THE UNIVERSITY OF ARIZONA

New Academic Program Workflow Form

General

Proposed Name: Security Computing

Transaction Nbr: 00000000000077

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, Security Computing

Transcript: Y Undergraduate Certificate, Security Computing

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 Security Computing Certificate is designed to provide students in related fields with the opportunity to earn a certificate in the fast-growing and highly desired cybersecurity career field. Currently, the only way to access this curricula is to take the BAS in Cyber Operations (BAS-CO) undergraduate degree offered by the College of Applied Science & Technology (CAST). This certificate is designed to provide access to this curricula beyond just CAST students to allow other degree seeking students across the University of Arizona as well as non-degree seeking students.

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/%
14206933	Li Xu	2910	Professor	Doctor of Philosophy	1.00
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
22083818	Diana Saldana Jimenez	2910	Assit. Prof. Pract.	Doctor of Philosophy	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. Instor.	Master of Science	1.00

Additional Faculty:

none

Current Student & Faculty FTE

DEPARTMENT	UGRD HEAD COUNT	GRAD HEAD COUNT	FACULTY FTE
2910	1081	0	14.00

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	30	60	90	0	0	0	14.00	14.00	14.00

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 the certificate.

Other Support Needed over the Next Three Years:

none

Comments During Approval Process

9/11/2020 9:48 AM

PAULEWAGNER

Comments
Approved.

9/11/2020 9:49 AM

LDENNO

Comments
Approved.

9/14/2020 11:27 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: Security Computing 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
Undergraduate Major in Intelligence & Information Operations

Certificate Description: The 18-credit hour Undergraduate Certificate in Security Computing will teach students how to apply the Python programming language to solve cybersecurity problems and conduct digital investigations. Students will learn how to develop, debug, execute, and deploy offensive and defensive python scripts; how to develop algorithms, determine the complexity of the algorithm, and identify cases in which the algorithm would/would not provide a reasonable approach for solving the specific problem; how to use Python to visualize security datasets; and how to develop Python-based machine learning models to detect, analyze, and defeat cyber deception operations. Upon completion of the certificate, students will be able to evaluate the strengths and weaknesses associated with the use of automated tools to solve complex security-related problems; create and use Python-based algorithmic solutions; and be able to apply existing Python libraries to support common security-related tasks.

Purpose

The Security Computing Certificate is designed to provide students in related fields with the opportunity to earn a certificate in the fast-growing and highly desired cybersecurity career field. Currently, the only way to access this curricula is to take the BAS in Cyber Operations (BAS-CO) undergraduate degree offered by the College of Applied Science & Technology (CAST). This certificate is designed to provide access to this curricula beyond just CAST students to allow other degree seeking students

across the University of Arizona as well as non-degree seeking students.

Target Audience(s)

This program serves students from across the university, and specifically those without the scripting, programming, and/or algorithm development background necessary to successful design, build and/or modify cybersecurity-focused applications. The required courses are designed to build the requisite knowledge, skills, and abilities necessary to address application shortfalls in a changing cyber environment. Due to the constantly changing nature of malware; evolving threat tactics and techniques; the big data problem in both the Cyber and Intelligence fields; and the diverse nature of proprietary cyber and IT related software, this certificate is an excellent complement to the Cyber Operations, Applied Computing, and Intelligence & Information Operations degree programs.

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. This certificate also meets the critical coding skills needed by our: industry partners; the Department of Defense; Federal, State, and Local government agencies; and non-governmental organizations.

Students who could most benefit from this certificate will typically major in: Cyber Operations; MIS; Computer Science; various disciplines within Engineering; or any of the Intelligence or Information related-degrees at the University of Arizona. 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 use this certificate to supplement their computer science or engineering degree – thus benefitting other units on campus. Moreover, degree and non-degree seeking students could earn the certificate by taking the six required courses.

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): - (New) CYBV312 Introduction to Security Scripting (3) - APCV320 Computational Thinking & Doing (3) - CYBV473 Violent Python (3) - APCV361 Data Analysis & Visualization (3) - CYBV474 Advanced Analytics for Security Professionals (3) - (New) CYBV475 Cyber Deception Detection (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)
APCV320	3	Computational Thinking and Doing	This course covers basics of programming and techniques used by computing professionals in a variety of application areas. Topics include computation, programs, algorithms, programming languages, complexity, and computability. The course also explores how these concepts and techniques are applied in Informatics.	None	Online, In-person, Hybrid	F, Sp, Su	Yes
APCV361	3	Data Analysis and Visualization	This course will lay a foundation for students to understand how to process, analyze, and visualize data. Topics include data collection and integration, exploratory data analysis, statistical inference and	APCV320 and APCV302 or consent of instructor	Online, In-person, Hybrid	F, Sp	Yes

