BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION,
INFORMATION OR DISCUSSION

TOPIC: University of Maryland University College, M.S. in Cybersecurity Policy

COMMITTEE: Education Policy

DATE OF COMMITTEE MEETING: March 24, 2010

SUMMARY: The proposed program in M.S. in Cybersecurity Policy complements UMUC's existing suite of programs in the areas of information assurance and homeland security. In particular, the proposed new program is an outgrowth of the existing M.S. in Cybersecurity, which focuses on technical and applied aspects of maintaining secure cyberspace. The proposed program, by contrast, will focus on issues related to developing and administering effective policies in the area of cybersecurity.

The program will provide baccalaureate-holding, mid-career professionals the opportunity to obtain a specialized graduate education in preparation for leadership and policy-making roles of increasing responsibility within the cybersecurity field in both public and private settings. Additionally, the program will prepare those interested in seeking entry to this field.

As a recent emerging field, there are no comparable programs at any other public institution in Maryland and there are hundreds of positions in cybersecurity available in the Maryland/DC region. Graduates of this program may qualify for such positions as Chief Security Officer, Cyber Security Manager or Administrator, Cyber Policy Analyst, Cyber Intelligence Analyst, federal, state and local government manager, and Legislative Aide.

As one of six universities in Maryland certified by the National Security Agency (NSA) as a National Center of Academic Excellence (CAE), UMUC is well positioned to provide advanced education in cybersecurity policy and students would be eligible for scholarship support through the NSA CAE. It is projected that the program would initially enroll fifteen students and grow to a "steady-state" of sixty students within three years.

ALTERNATIVE(S): The Regents may not approve the program or may request further information.

FISCAL IMPACT: No additional funding is necessary. The program will be supported through reallocated funds and tuition.

CHANCELLOR'S RECOMMENDATION: That the Committee on Education Policy recommend that the Board of Regents approve the proposal from the University of Maryland University College to offer the M.S. in Cybersecurity Policy.

COMMITTEE RECOMMENDATION: Approval. DATE: March 24, 2010

BOARD ACTION: DATE:

SUBMITTED BY: Irwin Goldstein (301) 445-1992 irv@usmd.edu

University of Maryland University College
Office of the Provost and Chief Academic Officer

March 5, 2010

James E. Lyons, Sr., Ph.D.
Secretary
Maryland Higher Education Commission
839 Bestgate Rd., Suite 400
Annapolis, MD 21401

Dear Dr. Lyons:

Attached is a proposal from University of Maryland University College (UMUC) for a new graduate degree program, the Master of Science in Cybersecurity Policy. If approved by the Maryland Higher Education Commission and the Board of Regents of the University System of Maryland, the Cybersecurity Policy degree program will be launched in the Fall 2010 semester.

The proposed new program complements UMUC's existing suite of programs in the areas of information assurance and homeland security. In particular, the proposed new program is an outgrowth of our Master of Science in Cybersecurity, which focuses on technical and applied aspects of maintaining secure cyberspace. The proposed new program, by contrast, will focus on more abstract issues related to developing and administering effective policies in the area of cybersecurity.

The proposed new program will provide a needed pathway for professionals to enter or advance in the rapidly growing, and changing, cybersecurity sector. The Cybersecurity Policy program is congruent with UMUC's long-term relationship with the U.S. Department of Defense and with the emerging needs of current and future Maryland-based employers in both the public and private sectors.

We very much look forward to adding the new Master of Science in Cybersecurity Policy program to our graduate-level offerings. If you have any questions or need additional information about the proposed program, please feel free to contact me.

Sincerely,

Greg von Lehmen, Ph.D.
Provost & Chief Academic Officer

cc: Dr. Irwin Goldstein

UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR

X New Instructional Program
Substantial Expansion/Major Modification
Cooperative Degree Program

University of Maryland University College
Institution Submitting Proposal

Master of Science in Cybersecurity Policy
Title of Proposed Program

Master of Science Degree to be Awarded	**Fall 2010** Projected Implementation Date
TBD Proposed HEGIS Code	**TBD** Proposed CIP Code
Graduate School of Management and Technology Department in which program will be located	**Michael S. Frank, Ph.D.** Department Contact
301-985-7200 Contact Phone Number	**graddean@umuc.edu** Contact E-Mail Address
Signature of President or Designee	**3/5/2010** Date

Mission

The mission of University of Maryland University College (UMUC) is to offer top-quality educational opportunities to adult students in Maryland, the nation, and the world, setting the global standard for excellence in adult education. By offering academic programs that are respected, accessible, and affordable, UMUC broadens the range of career opportunities available to students, improves their lives, and maximizes their economic and intellectual contributions to Maryland and the nation.

