



NEW ACADEMIC PROGRAM – MAJOR
Preliminary Proposal Form

I. Program Details

- a. Name (and Degree Type) of Proposed Academic Program: Master of Science, Cyber & Information Operations
 - i. Emphases (if applicable):
- b. Academic Unit(s)/College(s): College of Applied Science & Technology
- c. Campus/Location(s): AZOnline, Main/Fully Online
- d. First Admission Term: Fall, 2023
- e. Primary Contact and Email:

II. Executive Summary:

- There is continued and increasing demand, both within the United States and worldwide, for qualified cyber professionals. *Cybersecurity Ventures*, a leading professional publication in the cybersecurity field, reports that there were 3.5 million unfilled jobs in 2021. It is not simply government and defense industries that are seeking qualified cyber professionals. Cybersecurity is the #1 business risk, with cybercrime expected to cost the world \$7 trillion USD in 2022. Because of this high demand, CAST has seen enrollment in its Cyber Operations undergraduate degree and certificate programs grow from 274 in 2019 to 1311 in Fall 2022, a growth rate of 380% over three years. CAST believes that the demand for the MS in Cyber Operations will follow this trajectory, and will likely outpace our ability to meet that demand.
- CAST's BAS In Cyber Operations is one of only 24 Center of Academic Excellence in Cyber Operations programs in the nation, and has been recognized as the #1 online Cybersecurity program in the country. A significant number of the students in our bachelor's program already possess a bachelor's degree and even a graduate degree, but choose to enroll in our BAS in Cyber Operations program to gain the knowledge and skills necessary to be employable in what is one of the fastest growing career fields worldwide. Many of these students, as well as students working toward their first bachelor's degree in our program, have expressed a desire to enroll in a CAST MS in Cyber Operations program.
- The proposal for a Master of Science in Cyber Operations program is part of CAST's strategic plan to build both competency and capacity in the Cybersecurity workforce. Students who graduate with the MS in Cyber Operations degree will have tremendous opportunities in government, defense, and private industry, as this graduate program will meet the most demanding academic and technical requirements. Many federal government jobs require a graduate degree in order to offer competitive compensation, thus this program further prepares CAST graduates for success in these positions. Graduates will also be well-qualified to teach future

generations of Cyber Operations students, which is an area within the discipline where there is a significant gap in the number of qualified professionals with the knowledge and skills to be instructors at any level.

- The MS in Cyber & Information Operations degree program will be offered fully online through CAST's unique and state-of-the-art Cyber Virtual Learning Environment (VLE). The academic and research content of the VLE is built around Cyberapolis, a virtual world where students learn and practice both their offensive and defensive cyber skills. The VLE is an unstructured, synthetic, live environment designed to replicate the real internet; providing a realistic, non-scripted platform that forces students to synthesize and apply what they learn. By offering the MS fully online leveraging the VLE, we will be able to offer graduate students anywhere in the world an exciting, interactive learning and research-based experience through the most sophisticated artificial virtual world currently in operation.
- The MS in Cyber & Information Operations degree program is designed as a cohort model, primarily targeted toward working professionals. CAST is recognized for excellence in serving post-traditional students: this proposed MS program will leverage that expertise to provide an accessible and flexible graduate program to working professionals both in and out of the technologically-oriented disciplines. CAST has always been at the forefront of online education, ensuring that online classes provide the greatest possible opportunity for interaction, collaboration, hands-on learning, and research while recognizing the challenges faced by working adults. The cohort model will further facilitate the building of the kinds of relationships among students that is proven factor in success in graduate programs.

III. Brief Program Description: The Master of Science in Cyber & Information Operations prepares graduates for cyber-related occupations and leadership positions in government, defense, law enforcement, and private industry. The curriculum includes both offensive and defensive cyber security and information operations content delivered within our state-of-the-art Cyber Virtual Learning Environment to ensure graduate students have extensive hands-on experiences and research opportunities to develop the knowledge, skills, and abilities necessary to succeed. The MS in Cyber & Information Operations will be offered fully online in a cohort model in order to provide the greatest accessibility and flexibility to working professionals.

IV. Program Rationale: The MS in Cyber & Information Operations is built off of CAST's incredibly successful and nationally recognized BAS in Cyber Operations; one of 24 programs nationwide designated by the National Security Agency as a Center of Academic Excellence in Cyber Operations. It will also draw on faculty expertise from related programs in the college, including BAS programs in Applied Computing and Intelligence and Information Operations. This will be the first graduate program offered by CAST since the college was established in 2019. The work CAST does in Cyber Operations is recognized across the University through internship programs with UITS as well as through a partnership with Facilities Management to strengthen the security of the University's wider infrastructure. According to University of Arizona President Robert C. Robbins, "Cyber is a critical component of the 4th industrial revolution. We're in the right place at the right time for preparing our students. We have a lot to offer the world. The impacts of the Fourth Industrial Revolution will be

felt in all human endeavors and at all levels of our lives: the global economy, businesses, our society, nations and communities, and the individual." Because Cyber Operations is a relatively new field, there are very few graduate programs that offer students the opportunity to become academically competent in the areas of cyber security, intelligence, and information operations while gaining the technical skills necessary to monitor, detect, investigate, analyze, and respond to security events; to protect systems against cybersecurity risks, threats, and vulnerabilities; and design and implement systems and processes intended to keep electronic information secure. The proposed CAST MS in Cyber & Information Operations will offer precisely this type of graduate program. CAST is actively coordinating with other colleges that offer coursework in related disciplines, including the MS in Cybersecurity degree offered by Management and Information Science in Eller, the Electrical and Computer Engineering degree in the College of Engineering, and the Software Engineering degree in the College of Engineering.

V. Projected Enrollment for the First Three Years:

Year 1	Year 2	Year 3
20	40	60

VI. Evidence of Market Demand: According to *Cyber Seek*, a project of the National Institute for Cybersecurity Education (NICE), there are currently [714, 548 cybersecurity job openings nationwide](#). Arizona in particular is at the highest level for critical shortages of qualified cybersecurity professionals, with a [supply/demand ratio](#) of <0.67. The U.S. Bureau of Labor Statistics projects "information security analyst," (only one of the numerous occupations for which a Cyber Operations graduate degree is a desired pathway) will be the tenth fastest growing occupation over the next decade, with an employment growth rate of 31 percent compared to the 4 percent average growth rate for all occupations. While there is [a concerted effort](#), especially by the technology industry, to meet some of the demand through industry certifications, K-12 education initiatives, and community college programs, these efforts do not preclude the need for the highly qualified cyber professionals with advanced degrees who can provide instruction, curriculum design, and capacity building across the cybersecurity career spectrum. Also, the need for cybersecurity professionals with advanced degrees to fill leadership positions across industry, government, and defense is growing exponentially. As an example, [Cybersecurity Ventures](#) predicts that by 2025, 35% of Fortune 500 companies will have board members with cybersecurity experience, and by 2031 that will climb to 50 percent.

VII. Similar Programs Offered at Arizona Public Universities:

- University of Arizona
 - Master of Science in Cybersecurity. This program has two tracks: the Information System track places an emphasis on information security and risk management; the Physical Systems track has an engineering focus with an emphasis on systems security.