			modeling, machine learning, and data visualization. The emphasis of the course topics will be placed on integration and synthesis of concepts and their application to solving problems. Students will explore these topics using software tools.				
CYBV473	3	Violent Python	CYBV 473 will provide students with advanced practical applications of Python programming to support offensive and defensive cybersecurity operations. A crosscut of Python concepts, tools, and techniques will be presented. Students will use interactive programming activities to master and create advanced Python tools to support common cybersecurity tasks.	APCV320 or consent of instructor	Online, In-person, Hybrid	F, Sp, Su	Yes
CYBV474	3	Advanced Analytics for Security Operations	CYBV474 provides students an in-depth examination of how the Python scripting language can be used to support advanced analysis in offensive and defensive security operations. Students will use hands-on scripting exercises to evaluate the strengths and weaknesses of automated tools to solve complex security-related problems; practice creating and using Python-based algorithmic solutions; and gain a technical understanding on how to apply the existing Python libraries to support common security-related tasks.	CYBV473 or consent of instructor	Online, In-person, Hybrid	F, Sp, Su	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.

- *CYBV312 and CYBV475 have been submitted and are currently awaiting approval from the curriculum process.*

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)
CYBV312	3	Introduction to Security Scripting	CYBV 312 will provide students with an introduction to the practical applications of Python programming in support of cybersecurity and digital investigation activities. The course will provide students with a solid foundation of the use of python language elements along with a practical understand on how to develop, debug, execute and deploy python scripts.	None	Online, In-person, Hybrid	F, Sp, Su	Yes
CYBV475	3	Cyber Deception Detection	CYBV475 will provide students with an in-depth investigation into the use of cyber deception techniques in both offensive and defensive operations. The course will focus on the development of new methodologies to create, detect, analyze, and respond to online cyber deception campaigns. Students will use interactive programming exercises to detect and counter fake news; fake images; deep fake video and audio; advanced data hiding methods; covert communications; and covert tagging and tracking methods.	CYBV312 & CYBV473 or consent of instructor	Online, In-person, Hybrid	F, Sp, Su	Yes

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
Li Xu, PhD	Applied Computing, Teaches APCV320, APCV361 and CYBV473
Diana Saldana, PhD	Applied Computing, Teaches APCV320 and APCV361
Mohammed Meky, PhD	Cyber Operations, Teaches CYBV312
Mike Duren, MS	Cyber Operations, Teaches CYBV312, CYBV474, and CYBV475
Chet Hosmer, BS	Cyber Operations, Teaches CYBV312, CYBV473, CYBV474, and CYBV475

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 and Applied Computing 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 program 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:

- Define and demonstrate the basic building blocks of the Python scripting language.
- Describe and demonstrate how to use and experiment with a Python integrated development environment.
- Describe and demonstrate access to and inventory of a file system.
- Demonstrate the use of key python built in data types including strings, lists, sets and dictionaries to cybersecurity related challenges.
- Develop and demonstration scripts than can search, parse and index text and binary files to uncover key evidence.
- Describe and demonstrate how to access and utilize key Python standard libraries, including but not limited to OS, SYS, CSV, JSON, RE, PATHLIB, HASHLIB, LOGGING, ARGPARSE, and PICKLE
- Describe and demonstrate how to discover, install, and utilize 3rd party library Python libraries
- Define and identify Computer Science terms and concepts in Computational Thinking
- Analyze and estimate what and how computers do program operations in at least two programming languages (Python and bash)

