September 30, 2011

MEMORANDUM

TO: Darryll Pines
Dean, A. James Clark School of Engineering

FROM: Elizabeth Beise
Associate Provost for Academic Planning and Programs

SUBJECT: Proposal to Establish a Cybersecurity Option to the Post-Baccalaureate Certificate in Engineering (PCC log no. 11004)

At its meeting on September 16, 2011, the Senate Committee on Programs, Curricula and Courses approved your proposal to establish a Cybersecurity option to the Post-Baccalaureate Certificate in Engineering. A copy of the approved proposal is attached.

The option is effective Spring 2012. The School should ensure that the option is fully described in the Graduate Catalog and in all relevant descriptive materials, and that all advisors are informed.

MDC/

Enclosure

cc: David Salness, Chair, Senate PCC Committee
Sarah Bauder, Office of Student Financial Aid
Reka Montfort, University Senate
Erin Howard, Office of Information Technology
Donna Williams, Institutional Research & Planning
Anne Turkos, University Archives
Linda Yokoi, Office of the Registrar
Arthur Popper, Graduate School
William Fourney, A. James Clark School of Engineering
George Syrmos, Office of Advanced Engineering Education
Proposal for approving an academic option in Cybersecurity to the existing Post-Baccalaureate Certificate in Engineering program through the Office of Advanced Engineering Education.

JUSTIFICATION/REASONS/RESOURCES (Briefly explain the reason for the proposed action. Identify the source of new resources that may be required. Details should be provided in an attachment.)

See attached.

APPROVAL SIGNATURES - Please print name, sign, and date

1. Department Committee Chair

2. Department Chair George Syrmos 6/10/11

3. College/School PCC Chair

4. Dean Mark Shayman (Assoc. Dean for Grad. Programs) 7/20/11

5. Dean of the Graduate School (if required)

6. Chair, Senate PCC

7. Chair of Senate

8. Vice President for Academic Affairs & Provost

VPAAP 8-05
Proposal for a new academic option in Cybersecurity to the existing Post-Baccalaureate Certificate in Engineering program

Government, industry, and consumers depend on secure and reliable networks and information systems for daily communications and transactions. Vulnerabilities to cyber-attacks could lead to significant disruptions in telecommunications, data storage, banking, utilities, and transportation services. Addressing the cybersecurity threat requires innovative collaboration between IT security professionals, computer scientists, and computer engineers that take into account the roles of developers, vendors, customers, and end users. To develop the curriculum for the Cybersecurity Engineering program, we formed an advisory group that consisted of public, private, and academic experts, specifically faculty from the new Maryland Cybersecurity Center, lead innovators from our own Office of Information Technology and the UMCP/Fraunhofer USA Center for Experimental Software Engineering, governmental experts from the National Security Agency, and industry experts from Raytheon and SAIC.

The University of Maryland’s proximity to the nation’s capital and close interactions with key federal agencies, such as the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST), make College Park an ideal place for cybersecurity education and technology development. Maryland leads the nation in information technology jobs and more than half of the nation’s internet traffic passes through the Washington, D.C. metropolitan area. As the University System of Maryland’s flagship campus, the University of Maryland, College Park, will help “connect the dots” in the region’s burgeoning federal and private cyber initiatives. The nearby location of the nation’s US Cyber Command gives us the opportunity to serve both the nation and the state.

This new specialization will be administered through the Office of Advanced Engineering Education (OAEE) making sure that the necessary student services are provided. As with all programs in OAEE, curriculum and academic oversight for the core and elective courses in the series will be through a faculty advisory committee that will collaborate with the OAEE Executive Director, making sure that both commitment to support this new specialization and academic excellence are in place. Evaluation and assessment of this option will be performed by the Department of Electrical and Computer Engineering, the faculty advisory committee and OAEE. The new specialization will comply with all UMCP policies and requirements for graduate education.

Students expected to participate in the program are engineers, computer scientists, and technical professionals interested in information security. The curriculum presented represents the beginning of what will be an evolving program that will continue to offer the latest developments in this rapidly changing and critically important field of study.
CORE COURSES (4 courses with the approval of the academic advisor)

**ENPM 808 Programming in C for Cybersecurity Applications (3 credits)**
This course teaches the fundamentals of programming in C and the skills including data structures and algorithms that students need for solving typical telecommunication engineering problems in cyber security area by writing programs in C. Control flow statement, arrays, pointers and dynamic memory allocation will be reviewed. Developing data structures such as queues, stacks and linked lists and network applications including sockets, packet sniffing in C will be discussed. The course concludes with an introduction to data encryption and basic programming techniques for addressing data security related issues. In addition to the weekly reading and programming assignments, students are required to complete a final project and make a presentation. Students taking this course do not need to have any previous programming experience.