- Arizona State University offers three master’s degree programs related to the discipline of cybersecurity:
 - Master of Science in Computer Science with an emphasis in Cyber Security
 - Master of Arts in Global Security with an emphasis in Cybersecurity
 - Master of Arts in Emergency Management & Homeland Security with an emphasis in Cybersecurity

- Northern Arizona University
 - Master of Science in Cybersecurity (it is not clear whether this program is being offered at this time)

- Resources
 - a. Summarize new resources required to offer the program: The MS in Cyber & Information Operations will require 1 FTE instructor during the first year of the program. The master’s level classes will be taught by current CAST Cyber Operations faculty who are members of the graduate faculty: their currently assigned undergraduate classes will be backfilled by a new faculty hire in the Cyber Operations program to cover the first and second year. Current CAST Cyber Operations faculty will teach summer school sessions (2 @ \$7600). A new faculty hire is planned for the third year. During the first year, administration of the program will be handled by current staff and administrators. The need for additional staff will be reevaluated at the end of the first year. The cost to have students participate in the VLE is \$810/year.
 - b. Estimate total expected cost: (see below)
 - c. Estimate total expected revenue of the program: (see below)

MS in Cyber & Information Operations Projected Budget					
	# of Students	Gross Tuition Revenue	Projected Expenses		Total Expenses
		\$750/unit x 18units/year=\$13500	VLE @ \$810/student per year	Faculty FTE @ \$125,200	
Year 1	20	\$270,000	\$16,200	\$125,200	\$141,400
Year 2	40	\$540,000	\$32,400	\$125,200	\$157,600
Year 3	60	\$810,000	\$48,600	\$235,200	\$283,800

IX. Required Signatures (*the following should be included in the notification memo to campus after ABOR approval*):

a. Program Director/Main Proposer:

i. Signature: Nicole Kontak

ii. Name and Title: Nicole Kontak, Assistant Dean for Curricular and Academic Affairs

iii. Date:

b. Managing Unit/Department Head:

i. Signature: J.P.

ii. Name and Title: Josh Pauli, Department Head for Cyber, Intelligence & Information Operations

iii. Date:

c. College Dean/Associate Dean:

i. Signature: Linda Denno

ii. Name and Title: Linda Denno, Associate Dean

iii. Date:












MS in CybOps Preliminary_Proposal_Majors


Final Audit Report

2022-09-15


Created:	2022-09-15
By:	Linda Denno (lddenno@email.arizona.edu)
Status:	Signed
Transaction ID:	CBJCHBCAABAAijmoyMi4iH5jS_W4sxaWnlGywYXiU5mm

"MS in CybOps Preliminary_Proposal_Majors" History

-  Document created by Linda Denno (lddenno@email.arizona.edu)
2022-09-15 - 8:43:30 PM GMT
-  Document emailed to Nicole Kontak (nicoler@arizona.edu) for signature
2022-09-15 - 8:44:43 PM GMT
-  Email viewed by Nicole Kontak (nicoler@arizona.edu)
2022-09-15 - 10:11:44 PM GMT
-  Document e-signed by Nicole Kontak (nicoler@arizona.edu)
Signature Date: 2022-09-15 - 10:12:06 PM GMT - Time Source: server
-  Document emailed to jjpauli@email.arizona.edu for signature
2022-09-15 - 10:12:08 PM GMT
-  Email viewed by jjpauli@email.arizona.edu
2022-09-15 - 10:43:04 PM GMT
-  Signer jjpauli@email.arizona.edu entered name at signing as Josh Pauli
2022-09-15 - 10:43:52 PM GMT
-  Document e-signed by Josh Pauli (jjpauli@email.arizona.edu)
Signature Date: 2022-09-15 - 10:43:53 PM GMT - Time Source: server
-  Document emailed to lddenno@arizona.edu for signature
2022-09-15 - 10:43:55 PM GMT
-  Email viewed by lddenno@arizona.edu
2022-09-15 - 10:44:10 PM GMT
-  Signer lddenno@arizona.edu entered name at signing as Linda L Denno
2022-09-15 - 10:45:11 PM GMT


 Document e-signed by Linda L Denno (ldenno@arizona.edu)

Signature Date: 2022-09-15 - 10:45:13 PM GMT - Time Source: server

 Agreement completed.

2022-09-15 - 10:45:13 PM GMT

To: Nicole Kontak, Assistant Dean for Curricular and Academic Affairs,
College of applied Science & Technology
Josh Pauli, Department Head for Cyber, Intelligence & Information Operations,
College of Applied Science & Technology

From: Greg Heileman, PhD, Vice Provost for Undergraduate Education 


Date: November 15, 2022

Subject: Approval of Preliminary Proposal for Master of Science, Cyber & Information Operations

Thank you for submitting the preliminary review proposal for the Master of Science, Cyber & Information Operations degree. The proposed academic program should provide an excellent educational opportunity and a useful degree in which students who graduate with the MS in Cyber & Information Operations degree will have tremendous opportunities in government, defense and private industry as this graduate program will meet the most demanding academic and technical requirements. We believe your ideas are sufficiently well developed that it now makes sense to advance through the stages of the formal academic program approval process.

Please proceed to the development of a full proposal, and do not hesitate to reach out the Curricular Affairs Office for assistance with this process.

CC: Liesl Folks, Senior Vice President for Academic Affairs and
Provost Liz Sandoval, Director, Curricular Affairs
Linda Denno, Associate Dean



New Academic Program Workflow Form

General

Proposed Name: Cyber & Information Operations

Transaction Nbr: 00000000000166

Plan Type: Major

Academic Career: Graduate

Degree Offered: Master of Science

Do you want to offer a minor? N

Anticipated 1st Admission Term: Fall 2023

Details

Department(s):

UAZS

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

Campus(es):

MAIN

LOCATION	DESCRIPTION
TUCSON	Tucson

ONLN

LOCATION	DESCRIPTION
ONLN	Online

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

Plan admission types:

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

Non Degree Certificate (UCRT only): Y

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 Master of Science Cyber and Information Operations

Transcript: Y Master of Science Cyber and Information Operations

Conditions for Admission/Declaration for this Major:

-BA/BAS/BS or equivalent degree and meets admissions criteria of the Graduate College.

-Successful completion of CYBV500: Security Computing or prior undergraduate coursework in computer programming.

Requirements for Accreditation:

N/A

Program Comparisons

University Appropriateness

The Master of Science in Cyber & Information Operations prepares graduates for cyber-related occupations and leadership positions in government, defense, law enforcement, and private industry. The curriculum includes both offensive and defensive cyber security and information operations content delivered within our state-of-the-art Cyber Virtual Learning Environment to ensure graduate students have extensive hands-on experiences and research opportunities to develop the knowledge, skills, and abilities necessary to succeed. The MS in Cyber & Information Operations is offered fully online in a cohort model in order to provide the greatest accessibility and flexibility to working professionals. The MS in Cyber & Information Operations is built off of CAST's incredibly successful and nationally recognized BAS in Cyber Operations; one of 24 programs nationwide designated by the National Security Agency as a Center of Academic Excellence in Cyber Operations. It will also draw on faculty expertise from related programs in the college, including BAS programs in Applied Computing and Intelligence and Information Operations. This will be the first graduate program offered by CAST since the college was established in 2019. The work CAST does in Cyber & Information Operations is recognized across the University through internship programs with UITS as well as through a partnership with Facilities Management to strengthen the security of the University's wider infrastructure. According to University of Arizona President Robert C. Robbins, "Cyber is a critical component

of the 4th industrial revolution. We're in the right place at the right time for preparing our students. We have a lot to offer the world. The impacts of the Fourth Industrial Revolution will be felt in all human endeavors and at all levels of our lives: the global economy, businesses, our society, nations and communities, and the individual." CAST is actively coordinating with other colleges that offer coursework in related disciplines, including the MS in Cybersecurity degree offered by Management and Information Science in Eller, the Electrical and Computer Engineering degree in the College of Engineering, and the Software Engineering degree in the College of Engineering.

