



November 15, 2024

Sanjay Rai, Ph.D.
Secretary of Higher Education
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Rai:

The University of Baltimore is proposing a new Master of Science in User-Centered Cybersecurity (proposed CIP 11.0105 and proposed HEGIS code 0705.00). This is a 30-credit program that will prepare graduates for roles in cybersecurity and user experience design, given the increasing demand for professionals who can design secure systems that are both effective and user-friendly.

Computer and mathematical occupations are the fastest growing fields in Maryland. The envisioned degree will play a pivotal role in training highly qualified information technology professionals, specifically software engineers, system analysts, and programmers in the region through dual modality offerings. It will achieve this by educating participants on practical usability and user-centered design principles, including knowledge of how to apply usability in various cybersecurity fields across multiple sectors.

The proposed master's program will equip professionals with the knowledge and skills to design and implement cybersecurity systems that are not only secure but also user-friendly. By focusing on both technical skills and an understanding of human behavior and interaction, graduates will be better prepared to create systems that users can easily adopt, reducing the risk of security breaches caused by human error. As cybersecurity threats continue to evolve, there is a clear need for professionals who can bridge the gap between technical security measures and real-world user behavior, making this program a critical addition to the field.

If you have any questions, please contact Aaron Wachhaus at 410-837-6113 or awachhaus@ubalt.edu.

Sincerely,

p.p. Aaron Wachhaus, Associate Provost - Academic Affairs
Ralph O. Mueller, Senior Vice President and Provost

Encl.

cc: Dr. Candace Caraco, Associate Vice Chancellor for Academic Programs, Academic & Enrollment Services and Articulation



**Cover Sheet for In-State Institutions
New Program or Substantial Modification to Existing Program**

Institution Submitting Proposal	
---------------------------------	--

Each action below requires a separate proposal and cover sheet.

- | | |
|-----------------------------|---|
| New Academic Program | Substantial Change to a Degree Program |
| New Area of Concentration | Substantial Change to an Area of Concentration |
| New Degree Level Approval | Substantial Change to a Certificate Program |
| New Stand-Alone Certificate | Cooperative Degree Program |
| Off Campus Program | Offer Program at Regional Higher Education Center |

Payment Submitted:	Yes	Payment Type:	R*STARS #	JBII1812	Payment Amount:	Date Submitted:
	No		Check #	JBII1812		

Department Proposing Program			
Degree Level and Degree Type			
Title of Proposed Program			
Total Number of Credits			
Suggested Codes	HEGIS:	CIP:	
Program Modality	On-campus	Distance Education (fully online)	Both
Program Resources	Using Existing Resources	Requiring New Resources	
Projected Implementation Date <small>(must be 60 days from proposal submission as per COMAR 13B.02.03.03)</small>	Fall	Spring	Summer Year:
Provide Link to Most Recent Academic Catalog	URL: https://www.ubalt.edu/academics/uploads/catalogs/24-25_grad_catalog/2024-25-Grad-Catalog.pdf		

Preferred Contact for this Proposal	Name:
	Title:
	Phone:
	Email:

President/Chief Executive	Type Name:
	Signature: Date:

	Date of Approval/Endorsement by Governing Board:
--	--

UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR

- New Instructional Program
- Substantial Expansion/Major Modification
- Cooperative Degree Program
- Within Existing Resources, or
- Requiring New Resources

University of Baltimore

Institution Submitting Proposal

MS in User-Centered Cybersecurity Program

Title of Proposed Program

Master's Degree

Award to be Offered

Fall 2025

Projected Implementation Date

0705.00

Proposed HEGIS Code

11.0105

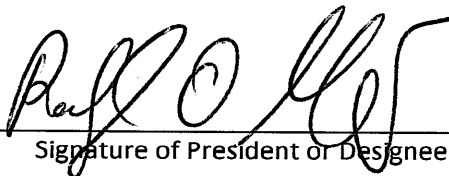
Proposed CIP Code

Yale Gordon College of Liberal Arts & Sciences
Department in which program will be located

Greg Walsh
Department Contact

410-837-5473
Contact Phone Number

gwalsh@ubalt.edu
Contact E-Mail Address


Signature of President or Designee

11/11/2024
Date

User-Centered Cybersecurity Program Proposal

A. Centrality to Institutional Mission and Planning Priorities

Provide a description of the program, including each area of concentration (if applicable), and how it relates to the institution's approved mission.

As technology increasingly permeates every aspect of our lives, ensuring the secure use of digital systems has become a pressing concern. Despite advances in technical security measures, human error and usability issues remain significant cyber-attack vulnerabilities. This gap is because humans are often unaware of their vulnerabilities or fail to follow best practices due to poorly designed interfaces and systems. To effectively mitigate these risks, technology professionals must develop an understanding of the people they serve – their needs, behaviors, and limitations. By incorporating user-centered design principles into cybersecurity topics, we can empower professionals with the knowledge and skills to create more secure, usable technologies.

The University of Baltimore's mission statement emphasizes our commitment to providing career-focused education for both aspiring and current professionals. This approach ensures the region benefits from highly educated leaders who contribute significantly to the broader community. The landscape of government, industry, and education-related cybersecurity issues continues to expand due to the ever-increasing integration of technology into all sectors. Our proposed program, with its potential to equip individuals with the essential skills to apply usability and user-centered design techniques effectively in the field of information technology and cybersecurity, could have a significant impact on the region and reinforce Maryland's leadership role in these fields and has been designed with consultation from public and private sector professionals.

The Master of Science in User-Centered Cybersecurity is closely aligned with the University of Baltimore's mission to provide career-focused education that prepares professionals for meaningful contributions to the workforce and community. This program is designed to address the increasing demand for cybersecurity professionals who not only possess technical expertise but also understand the human factors that influence cybersecurity risks. By emphasizing user-centered design principles and usability in security systems, the program ensures that graduates can design solutions that are both effective and accessible to end users.

The University of Baltimore is dedicated to serving the needs of the broader community by producing highly educated leaders who can contribute to regional and national industries. With Maryland being a hub for cybersecurity, the need for professionals who can bridge the gap between technical security measures and human behavior is crucial. This program will help the institution fulfill its mission by preparing students to enter the workforce with a specialized skill set that is highly relevant to current industry needs. As

technology continues to permeate all sectors, cybersecurity professionals must develop solutions that account for both technical vulnerabilities and user behaviors, which is a key focus of this program.

The program supports several key goals outlined in Maryland's State Plan for Higher Education, particularly in the areas of access, success, and innovation. The plan emphasizes the importance of providing equitable access to high-quality, affordable education, and the University of Baltimore's cybersecurity program is designed with this in mind. The dual-modality format, offering both in-person and online courses, makes the program accessible to a wider range of students, including working professionals and those from underserved populations. This approach aligns with the state's goal of increasing access to education for all Maryland residents.