UMUC proposes to create a new Master of Science in Cybersecurity Policy. The proposed new program is an outgrowth of our Master of Science in Cybersecurity, which focuses on technical and applied aspects of maintaining secure cyberspace. The proposed new program, by contrast, will focus on more abstract issues related to developing and administering effective policies in the area of cybersecurity.

Rationale for the Program

Cyberspace is now a key frontline domain for U.S. defense, along with air, land, and sea. For this reason, in June 2009, the Department of Defense established the U.S. Cyber Command ("Cybercom") as a unit in the U.S. Strategic Command. Cybercom is led by the director of the National Security Agency at Fort Meade, MD. In the order creating Cybercom, Secretary of Defense Robert Gates referred to cyberspace as "a distinct military domain." UMUC's Master of Science in Cybersecurity Policy will educate highly-qualified cyber security professionals capable of leading the effort to defend this critical component of our national security.

The proposed new MS in Cybersecurity Policy is being created as the result of an external review of UMUC's existing Cybersecurity Master of Science program. The external reviewer, Dr. William W. Agresti, holds the rank of Professor in the Carey Business School at Johns Hopkins University. He is a nationally recognized expert in information systems security and large-scale project management. The Cybersecurity faculty, working with Dr. Agresti, identified the area of Cybersecurity Policy as a market requiring specific educational preparation that would be distinct from our existing program focusing on technical aspects of Cybersecurity.

The proposed new Master of Science in Cybersecurity Policy degree program will contribute to fulfillment of UMUC's mission by providing baccalaureate-holding professionals the opportunity to obtain a specialized graduate education in preparation for leadership and policy-making roles of increasing responsibility within the cybersecurity community in both private and public settings.

In assessing UMUC's proposed new MS in Cybersecurity Policy under *Fordice*, we note that the program cannot be traceable to prior segregation in Maryland. Cybersecurity is a new field that did not exist when Maryland had a segregated system of higher education. Additionally, there is no duplication with other programs at public institutions of higher education, as there are no comparable programs at any of these institutions, including any of the HBCUs.

Potential Market

According to the report *CyberMaryland*, released in December 2009 by the Maryland Department of Business and Economic Development, global information technology spending was estimated at $796 billion in 2009, with cybersecurity accounting for up to 20% of that amount. INPUT, a market research firm, projects that the demand for cybersecurity products and services by the federal government alone will increase from $7.9 billion in 2009 to $11.7 billion in 2014.

The presence of fifty federal agencies and research facilities has made Maryland the "Epicenter of Cyber Security," according to the *CyberMaryland* report. The same report notes that Maryland currently has more than 60,000 job in cybersecurity, one of the highest concentrations of technology positions in the country. The *CyberMaryland* report articulates a priority of the State of Maryland to "Develop an educational pipeline to train new cyber security talent and advance workforce development," and further to "Develop workforce training programs to address industry needs." The report notes that "Cyber security requires a workforce that is ready to meet the field's technical and **policy demands**" (emphasis added), leading to a stated objective for Maryland to "develop an academic cyber security curriculum for degree or certification at the post-secondary level, community colleges, four-year colleges and universities.

UMUC is one of six universities in Maryland certified by the National Security Agency (NSA) as National Centers of Academic Excellence (CAE); the goal of the CAE program is "to reduce vulnerability in our national information infrastructure by promoting higher education and research in [Information Assurance] and producing a growing number of professionals with [Information Assurance] expertise in various disciplines." With the CAE designation, UMUC is thus well-positioned to provide advanced education in cybersecurity policy.