Arizona University System

NBR	PROGRAM	DEGREE	#STDNTS	LOCATION	ACCRDT
1	CS emphasis in Cybersecurity	MS	1	ASU Tempe and Online	Y
2	Global Security	MA	1	ASU online	Y
3	Emer Mgmt /HomeInd Sec Cybrsec	MA	1	ASU	Y
4	Cybersecurity	MS	1	NAU Online	Y
5	Cybersecurity	MS	61	University of Arizona Online	Y

Peer Comparison

Similarities: The Penn State program is very comparable to CAST's proposed program. Penn State prepares students for government, DoD, military, and federal positions in cyber security. The required pre-admission expectations are also similar with regards to any undergraduate degree being admissible with the necessity of students having experience with programming languages. Both programs also offer a thesis or research option. Both programs cover offensive and defensive cybersecurity and information warfare coursework.

Differences: The Texas A&M degree is different, mainly with regards to the degree being in Engineering and having a large engineering focus. However, we highlighted the specific cyber focused courses in the program in the comparison chart to show the alignment in cyber content and offensive and defensive cybersecurity coursework, which is current and relevant curriculum.

Faculty & Resources

Faculty

Current Faculty:

INSTR ID	NAME	DEPT	RANK	DEGREE	FCLTY/%
22056021	Ryan Straight	2910	Assoc. Prof. Pract.	Doctor of Philosophy	.10
22063853	William Mapp	2910	Assoc. Prof. Pract.	Doctor of Philosophy	.10
22074078	Thomas Jewkes	2910	Assit. Prof. Pract.	Master of Science	.10
22078226	Paul Wagner	2910	Assoc. Prof. Pract.	Master of Science	.10
22080699	Heidi Calhoun-lopez	2910	Assit. Prof. Pract.	Juris Doctor	.10
22081494	Jordan Vanhoy	2910	Assit. Prof. Pract.	Master of Science	.10
22083351	Chester Hosmer	2910	Assit. Prof. Pract.	Bachelor of Science	.10
22086411	Michael Galde	2910	Assit. Prof. Pract.	Master of Science	.10
22088394	Michael Duren	2910	Assit. Prof. Pract.	Master of Science	.10
22091418	Dalal Alharthi	2910	Assit. Prof	Doctor of Philosophy	.10
22094003	Joshua Pauli	2910	Professor	Doctor of Philosophy	.10
22095567	Robert Honomichl	2910	Assit. Prof. Pract.	Master of Science	.10
23569467	Michael Benson	2910	Assit. Prof. Pract.	Master of Science	.10

Additional Faculty:

The MS in Cyber & Information Operations will require 2 FTE instructors during the first year of the program. The master's level classes will be taught by current CAST Cyber & Information Operations faculty who are members of the graduate faculty: their currently assigned undergraduate classes will be backfilled by a new faculty hire in the Cyber & Information Operations program to cover the first and second year. A new faculty hire is planned for the second year and two new faculty hires are planned for the third year. During the first year, administration of the program will be handled by current staff and administrators. The need for additional staff will be reevaluated at the end of the first year.

Current Student & Faculty FTE

DEPARTMENT	UGRD HEAD COUNT	GRAD HEAD COUNT	FACULTY FTE
2910	968	0	19.00

Projected Student & Faculty FTE

DEPT	UGRD HEAD COUNT			GRAD HEAD COUNT			FACULTY FTE		
	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3
2910	0	0	0	50	100	115	2.00	3.00	5.00

Library

Acquisitions Needed:

N/A

Physical Facilities & Equipment

Existing Physical Facilities:

The curriculum includes both offensive and defensive cyber security and information operations content delivered within our state-of-the-art Cyber Virtual Learning Environment to ensure graduate students have extensive hands-on experiences and research opportunities to develop the knowledge, skills, and abilities necessary to succeed. The MS in Cyber & Information Operations is offered fully online in a cohort model in order to provide the greatest accessibility and flexibility to working professionals.

Additional Facilities Required & Anticipated:

N/A

Other Support

Other Support Currently Available:

There is a robust student services team in CAST to support students: academic advisors, retention specialist, and recruitment and enrollment team. CIIO also has numerous support staff.

Other Support Needed over the Next Three Years:

We may consider hiring Graduate Advisors (professional staff) to accommodate the growing number of students.

Comments During Approval Process

12/13/2022 9:43 AM

NICOLER

Comments
Approved.

1/12/2023 2:32 PM

ESANDMAR

Comments
Approved.



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

I. **MAJOR REQUIREMENTS**– complete the table below by listing the major requirements, including required number of units, required core, electives, and any special requirements, including emphases* (sub-plans), thesis, internships, etc. Note: information in this section must be consistent throughout the proposal documents (comparison charts, four-year plan, curricular/assessment map, etc.).

GRADUATE

Total units required to complete the degree	30
Pre-admissions expectations (i.e., academic training to be completed prior to admission)	<p>-BA/BAS/BS or equivalent degree and meets admissions criteria of the Graduate College.</p> <p>-Successful completion of CYBV500: Security Computing or prior undergraduate coursework in computer programming.</p>
<p>Major requirements. List all major requirements including core and electives. If applicable, list the emphasis requirements for each proposed emphasis*. 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.</p>	<p>CORE (24 units):</p> <ul style="list-style-type: none"> • CYBV501: Principles of Cybersecurity—3 units • CYBV523: Covert Python—3 units • CYBV529: Cyber Law, Ethics & Policy—3 units • CYBV579: Cloud Security—3 units • CYBV626: Traffic Analysis—3 units • CYBV660: Zero Trust Defensive Techniques—3 units • CYBV685: Information Warfare—3 units • CYBV 909: Master’s Report in Cyber & Information Operations—3 units <p>OR</p> <ul style="list-style-type: none"> • CYBV 910: Master’s Thesis in Cyber & Information Operations—3 units <p>ELECTIVES (Choose 2 courses)</p> <ul style="list-style-type: none"> • CYBV525: Cyber Physical Systems – 3 units • CYBV528: Operational Tradecraft in the Information Environment—3 units • CYBV581: Privacy and Regulatory Requirements in Cybersecurity – 3 units • CYBV630: Industrial Control System Security – 3 units • CYBV680: Computational Propaganda—3 units • CYBV683: Strategic Cyber Management—3 units • CYBV 696: Special Topics in Cyber & Intelligence Operations



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Research methods, data analysis, and methodology requirements (Yes/No). If yes, provide description.	Research methodologies and data analyses are incorporated into the Master's Report/Thesis courses.
Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	No
Master thesis or dissertation required (Yes/No). If yes, provide description.	A master's thesis is an option if students plan on continuing into a doctoral program.
Additional requirements (provide description)	N/A
Minor options (as relevant)	No required minor options.

II. **CURRENT COURSES**—using the table below, list all existing courses included in the proposed major. You can find information to complete the table using the [UARIZONA 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 program 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 or remove rows to the table, as needed.