Additionally, the program contributes to the success of the state plan by equipping students with the practical skills necessary for career advancement. By focusing on usability and user-centered design in cybersecurity, the program ensures that graduates are prepared to meet the challenges of an evolving industry and excel in their careers. The state plan also highlights the need for innovation in education to keep pace with workforce needs, and this program addresses this by offering a unique focus on the human elements of cybersecurity. This innovative approach positions the University of Baltimore as a leader in cybersecurity education and directly supports the state's goal of fostering cutting-edge academic programs that prepare students for the jobs of the future.

The Master of Science in User-Centered Cybersecurity is not only a critical addition to UBalt's academic offerings but also a vital contribution to Maryland's broader higher education landscape. By addressing a growing need in both the regional and national cybersecurity sectors, the program helps fulfill both the institution's mission and the state's objectives for advancing education, workforce development, and community engagement.

Explain how the proposed program supports the institution's strategic goals and provide evidence that affirms it is an institutional priority.

The proposed Master of Science in User-Centered Cybersecurity directly supports the University of Baltimore's strategic goals, particularly those outlined in its mission and strategic plan. UBalt's strategic priorities emphasize career-focused education, community engagement, and leadership development, all of which are at the core of this program.

First, the university's strategic goal to provide career-focused education is realized through this program's alignment with the growing needs of the cybersecurity industry. The program is designed to equip students with the specialized skills necessary to succeed in the rapidly expanding field of cybersecurity. As Maryland is a hub for technology and cybersecurity, there is a growing demand for professionals who not only understand technical security measures but also how usability and human factors influence security vulnerabilities. By preparing students to address these challenges, the

program ensures that UBalt remains a leader in providing relevant, future-focused education.

Second, the program supports the institution's goal of community and civic engagement by responding to the cybersecurity needs of both the public and private sectors. Maryland, as a leader in the cybersecurity field, requires professionals who can contribute to securing digital systems across multiple sectors, including government, healthcare, and education. The program's focus on user-centered design in cybersecurity addresses the human factors that can be exploited in cyber-attacks, ensuring that graduates are not only technically proficient but also able to engage with and serve the community by improving the security and usability of systems that affect everyday users. This aligns with UBalt's commitment to producing graduates who can make a positive impact on their communities.

Furthermore, the university's strategic priority of developing leaders who can thrive in their fields is central to this program. The Master of Science in User-Centered Cybersecurity is designed to produce graduates who are not just capable of following industry trends but also leading innovation in the field. By focusing on both usability and technical security, the program produces professionals who can bridge the gap between cybersecurity and user experience, making them highly valuable in leadership roles within organizations.

There is evidence that this program is an institutional priority, demonstrated by its alignment with UBalt's long-term focus on technology-driven education and workforce development. The university has a strong history of offering programs in interaction design and information architecture, as well as a Bachelor's in Applied Information Technology, all of which have been integral to serving the region's technology workforce. The development of this new graduate program is a natural extension of the university's commitment to advancing education in fields that meet the evolving needs of the community and industry.

Additionally, the program proposal has been developed in consultation with both public and private sector professionals, further affirming its alignment with industry needs and its priority status within the institution. This collaborative development ensures that the program is not only aligned with UBalt's strategic goals but also meets the demands of the current job market, making it a high-priority initiative for the university.

By supporting UBalt's strategic goals of career readiness, community impact, and leadership development, the Master of Science in User-Centered Cybersecurity positions the university as a leader in innovative education, directly aligning with its mission and long-term strategic objectives.

Provide a brief narrative of how the proposed program will be adequately funded for at least the first five years of program implementation.

The program, in its current configuration, will be managed by our existing faculty lines, thereby eliminating the need for additional resources in terms of new faculty hires. Our current faculty members possess the capability to effectively instruct within the program, as we can reassign them from other programs as needed. Furthermore, we are prepared to leverage adjunct faculty members as needed to ensure the program's successful delivery. Please find detailed financial information in Section L of this proposal.

Provide a description of the institution's commitment to:

a) ongoing administrative, financial, and technical support of the proposed program

The program's needs will be met within the capacity of the existing faculty's teaching loads. To the extent necessary, overload compensation will be utilized.

b) continuation of the program for a period of time sufficient to allow enrolled students to complete the program.

We are committed to offering the program as long as reasonably necessary to build sufficient and sustainable enrollments.

B. Critical and Compelling Regional or Statewide Need as Identified in the State Plan

Demonstrate demand and need for the program in terms of meeting present and future needs of the region and the State in general based on one or more of the following:

a) The need for the advancement and evolution of knowledge

The need for a master's program in user-centered cybersecurity is supported by the evolving requirements in the field and the increasing demand for cybersecurity professionals equipped with user-centered design expertise. Maryland, for example, had over 30,000 cybersecurity job openings in 2023, but there was a significant skills gap, with one in four positions going unfilled. The Maryland Department of Labor has actively invested in innovative training approaches, including cyber ranges that provide hands-on experience, which employers value highly. This highlights the critical need for advanced education programs that can produce well-trained professionals who meet the market's demand for skills in cybersecurity (Maryland Department of Labor, 2024).

Moreover, there is a broader national and global trend recognizing the importance of integrating human-centered design into cybersecurity to ensure security systems are not only technically robust but also usable and effective for a diverse range of users. Research indicates that traditional cybersecurity tools are often overly complex and do not adequately account for the human element, which can result in security breaches due to user error or frustration (Morris, 2024). Addressing this through education in user-

centered cybersecurity will equip graduates with the knowledge to design systems that align with how people interact with technology, reducing the likelihood of user-induced vulnerabilities (Haney, 2023).

Recently, NIST changed the name of its *Usable Cybersecurity* program to *Human-Centered Cybersecurity* to better reflect the broader scope of its work beyond usability. This renaming highlights a shift in focus to encompass the entire spectrum of human interactions with cybersecurity systems, including not just usability but also how social, organizational, and technological factors impact cybersecurity. NIST recognized that usability, while critical, is just one piece of the puzzle; a more holistic approach is needed to ensure security systems are effective when interacting with people at every level (Haney, 2023).

The name change underscores the growing recognition that cybersecurity is not just a technical issue but also a human one. This reflects the core need for a program like the proposed *Master of Science in User-Centered Cybersecurity*, which is designed to train professionals to focus on the human aspects of security systems. As NIST's shift indicates, there is an increasing demand for cybersecurity professionals who understand human behavior and can design systems that are secure and user-friendly. The change from "usable" to "human-centered" signals that future cybersecurity efforts must integrate broader human factors, such as cognitive science and social influences, into the design and implementation of security measures.

By emphasizing human-centered design, the proposed program would align with NIST's evolved approach, preparing graduates to address not just usability but the wider range of human factors that impact cybersecurity. This shift illustrates a critical gap in the current training and workforce, where many professionals are technically proficient but lack the skills to design systems that effectively account for human behavior, compliance, and the overall user experience. Therefore, NIST's change reflects an industry-wide recognition of the need for educational programs that focus on human-centered cybersecurity, reinforcing the relevance and importance of your proposed program.

