can be found in the UA directory/phonebook. Add rows as needed. Delete the EXAMPLE rows before submitting/uploading. NOTE: full proposals are distributed campus-wide, posted on committee agendas and should be considered "publicly visible". Contact Liz Sandoval if you have concerns about CV information being "publicly visible".

Faculty Member	Involvement
Jason Denno, MS, MBA	Cyber Operations Teaches CYBV400, CYBV435, and CYBV460
Paul Wagner, MS, MBA	Cyber Operations, Teaches CYBV302, CYBV303, and CYBV326
Michael Galde, MS	Cyber Operations, Teaches CYBV326
Tom Jewkes, MS	Cyber Operations, Teaches CYBV400, CYBV435, and CYBV460
Jordan VanHoy, MS	Cyber Operations, Teaches CYBV302, CYBV303, and CYBV326

Additional Faculty – Describe the additional faculty needed during the next three years for the initiation of the program and list the anticipated schedule for addition of these faculty members.

None. All program growth due to increased enrollment in the Cyber Defense Certificate will be addressed by the current Cyber Operations program Full Time and Adjunct Faculty.

Library Acquisitions Needed – Describe additional library acquisitions needed during the next three years for the successful initiation of the program.

None

Physical Facilities & Equipment - Assess the adequacy of existing physical facilities and equipment available for the proposed certificate. Include special classrooms, laboratories, physical equipment, computer facilities, etc. Describe additional physical facilities and equipment that will be required or are anticipated during the next three years for the proposed program.

None

Other Support - Describe other support currently available for the proposed certificate. Include support staff, university and non-university assistance. List additional staff and other assistance needed for the next three years.

None

Marketing & Recruitment - Provide a detailed and robust marketing strategy for this certificate.

1. The Cyber Operations program is already a robust existing program with over 580 declared majors. We have implemented a marketing plan for the degree and undergraduate certificate programs that consists of the following:
   a. UA Cyber Operations program website located at: https://cyber-operations.azcast.arizona.edu. Our program website provides detailed information on: our National Security Agency (NSA) designation as a National Center of Academic Excellence in Cyber Operations (CAE-CO); detailed information on our three existing subplans (Cyber Engineering, Defense & Forensics, and Cyber Law & Policy) to include sample program schedules and course descriptions/learning outcomes; the UA CyberApolis Cyber Virtual Learning Environment; Cyber Operations Career information; Cyber Operations Faculty; and admissions requirements. Our Cyber Operations program website links to the UA Main website and the UA admissions application website.
   b. The Cyber Operations program is also fully integrated into Arizona Online and its website located at: https://online.arizona.edu/programs/undergraduate/online-bachelor-applied-science-cyber-operations-applied-science-bas. This website provides high level details on the Cyber Operations program, a program video, and links to admissions and the application. This site also provides links back to the UA Cyber Operations program website.
   c. The UA Cyber Operations program is also prominently displayed on the front/landing page of the CyberDegrees.org website located at: https://www.cyberdegrees.org/listings/best-online-cyber-security-bachelors-degrees/. This site lists the "18 Best Online Cyber Security Bachelor's Degrees in 2018". This site directly links to the Arizona Online's Cyber Operations website listed above. The Cyber Degrees website also provides high level details on the Cyber Operations program and our Cyber Virtual Learning Environment.
   d. The Cyber Operations program has developed a detailed program brochure. The brochure is a multifold 10-page document that provides most of the information from the Cyber Operations program website as well as contact information for Admissions and the Cyber Operations program office. This brochure is given out at various Student Services and Cyber Operations program recruiting events. They are also made available on the UA Sierra Vista and other Distance campuses.
   e. CAST has also developed a one-page Cyber Operations pamphlet with high level program details and contact information for both Admissions and the Cyber Operations program office. These pamphlets are given out at various Student Services and Cyber Operations program recruiting events. They are also made available on the UA Sierra Vista and other Distance campuses.
   f. CAST has also included the Cyber Operations program in its IT Industry academic program pamphlet and marketing materials. The pamphlet is given out at various Student Services and Cyber Operations program recruiting events. They

are also made available on the UA Sierra Vista and other Distance campuses.

g. The UA Distance Campus network also markets the Cyber Operations program through their monthly newsletter that goes to current and prospective students.
h. Finally, the Cyber Operations program has developed a detailed web-magazine-like monthly newsletter called “The Packet”. The Packet is sent to all current, prospective, and graduated Cyber Operations Students. The Packet is also sent to all of the Cyber Operations industry, government, and transfer pathway academic partner institutions. The Packet is a 20 to 40-page document that provides students details on: Major Cyber related events for the month; upcoming semester course offerings; UA Spotlight on two or more of our Cyber Operations Faculty; important dates and program information; cyber certification opportunities; as well as information on pre-vetted scholarship, internship, and job opportunities that are available to our students.