N/A - No existing courses will be included in the proposed major

III. **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 (i.e., CHEM 4XX). Add rows as needed.

Course prefix and number (include cross-listings)	Units	Title	Pre-requisites	Modes of delivery (online, in-person, hybrid)	Status*	Anticipated first term offered	Typically Offered (F, W, Sp, Su)	Dept signed party to proposal? (Yes/No)	Faculty members available to teach the courses
CYBV500	3	Security Programming		Online	D	Summer, 2023	SU	Yes	Yes
CYBV501	3	Principles of Cybersecurity		Online	D	Fall, 2023	F	Yes	Yes



THE UNIVERSITY OF ARIZONA

ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

CYBV523	3	Covert Python		Online	D	Fall, 2023	F	Yes	Yes
CYBV525	3	Cyber Physical Systems			D	Fall, 2024			
CYBV528	3	Operational Tradecraft in the Information Environment		Online	D	Fall, 2024	F	Yes	Yes
CYBV529	3	Cyber Law, Ethics & Policy		Online	D	Fall, 2023	F	Yes	Yes
CYBV579	3	Cloud Security		Online	D	Spring, 2024	Sp	Yes	Yes
CYBV581	3	Privacy and Regulatory Requirements in Cybersecurity		Online	D	Fall, 2024	F	Yes	Yes
CYBV626	3	Traffic Analysis		Online	D	Spring, 2024	Sp	Yes	Yes
CYBV630	3	Industrial Control System Security		Online	D	Fall, 2024	Sp	Yes	Yes
CYBV660	3	Zero Trust Defensive Techniques		Online	D	Spring, 2024	Sp	Yes	Yes
CYBV680	3	Computational Propaganda		Online	D	Fall, 2024	F	Yes	Yes
CYBV683	3	Strategic Cyber Management		Online	D	Fall, 2024	F	Yes	Yes
CYBV685	3	Information Warfare		Online	D	Spring, 2025	F	Yes	Yes
CYBV 696	3	Special Topics in Cyber & Information Operations		Online	D	Spring, 2025	S	Yes	Yes
CYBV909	3	Master’s Report in Cyber & Information Operations		Online	D	Spring, 2025	Sp	Yes	Yes
CYBV910	3	Master’s Thesis in Cyber & Information Operations		Online	D	Spring, 2025	Sp	Yes	Yes

*In development (D); submitted for approval (S); approved (A)

Click or tap here to enter text.

IV. FACULTY INFORMATION- complete the table below. If UA Vitae link is not provided/available, add CVs to a Box folder and provide that link. UA Vitae profiles can be found in the [UARIZONA 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 [Office of Curricular Affairs](#) if you have concerns about CV information being “publicly visible”.



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Faculty Member	Involvement	UA Vitae link or Box folder link
Robert Honomichl	CYBV500	All faculty CVs https://arizona.box.com/s/qcpn1edbxqamiub7w3htpk13y2td6a4r
Josh Pauli	CYBV501	
Mike Duren	CYBV523	
Mike Galde	CYBV525	
Mike Benson	CYBV528	
Heidi Calhoun-Lopez	CYBV529	
Dalal Al-Harathi	CYBV579	
Jordan Van Hoy	CYBV581	
Chet Hosmer	CYBV626	
Chet Hosmer	CYBV630	
Tom Jewkes	CYBV660	
Mike Benson	CYBV680	
Eric Mapp	CYBV683	
Paul Wagner	CYBV685	
Ryan Straight	CYBV909	
Ryan Straight	CYBV910	

V. **GRADUATION PLAN** – provide a sample degree plan, based on your program that includes all requirements to graduate with this major and takes into consideration course offerings and sequencing. *Undergraduate programs: please complete [Addendum D: 4-Year Plan for Degree Search](#). Use generic title/placeholder for requirements with more than one course option (e.g., Upper Division Major Elective, Minor Course, Second Language, GE Tier 1, GE Tier 2). Add rows as needed.*

Semester 1		Semester 2		Semester 3		Semester 4	
Course prefix and number	Units	Course prefix and number	Units	Course prefix and number	Units	Course prefix and number	Units
CYBV501	3	CYBV579	3	CYBV Elective	3	CYBV909 (or)	3
CYBV523	3	CYBV626	3	CYBV Elective	3	CYBV910	3
CYBV529	3	CYBV630	3	CYBV685	3		



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Total	9	Total	9	Total	9	Total	3

Semester 5		Semester 6		Semester 7		Semester 8	
Course prefix and number	Units	Course prefix and number	Units	Course prefix and number	Units	Course prefix and number	Units
Total		Total		Total		Total	



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

VI. **Curriculum Map and Assessment Map** - Complete this table as a summary of your learning outcomes and assessment plan, using these examples as a model. If you need assistance completing this table and/or the Curriculum Map, please contact the [Office of Instruction and Assessment](#). Attach your Curriculum Map here.

Curriculum Map

Course/Grad Checkpoint	Outcome 1 Demonstrate and apply knowledge of offensive cyber operations.	Outcome 2 Demonstrate and apply knowledge of defensive cyber operations.	Outcome 3 Identify, evaluate, and defend against Information Operation campaigns.	Outcome 4 Explain the relationship among and apply knowledge of cyber ethics, cyber policy, and US and International cyber laws.
CYBV 501	I	I	I	I
CYBV 523	P	P		
CYBV528			P	
CYBV 529				P/A
CYBV 579		P/A		
CYBV 581	P/A			P/A
CYBV 626	P/A	P/A		
CYBV 630	P/A	P/A		P/A
CYBV 660		P/A		
CYBV 680	P/A		P/A	
CYBV 683				P/A
CYBV 685	P/A		P/A	
CYBV 909/910	P/A	P/A	P/A	P/A

I = Introduced P = Practiced A = Assessed



THE UNIVERSITY
OF ARIZONA

ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Program: MS Cyber & Information Operations

Learning Outcome #1: Demonstrate and apply knowledge of offensive cyber operations.
Concepts: Understanding of offensive cyber operations; who has authority to conduct offensive cyber operations; and how those operations are conducted and assessed upon completion.
Competencies: Demonstrated mastery of the phases of offensive cyber operations; apply knowledge of how offensive cyber operations are conducted; assess the success of offensive cyber operations.
Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master's Report or Thesis.
Measures: Instructor grading of course-embedded exams, practical exercises, & lab reports and through the final Master's Report or Thesis.
Learning Outcome #2: Demonstrate and apply knowledge of defensive cyber operations.
Concepts: Secure critical infrastructures; prevent and respond to cyberattacks; understand and apply network security; understand and computer security; understand and explain security principles and vulnerabilities.
Competencies: Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals; monitor networks to prevent and respond proactively to cyberattacks; safely perform static and dynamic analysis of unknown software
Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master's Report or Thesis.
Measures: Instructor grading of course-embedded exams, practical exercises, & lab reports and through the final Master's Report or Thesis.
Learning Outcome #3: Identify, evaluate, and apply tactics, techniques, and procedures used to conduct and defend against Information Operation campaigns.
Concepts: Information Warfare; Students will apply knowledge to detect, protect, and craft information campaigns.
Competencies: Students will recognize online influence efforts in order to be able to detect, deconstruct, and counter adversarial information warfare campaigns.
Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master's Report or Thesis.
Measures: Instructor grading of course-embedded exams, practical exercises, & lab reports and through the final Master's Report or Thesis.
Learning Outcome #4: Explain the relationship among and apply knowledge of cyber ethics, cyber policy, and US and International cyber laws.
Concepts: Identify and apply ethical and legal dilemmas in cyberspace; relevant state, national, and international laws and policies governing cyberspace; demonstrate understanding of criminal penalties related to unethical hacking, data privacy, and misuse of technology.



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Competencies: Students will demonstrate their ability to apply knowledge of Cyber ethics, law, and policy in the private, corporate, and government sectors; apply knowledge to the creation of new cyber policy.
Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.
Measures: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.

VII. **PROGRAM ASSESSMENT PLAN-** using the table below, provide a schedule for program evaluation 1) while students are in the program and 2) after completion of the major. Add rows as needed. Delete **EXAMPLE** rows.