Aurora Infosec, a New Zealand cybersecurity consulting firm argues that **human-centered design** needs to become central to cybersecurity. Their article “**The Future of Cybersecurity: Human-Centred Design**” emphasizes that effective security systems must account for how users interact with technology, prioritizing ease of use to reduce human errors. as this approach directly addresses the core issue of how people interact with security systems. Rather than solely focusing on technical defenses, the human-centered approach aims to design technology that aligns with human behavior, making security systems more intuitive and user-friendly. This shift is critical because many security breaches result not from technical failures but from human errors—82% of breaches involve the human element, such as social engineering attacks, mistakes, or misuse (Petrescu, 2023).

One of their key arguments is that the traditional approach to cybersecurity, which often focuses on changing user behavior through training and awareness programs, is

insufficient. Instead, a more effective long-term solution is to design security systems that are inherently easier for users to navigate and interact with. By applying **human-centered design** principles throughout the software development lifecycle (SDLC), organizations can create security features that are both intuitive and robust. This minimizes the likelihood of user errors, reduces friction between users and security protocols, and ultimately strengthens the overall security posture of organizations (Petrescu, 2023).

Additionally, their article outlines how using behavioral science to influence user behavior—while helpful—is not enough to manage human risks effectively. Instead, security systems must be designed to work with human limitations and cognitive biases, ensuring that users can comply with security protocols without needing extensive training or experience (Petrescu, 2023). This reflects a significant shift in the cybersecurity industry, where the emphasis is moving away from trying to "fix" user behavior and towards building systems that are secure by design and account for human interaction from the outset.

Incorporating **human-centered design** in cybersecurity also tackles the issue of "security fatigue," where users become overwhelmed by complex or intrusive security measures, leading them to circumvent protocols. By making security features more intuitive and reducing the cognitive load on users, human-centered design can reduce these risks (Petrescu, 2023).

Given this clear demand for skills and the state's investment in closing the workforce gap, a master's degree in user-centered cybersecurity would not only meet present needs but also prepare for future challenges in the region and beyond. This advancement in knowledge is critical to addressing both the technical and human factors in cybersecurity, ensuring long-term security solutions that are both effective and usable.

b) Societal needs, including expanding educational opportunities and choices for minority and educationally disadvantaged students at institutions of higher education

As a primarily Black institution (PBI), the University of Baltimore is uniquely positioned to offer students educational pathways that can significantly enhance their social mobility and career opportunities. By providing access to a specialized program like the master's in user-centered cybersecurity, the university can empower students from historically underrepresented communities to enter a high-demand field. Cybersecurity is a rapidly growing industry with excellent job prospects, and equipping students with the skills to design systems that are both secure and usable positions them for leadership roles in the sector. This not only provides graduates with greater earning potential but also helps bridge the digital divide by fostering diversity in an industry that urgently needs it. Through this program, students can gain cutting-edge skills, opening doors to advanced career opportunities while contributing to a more inclusive and equitable workforce.

The proposed master's program in user-centered cybersecurity addresses critical societal needs by advancing the concept of usable security, which focuses on creating more inclusive and equitable digital experiences. Traditional cybersecurity solutions often overlook the usability of security tools and systems, particularly for minority and educationally disadvantaged populations, who may not have been considered in the initial design phases of these technologies. This oversight has contributed to a digital divide, where marginalized groups may struggle with complex security measures that are not user-friendly or accessible (Haney, 2023)(Adams & Sasse, 1999).

Usable security is an essential component of ensuring that all individuals, regardless of their background or level of technical expertise, can engage with cybersecurity in meaningful ways. By integrating human-centered design into cybersecurity, this program seeks to create systems that are not only secure but also intuitive and user-friendly. This approach addresses the barriers that many underserved groups face in adopting secure behaviors, such as managing passwords or identifying phishing attempts, which are often designed without their needs in mind (Morris, 2024) (Science of Security Virtual Organization, n.d.).

Maryland has already recognized the importance of fostering diversity in the cybersecurity workforce. The state's commitment to developing educational programs that reach underrepresented populations, including women, people of color, and individuals with differing abilities, aligns perfectly with the goals of this program. By providing students from these groups with the skills needed to succeed in cybersecurity, the program contributes to a more diverse workforce, which is essential for designing security solutions that reflect the needs of all users.

Ultimately, this program will not only meet the technical and workforce needs of the state but also play a key role in addressing societal inequities by ensuring that cybersecurity systems are accessible to all. Through a focus on usable security and human-centered design, graduates will be equipped to create more equitable and inclusive digital environments, making cybersecurity more effective and accessible for everyone.

Provide evidence that the perceived need is consistent with the Maryland State Plan for Postsecondary Education.

The creation of a Master's in User-Centered Cybersecurity aligns well with the goals of the Maryland State Plan for Postsecondary Education by addressing the state's need for a highly skilled, diverse workforce. Maryland is a national hub for cybersecurity, with significant job openings that remain unfilled due to a shortage of qualified professionals. The program's focus on user-centered cybersecurity directly responds to this gap by ensuring that graduates are prepared to meet the state's growing demand for cybersecurity experts who can design and implement security solutions that are accessible and effective for all users, including underrepresented populations (U.S. Bureau of Labor Statistics, 2024b).

Furthermore, the Maryland Department of Labor emphasizes the importance of developing inclusive training programs that provide opportunities for populations typically underrepresented in cybersecurity, including women and people of color. This focus on equitable training aligns with the goals of the Maryland State Plan, which advocates for expanding educational opportunities and career pathways for minority and disadvantaged students. The user-centered approach of the proposed master's program ensures that cybersecurity solutions are designed with diverse user needs in mind, thereby fostering inclusion and equity in the field (Morris, 2024).

Additionally, a user-centered cybersecurity masters program aligns with several specific priorities outlined in the Maryland State Plan:

Priority 5: Maintain the commitment to high-quality postsecondary education: By providing students with a comprehensive understanding of cybersecurity principles and practices, a user-centered cybersecurity masters program can help maintain the quality of higher education in Maryland.

Priority 7: Enhance the ways postsecondary education is a platform for ongoing lifelong learning: A user-centered approach encourages continuous learning and professional development, which aligns with this priority.

Priority 8: Promote a culture of risk-taking: By encouraging students to think creatively and develop innovative solutions to cybersecurity challenges, a user-centered cybersecurity masters program can promote a culture of risk-taking.

C. Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State

1. Describe potential industry or industries, employment opportunities, and expected level of entry (ex: mid-level management) for graduates of the proposed program.

We expect our graduates to be employed in a variety of industries that rely on cybersecurity professionals, including federal, state, and local government, public institutions, and private industry. Cybersecurity is a critical concern across sectors, from financial services, healthcare, and education to telecommunications and retail. Maryland, in particular, has a high demand for cybersecurity professionals due to its proximity to government agencies and tech-focused private sectors.