- Apply Computational Thinking to solve problems and design systems in practical applications
- Identify optimization problems and approaches to resolve them
- Identify principles and concepts in statistics and machine learning
- Apply statistical modeling and analysis to develop simulations
- Create plot visualizations to explore simulation models
- Apply machine learning algorithms to learn from data
- Analyze experimental data and communicate test results
- Build models based on experimental data and test the models in problem solving
- Define and demonstrate the basic building blocks of the Python scripting language
- Describe and demonstrate how to build a password cracker with Python
- Identify and describe how Python can be used to script attacks for penetration testing.
- Define and describe how Python can be implemented to support digital forensic investigations.
- Identify and describe the tools that can be developed using the Python scripting language to conduct network analysis and monitoring.
- Describe and explain how Python can be used build customized tools to sniff, parse and exploit the 802.11 and Bluetooth wireless protocols.
- Identify and explain how to design and develop web scraping and anonymous web browsing tools using Python.
- Describe and demonstrate how Antivirus protections can be evaded/bypassed with simple Python scripts
- Identify elements of cyber-operations that can benefit from advanced Python scripts
    - Digital Forensics
    - Digital Forensics for Incident Response (DFIR)
    - Asset Mapping
    - Network Monitoring
    - Host Monitoring
    - User Behavior Monitoring
    - Threat Intelligence
    - Log Analysis
    - Deception Methods
- Describe and explain how Python scripts, specialized libraries and tools could be deployed in each of these areas
- Identify principles and concepts relating to advanced deception methods, techniques, and objectives
- Develop strategies and specific methods to detect, uncover and trace perpetrators that are utilizing deception methods for crowd manipulation, propaganda dissemination or social engineering.
- Identify the use of covert communications, data hiding and other advanced methods of clandestine methodologies
- Uncover and extract unique features and behaviors that can in turn be used to train machine learning engines for the purpose of generating indications and warnings and/or critical observables
- Analyze and expose fake images, audio, video, and textual content
- Develop new methods of concealed survivable covert marking technologies that can be used to track and monitor illicit activity
- Develop decoys, traps and lures that can be employed to manipulate bad actors in order discover their objectives, techniques, and identities

Topics covered:

- Development of: Penetration Testing scripts; Intrusion Detection scripts; Forensic Analysis scripts; Data Hiding scripts; Data tagging scripts; Cyber Threat Information analysis and sharing scripts
- Proprietary cyber-related application Python extension development
- Design and analysis of Cyber-focused algorithms
- Design of scripts to parse and analyze network protocols; network traffic (Alerts, Session, NETFLOW, PSTR, and PCAP data)
- Cyber data processing, sorting, searching, and carving
- Development of Cyber deception detection scripts to identify fake audio, video, images, and text

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: Evaluate how variability affects outcomes; how to identify anomalous events; how to integrate and differentiate continuous functions of multiple variables; and how to solve complex problems using computation and scripting languages.	Course-embedded assessments	Exams, practical exercises, & reports Comprehensive research project and report	End of APCV320 End of APCV361 End of CYBV312 End of CYBV474 End of CYBV475
Outcome 2: Analyze and evaluate how networks work at the infrastructure, network and applications layers; how they transfer data; how 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 CYBV312 End of CYBV473
Outcome 3: Analyze and assess how knowledge about 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 CYBV312 End of CYBV473 End of CYBV474 End of CYBV475

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 programmatic 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**
	30	60	90

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 have 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:

- Cyber Application Developer
- Security Programmer
- Chief Security Engineer
- Vulnerability Researcher
- Cybersecurity Engineer
- Cybersecurity Application Analyst
- Cybersecurity Consultant
- Cybersecurity Investigator
- Cyber Operations Analyst
- Cyber Attribution Analyst
- Information Warfare Analyst
- Disinformation Analyst

Local worksites for Cyber Defense students include:

Raytheon
IBM
Verizon
Leidos
General Dynamics
Lockheed Martin

SAIC
Boeing
Kforce Inc.
HuntSource
Arizona Department of Public Safety
Arizona Critical Infrastructure Providers (e.g. TEP, APS, SRP, etc.)

Similar programs:

There are no undergraduate certificate programs that are as focused and comprehensive as the proposed Security Programming certificate. Most existing certificate programs in this general area either provide a broad overview of computer science and cybersecurity principles or they are non-credit continuing education programs. Although CAST's Security Programming Certificate is focused on solving cybersecurity and Intelligence problems; the knowledge, skills, and abilities are transferable to any field. The University of Arizona will be a leader in this space both for the value proposition and necessity outlined above.

Undergraduate Certificate Programs

PennState – Undergraduate Certificate – Information Sciences and Technology
https://www.worldcampus.psu.edu/degrees-and-certificates/information-sciences-and-technology-certificate/courses

Northwestern – Programming Certificate
https://sps.northwestern.edu/post-baccalaureate/programming/

University of Colorado Denver – Undergraduate Certificate – Cybersecurity and Secure Computing
https://engineering.ucdenver.edu/academics/departments/computer-science-and-engineering/computer-science-certificates/cyber-security-and-secure-computing

Wright State University – Undergraduate Certificate - Cyber Security Analytics
https://engineering-computer-science.wright.edu/computer-science-and-engineering/cyber-security-analytics-undergraduate-certificate