Assessment Measure	Source(s) of Evidence	Data Collection Point(s)
Job Placement Statistics	Student/Alumni Survey	At graduation and as part of alumni survey
Academic Program Review	Reviewers’ responses	Every 7 years
Program Curriculum Review	Interdisciplinary Board reviewer’s response	Biannually
Advisory Board Program Review	Advisory Board reviewer’s response	Biannually

To provide information to the Department Head, faculty members, and Advisory Board, the MS in Cyber & Information Operations program office will administer surveys to the graduates of the MS in Cyber & Information Operations degree program. The first survey will be administered in the CYBV 909/910 culminating course and will be a required course component. This survey is designed to provide more general information about student opinions on the degree program’s alumni support options, job placement, and preparedness to work in the Cyber Operations field. Subsequently, this survey will be emailed out three months after graduation, with a telephone call reminder to complete the survey. It will be emailed out again nine months after graduation, with a reminder call if necessary. Thereafter, the survey will be administered once per year to continue to provide longitudinal data to the Program Director, faculty members, and the Advisory Board.

Further program assessment will be provided by the Advisory Board. The Advisory Board consists of leaders in different portions of the cyber field, including those working in the government, the military, and private sector. The Advisory Board will be convened twice each calendar year for a meeting with the current faculty members and the Department Head to review the MS in Cyber & Information Operations graduate curriculum to be certain it is adjusting as needed to meet market demands and to ensure that the knowledge, skills, and abilities employers are seeking are being addressed by our curriculum.



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

VIII. **ANTICIPATED STUDENT ENROLLMENT**-complete the table below. What concrete evidence/data was used to arrive at the numbers?

5-YEAR PROJECTED ANNUAL ENROLLMENT					
	1 st Year	2 nd Year	3 rd Year	4 th Year	5 th Year
Number of Students	50	100	115	115	125

Data/evidence used to determine projected enrollment numbers:

Estimated enrollment is based upon both the unprecedented growth in and reputation of our BAS In Cyber Operations and the fact that CAST has continuously received requests to offer a master’s degree in MS in Cyber & Information Operations. A significant number of the students in our bachelor’s program already possess a bachelor’s degree and even a graduate degree but choose to enroll in our BAS in Cyber Operations program to gain the knowledge and skills necessary to be employable in what is one of the fastest growing career fields worldwide. Many of these students, as well as students working toward their first bachelor’s degree in our program, have expressed a desire to enroll in a CAST MS in Cyber & Information Operations program. There is continued and increasing demand, both within the United States and worldwide, for qualified cyber professionals. *Cybersecurity Ventures*, a leading professional publication in the cybersecurity field, reports that there were 3.5 million unfilled jobs in 2021. It is not simply government and defense industries that are seeking qualified cyber professionals. Cybersecurity is the #1 business risk, with cybercrime expected to cost the world \$7 trillion USD in 2022. Because of this high demand, CAST has seen enrollment in its Cyber Operations undergraduate degree and certificate programs grow from 274 in 2019 to 1311 in Fall 2022, a growth rate of 380% over three years. CAST believes that the demand for the MS in Cyber & Information Operations will follow this trajectory and will likely outpace our ability to meet that demand. Moreover, CAST has had a number of its Cyber Operations, Applied Computing, and Intelligence & Information Operations undergraduate students receive full scholarships from the Department of Defense Cyber Scholarship Program (CySP), which will provide a significant percentage of the projected enrollment in this Master’s program.

IX. **ANTICIPATED DEGREES AWARDED**- complete the table below, beginning with the first year in which degrees will be awarded. How did you arrive at these numbers? Take into consideration departmental retention rates. Use [National Center for Education Statistics College Navigator](https://nces.ed/ipeds/datacenter/collegenavigator/) to find program completion information of peer institutions offering the same or a similar program.

PROJECTED DEGREES AWARDED ANNUALLY					
	1 st Year	2 nd Year	3 rd Year	4 th Year	5 th Year
Number of Degrees	0	35	50	60	70

ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Data/evidence used to determine number of anticipated degrees awarded annually:

The MS in Cyber & Information Operations degree program is designed as a cohort model, primarily targeted toward working professionals. The anticipated degrees awarded annually takes into account both full-time students and part-time progress toward completion in two academic years. While it is of course expected that some students will progress more quickly and some more slowly, we believe the cohort model will provide the necessary support structure for most students to progress along with their cohort. CAST has always been at the forefront of online education, ensuring that online classes provide the greatest possible opportunity for interaction, collaboration, hands-on learning, and research while recognizing the challenges faced by working adults. The cohort model will further facilitate the building of the kinds of relationships among students that is proven factor in success in graduate programs.

- X. PROGRAM DEVELOPMENT TIMELINE-** describe plans and timelines for 1) marketing the major and 2) student recruitment activities. The target audience consists of graduates from our BAS degrees in Cyber Operations, Applied Computing, and Intelligence & Information Operations, especially those who are awarded *Scholarship for Service* and *CySP* full-ride scholarships; students currently working in technology and related fields; veterans and military connected students; and other career-oriented post-traditional students. Our prospective student population is results-oriented and career-focused, with an interest in pursuing a graduate degree that will advance their current career or enable them to switch to a lucrative career in one of the fastest growing fields.
- 1) The MS in Cyber & Information Operations program will build on existing marketing that has successfully increased enrollment in our related BAS degrees by more than 500% over the past three years
 - a. The M.S in Cyber & Information Operations will be marketed on the newly built AZCAST.arizona.edu Cyber & Information Operations website. Once approved, the graduate program will leverage elements of the existing undergraduate program website, which provides detailed information on our National Security Agency (NSA) designation as a National Center of Academic Excellence in Cyber Operations (CAE-CO); the UArizona CyberApolis Cyber Virtual Learning Environment; Cyber & Intelligence Operations Career information; and Cyber & Intelligence Operations faculty. The M.S. in Cyber & Information Operations website will link to the UARIZONA Main website, AZOnline, and the UARIZONA graduate admissions application website.
 - b. The MS in Cyber & Information Operations will also leverage the current undergraduate program, which is 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/>. The Cyber Degrees website also provides high level details on our Cyber Virtual Learning Environment.
 - c. The MS in Cyber & Information Operations will develop detailed program brochures, including information about the uniqueness of the program, Graduate Admissions, the Cyber Virtual Learning Environment, and Career Opportunities.
 - d. CAST works closely with AZOnline Marketing to reach a statewide, national, and international market. CAST has been in close consultation throughout the development of the MS in Cyber & Information Operations program to ensure that, once the



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

- program receives final approval, a coordinated marketing campaign can be implemented immediately.
- e. 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 & Information Operations students. *The Packet* is also sent to all of the Cyber Operations industry, government, and academic partner institutions. *The Packet* is a 20 to 40-page document that provides students details on: Major Cyber & Information Operations related events for the month; upcoming semester course offerings; UARIZONA Spotlight on two or more of our Cyber & Information 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. The MS in Cyber Operations will be featured prominently in *The Packet* once approved.
- 2) We will implement an initial student recruitment plan that consists of the following:

By means of digital and print media, radio ads, outdoor advertising such as news releases, direct mail, direct e-mail, website, social media, and personal outreach by the Student Services Team, our promotion and communication efforts will focus on raising awareness of the value of obtaining a Master of Science degree in Cyber & Information Operations, 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. Once the students have moved beyond awareness and interest in the college, we will leverage interactive communication channels (Slate) 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 can access details to reinforce the value of obtaining their degree here, from seeing the lower tuition rates available to CAST and AZOnline students to learning more about the nationally recognized caliber of the curriculum.
- XI. **Program Fees and Differential Tuition (PFDT) Request** – For implementation of fees, you must work with [University Fees](#). The annual deadline is December 1. For any questions, please contact the [University Fees Program Manager](#).

We anticipate the majority of our students will enroll in the AZOnline campus. We are setting tuition for that campus at \$750/unit. We will also offer this program on main campus through the main campus resident tuition model, although all classes will be fully online. We will not be asking for additional specific program fees or differential tuition. The latter will make the MS in Cyber & Information Operations available to Arizona residents and allow students in other graduate programs on main campus to take graduate classes in Cyber Operations.