Graduates will be particularly well-suited for roles in cybersecurity and user experience design, given the increasing demand for professionals who can design secure systems that are both effective and user-friendly. They may find employment as **Information Security Analysts**, **User Experience (UX) Designers** focused on secure interfaces, and **Computer Network Architects** who are tasked with building secure data

communication networks. These roles often exist in industries like defense, financial services, healthcare, and IT consulting.

Given their specialized knowledge in usability and human-centered design, we expect graduates to enter the workforce in mid-level positions, such as **security analysts, cybersecurity consultants, or UX security designers**. Over time, their unique expertise may allow them to move into management roles, such as **cybersecurity project managers or user-centered security leads** within organizations.

With cybersecurity-related jobs projected to grow significantly, including a 35% increase in the number of **Information Security Analysts** (U.S. Bureau of Labor Statistics, 2024a), and with Maryland having one of the highest concentrations of cybersecurity professionals (U.S. Bureau of Labor Statistics, 2024b), we anticipate that our graduates will be highly competitive in the job market. The annual mean wage for cybersecurity roles in Maryland is around \$138,000, providing significant financial incentives for professionals in this field (U.S. Bureau of Labor Statistics, 2024b)(U.S. Bureau of Labor Statistics, 2024).

Moreover, as organizations increasingly recognize the need for systems that prioritize the user experience without compromising security (Haney, 2023)(Morris, 2024)(Petrescu, 2023), graduates will be in high demand for their ability to bridge the gap between technical security measures and human usability, ensuring that systems are secure and intuitive.

2. Present data and analysis projecting market demand and the availability of openings in a job market to be served by the new program.

Based on comprehensive analysis and alignment between cybersecurity roles and their corresponding Bureau of Labor Statistics (BLS) codes, several key positions in the cybersecurity field necessitate training in User-Centered Design (UCD) due to their direct impact on user interaction with systems and security protocols. These positions include:

- **Cyber Defense Analyst, Cyber Defense Forensics Analyst, Incident Responder, Security Architect, Systems Security Analyst, and Vulnerability Assessment Analyst**, mapped to BLS code **15-1212: Information Security Analysts**.
- **Information Systems Security Manager, IT Project Manager, and Cyber Policy and Strategy Planner**, mapped to BLS code **11-3021: Computer and Information Systems Managers**.
- **Systems Requirements Planner**, mapped to BLS code **15-1211: Computer Systems Analysts**.
- **Software Developer and Systems Developer**, mapped to BLS code **15-1252: Software Developers**.

Professionals in these roles are responsible for designing, implementing, or managing security systems that impact end users. As cybersecurity threats continue to evolve, UCD training becomes imperative for equipping these professionals with the necessary skills to

create intuitive and user-friendly solutions, reducing the risk of user errors and enhancing security.

Demand in Maryland and the MD-VA-DC-WV Region:

According to the May 2023 **Occupational Employment and Wage Statistics (OEWS)**, Maryland has one of the highest concentrations of **Information Security Analysts**, with a **location quotient of 2.55** (indicating a demand 2.55 times the national average)(U.S. Bureau of Labor Statistics, 2024). The surrounding region, including Washington, D.C., Virginia, and West Virginia, shows an even greater concentration, with a **location quotient of 4.66** (U.S. Bureau of Labor Statistics, 2024c). This suggests a significant demand for cybersecurity professionals in the region, particularly in roles that require UCD training.

Furthermore, in Maryland alone, there are approximately **7,890 Information Security Analysts**, with an annual mean wage of **\$138,180** (U.S. Bureau of Labor Statistics, 2024b) (U.S. Bureau of Labor Statistics, 2024). Similarly, **Computer Network Architects**—who are also responsible for designing secure networks—are in high demand, with an average annual wage of **\$151,840** (U.S. Bureau of Labor Statistics, 2024a). These data underscore the lucrative opportunities available for professionals equipped with UCD expertise in the cybersecurity sector.

BLS Job Title	Common Job Titles	Maryland Need	MD-VA-DC-WV
15-1212 Information Security Analysts	<ul style="list-style-type: none"> • Adversary Emulation Specialist (Red Team) • Cyber-defense Analyst (Blue Team) • Information Systems Security Manager • Vulnerability Assessment Analyst • Security Architect 	2.55	4.66
15-1252 Software Developers	<ul style="list-style-type: none"> • Systems Developer 	1.05	2.13
15-1211 Computer Systems Analysts	<ul style="list-style-type: none"> • Secure Software Assessor 	1.57	1.76

11-3021 Computer and Information Systems Managers	<ul style="list-style-type: none"> • Systems Requirements Planner 	1.30	1.55
---	--	------	------

The projected growth for **Information Security Analysts** nationally is expected to be **35% from 2022 to 2032**, significantly faster than the average for all occupations (U.S. Bureau of Labor Statistics, 2024). Given the concentration of cybersecurity positions in the Maryland region, this trend will likely be mirrored locally. Similarly, roles such as **Computer Systems Analysts, Software Developers, and IT Project Managers** are also expected to experience substantial growth due to the increasing complexity of cyber threats and the need for secure, user-friendly systems (U.S. Bureau of Labor Statistics, 2024a).

UCD training is vital for these professionals to design security measures that users can easily adopt and adhere to, which not only enhances security compliance but also reduces the likelihood of security breaches resulting from user errors (Petrescu, 2023)(Morris, 2024). In fields such as financial services, healthcare, and government, where secure and intuitive interfaces are critical, UCD expertise will provide a competitive edge for professionals and enhance overall system security (Haney, 2023)(Petrescu, 2023).

The importance of a *Master of Science in User-Centered Cybersecurity* stems from the growing recognition that traditional cybersecurity measures often overlook the human element, which plays a crucial role in the effectiveness of security systems. As highlighted in the data, cybersecurity tools are typically designed by technical professionals for other technical users, leading to complex systems that are difficult for the average user to navigate. This complexity results in frequent user errors, non-compliance with security protocols, and even intentional workarounds that compromise security (Hielscher et al., 2023)(Morris, 2024).

Research from NIST and other cybersecurity organizations emphasizes the need for systems designed with usability in mind. A lack of usability in cybersecurity systems leads to frustration, errors, and reduced adoption of necessary security measures (Haney, 2023). This gap between system complexity and user needs has been identified as a significant vulnerability, with 82% of breaches involving the human element, such as social engineering attacks and user errors (Petrescu, 2023). Moreover, the cybersecurity industry is beginning to realize that addressing human interaction with security systems through human-centered design is essential to reducing risks and ensuring that security measures are not just effective in theory but also in practice (Zurko & Simon, 1996).

Despite the growing awareness of these issues, many cybersecurity professionals still lack the training and tools necessary to implement user-centered design principles into their systems. As studies on security managers indicate, even when security friction—where security measures interfere with work—is recognized, professionals are often unable to resolve it due to a lack of usable security tools and a focus on compliance with

technical standards rather than human usability (Hielscher et al., 2023). This gap between usability and security has created an urgent need for cybersecurity professionals trained specifically in human-centered design.