2. We have implemented an initial student recruitment plan that consists of the following:

By means of digital and print media, radio ads, outdoor advertising such as rented billboards, news releases, direct mail, direct e-mail, website, social media, and personal outreach by the Advising Team, our promotion and communication efforts will focus on raising awareness of the value of obtaining a degree in Cyber Operations or one of our Undergraduate Certificate, along with generating interest in and providing information about career opportunities for cyber professionals. We use traditional advertising channels, which reach a wider audience, to achieve this objective, paired with making individual connections with prospective students. We make additional contact with prospective students through outreach to community colleges by meeting with community college instructors and administrators to create partnerships to streamline the options students have to transfer seamlessly from their community college program into the Cyber Operations department to complete their BAS degree. In addition, our Advising Team members hold office hours on site at the community college campuses to make themselves available to prospective students for informal visits and conversations to help examine options for credit transfer. These informal conversations augment the more formal classroom visits also conducted by the Advising Team to provide information to prospective students in a larger presentation setting. Once the students have moved beyond awareness and interest in the college, we leverage interactive communication channels to begin building a relationship and move individuals through the final stages of the decision process to move forward with applying to the University of Arizona. The objective is to raise awareness and communicate the college’s value proposition to prospects, and the community at large. The goal is to drive traffic to the CAST website where visitors can search for information and begin engaging with the college. From the CAST website, students and their families can access details to reinforce the value of obtaining their degree here, from seeing the lower tuition rates available to CAST and University of Arizona Online, to learning more about the nationally-recognized caliber of the curriculum of the Cyber Operations BAS.

Financial - Provide a copy of the budget for the certificate including start-up costs and the anticipated costs for the first three years. Include some indication of how this fits with the overall department budget.

See attached

Student Learning Outcomes and Assessment – describe what students should know, understand, and/or be able to do after completing this certificate, and how student outcomes will be assessed.

In completing the Certificate, students will be able to:

- Analyze Linux operating system components from the standpoint of security
- Scrutinize which processes are running-and which may represent a threat
- Evaluate logs, analytics, and auditing reports to pinpoint vulnerabilities
- Gather critical information through advanced scripting techniques
- Exercise critical thinking strategies including reasoning, problem solving, analysis and evaluation by:
    - Implementing OS hardening through industry standards
    - Troubleshooting common security problems
    - Detecting threats within networks
    - Analyzing security logs and auditing reports
- Understand PowerShell, write scripts, functions, and modules
- Enforce Continuous Secure configuration enforcement
- Manage Server Hardening
- Manage Active Directory with PowerShell
- Investigate and manage PKI, Smart Tokens, Smart Cards, and TPMs
- Restrict and manage admin and user privileges
- Understand and explain anti-exploitation
- Establish Role-Based Access Control
- Understand windows firewall and use PowerShell to create and enforce Firewall and IPsec Rules
- Identify the major network components and protocols that enable communications and data transfer.
- Define and describe the principal characteristics, functions and protocols of the Application Layer, Transport Layer, Network Layer and Link Layer.
- Define and explain Wireless and mobile network architectures and protocols
- Explain the principles of computer security
- Exercise critical thinking strategies including reasoning, problem solving, analysis and evaluation by:
    - Analyzing network traffic and their protocol and services
    - Identifying and differentiating between connection and connectionless protocols
    - Enumerating network architectures through active and passive mapping and scanning
    - Using scanning techniques to determine the security posture of a network
- Define and explain how Intelligence is used as part of Incident Response
- Identify and describe the basics of the Intelligence cycle
- Identify and describe the basics of the Incident Response cycle
- Explain and demonstrate the techniques for targeting adversaries
- Describe how to detect the presence of adversaries within your network
- Describe how to use the F3EAD process to conduct Intelligence-driven Incident Response
- Describe the technologies and methods utilized to actively defend systems and networks.
- Describe, evaluate, and operated a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals.
- Explain how to consume and create Cyber Threat Intelligence (CTI) within an Active Cyber Defense program.

- Describe and demonstrate how to conduct Network Security Monitoring (NSM) and Hunt Team operations.
- Demonstrate and explain the preparation, identification, containment, eradication, recovery and lessons learned incident response cycle.
- Identify and explain how environment and threat manipulation techniques can mitigate security vulnerabilities.