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Appendix C. ABOR Form

Request to Establish New Academic Program in Arizona

University: University of Arizona

Name of Proposed Academic Program: Master of Science in Cyber & Information Operations
Academic Department: College of Applied Science & Technology: Cyber, Intelligence, & Information Operations
Geographic Site: University of Arizona Sierra Vista Campus, ONLN Campus
Instructional Modality: icourse/fully online/ONLN Campus
Total Credit Hours: 30
Proposed Inception Term: Fall, 2023
<p>Brief Program Description:</p> <p>The Master of Science in Cyber & Information Operations prepares graduates for cyber-related occupations and leadership positions in government, defense, law enforcement, and private industry. The curriculum includes both offensive and defensive cyber security and information operations content delivered within our state-of-the-art Cyber Virtual Learning Environment to ensure graduate students have extensive hands-on experiences and research opportunities to develop the knowledge, skills, and abilities necessary to succeed. The MS in Cyber & Information Operations is offered fully online in a cohort model in order to provide the greatest accessibility and flexibility to working professionals. The MS in Cyber & Information Operations is built off of CAST’s incredibly successful and nationally recognized BAS in Cyber Operations; one of 24 programs nationwide designated by the National Security Agency as a Center of Academic Excellence in Cyber Operations. It will also draw on faculty expertise from related programs in the college, including BAS programs in Applied Computing and Intelligence and Information Operations. This will be the first graduate program offered by CAST since the college was established in 2019. The work CAST does in Cyber & Information Operations is recognized across the University through internship programs with UITS as well as through a partnership with Facilities Management to strengthen the security of the University’s wider infrastructure. According to University of Arizona President Robert C. Robbins, "Cyber is a critical component of the 4th industrial revolution. We're in the right place at the right time for preparing our students. We have a lot to offer the world. The impacts of the Fourth Industrial Revolution will be felt in all human endeavors and at all levels of our lives: the global economy, businesses, our society, nations and communities, and the individual." CAST is actively coordinating with other colleges that offer coursework in related disciplines, including the MS in Cybersecurity degree offered by Management and Information Science in Eller, the Electrical and Computer Engineering degree in the College of Engineering, and the Software Engineering degree in the College of Engineering.</p>
Learning Outcomes and Assessment Plan: MS Cyber & Information Operations
Learning Outcome #1: Demonstrate and apply knowledge of offensive cyber operations.



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

<p>Concepts: Understanding of offensive cyber operations; who has authority to conduct offensive cyber operations; and how those operations are conducted and assessed upon completion.</p>
<p>Competencies: Demonstrated mastery of the phases of offensive cyber operations; apply knowledge of how offensive cyber operations are conducted; assess the success of offensive cyber operations.</p>
<p>Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>
<p>Measures: Instructor grading of course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>
<p>Learning Outcome #2: Demonstrate and apply knowledge of defensive cyber operations.</p>
<p>Concepts: Secure critical infrastructures; prevent and respond to cyberattacks; understand and apply network security; understand and computer security; understand and explain security principles and vulnerabilities.</p>
<p>Competencies: Describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals; monitor networks to prevent and respond proactively to cyberattacks; safely perform static and dynamic analysis of unknown software</p>
<p>Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>
<p>Measures: Instructor grading of course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>
<p>Learning Outcome #3: Identify, evaluate, and apply tactics, techniques, and procedures used to conduct and defend against Information Operation campaigns.</p>
<p>Concepts: Information Warfare; Students will apply knowledge to detect, protect, and craft information campaigns.</p>
<p>Competencies: Students will recognize online influence efforts in order to be able to detect, deconstruct, and counter adversarial information warfare campaigns.</p>
<p>Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>
<p>Measures: Instructor grading of course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>
<p>Learning Outcome #4: Explain the relationship among and apply knowledge of cyber ethics, cyber policy, and US and International cyber laws.</p>
<p>Concepts: Identify and apply ethical and legal dilemmas in cyberspace; relevant state, national, and international laws and policies governing cyberspace; demonstrate understanding of criminal penalties related to unethical hacking, data privacy, and misuse of technology.</p>
<p>Competencies: Students will demonstrate their ability to apply knowledge of Cyber ethics, law, and policy in the private, corporate, and government sectors; apply knowledge to the creation of new cyber policy.</p>
<p>Assessment Methods: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>
<p>Measures: This outcome will be assessed through course-embedded exams, practical exercises, & lab reports and through the final Master’s Report or Thesis.</p>



ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

Projected Enrollment for the First Three Years:

3-Year Projected Annual Enrollment: 1st year: 50 students; 2nd year: 100 students; 3rd year: 115 students.

Evidence of Market Demand:

According to *Cyber Seek*, a project of the National Institute for Cybersecurity Education (NICE), there are currently [714, 548 cybersecurity job openings nationwide](#). Arizona in particular is at the highest level for critical shortages of qualified cybersecurity professionals, with a [supply/demand ratio](#) of <0.67. The U.S. Bureau of Labor Statistics projects “information security analyst,” (only one of the numerous occupations for which a Cyber Operations graduate degree is a desired pathway) will be the tenth fastest growing occupation over the next decade, with an employment growth rate of 31 percent compared to the 4 percent average growth rate for all occupations. While there is [a concerted effort](#), especially by the technology industry, to meet some of the demand through industry certifications, K-12 education initiatives, and community college programs, these efforts do not preclude the need for the highly qualified cyber professionals with advanced degrees who can provide instruction, curriculum design, and capacity building across the cybersecurity career spectrum. Also, the need for cybersecurity professionals with advanced degrees to fill leadership positions across industry, government, and defense is growing exponentially. As an example, [Cybersecurity Ventures](#) predicts that by 2025, 35% of Fortune 500 companies will have board members with cybersecurity experience, and by 2031 that will climb to 50 percent.

Similar Programs Offered at Arizona Public Universities:

- University of Arizona
 - Master of Science in Cybersecurity. This program has two tracks: the Information System track places an emphasis on information security and risk management; the Physical Systems track has an engineering focus with an emphasis on systems security.
- Arizona State University offers three master’s degree programs related to the discipline of cybersecurity:
 - Master of Science in Computer Science with an emphasis in Cyber Security
 - Master of Arts in Global Security with an emphasis in Cybersecurity
 - Master of Arts in Emergency Management & Homeland Security with an emphasis in Cybersecurity
- Northern Arizona University
 - Master of Science in Cybersecurity (it is not clear whether this program is being offered at this time)

FOR CURRICULAR AFFAIRS USE ONLY

Objection(s) Raised by Another Arizona Public University? YES NO

Has another Arizona public university lodged a written objection to the proposed program with the proposing university and the Board of Regents within seven days of receiving notice of the proposed program?

If Yes, Response to Objections:

Please provide details of how the proposing university has addressed the objection. If the objection remains unresolved, please explain why it is in the best interests of the university system and the state that the Board override it.



THE UNIVERSITY
OF ARIZONA

ACADEMIC PROGRAM – ADDITIONAL INFORMATION FORM

To be used once the preliminary proposal has been approved.

New Resources Required? (i.e., faculty and administrative positions; infrastructure, etc.):

The MS in Cyber & Information Operations will require 2 FTE instructors during the first year of the program. The master's level classes will be taught by current CAST Cyber & Information Operations faculty who are members of the graduate faculty: their currently assigned undergraduate classes will be backfilled by a new faculty hire in the Cyber & Information Operations program to cover the first and second year. A new faculty hire is planned for the second year and two new faculty hires are planned for the third year. During the first year, administration of the program will be handled by current staff and administrators. The need for additional staff will be reevaluated at the end of the first year. The cost to have students participate in the VLE is \$810/year.