A recent online search for open cybersecurity positions yielded hundreds of available positions in the Maryland and DC area, with companies such as

- Accenture
- Arksight Cybersecurity Professionals
- BAE Systems
- Boeing
- Booz Allen Hamilton
- CACI International
- Computer Sciences Corporation (CSC)
- Federal Government Jobs
- GE
- General Dynamics
- Homeland Security
  Honeywell International
- IBM
- Immigration and Customs Enforcement
- L3 Communications
- Lockheed Martin Corporation
- ManTech, ManTech International
- ManTech Mission Cyber & Technology Solutions
- MITRE
- Northrup Grumman Corporation
- PricewaterhouseCoopers
- Raytheon
- SAIC
- Siem Cybersecurity Professionals
- SRS Technologies
- Trilogy Technical Services
- Wood Consulting Services

Student Audience

The proposed program will serve baccalaureate-holding mid-career cybersecurity professionals as well as those seeking entry into the career field. UMUC students would be eligible, under the NSA CAE designation, to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program.

Depending upon their prior educational and professional backgrounds, graduates of this program may qualify for the following types of positions:

- Chief Security Officer
- Cyber Security Manager or Administrator
- Cyber Policy Analyst
- Cyber Intelligence Analyst
- Federal, State, and Local Government Manager
- Legislative Aide

Projected Enrollments

Enrollments for the Cybersecurity Policy MS program in the Fall Term in the first five years of the program are projected to be as follows:

Year	Projected Enrollment
2010	15
2011	20
2012	30
2013	60
2014	60

Catalog Description and Educational Objectives

Society has become increasingly reliant on information and communications technologies — and increasingly vulnerable to cyberspace threats. The Master of Science (MS) in Cybersecurity Policy is designed for mid-career professionals who wish to help meet the challenges posed by increasing cyber threats. The MS in Cybersecurity Policy uses a multidisciplinary approach, drawing from fields such as management, law, ethics, science, technology, business, psychology, and sociology, to provide students with the broad background necessary to recognize and analyze possible policy opportunities for resolving cybersecurity problems. The curriculum examines strategies for societal responses to cybersecurity threats at enterprise, national and global levels. The roles of government, inter-organizational alliances, and international cooperatives are explored, as well as legal concepts such as privacy, intellectual property, and civil liberties.

Student Learning Outcomes

Graduates of the Cybersecurity Policy Program will be able to

- Assess the scale and scope of the risk of potential cyber threats at the enterprise, national and global level.
- Assess measures to prevent anticipated cyber intrusions and to ensure business continuity.
- Assess organizational controls that can detect cyber intrusions as quickly as possible.
- Assess responses to unanticipated as well as anticipated cyber intrusions to restore the operations of one's organization as quickly as possible.
- Work with people in one's organization and in other organizations to secure access to cyberspace and to design effective policies to counter specific cyber intrusions launched from anywhere in the world.
- Employ the experiences from past cyber intrusions to mitigate future cyber threats.
- Formulate and implement policies on an organizational, national and international level to help organizations, individually and collectively, successfully prevent, detect and recover from cyber intrusions.
- Identify the requisite technical components of a response to help organizations, individually and collectively, successfully prevent, detect and recover from cyber intrusions.

Curriculum and Requirements

The 36-credit curriculum consists of six 6-credit courses, including 12 credits of foundation coursework, 18 credits of professional, specialty coursework, and a 6-credit integrative capstone course. The curriculum is built upon an overarching framework examining cybersecurity at the enterprise, national, and global levels. The course work will include a required student project, thus qualifying the curriculum for Professional Science Masters (PSM) designation. The Professional Science Master's (PSM) is a type of graduate degree that is designed to allow students to pursue advanced training in science or mathematics, while simultaneously developing workplace skills highly valued by employers.

The structure of the curriculum is shown below; all courses are 6 credits each and must be taken in sequence. The curriculum does not include a thesis option.