Topics covered:

- Linux operating system architecture; Linux administration; and Linux operating system hardening
- Windows operating system architecture; Windows administration; and Windows operating system hardening
- Network protocols; network traffic capture and analysis; and network security principles
- Design of defensible network architectures; passive and active devices; threat hunting; incident response; threat and environment manipulation
- Tactical, Operational, & Strategic Cyber Threat Intelligence consumption; creation; and sharing
- Zero Trust Networking

Assessment Plan– identify factors that indicate that completion of the certificate enhances the undergraduate experience. Describe measures for programmatic assessment, and provide a detailed plan for assessing certificate outcomes.

Learning Outcomes	**Sources(s) of Evidence**	**Assessment Measures**	**Data Collection Points**
Outcome 1: Describe, evaluate, and construct a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals.	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of CYBV302 End of CYBV303 End of CYBV400 End of CYBV435 End of CYBV460
Outcome 2: Demonstrate a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; evaluate network protocols work to enable communication; and how the lower-level network layers support the upper ones.	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of CYBV302 End of CYBV303 End of CYBV400 End of CYBV435 End of CYBV460
Outcome 3: Evaluate and assess the various types of vulnerabilities and their underlying causes; how security principles interrelate and are typically employed to achieve assured solutions; and explain how failures in fundamental	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of CYBV302 End of CYBV303 End of CYBV400 End of CYBV435 End of CYBV460

security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation.			
Outcome 4: evaluate and assess an adversary's motivation, intentions, and methods are collected, analyzed, and disseminated to help security personnel and business staff to align resources and protect critical assets within an enterprise architecture.	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of CYBV302 End of CYBV303 End of CYBV400 End of CYBV435 End of CYBV460

Certificate Outcomes and Assessment– identify factors that indicate that completion of the certificate enhances the undergraduate experience. Describe measures for programmatic assessment, and provide a detailed plan for assessing certificate outcomes.

Certificate Outcomes

Factors indicating that the Certificate leads to gainful employment and/or advancement include: Offers of employment to interns* at their place of internship*, employment at a desirable position (as articulated by the student) within one year of earning the certificate, promotion in professional setting within one year of earning the certificate, and long-term satisfaction with working conditions (2, 5, and 10 years out from earning the certificate). Indication from annual surveys of our former students that the certificate was a factor in their employment success

*interns and internship are not associated with academic credit or part of a programatic offering

Assessment Plan
Certificate Outcomes will be assessed:

- Annually through an outgoing survey of Certificate Students regarding the above factors.
- Annually through a survey of employers as identified by those who earned the certificate.

Certificate Demand
Anticipated Enrollment and General Demand:

This certificate program will target:

1. Current UA students interested in augmenting their current degree program with this particular skill set (e.g., this is a great certificate to add to a major like Computer Science, Management Information Systems, and the various Engineering degree programs)
2. Returning Cyber Operations students already working in the field wanting to improve their skills and/or increase their eligibility for promotion
3. New non-degree seeking students from our corporate and government partnerships

3-Year Projected Annual Enrollment			
Projected Number of Students	**1st Year**	**2nd Year**	**3rd Year**
	35	65	100

General Demand

CAST's Cyber Operations program has already generated more than 580 declared majors and 116 Undergraduate Certificate seeking students (our current Cybersecurity Certificate UGC) after only four years since its inception. The reason this degree program and its associated undergraduate certificates has been—and will continue to be—one of the most popular programs at the University of Arizona is that it is preparing students for a career field in which the number of open positions far outweighs the number of qualified applicants. The program was designated as one of twenty-one (21) of the National Security Agency's National Centers of Academic Excellence in Cyber Operations (https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/), and a recent identification by the Department of State as a Champion University Program, making it one of the top Cyber programs in the Nation. The rate of enrollment has increased every semester and shows no signs of slowing down in the immediate future. Due to the increasing demand for highly qualified cyber professionals and the growing awareness of the UA Cyber Operations program, we believe the estimated rate of growth underpinning the anticipated student enrollment numbers are conservative.