The proposed master's program directly addresses these gaps by equipping professionals with the knowledge and skills to design and implement cybersecurity systems that are not only secure but also user-friendly. By focusing on both technical skills and an understanding of human behavior and interaction, graduates will be better prepared to create systems that users can easily adopt, reducing the risk of security breaches caused by human error (Haney, 2023)(Morris, 2024). As cybersecurity threats continue to evolve, there is a clear need for professionals who can bridge the gap between technical security measures and real-world user behavior, making this program a critical addition to the field.

D. Reasonableness of Program Duplication

D.1 Similar programs in the State and/or same geographical area.

While numerous graduate programs in the state offer degrees in cybersecurity, these programs typically focus on the technical aspects of the field, such as encryption, network defense, and threat analysis. However, as cyber threats become more sophisticated, the role of human behavior and system usability in maintaining security has become increasingly evident. Despite this growing awareness, no existing cybersecurity programs in Maryland explicitly integrate user-centered design principles—critical for addressing the usability challenges that lead to security vulnerabilities.

There are a number of degree programs in Maryland that use the word “Cybersecurity” in their title. While the idea of cybersecurity is popular within the state, the concept of User-centered Cybersecurity is novel. We have compiled a list of the graduate programs and courses that may focus on User-Centered Design in Table 1. To determine if a course focused on or mentioned user-centered design, we read each program’s course description and looked for instances of “usability”, “user-centered design”, “human-centered design”, or “human-centered interaction”.

Table 1
Graduate degree programs in Maryland that have "Cybersecurity" in the title.

Institution	Degree Name	UCD Related Courses
Capitol Technology University	Master of Science in Cybersecurity	None
Hood College	Master of Science in Cybersecurity	None
Johns Hopkins University	Master of Science in Security Informatics	None
University of Maryland, Baltimore County	Master of Science in Cybersecurity	None

University of Maryland, Global Campus	Master of Science in Cybersecurity	None
University of Maryland, College Park	Master of Engineering in Cybersecurity	None

As user experience and human-centered design have gained prominence in various fields, several graduate programs in Maryland now offer degrees focused on enhancing usability and user interaction with technology. These programs, which emphasize user-centered design, human-computer interaction, and interaction design, prepare students to create intuitive, accessible, and effective digital experiences. However, in reviewing these curricula, it becomes evident that they often overlook the critical area of cybersecurity. In an era where security breaches can have severe consequences for both users and organizations, ensuring that digital systems are both user-friendly and secure is paramount. Despite their focus on the human element of technology, these programs rarely address the security implications of poor design, leaving a significant gap in their approach. The following analysis examines these user-centered design programs and highlights the absence of courses that integrate cybersecurity principles into their curricula.

We analyzed graduate programs that focus on Human-Computer Interaction, Human-Centered Design, or Interaction Design. Table 2 presents the programs in Maryland that have some proximity to user-centered design and the courses they offer in cybersecurity. To determine if a course focused on cybersecurity or contained some aspect of it, we read each program’s course description and looked for instances of “cybersecurity”, “security”, or “threat”.

Table 2
User-centered design-focused programs and cybersecurity courses they offer.

Institution	Degree Name	Cybersecurity Related Courses
University of Maryland, College Park	Master of Science in Human-Computer Interaction	None
MICA	Master of Professional Studies in User Experience Design	None
University of Maryland, Baltimore County	Master of Science in Human-Centered Computing	None
Loyola University of Maryland	Master of Arts in Emerging Media	ME 601.W01: Exploring Digital Culture

The analysis of graduate programs in Maryland reveals a significant gap in both cybersecurity and user-centered design education. Traditional cybersecurity programs focus heavily on technical skills but fail to address the critical role of usability and human-centered design in creating secure systems that people can actually use. On the other hand, programs centered on user experience and human-computer interaction emphasize designing for users but often neglect the essential security concerns that are increasingly central to digital interactions. The University of Baltimore's Master of Science in User-Centered Cybersecurity uniquely bridges this divide, offering a forward-thinking curriculum that combines the strengths of both disciplines. By equipping graduates with expertise in both cybersecurity and user-centered design, this program addresses a growing demand for professionals who can design secure, user-friendly systems. In doing so, it positions the University of Baltimore at the forefront of innovative cybersecurity education and fills an important void in the current academic landscape.

E. Relevance to High-demand Programs at Historically Black Institutions (HBIs)

According to the current MHEC Program Inventory, none of the HBIs in the State currently offer graduate degrees in user-centered cybersecurity. Thus, we do not expect any impact on high-demand HBI programs.

F. Relevance to the Identity of Historically Black Institutions (HBIs)

We expect no effect on the uniqueness, institutional identities, and missions of HBIs since none of the HBIs in the State currently provide graduate programs that emphasize user-centered cybersecurity.

G. Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes

Describe how the proposed program was established, and also describe the faculty who will oversee the program.

Faculty interviewed industry, government, and education leaders and discovered the lack of user-centered knowledge among existing security professionals. The program will be offered by the Yale Gordon College of Arts and Sciences, home of the MS in Interaction Design and Information Architecture and the BS in Applied Information Technology. Our College's experience in these subjects comes from offering both information technology, cybersecurity, and user-centered design programs to students in the region for over 20 years. It is from these programs that the faculty overseeing the program will be chosen.

Describe educational objectives and learning outcomes appropriate to the rigor, breadth, and (modality) of the program.

There are five learning outcomes for this program. These learning outcomes focus on human-centered security design, research and evaluation, data-driven decision-making, ethical and accessible design, and security usability testing and iteration.

1. **Human-Centered Security Design:** Graduates will apply psychological, physiological, and cognitive principles of human behavior to design, develop, and evaluate secure, usable interfaces that align with user needs and security requirements.
2. **Research and Evaluation:** Graduates will design, conduct, and critically evaluate research studies—including diary studies, surveys, and usability tests—to gather data that informs security and usability improvements in cyber systems.
3. **Data-Driven Decision Making:** Graduates will prioritize and communicate user research findings based on their impact on users, strategic goals, and security implications, ensuring decisions are grounded in comprehensive data analysis.
4. **Ethical and Accessible Design:** Graduates will integrate ethical, legal, and accessibility considerations into the development of secure systems, ensuring inclusivity while adhering to privacy and security standards such as GDPR and CCPA.
5. **Security Usability Testing and Iteration:** Graduates will conduct user-centered testing and iteratively improve cybersecurity solutions by identifying usability pitfalls, leading questions, and human behavioral patterns that affect security.

Explain how the institution will:

a) provide for assessment of student achievement of learning outcomes in the program

Program goals have been mapped across all courses in the curriculum and assessments for each competency and goal occur within courses. Rubrics are developed by the department and used to assess artifacts collected by faculty bi-annually. Departmental assessment meetings discuss ways to improve student outcomes across the curriculum and improvements are not limited to the courses where the assessment occurs.

b) document student achievement of learning outcomes in the program

As described above, assessment is a faculty-driven cycle of continuous improvement. While assessment results document student achievement, they are also used to drive curriculum change.

Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements.

The total number of credits for this program is 30. Students will take 12 credits of security-focused courses and 12 credits of usability-focused credits. Students will also take six credits of electives from a defined list.

Required Security Courses (12 credits):

Course Number	Title	Credits
AITC 670	Usable Security and Privacy	3
IDIA 672	Human Factors in Security Design	3
AITC 676	Documentation and Testing for Usable Security	3
AITC 674	Requirements Elicitation and UX	3

Required Usability Courses (12 credits):

Course Number	Title	Credits
IDIA 660	Usability and Accessibility in Cybersecurity	3
IDIA 662	Designing for Security	3
IDIA 640	Human Computers and Cognition	3
IDIA 642	Applied User Research for UX	3

Electives (6 credits):

Course Number	Title	Credits
IDIA 630	Information Architecture	3
IDIA 612	Interaction Design	3
IDIA 712	Advanced Interaction Design	3
IDIA 740	Topics in Computers and Cognition	3
IDIA 742	Topics in Advanced User Research	3

Course Descriptions

AITC 670 Usable Security and Privacy

This seminar explores the critical intersection of security, privacy, and usability. Students will gain a foundational understanding of key concepts, practical skills, and a deep appreciation for the human element in security. By analyzing real-world case studies, applying user-centered design principles, and evaluating ethical considerations, students will develop the expertise to design and implement effective, user-friendly security solutions.

Pre-requisite: IDIA 672 Human Factors in Security

AITC 674 Requirements Elicitation and UX

Bridges user experience design concepts with traditional software requirements elicitation processes and cybersecurity. Students learn about and implement best practices in requirements elicitation, maintaining the focus completely on the user experience rather than other functional and non-functional requirements that are traditionally at the core of the process of identifying software specifications.

Pre-requisite: IDIA 672 Human Factors in Security

AITC 676 Documentation and Testing for Usable Security

Focuses on the deliberate inclusion of concepts and practices related to user experience into software testing and documentation, which are processes that are closely tied to cybersecurity. Students will learn about testing and documentation tools and techniques, and the course content will focus on aspects related directly to usability and user experience. The material covered in this course takes the students from the initial steps of the process of testing as well as documentation, all the way to finished reports and documents. The instructor will utilize free and open-source software for practical examples throughout the course.

Pre-requisite: IDIA 672 Human Factors in Security

IDIA 612 Interaction Design

Explores electronic environments as fluid spaces where interactions among people, machines and media (words, images, sounds, video, animations, simulations) must be structured for the unforeseen. The course focuses on planning, analyzing, prototyping, and integrating interaction design with interface design. Lab fee required.

Prerequisite: PBDS 501 or passing score on HTML Proficiency Exam.

IDIA 630 Information Architecture

Students develop recommendations for site structure, navigation, labeling, metadata, and content strategy for a specific business model, audience, and context. Students base their recommendations on user research, requirements gathering, competitive analysis, and site analysis, including accessibility analysis. Lab fee required.

Prerequisite: PBDS 501 or passing score on a specified equivalent HTML proficiency exam.

IDIA 640 Humans Computers and Cognition

Introduces concepts, theories, and methods that support the study of human-computer interaction and user-centered system design. Students apply concepts from cognitive psychology and visual processing to explore human problem-solving, learning, knowledge representation, and problems of interface design. Prepares students to understand and analyze research based on empirical study of human behavior in its variety and complexity and on models of learning and understanding.

IDIA 642 Applied User Research for UX

Introduces the chief methods for studying users' interactions with software and information resources in ways that support design decisions. Encompasses both quantitative and qualitative methods, including methods such as surveys, focus groups, field studies, and traditional usability studies.

IDIA 660 Usability and Accessibility in Cybersecurity

Examines the critical challenges of usability and accessibility within cybersecurity. This course emphasizes user-centered design and iterative development to create secure, intuitive, and inclusive cybersecurity experiences. Students will engage in user testing methodologies to evaluate and enhance cybersecurity tools and practices, ensuring they are effective and accessible for diverse user populations.

Prerequisite: IDIA 640 Humans, Computers, and Cognition.

IDIA 662 Designing for Security

Bridges the gap between cybersecurity and user experience (UX) design, providing students with the skills to create secure systems that are also user-friendly. Through hands-on activities and theoretical study, students will learn how poor usability can compromise security and how human-centered design principles can enhance security features. Topics include designing intuitive authentication systems, addressing common usability pitfalls in security, and conducting usability testing to improve system effectiveness. This course is ideal for programmers and cybersecurity professionals looking to integrate UX principles into security solutions.

IDIA 672 Human Factors in Security

The human factor in cybersecurity threats is often overlooked, and solutions often focus upon forcing humans to adapt to the technological fix. This course examines the neurocognitive, psychological, and physical aspects of human cognition that impact the development and deployment of cybersecurity tools. It emphasizes the methodological approaches to designing security tools and interfaces that work alongside human cognition. Students will examine the levels of analysis at which humans interact with cybersecurity solutions from the internal through the organizational. The focus will be on how cybersecurity professionals and solutions can better leverage human abilities to improve cybersecurity.

IDIA 712 Advanced Interaction Design

Intensive exploration of topics in advanced interaction design of mutual interest to students and faculty. Content varies according to the concurrent interests of faculty and students. Course may be repeated for credit when the topic changes. Lab fee required. Prerequisite: PBDS 501 or passing score on the hypermedia proficiency exam.

IDIA 740 Topics in Computers and Cognition

Intensive exploration of topics in human/computer interaction and cognition of mutual interest to students and faculty. Content varies depending on the interests of faculty and students. Course may be repeated for credit when topic changes. Lab fee required. Prerequisite: IDIA 640 or permission of instructor.

IDIA 742 Topics in User Research

Intensive exploration of topics in user research of mutual interest to students and faculty. Content varies depending on the interests of faculty and students. Course may be repeated for credit when the topic changes. Lab Fee required. Prerequisite: PBDS 501 or passing score on the hypermedia proficiency exam in addition to IDIA 642.

Discuss how general education requirements will be met, if applicable.

Not applicable to graduate degrees.

Identify any specialized accreditation or graduate certification requirements for this program and its students.

There are no accreditation or graduate certifications required for this program.

If contracting with another institution or non-collegiate organization, provide a copy of the written contract.

Not applicable.

Provide assurance and any appropriate evidence that the proposed program will provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial resources, and costs and payment policies.

UBalt's website is a valuable resource that offers students a wealth of up-to-date information. This includes details about program curricula, course and degree requirements, expected technology competencies and skills for each degree, technical equipment prerequisites for courses, academic support services, available financial aid resources, comprehensive cost breakdowns, and payment policies. Additionally, students can access information about our state-of-the-art learning management system (LMS), Canvas, which serves as a vital platform for their educational journey.