Continuing Education Certificate Programs

Cornell University – Python Programming Certificate Program
https://www.ecornell.com/certificates/technology/python-programming/#_

University of Washington – Certificate in Python Programming
https://www.pce.uw.edu/certificates/python-programming

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

Li Xu, Program Director, Applied Computing, College of Applied Science & Technology, lxu@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	[redacted]	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 Security Computing will teach students how to apply the Python programming language to solve cybersecurity problems and conduct digital investigations. Students will learn how to develop, debug, execute, and deploy offensive and defensive python scripts; how to develop algorithms, determine the complexity of the algorithm, and identify cases in which the algorithm would/would not provide a reasonable approach for solving the specific problem; how to use Python to visualize security datasets; and how to develop Python-based machine learning models to detect, analyze, and defeat cyber deception operations. Upon completion of the certificate, students will be able to evaluate the strengths and weaknesses associated with the use of automated tools to solve complex security-related problems; create and use Python-based algorithmic solutions; and be able to apply existing Python libraries to support common security-related tasks.	https://www.worldcampus.psu.edu/degrees-and-certificates/information-sciences-and-technology-certificate/overview As information technology continues to change, businesses and organizations will need computer and IT professionals with the right skills and training to help them meet their technology needs. Our certificate program is designed to prepare you for a leadership role in any IST–related field. You can enhance your existing skills or prepare for further study as you explore the social, ethical, and policy issues surrounding information technology. This online certificate program will give you the opportunity to interact with dedicated educators from one of the nation's most respected research universities. These are the same faculty who teach on-campus courses in Penn State's highly regarded IST programs.	https://sps.northwestern.edu/post-baccalaureate/programming/ The Programming post-baccalaureate certificate helps students develop skills in programming as well as systems analysis, database design and administration, and information technology project management. Working with Java, students learn how to program, but they also learn how to meet the business requirements of enterprise design, software implementation, data needs and databases, and how information systems serve the larger goals of a business or organization.

Target careers	-Large, Mid, and Small Retail and Manufacturing Companies -Managed Service Providers -Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners	-Large, Mid, and Small Retail and Manufacturing Companies -Managed Service Providers -Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners	-Large, Mid, and Small Retail and Manufacturing Companies -Managed Service Providers -Federal, State, and Local Government Agencies - Department of Defense -Intelligence Community Partners
Minimum total units required	18	12	12
Minimum upper-division units required	18	12	12
Total transfer units that may apply to certificate	None	None	None
List any special requirements to declare/admission to this certificate (completion of specific coursework, minimum GPA, interview, application, etc.)	Minimum 2.5 GPA Complete all pre-requisite coursework	A baccalaureate degree with above-average grades with courses in science and mathematics (through integral calculus) is required for entry. Additionally, applicants must have a minimum academic profile code (APC) of 324. Eligibility for TOP SECRET security clearance with access to SPECIAL COMPARTMENTED INFORMATION (SCI) is required for U.S. students. Applicants not meeting the mathematics requirements may be considered for entry via a refresher quarter.	Statement of purpose Current resume or CV
Certificate requirements. List all certificate requirements including core and electives. Courses listed must include course prefix, number, units, and	(New) CYBV312 Introduction to Security Scripting (3) APCV320 Computational Thinking & Doing (3) CYBV473 Violent Python (3) APCV361 Data Analysis and Visualization (3)	IST110 Information, People, and Technology (3) IST210 Organization of Data (3) IST220 Networking and Telecommunications (3)	Complete four of the following: CIS 212 Intro to Object-Oriented Programming (3) CIS 317 Database Systems Design (3)

title. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.).	CYBV474 Advanced Analytics for Security Operations (3) (New) CYBV475 Cyber Deception Detection (3)	IST250 Introduction to Web Design and Development (3)	CIS 323 Python for Data Science* (3) CIS 324 Applied Data Science* (3) CIS 370 System Analysis and Design (3)
Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	None	None	None
Additional requirements (provide description)	None	None	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	30	60	90
Net increase in college SCH UG	540	1080	1620
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	$175,500	$351,000	$526,500
Distance Learning Revenues			
Reallocation from existing College funds (attach description)			
Other Items (attach description)			
Total Continuing	$175,500	$351,000	$526,500
One-time Sources			
College fund balances			
Institutional Strategic Investment			
Gift Funding			
Other Items (attach description)			
Total One-time			
TOTAL SOURCES	$175,500	$351,000	$526,500
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	$0	$0	$0
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	$175,500	$351,000	$526,500

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