Needs Served by the Certificate

According to the Bureau of Labor Statistics, the rate of growth for jobs in cybersecurity is projected at 32% from 2018–2028—much faster than the average for all other occupations. The field of Cybersecurity in the U.S. employed nearly 997,058 people in

2020 yet still maintains a 0% unemployment rate. CyberSeek, an organization dedicated to monitoring the cybersecurity talent gap, noted that over 504,316 current cybersecurity job openings still remain unfilled. Additionally, according to the National Initiative for Cybersecurity Education (NICE), the demand for cybersecurity talent will increase annually by approximately 1.5 million jobs globally through 2022. The reason CAST's degree and certificate programs have been—and will continue to be—some of the most popular programs at the University of Arizona is that they are preparing students for a career field in which the number of open positions far outweighs the number of qualified applicants. The median annual wage according to the Bureau of Labor Statistics is $99,730 as of May 2019.

Sources: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
https://www.cyberseek.org/heatmap.html

Related Positions:

- Chief Security Engineer
- Vulnerability Researcher
- Cybersecurity Engineer
- Cyber Operations Officer
- Cybersecurity Systems Analyst
- Computer Network Defender
- Cyber Network Defender
- SOC Analyst/Operator
- Incident Responder
- IT Security Analyst
- Cybersecurity Analyst
- Cybersecurity Consultant
- Cyber Operations Analyst
- Cyber Threat Intelligence Analyst
- Cyber Threat Intelligence Manager
- Counter Cyber Threat Intel Analyst
- Threat Operations Consultant
- Cyber Network Defender
- Cybersecurity Investigator
- Cyber Operations Analyst
- Cyber Attribution Analyst

Local worksites for Cyber Defense students include:

Raytheon
Bank of America
Wells Fargo
IBM
Kforce Inc.
HuntSource
Arizona Department of Public Safety

Arizona Critical Infrastructure Providers (e.g. TEP, APS, SRP, etc.)
Verizon
Leidos
General Dynamics
Lockheed Martin
SAIC
Boeing

Similar programs:

The University of Arizona will be the leader in this space. Currently there are a number of cybersecurity related undergraduate certificates offered but they predominantly offer only generalized cybersecurity curricula and require the student to be degree seeking. Cyber defense is a must for every organization and requires specialized curricula to meet the technical demands necessary to prepare students to effectively design, maintain, and defend networks against advanced cyber threats. Our specialized Cyber Defense Undergraduate Certificate will provide the specialized knowledge, skills, and abilities to both degree and non-degree seeking students.

Arizona State University – Undergraduate Certificate – Applied Cybersecurity
https://webapp4.asu.edu/programs/t5/majorinfo/ASU00/ASACSCERT/undergrad/true?init=false&nopassive=true

Texas A&M – Undergraduate Certificate – Cybersecurity Engineering
https://catalog.tamu.edu/graduate/colleges-schools-interdisciplinary/engineering/interdepartmental-degree-programs/cybersecurity-engineering-certificate/

American Military University – Undergraduate Certificate – Cybersecurity
https://www.amu.apus.edu/academic/schools/science-technology-engineering-and-math/certificate-ug/cybersecurity.html

C. Collaborations

There will be no collaborations with other departments or universities for this certificate program other than donated courses toward this program if depts. choose to do so.

Contacts and Administration

List the name and contact information for the primary point of contact for the certificate.

Jason Denno, Director - Cyber, Intelligence & Information Operations, College of Applied Science & Technology, jasondenno@arizona.edu

List the name and contact information for the person or persons who will serve in the 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 the managing academic unit.)

Jason Denno, Director - Cyber, Intelligence & Information Operations, College of Applied Science & Technology, jasondenno@arizona.edu

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.*

Jason Denno, Director - Cyber, Intelligence & Information Operations, College of Applied Science & Technology, jasondenno@arizona.edu

Tom Jewkes, Assistant Professor of Practice – Cyber Operations, College of Applied Science & Technology, tjewkes@arizona.edu

Chet Hosmer, Assistant Professor of Practice – Security Computing, College of Applied Science & Technology, chesterhosmer@arizona.edu

Undergraduate Certificate Peer Comparison Chart- Select two peers for completing the comparison chart from (in order of priority) ABOR-approved institutions, AAU members, and/or other relevant institutions recognized in the field. The comparison chart will be used to identify typically required coursework, themes, and experiences for certificate programs within the discipline. The comparison programs are not required to have the same certificate name as the proposed UA program. Information for the proposed UA program must be consistent throughout the proposal documents. Delete EXAMPLE columns once ready to submit/upload.