Plan to Request Program Fee/Differentiated Tuition? YES NO

Estimated Amount:

Program Fee Justification:

Note: The fee setting process requires additional steps and forms that need to be completed. Please work with your [University Fees](#) office to complete a fee request.

Specialized Accreditation? YES NO

Accreditor:

The name of the agency or entity from which accreditation will be sought

Graduate Major 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 majors within the discipline. The comparison programs are not required to have the same degree type and/or major name as the proposed UA program. Information for the proposed UA program must be consistent throughout the proposal documents.

Program name, emphasis (sub-plan) name (if applicable), degree, and institution	Proposed UA Program: MS Cyber & Information Operations	Peer 1: MS Cybersecurity Analytics and Operations Penn State (ABOR Peer)	Peer 2: ME in Engineering with a Specialization in Cybersecurity Texas A&M (ABOR Peer)
Current # of enrolled students			
Major Description. Includes the purpose, nature, and highlights of the curriculum, faculty expertise, emphases (sub-plans; if any), etc.	<p>The Master of Science in Cyber & Information Operations prepares graduates for cyber-related occupations and leadership positions in government, defense, law enforcement, and private industry. The curriculum includes both offensive and defensive cyber security and information operations content delivered within our state-of-the-art Cyber Virtual Learning Environment to ensure graduate students have extensive hands-on experiences and research opportunities to develop the knowledge, skills, and abilities necessary to succeed. The MS in Cyber & Information Operations is offered fully online in a cohort model in order to provide the greatest accessibility and flexibility to working professionals. The MS in Cyber & Information Operations is built off of CAST's incredibly successful and nationally recognized BAS in Cyber Operations; one of 24 programs nationwide designated by the National Security Agency as a Center of Academic Excellence in Cyber Operations.</p>	<p>The Master of Science in Cybersecurity Analytics and Operations program is designed to create a deep understanding of cybersecurity analytics and operations, by blending education relating to technology, incident response, strategic planning, and crisis management. The program also aims to prepare the next generation of cybersecurity analysts to better protect digital information from attack through cyberdefense strategies, including incident response, strategic planning, and crisis management. With a foundation in mathematics and computer programming, students will be prepared to recognize, analyze, defend against, and manage risks related to a wide range of threats to online information, data stores, and networks.</p>	<p>The dependence of public, private, not-for-profit and non-governmental organizations on cyber systems for the security, safety and privacy of the individuals they serve and the enterprises they operate increases as the digital age advances.</p> <p>As society becomes more and more connected, and as smart systems continue to evolve, there is a clear need for engineers in all fields to develop a good understanding of cybersecurity principles. For example, a biomedical engineer needs to understand the cybersecurity implications of medical devices and the privacy of medical records and a civil engineer needs to understand the cybersecurity implications of connected and smart communities.</p> <p>We offer a Master of Engineering in Engineering with a specialization in cybersecurity to address this need for an engineering workforce well versed in cybersecurity concerns.</p>

Target careers	<ul style="list-style-type: none"> - Government - Defense - Law Enforcement - Private Industry 	<ul style="list-style-type: none"> - Cyber Analyst - Cyber Defense - Cyber Incident Response - Cyber Strategic Planning - Cyber Crisis Management <p>(State, Government, Department of Defense, Federal Government, Military branches)</p>	<p>Engineering Focus (as the degree is a Master of Engineering) with an emphasis on cyber:</p> <p>Biomedical Engineering</p>
Total units required to complete the degree	<p style="text-align: center;">30</p>	<p style="text-align: center;">30</p>	<p style="text-align: center;">30</p>
Pre-admission expectations (i.e. academic training to be completed prior to admission)	<p>BA/BAS/BS or equivalent degree and meets admissions criteria of the Graduate College (minimum 3.0 GPA for undergraduate degree).</p> <p>Successful completion of CYBV500: Security Computing or prior undergraduate coursework in computer programming.</p>	<p>Because cybersecurity analytics and operations career opportunities exist in many disciplines, students with a wide range of disciplinary backgrounds may be accepted into the program. A bachelor's degree in a related area (e.g., engineering and science), while not necessary for admission, is helpful in the successful completion of the degree.</p> <p><i>Entrance Requirement regarding Mathematics:</i> Applicants must complete a Calculus course equivalent to Penn State University's MATH 110 or MATH 140.</p> <p><i>Entrance Requirement regarding Programming:</i> Applicants must complete two introductory-level programming courses where both courses used the same language. If an applicant believes his/her work experience satisfies the background, he/she should include a recommendation letter from a technical colleague</p>	<p>Students interested in the Master of Engineering in Engineering program must meet and follow the requirements outlined below to be considered for admission:</p> <p>Bachelor or Master of Science in an engineering discipline</p> <p>Minimum GPA of 3.0 for undergraduate degree and at the graduate level</p>
Major requirements. List all major requirements including core and electives. If applicable, list the emphasis requirements. Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Include any limits/restrictions	<p>CORE (complete 24 units): CYBV501 (3): Principles of Cybersecurity CYBV523 (3): Covert Python CYBV529 (3): Cyber Law, Ethics & Policy CYBV579 (3): Cloud Security CYBV626 (3): Traffic Analysis CYBV660 (3): Zero Trust Defensive Techniques CYBV685 (3): Information Warfare CYBV 909 (3): Master's Report in Cyber & Information Operations</p> <p style="text-align: center;">OR</p>	<p>REQUIRED: IST 543 (3) Foundations of Software Security IST 554 (3) Network Management and Security IST 815 (3) Foundations of Information Security and Assurance IST 820 (3) Cybersecurity Analytics IST 825 (3) Technologies for Web and E-Commerce Application Security</p> <p>ELECTIVES: 9-12 credits from a list available in program office.</p> <p>CULMINATING EXPERIENCE:</p>	<p>Three cybersecurity core curriculum courses that lay the foundation for cybersecurity (9 credit hours). Various options, examples below: CYBR 601/CSCE 701 (3) Foundations of Cybersecurity CYBR 602/CSCE 702 (3) Law and Policy in Cybersecurity CYBR 630/ECEN 759 (3) Hardware Security CSCE 713 Software Security (3)</p> <p>Five directed electives that enable the student to link cybersecurity to discipline-specific areas of study (15</p>

<p>needed (house number limit, etc.). Provide email(s)/letter(s) of support from home department head(s) for courses not owned by your department.</p>	<p>CYBV 910 (3): Master’s Thesis in Cyber & Information Operations</p> <p>ELECTIVES (Choose 2): CYBV525 (3): Cyber Physical Systems CYBV528 (3): Operational Tradecraft in the Information Environment CYBV581 (3): Privacy and Regulatory Requirements in Cybersecurity CYBV630 (3): Industrial Control System Security CYBV680 (3): Computational Propaganda CYBV683 (3): Strategic Cyber Management CYBV 696 (3): Special Topics in Cyber and Intelligence Operations</p>	<p>One of the following: IST 594 (3) Research Topics (Scholarly Paper) IST 600 (6) Thesis Research</p>	<p>credit hours). Various options, examples below: CYBR 604/CSCE 704 (3) Data Analytics for Cybersecurity CYBR 661/PSAA 608 (3) Cybersecurity Policy, Issues and Operations - A Manager’s Guide CYBR 660/INTA 690 (3) Cybersecurity Literacy for the Global Arena CYBR 684 (3) Professional Internship CYBR 603 (3) Cybersecurity Risk</p> <p>One foundational elective that provides a deeper knowledge in one of the discipline-specific areas (3 credit hours). Various options, examples below: CSCE 678/ECEN 757 (3) Distributed Systems and Cloud Computing CSCE 604 (3) Programming Languages CSCE 612 (3) Applied Networks and Distributed Processing</p> <p>One free elective to be selected in consultation with faculty advisor (3 credit hours). Various options, examples below: CSCE 652 (3) Software Reverse Engineering CYBR 776/ECEN 776 (3) Unconditionally Secure Electronics CYBR 711/CSCE 711 (3) Foundation of Modern Cryptography CSCE 704/CYBR 604 (3) Data Analytics for Cybersecurity</p>
<p>Research methods, data analysis, and methodology requirements (Yes/No). If yes, provide description.</p>	<p>Research methodologies and data analysis are incorporated in the Master’s Report/Thesis</p>	<p>Not required.</p>	<p>Not required.</p>
<p>Internship, practicum, applied course requirements (Yes/No). If yes, provide description.</p>	<p>Not required.</p>	<p>Not required.</p>	<p>Not required.</p>
<p>Master thesis or dissertation required (Yes/No). If yes, provide description.</p>	<p>No (Optional Thesis).</p>	<p>No (Optional Thesis).</p>	<p>No.</p>