Within Canvas, we provide a range of student tutorials to assist with LMS navigation, ensuring students can make the most of its features. Moreover, individual courses can offer resource materials through this platform, further enhancing the learning experience.

Our commitment to student success extends to ensuring accessibility. The University's Office of Disability and Access Services maintains a dedicated website and physical office with regular office hours. We also provide access to video and audio technologies to assist students who require accommodation.

The Division of Student Support and Access Services, along with the Bogomolny Library, offer a diverse array of academic and other support services. These encompass access to counseling resources, available 24/7, to address the various needs of our students and foster their overall well-being.

The program director will work with the website content manager to ensure that the MS in User-Centered Cybersecurity curriculum content pages are developed and posted. The catalog will be revised to reflect the new program requirements, and an updated Guide to Graduation for the MS in User-Centered Cybersecurity will be provided for the major. Information about course formats and technology assumptions, as well as any equipment requirements, will be available, as usual, to students in the course schedule. Each student will receive a syllabus that outlines student learning outcomes, course format, technology

needs, and campus resources. These resources include the Office of Disability and Access Services, the Academic Support Center (which has a Writing Center), and the Office of Technology Services.

Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available.

The program director will communicate with the Yale Gordon Collge of Arts and Sciences and university marketing departments to ensure that any marketing materials, such as program fact sheets, reflect the new curriculum. See above for information about the catalog and website. The catalog is updated annually and posted online, in addition to the routine program web page updates.

H. Adequacy of Articulation

The Program is within the scope of Accelerated BS-MS programs within the University of Baltimore, as articulated by the University System of Maryland’s rules for Accelerated Programs. Under this Policy, an undergraduate student with a GPA of 3.5 or higher is allowed to take up to 9 graduate credits and double count them towards their graduate degree.

I. Adequacy of Faculty Resources

Provide a brief narrative demonstrating the quality of program faculty. Include a summary list of faculty with appointment type, terminal degree title and field, academic title/rank, status (full-time, part-time, adjunct) and the course(s) each faculty member will teach in the proposed program.

Faculty Member	Appointment Type	Field	Status	Terminal Degree	Academic Rank	Courses to be taught
Bridget Blodgett	Tenured	Online Communities / Programming	Full-time	PhD	Associate Professor	IDIA and AITC courses
Cory Newman	Contract	Interaction Design / Programming	Full-time	DSc (ABD)	Lecturer	AITC courses
Kathryn Summers	Tenured	Accessibility/Usability	Full-time	PhD	Professor	IDIA courses
Greg Walsh	Tenured	User-centered Design	Full-time	PhD	Associate Professor	IDIA courses
Giovanni Vincenti	Tenured	Applied Information Technology	Full-time	DSc	Associate Professor	AITC courses

Demonstrate how the institution will provide ongoing pedagogy training for faculty in evidence-based best practices, including training in:

a) Pedagogy that meets the needs of the students

The University of Baltimore provides periodic training to its faculty on the use of the latest online and face-to-face teaching tools through its Center for Excellence in Learning, Teaching and Technology (CELTT). It also offers professional development opportunities through attending national conferences and training, such as Coursera, EdX, etc. In addition, the faculty is afforded opportunities to attend continuing professional education sessions through other providers of technical skills training, such as Coursera and Udemy.

b) The learning management system (LMS)

The University of Baltimore provides periodic necessary trainings in its Learning Management System—Canvas—through its Center for Excellence in Learning, Teaching and Technology (CELTT) as well as periodic quality reviews of the faculty's utilization of LMS.

Evidenced-based best practices for distance education, if distance education is offered.

Similar to LMS training, The University of Baltimore's CELTT provides periodic training in online teaching to its faculty. Additionally, the faculty of the Yale Gordon College of Arts and Sciences coordinates informal, collegial discussions about course design and delivery. Student evaluation data is used to improve course design and effectiveness.

J. Adequacy of Library Resources

The program does not require substantial additional library resources beyond those already provided by the University of Baltimore's Bogomolny Library which provides an adequate level of access to academic books and journals. Bogomolny Library also provides access to a number of datasets that can be used in usability and cybersecurity projects.

K. Adequacy of Physical Facilities, Infrastructure and Instructional Equipment

The University of Baltimore's current facilities provide excellent conditions for user-centered cybersecurity work through our User Research Lab and through our current computer labs. The University also provides students with loaner laptops whenever they need them. Our classrooms are adequately equipped for both online and face-to-face instruction, and they have up-to-date IT infrastructure.

The University of Baltimore provides every student with an email address, access to our learning management system (Canvas), and free access to Office 365 software (Word, Excel and PowerPoint). All faculty and credit-earning students are provided with an institutional e-mail account that integrates with the institution's learning management

system, Canvas. Open-access, comprehensive student support for the learning management system is provided in module format and includes “how to” video and print tutorials, links to student services, and tips for success in an online learning environment. Faculty can access an LMS training site and work with Canvas faculty fellows from their colleges and instructional designers for course design and technical support. Both faculty and staff have access to 24/7 phone and chat support.

L. Adequacy of Financial Resources with Documentation

Provide finance data for the first five years of program implementation. Enter figures into each cell and provide a total for each year. Also provide a narrative rationale for each resource category. If resources have been or will be reallocated to support the proposed program, briefly discuss the sources of those funds. Do not leave any cells blank (use “0” if no data is applicable).

The Yale Gordon College of Arts and Sciences anticipates a modest student gain per year because of this program. We assume that this program will attract students who primarily plan to take two courses, or six credits, per semester, similar to the way the majority of students currently pursue the MS, Interaction Design and Information Architecture degree. Also, due to our Regional tuition and fee structure for students in Maryland, Washington, D.C., Delaware, and parts of Virginia and Pennsylvania, this tuition estimate uses in-state tuition for all estimates. Future tuition estimates are modeled on a 2% increase per year while fees, including projected course fees, are not increased in the model. Future enrollment estimates are based on an initial surge in the second year due to Spring enrollments and then 10% annual growth.

Resource Categories	FY 2026	FY 2027	FY 2028	FY 2029	FY 2030
1. Tuition and Fee Revenue (c + g below)	\$155,508	\$279,534	\$296,588	\$314,050	\$331,920
a. Number of F/T students	2	4	4	4	4
b. Annual Tuition/Fee Rate	\$17,924	\$18,212	\$18,518	\$18,824	\$19,130
c. Total F/T Revenue (a*b)	\$35,848	\$72,848	\$74,072	\$75,296	\$76,520
d. Number of P/T students	10	17	18	19	20
e. Credit Hour Rate	\$993 + \$25	\$1009+ \$25	\$1,026 + \$25	\$1,043 + \$25	\$1,060 + \$25

f. Annual Credit Hours	12	12	12	12	12
g. Total P/T Revenue (d*e*f)	\$119,660	\$206,686	\$222,516	\$238,754	\$255,400

Complete Table 2: Program Expenditures and Narrative Rationale. Provide finance data for the first five years of program implementation. Enter figures into each cell and provide a total for each year. Also provide a narrative rationale for each expenditure category.