Certificate name, institution	**Proposed UA Program:**	**Peer 1:**	**Peer 2:**
Current# of enrolled students		Current enrolled students statistics, completion rate statistics, nor gainful employment disclosures are available for this program.	Current enrolled students statistics, completion rate statistics, nor gainful employment disclosures are available for this program.
Certificate program description	The 18-credit hour Undergraduate Certificate in Cyber Defense will provide students the skills necessary to design defensible network architectures; employ active and passive defensive technologies; arm those defensive technologies with tactical Cyber Threat Intelligence (CTI); conduct Network Security Monitoring (NSM) and Threat Hunting operations; respond to security incidents; and how to manipulate network environments in order to defend against advanced cyber threats. Students will conduct interactive exercises to secure Linux and Windows operating systems; conduct network traffic flow analysis and forensics; conduct anomaly/intrusion detection and identification; identify and block command and control operations; conduct Incident Response (IR) activities; and how to implement and manage Zero Trust Networks (ZTN) within on-premises and cloud-based environments. Upon completion of the certificate, students will have a sound understanding of the technologies and methods utilized to defend systems and networks. They will be able to describe, evaluate, and operate a defensive network architecture; employing multiple layers of protection using technologies appropriate to meet mission security goals.	https://webapp4.asu.edu/programs/t5/majorinfo/ASU00/ASACSCERT/undergrad/true?init=false&nopassive=true The applied cybersecurity certificate program is designed to build competencies in security operations, risk assessment, network security, and governmental and regulatory compliance in an interdisciplinary learning setting. Building upon core skills that students bring with them from their majors, students practice dealing with cyber threats and resolving issues from multiple perspectives. This certificate is an ideal supplement for students interested in careers in cybersecurity in both the private sector and within government agencies (FBI, Homeland Security, NSA, DOD) in positions such as: • chief information security officer • cyber risk analyst	https://www.amu.apus.edu/academic/schools/science-technology-engineering-and-math/certificate-ug/cybersecurity.html Cybersecurity certifications and advanced knowledge are crucial in the never-ending challenge of organizational security. The online undergraduate certificate in cybersecurity from American Military University (AMU) enables you to: • Understand digital forensics tools, techniques, and methods, as well as cybercrime and cyber war • Deepen your understanding of the social and legal impacts of cyber terrorism, cyberstalking, and cyber bullying • Develop more familiarity with regulatory compliance standards,

		• information security engineer • network security engineer • security operations center analyst The program is offered through a collaboration between the New College of Interdisciplinary Arts and Science, the Ira A. Fulton Schools of Engineering and the W. P. Carey School of Business.	including the Children's Online Privacy Protection Act (COPPA) and Sarbanes-Oxley This certificate is a useful step in cybersecurity certifications for beginners, especially if you want to expand your cybersecurity knowledge without committing to a degree program.
Target careers	-Large, Mid, and Small Retail and Manufacturing Companies -Banks & Investment Firms -Managed Service Providers -Hospitals -Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners	-Large, Mid, and Small Retail and Manufacturing Companies -Banks & Investment Firms -Managed Service Providers -Hospitals -Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners	-Large, Mid, and Small Retail and Manufacturing Companies -Banks & Investment Firms -Managed Service Providers -Hospitals -Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners
Minimum total units required	18	15	18
Minimum upper-division units required	18	15	18
Total transfer units that may apply to certificate	None	3	9
List any special requirements to declare/admission to this certificate (completion of specific coursework,	-Minimum 2.5 GPA -Complete all pre-requisite coursework	To enroll in this certificate program, students should have completed at least 45 credit hours in their declared majors and have a cumulative GPA of 2.00 or better.	All AMU undergraduate programs require a minimum of a high school diploma or equivalent (i.e., GED).

minimum GPA, interview, application, etc.)			
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 (house number limit, etc.).	CYBV302 Linux Security Essentials (3) CYBV303 Windows Security Essentials (3) CYBV326 Introductory Methods of Network Analysis (3) CYBV400 Active Cyber Defense (3) CYBV435 Cyber Threat Intelligence (3) CYBV460 Principles of Zero Trust Networks (3)	**Required Courses -- 3 credit hours** CSE 365: Information Assurance or IFT 202: Foundations of Information and Computer System Security(3) **Electives -- 9 credit hours** **Group A - Security Operations and Risk Management -- 3 credit hours** ACO 461: Security Operations (3) CIS 401: Managing Cyber Risks in Enterprise Business Processes (3) IFT 381: Information System Security (3) **Group B - Systems and Network Security OR Group C - Forensics/Cyber Crime -- 3 credit hours** Group B - Systems and Network Security: ACO 431: Network Security (3) CSE 466: Computer Systems Security (3) CSE 468: Computer Network Security (3) IFT 458: Middleware Programming and Database Security (3) IFT 475: Security Analysis (3) Group C - Forensics/Cyber Crime: CSE 469: Computer and Network Forensics (3) FOR 350: Computer Forensics (3) IFT 482: Network Forensics (3)	ISSC331 Legal Issues in Information Security (3) ISSC351 Computer Forensics (3) ISSC451 Cybercrime (3) ISSC452 Cybersecurity (3) ISSC457 Digital Forensics: Investigating Network Intrusions and Cybercrime Security (3) ITMG281 Law, Privacy, and Digital Data (3)