Additional requirements (provide description)		<p>Students who choose to complete a thesis must complete at least 6 credits in thesis research (IST 600 or IST 610). The thesis must be accepted by the advisers and/or committee members, the head of the graduate program, and the Graduate School, and the student must pass a thesis defense. Students in the non-thesis track must write a satisfactory scholarly paper while enrolled in IST 594 and complete at least 18 credits at the 500 level.</p>	
--	--	--	--

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



BUDGET PROJECTION FORM

Name of Proposed Program or Unit: Master of Science in Cyber & Information Operations, College of Applied Science &

Budget Contact Person: Frank Avitia: fja584@arizona.edu	Projected		
	1st Year 2023 - 20 24	2nd Year 2024 - 2025	3rd Year 2025 - 2026
METRICS			
Net increase in annual college enrollment UG			
Net increase in college SCH UG			
Net increase in annual college enrollment Grad	50	50	50
Net increase in college SCH Grad	-	35	50
Number of enrollments being charged a Program Fee			
New Sponsored Activity (MTDC)			
Number of Faculty FTE	2	1	2
FUNDING SOURCES			
<u>Continuing Sources</u>			
UG AIB Revenue			
Grad AIB Revenue	575,750	1,147,500	1,319,625
Program Fee Revenue (net of revenue sharing)			
F and A AIB Revenues			
Reallocation from existing College funds (attach description)			
Other Items (attach description)			
Total Continuing	\$ 575,750	\$ 1,147,500	\$ 1,319,625
<u>One-time Sources</u>			
College fund balances			
Institutional Strategic Investment			
Gift Funding			
Other Items (attach description)			
Total One-time	\$ -	\$ -	\$ -
TOTAL SOURCES	\$ 575,750	\$ 1,147,500	\$ 1,319,625
EXPENDITURE ITEMS			
<u>Continuing Expenditures</u>			
Faculty	220,000	330,000	550,000
Other Personnel	70,180	105,270	175,450
Employee Related Expense			
Graduate Assistantships			
Other Graduate Aid			
Operations (materials, supplies, phones, etc.)	40,500	81,000	93,150
Additional Space Cost			
Other Items (attach description)			
Total Continuing	\$ 330,680	\$ 516,270	\$ 818,600
<u>One-time Expenditures</u>			
Construction or Renovation			
Start-up Equipment			
Replace Equipment			
Library Resources			
Other Items (attach description)			
Total One-time	\$ -	\$ -	\$ -
TOTAL EXPENDITURES	\$ 330,680	\$ 516,270	\$ 818,600
Net Projected Fiscal Effect	\$ 245,070	\$ 631,230	\$ 501,025



NEW ACADEMIC PROGRAM – MAJOR
Supplemental Info Form

NOTE: This is being added to the proposal post Graduate Programs Executive Review Committee (GPERC) viewed and commented on the document. Below are their questions and the responses given by the proposing department/college.

1. How does the proposed program differ from the MS in Cybersecurity offered by Eller? It is not clear to me.

Our proposed MS in Cyber & Information Operations is much more technical than the Eller MS in Cybersecurity and is guided by the NSA's Center of Academic Excellence in Cyber Operations knowledge units and the Intelligence Community Center of Academic Excellence for Information Operations guidance. We would offer coursework in malware analysis, information warfare, protocol analysis, and other technical topics related to cyber operations and computer science. The Eller program is much more focused on data science and using information to make decisions regarding risk to business sectors. We met extensively with Sue Brown to ensure our programs maintained unique identities.

2. It says that CAST has an undergraduate BAS in Cyber Operations, but all 30 courses proposed for the new MS in Cyber Operations are brand new. Is the MS completely different from the BAS? Also developing this many courses to offer the program in Fall 2023 seems to be a challenge.

Our MS proposes ultimately creating 17 new graduate content courses (three are project / report / thesis), not 30. Further, we are using a cohort model where we will only offer three MS courses in Fall 2023 and three more in Spring 2024, which we can cover with our current faculty. We're also hiring faculty in clusters annually for the foreseeable future. The MS would build upon the program foci and faculty expertise at the BAS level.

3. I think this is a great time for a fully online Cyber & Information MS program using the innovative online VLS (but no details about VLS are included). I am more concerned about the similarities/differences between this program and others at UA (MS in

Cybersecurity) and ASU (MS Computer Science/Cybersecurity and MA Global Security/Cybersecurity). Are these in person or online programs? Do the courses differ? The Eller program should submit letter of support.

Our proposed MS will make use of the Virtual Learning Environment (VLE) for almost every class as described in the preliminary proposal document. The [required core and available electives of the ASU program](#) are more engineering and computer science focused, while our core and electives are focused on cyber and information operations. The overlap is very minimal. Further, ASU students must also meet the entrance requirements of the Fulton Schools of Engineering which mandates a much more extensive computer science and computer engineering background than our program requires. The ASU program is offered at the Tempe campus. We intend 100% online delivery. Given the differences in our programs, Eller is in support of our MS program and we provided the email of support based on meetings with Sue Brown and Bill Neumann.

4. Also, there is considerable change from the preliminary proposal in terms of student projections (20/year to 50/year) and faculty requirements (1 new to 3-4 new faculty). Is the revised projection of 50+ student each year warranted (the data/evidence used to support the number is the same as for 20/year)?

This increased projection was suggested by Greg Heileman, stemming from recommendations made by Provost Folks.

5. Additional information on the MS Report and MS Thesis (description, examples in the online format?) would be useful. So many new courses are needed (15 plus thesis or report); it would be helpful to assign instructors to these courses in the initial description to provide a better indication of coverage.

100% of the six new MS courses to be offered during the 2023-24 academic year assuming program approval are assigned to current faculty members in the CIO Department. Further faculty hiring and course development will continue to ensure courses are adequately created for graduate rigor and delivery.

- CYBV501: Principles of Cybersecurity: Honomichl
- CYBV523: Covert Python: Hosmer
- CYBV529: Cyber Law, Ethics & Policy: Calhoun-Lopez

- CYBV579: Cloud Security: Alharthi
- CYBV626: Traffic Analysis: Duren
- CYBV660: Zero Trust Defensive Techniques: Jewkes

Program Comparisons (as referenced on page 10)

Arizona University System

Arizona State University - Fall 2022 Enrollment	
MS in Computer Science (Cybersecurity)	18
MA in Global Security (Cybersecurity)	62
MA in Emer Mgmt & Homeland Sec (Cybersec Policy & Mgmt)	27

MCS in Computer Science (Cybersecurity)	93
---	----