Required Foundation Courses (12 credits)

- CSEC 610 Cybersecurity and Cyberspace
- CSEC 620 Human Aspects in Cybersecurity: Ethics, Legal Issues, and Psychology

Required Professional Courses (18 credits)

- CSEC 635 National Cybersecurity Policy and Law (new)
- CSEC 645 Enterprise Cybersecurity Policy (new)
- CSEC 655 Global Cybersecurity (new)

Required Capstone Course (6 credits)

- CSEC 670 Cybersecurity Capstone (new)

Course Descriptions

CSEC 610 Cyberspace and Cybersecurity (6 credits)
A study of the fundamentals in cyberspace and cybersecurity. Topics include cyber architecture, cyber services, protocols, algorithms, hardware components, software components, programming languages, various cybersecurity mechanisms, business continuity planning, security management practices, security architecture, operations security, physical security, cyber terrorism, and national security.

CSEC 620 Human Aspects in Cybersecurity: Ethics, Legal Issues, and Psychology (6 credits)
Prerequisite: CSEC 610. An examination of the human aspects in cybersecurity. Topics include ethics, relevant laws, regulations, policies, standards, psychology, and hacker culture. Emphasis will be placed on the human element and motivations for cyber crimes. Analysis will include examination of techniques that can be applied for enterprises to prevent such intrusions and attacks that threaten organizational data

CSEC 635 National Cybersecurity Policy and Law (6 credits) (new)
Prerequisite: CSEC 620. An exploration of the role of government in securing cyberspace. Topics include federal, state, and local entities involved in cybersecurity; relevant laws and regulation; concepts of civil liberties, intellectual property, and privacy; policy formulation and analysis; law enforcement; development and diffusion of standards; and national security. Discussion also covers public/private engagement models and opportunities and tools for government to encourage cybersecurity education, awareness, and research.

CSEC 645 Enterprise Cybersecurity Policy (6 credits) (new)
Prerequisite: CSEC 635. An exploration of organizational policies to respond to cybersecurity threats. Topics include strategic cybersecurity initiatives, cybersecurity in interorganizational relationships, increasing cybersecurity awareness in the organization, compliance issues, liability, and promoting a culture of sensitivity to cybersecurity issues.

CSEC 655 Global Cybersecurity (6 credits) (new)
Prerequisite: CSEC 645. An in-depth study of cybersecurity from a global perspective. Topics include cyberterrorism, cybercrime, and cyberwarfare; the international legal environment; nation- and region-specific norms regarding privacy and intellectual property; international standard setting; effects on trade (including offshore outsourcing); and opportunities for international cooperation.

CSEC 670 - Cybersecurity Capstone (6 credits) (new)
Prerequisite: CSEC 655. A study of, and exercise in, developing, leading, and implementing effective enterprise- and national-level cybersecurity programs. Focus is on establishing programs that combine technological, policy, training, auditing, personnel, and physical elements. Challenges within specific industries (such as health, banking, finance, and manufacturing) are discussed. Topics include enterprise architecture, risk management, vulnerability assessment, threat analysis, crisis management, security architecture, security models, security policy development and implementation, security compliance, information privacy, identity management, incident response, disaster recovery, and business continuity planning. A project reflecting integration and application of learning of cybersecurity is included.

Faculty Resources

The faculty members who will teach in the MS in CS all hold appropriate terminal or professional degrees. In addition, all have substantial professional experience in cyber security:

- Mary C. Carroll, J.D.
- Jeffrey A. Clark, Ph.D.
- Jim Q. Chen, Ph.D.
- Marius Crisan, Ph.D.
- Valentin Cristea, Ph.D.
- David Dampier, Ph.D.
- Roxanne Everetts, D.M.
- Moses Garuba, Ph.D.
- Mario A. Garcia, Ph.D.
- David L. Madison, Ph.D.
- Kara L. Nance, Ph.D.
- Tobias Philbin, Ph.D.
- Jim Tray, Ph.D.
- Henry W. Tsai, Ph.D.
- Richard Thayer, Ph.D.
- David O. Ward, J.D.

Impact on Students' Technology Fluency

Technology fluency is a core learning area for UMUC and is assessed at the institutional level as well as incorporated into all degree programs. All UMUC graduate students are required to complete, within their first six credits of graduate study, the fully online course UCSP 611 Introduction to Graduate Library Research Skills, which covers the appropriate use of online library and information resources. The entire curriculum of the proposed MS in Cybersecurity Policy program requires an advanced understanding of technology issues. Students will begin to achieve this advanced competency with enrollment in the required 6-credit foundation course CSEC 610 Cyberspace and Cyber Security, which has a strong focus on the technologies used in the cyberspace including information and telecommunication technologies and their use and impact in the modern workplace. In addition, the online portions of the program will help students to acquire and maintain a very high level of applied technological proficiency.