		Group D - Policy -- 3 credit hours ACO 351: Governance, Risk and Compliance (3) CIS 402: Privacy, Ethics and Compliance Issues (3) CSE 467: Data and Information Security (3) IFT 483: Developing Security Policy (3) **Group E - Project -- 3 credit hours** Students may take more than one semester of the Applied Project but only three credit hours will count towards the certificate. ACO 484: Internship or ACO 499: Individualized Instruction (3) CIS 440: Capstone in Information Systems (L) (3) CSE 485: Computer Science Capstone Project I (L) or CSE 486: Computer Science Capstone Project II (L)(3) IFT 401: Information Technology Capstone Project I or IFT 402: Information Technology Capstone Project II (3) Depending on a student's undergraduate program of study, prerequisite courses may be needed in order to complete the requirements of this certificate.	
Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	None	Yes. Students must select one course from the **Group E - Project -- 3 credit hours** Students may take more than one semester of the Applied Project but only three credit hours will count towards the certificate.	None

Additional requirements (provide description)	None	A student pursuing an undergraduate certificate must be enrolled as a degree-seeking student at ASU. Undergraduate certificates are not awarded prior to the award of an undergraduate degree. A student already holding an undergraduate degree may pursue an undergraduate certificate as a nondegree-seeking graduate student.	None

*Note: comparison of additional relevant programs may be requested.

THE UNIVERSITY OF ARIZONA®

BUDGET PROJECTION FORM

Name of Proposed Program or Unit:

Budget Contact Person:	Projected 1st Year 2021 – 2022	2nd Year 2022- 2023	3rd Year 2023- 2024
METRICS			
Net increase in annual college enrollment UG	35	65	100
Net increase in college SCH UG	630	1170	1800
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	0	0	0
FUNDING SOURCES			
Continuing Sources			
UG RCM Revenue (net of cost allocation)			
Grad RCM Revenue (net of cost allocation)			
Program Fee RCM Revenue (net of cost allocation)			
F and A Revenues (net of cost allocations)			
UA Online Revenues	$204,750	$292,500	$585,000
Distance Learning Revenues			
Reallocation from existing College funds (attach description)			
Other Items (attach description)			
Total Continuing	$204,750	$292,500	$585,000
One-time Sources			
College fund balances			
Institutional Strategic Investment			
Gift Funding			
Other Items (attach description)			
Total One-time			
TOTAL SOURCES	$204,750	$292,500	$585,000
EXPENDITURE ITEMS			
Continuing Expenditures			
Faculty	N/A	N/A	N/A
Other Personnel			
Employee Related Expense			
Graduate Assistantships			
Other Graduate Aid			
Operations (materials, supplies, phones, etc.)			
Additional Space Cost			
Other Items (attach description)			
Total Continuing			
One-time Expenditures			
Construction or Renovation			
Start-up Equipment			
Replace Equipment			

Library Resources			
Other Items (attach description)			
Total One-time			
TOTAL EXPENDITURES	$0	$0	$0
Net Projected Fiscal Effect	$204,750	$292,500	$585,000

College of Applied Science & Technology

1140 N. Colombo Ave.
Sierra Vista, AZ 85635
Tel: 520-458-8278
Fax: 520-458-5823
www.azcast.arizona.edu

To Whom It May Concern:

The College of Applied Science and Technology's Cyber Operations Program is proposing multiple cyber security undergraduate certificates. These include the following:

- Penetration Testing
- Security Computing
- Cyber Defense
- Digital Forensics
- Reverse Engineering
- Information Warfare

After conducting a local and national search for similar curriculum, it was determined that there is nothing comparable at the undergraduate level. There are no letters of support for these certificates due to this analysis.

If our search missed something or you have concerns about these certificate proposals, please reach out to me.

Thank you for your time.

Paul E. Wagner, MS, MBA
Interim Academic Dean
Department Head, Applied Technology
Assistant Professor of Practice
College of Applied Science and Technology
The University of Arizona