Table 2: Program Expenditures					
Resource Categories	FY 2026	FY 2027	FY 2028	FY 2029	FY 2030
1. Faculty (b + c below)	\$17,754	\$93,440	\$144,193	\$147,754	\$151,316
a. Number of FTE	0	0.5	1	1	1
b. Total Salary	\$16,450	\$76,350	\$113,150	\$116,450	\$119,750
c. Total Benefits	\$1,304	\$17,090	\$31,043	\$31,304	\$31,566
2. Admin Staff (b + c below)	\$0	\$0	\$0	\$0	\$0
a. Number of FTE	0	0	0	0	0
b. Total Salary	\$0	\$0	\$0	\$0	\$0
c. Total Benefits	\$0	\$0	\$0	\$0	\$0
3. Support Staff (b + c below)	\$0	\$0	\$0	\$0	\$0
a. Number of FTE	0	0	0	0	0
b. Total Salary	\$0	\$0	\$0	\$0	\$0
c. Total Benefits	\$0	\$0	\$0	\$0	\$0
4. Technical Support and Equipment	\$0	\$20,390	\$13,593	\$14,160	\$14,726
5. Library	\$0	\$0	\$0	\$0	\$0
6. New or Renovated Space	\$0	\$0	\$0	\$0	\$0
7. Other Expenses	\$1,841	\$3,257	\$3,399	\$3,540	\$3,682
Total (Add 1 through 7)	\$19,595	\$117,087	\$161,185	\$165,454	\$169,724

There is existing full-time faculty capacity to support the initial start-up of this new program. Since this program would share faculty and equipment resources with existing programs, the tables provide an incremental view of revenue and expenditures. Based upon the projected enrollment profile, the immediate resource expenses include salary for adjunct faculty, a program director summer stipend, and consumables paid for by charged course fees. Enrollment growth in the out-years will require additional full-time faculty and adjunct support. The Technical Support and Equipment and Other Expenses resource categories illustrate the planned equipment recapitalization and course consumables, respectively, that are funded with course fees.

M. Adequacy of Provisions for Evaluation of Program

The University has a shared governance process for curriculum approval. Both new courses and new programs are required to submit student learning outcomes (SLOs), which are then evaluated by faculty curriculum committees, plus staff in the deans' and provost's office.

The assessment of program student learning outcomes is faculty-driven. Assessment generally occurs within courses, but assessment results are shared and evaluated within the Yale Gordon College of Arts and Sciences.

Faculty are evaluated annually by their supervisor and dean. In addition, policies for tenure-track and tenured faculty call for in-depth peer review at regular intervals.

All courses undergo student evaluation using the college-wide software tool Explorance Evaluations. Students complete evaluations of their course and the instructor at the end of each semester, using an online form. Data from these evaluations are incorporated in the annual chair's evaluation of faculty and are used in faculty promotion and tenure decisions.

Student learning outcomes are assessed over a two-year cycle using direct and indirect measures. The primary assessment measures are direct assessments administered within courses, evaluated by faculty, reviewed by programs, and affirmed by the Yale Gordon College of Arts and Sciences as a whole.

Retention is a key metric of the quality of our courses and faculty and retention data is reviewed on an ongoing basis, as are student evaluations of faculty. These evaluations have highlighted improvements that can be implemented across the curriculum in course delivery and feedback.

As we implement the new curriculum, we have created a new assessment plan. Embedded assessments will be deployed beginning in Fall 2025 for the new program goals and the faculty will use this data to drive curriculum improvement.

N. Consistency with the State's Minority Student Achievement Goals

The University of Baltimore is an unusually diverse institution, with an average undergraduate age over 27, and a majority-minority undergraduate population. Approximately 47 percent of UB students are African American and 32 percent white.

The University serves nontraditional students, which includes many working adults. UBalt's current strategic plan underlines the importance of diversity, equity, and inclusion, and one of the strategic goals is specifically to strengthen UBalt's commitment to these core values.

O. Relationship to Low Productivity Programs Identified by the Commission

This program is not related to any low-productivity programs.

P. Adequacy of Distance Education Programs

The University of Baltimore has a long history of online education, offering the first fully online AACSB-accredited MBA program and having had the MS in Interaction Design and Information Architecture and PBC in User-Experience (UX) Design programs completely online for over ten years. As a University, we are versed in the technical, pedagogical, and social aspects of online learning.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. <https://doi.org/10.1145/322796.322806>

Haney, J. (2023, September 28). *NIST unveils newly named Human-Centered Cybersecurity program*. NIST. <https://www.nist.gov/blogs/cybersecurity-insights/nist-unveils-newly-named-human-centered-cybersecurity-program>

Hielscher, J., Schöps, M., Menges, U., Gutfleisch, M., Helbling, M., & Sasse, M. A. (2023). Lacking the tools and support to fix friction: results from an interview study with security managers. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)* (pp. 131-150).

Maryland Department of Labor announces \$1.8 million in funding for cyber ranges to address cybersecurity workforce gap - news - department of labor. Maryland Department of Labor. (2024, August 27). <https://labor.maryland.gov/whatsnews/laborannounces1.8mfundingforcyberranges.shtml>

Morris, J. (2024, May 16). *User-centric cyber security is the next big thing for the industry*. Fruto. <https://frutostudio.co.uk/blog/user-centric-cyber-security>

Petrescu, H. (2023, March 28). *The Future of Cybersecurity: Human-centred design*. Aura Research Division. <https://research.aurainfosec.io/advisory/the-future-of-cybersecurity-human-centred-design/>

Science of Security Virtual Organization. (n.d.). *User-centered design for security: Science of security virtual organization*. User-Centered Design for Security | Science of Security Virtual Organization. <https://sos-vo.org/projects/user-centered-design-security>

U.S. Bureau of Labor Statistics. (2024, April 3). *Information security analysts*. U.S. Bureau of Labor Statistics . <https://www.bls.gov/oes/current/oes151212.htm>

U.S. Bureau of Labor Statistics. (2024a, April 3). *Computer network architects*. U.S. Bureau of Labor Statistics. <https://www.bls.gov/oes/current/oes151241.htm>

U.S. Bureau of Labor Statistics. (2024b, April 3). *Maryland - May 2023 OEWS state occupational employment and wage estimates*. U.S. Bureau of Labor Statistics. https://www.bls.gov/oes/current/oes_md.htm

U.S. Bureau of Labor Statistics. (2024c, April 3). *Washington-Arlington-Alexandria, DC-VA-MD-WV - May 2023 OEWS metropolitan and Nonmetropolitan Area Occupational Employment and wage estimates*. U.S. Bureau of Labor Statistics. https://www.bls.gov/oes/current/oes_47900.htm

Zurko, M. E., & Simon, R. T. (1996). User-centered security. *Proceedings of the 1996 Workshop on New Security Paradigms - NSPW '96*, 27–33. <https://doi.org/10.1145/304851.304859>