Infrastructure and Resources

UMUC has sufficient library resources, and sufficient facilities and equipment — including its existing cyber laboratory — to support the proposed program.

UMUC will require no new general funds from the state to develop and launch this program. UMUC will reallocate internal funds to cover the course development and marketing expenses in the first two years of the program; thereafter, the program will be fully self-supporting.

Tables 1 and 2 following show Projected Resources and Expenditures based on the projected enrollments.

TABLE 1: RESOURCES

Resources Categories	(Year 1)	(Year 2)	(Year 3)	(Year 4)	(Year 5)
1. Reallocated Funds'	$35,119	$8,090	$0	$0	$0
2. Tuition/Fee Revenue[2] (c+g below)	$120,150	$166,680	$259,740	$540,000	$561,600
a. #F.T. Students	0	0	0	0	0
b. Annual Tuition/Fee Rate	N/A	N/A	N/A	N/A	N/A
c. Annual Full Time Revenue (a x b)	N/A	N/A	N/A	N/A	N/A
d. # Part Time Students	15	20	30	60	60
e. Credit Hour Rate	$445	$463	$481	$500	$520
f. Annual Credit Hours per student per year	18	18	18	18	18
g. Total Part Time Revenue (d x e x f)	$120,150	$166,680	$259,740	$540,000	$561,600
3. Grants, Contracts, & Other External Sources	$0	$0	$0	$0	$0
4. Other Sources	$0	$0	$0	$0	$0
TOTAL (Add 1 - 4)	**$155,269**	**$174,770**	**$259,740**	**$540,000**	**$561,600**

[1] UMUC will reallocate internal funds during Years I and II primarily for the development of the required new courses for the program as well as for initial marketing. From Year Ill onward the program will be fully self-supporting.

[2a-c] UMUC's graduate students are predominantly working adults who pursue their higher education activities part-time; therefore, no full-time students are included in this table.

[2d-f] This table uses UMUC's anticipated resident graduate credit hour rate with projected annual increase of 4%. Because of the online availability of the program, however, UMUC expects to enroll non-resident students as well, in which case the revenue will be higher than shown.

TABLE 2: EXPENDITURES

Expenditure Categories	(Year 1)	(Year 2)	(Year 3)	(Year 4)	(Year 5)
1. Total Faculty Expenses (b + c below)	$8,100	$33,750	$54,000	$81,000	$81,000
a. # FTE ($27,000 annual salary)	30%	125%	200%	300%	300%
b. Total Salary (Adjunct faculty)	$8,100	$33,750	$54,000	$81,000	$81,000
c. Total Benefits	N/A	N/A	N/A	N/A	N/A
2. Total Administrative Staff Expenses (b + c below)	$37,950	$37,950	$63,250	$94,875	$126,500
a. # FTE ($100K annual salary)	30%	30%	50%	75%	100%
b. Total Salary	$30,000	$30,000	$50,000	$75,000	$100,000
c. Total Benefits (26.5%)	$7,950	$7,950	$13,250	$19,875	$26,500
3. Total Support Staff Expenses (b + c below)	$15,813	$15,813	$15,813	$15,813	$15,813
a. # FTE ($50,000 annual salary)	25%	25%	25%	25%	25%
b. Total Salary	$12,500	$12,500	$12,500	$12,500	$12,500
c. Total Benefits (26.5%)	$3,313	$3,313	$3,313	$3,313	$3,313
4. Equipment	$0	$0	$0	$0	$0
5. Library (see Overhead)	$0	$0	$0	$0	$0
6. New or Renovated Space	$0	$0	$0	$0	$0
7. Other Expenses (Course development, marketing, overhead)	$93,406	$87,257	$71,854	$103,512	$120,589
TOTAL (Add 1 - 7)	**$155,269**	**$174,770**	**$204,917**	**$295,200**	**$343,902**