**ENPM 808 Operating Systems (3 credits)** Prerequisite: ENPM 808 Programming in C for Cybersecurity Applications, CMSC 106 Introduction to C Programming, or permission of the instructor. Operating systems are the basic building block on which programmers build applications and on which security-minded professionals rely, whether they are monitoring activity on a computer, testing applications for security, or determining how malicious code affected their network. This course covers advanced topics in operating systems including process management and communication, remote procedure calls, memory management (including shared memory and virtual memory), checkpointing and recovery, file system, I/O subsystem and device management, distributed file systems and security. The course consists of reading and discussing research papers and includes a course project. Please note: This course assumes knowledge of C programming and a previous operating systems class or knowledge in various issues such as process management, process synchronization, the critical section problem, CPU scheduling, memory management, secondary storage management.

**ENPM 808 Networks and Protocols (3 credits)** This course provides a deep understanding of TCP/IP protocol suite and routing in the internet. The course topics are: overview of TCP/IP, basics of IP protocol, basics of TCP protocol, Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), Internet Protocol Security (IPsec), Internet Control Message Protocol (ICMP), Simple Mail Transfer Protocol (SMTP), Domain Name Service (DNS), IPv6, Concepts of routing (Bellman-Ford and Dijkstra algorithms), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhance Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP).

**ENPM 808 Network Security (3 credits)** This course provides the necessary foundation on network security and an in-depth review of commonly-used security mechanisms and techniques. Specific topics that will be covered include network attacks, firewalls, intrusion detection and response, security protocols (in particular, IPsec, SSL, and Kerberos), Denial of Service (DoS) attacks/ detection/prevention, viruses and worms, DNS, email & Voice Over IP (VoIP) security, wireless infrastructure security, web security, and privacy.

**ENPM 808 Information Assurance (3 credits)** The first half of lectures provides an overview of cybersecurity. One third of these lectures focuses on the fundamentals of
cybersecurity like authentication, access control, and security models. The second third focuses on the practice of cybersecurity using Unix and Windows NT as case studies. The last third is dedicated to security in distributed systems including network security, and World Wide Web security. The second half of the lectures focuses on the information assurance process. First, information assets are enumerated and classified. Second, the main vulnerabilities and threats are identified. Third, a risk assessment is conducted by considering the probability and impact of the undesired events. Finally, a risk management plan is developed that includes countermeasures involving mitigating, eliminating, accepting, or transferring the risks, and considers prevention, detection, and response.

**ENPM 808 Network Intrusion & Detection (3 credits)** This course begins with the thorough review of protocol analysis where students will gain a detailed understanding of each layer of a protocol stack. Coverage will include Layer 2 (Ethernet, FDDI, Frame Relay, serial, etc.), Layer 3 (IPv4, IPv6), Layer 4 (TCP, UDP), and Layers 5-7 (SMB, Telnet, HTTP, DNP3, ModBus, NetBIOS, etc.). Students will learn how to identify protocol anomalies (e.g., SYN floods, half-on SYN, fragmentation attacks) at their most basic and more advanced (e.g., ARP cache poisoning). Examples will be used to build a foundation in understanding how to craft and detect network-based attacks using both signature and behavioral methods. Students will master the fundamentals of an intrusion detection and intrusion prevention system. They will study how netflow and other data can be correlated using security information and event management (SIEM) systems to better detect attacks and to resist intrusions. Students will learn through the use of basic tools such as a network sniffer (e.g., Wireshark) as well as more advanced intrusion detection and data leak prevention tools. Students will be required to generate custom rules to detect suspicious traffic using both Wireshark and SNORT. The course will also discuss the fundamentals of network incident response, including techniques for live forensics and best practices for preservation of evidence. At the end of the course, students will divide into red and blue teams where red teams will attempt to create malicious network packets that will avoid detection and the blue team will seek to detect suspicious events using a packet sniffer and an intrusion detection system.

**ENPM 808 Secure Software Testing & Construction (3 credits)** As software gets more complex, there is even more potential for vulnerabilities to remain in the production version. While traditional and emerging software testing methods are very good at detecting a large majority of “bugs” in the software, modifications to the methods are necessary to ensure vulnerabilities related to security are discovered and mitigated prior to release. In industry, there is also a cost-benefit analysis that determines the limits to pre-release testing, further enforcing the need to uniquely identify security vulnerabilities, potentially prioritizing their correction over other vulnerabilities. This course will cover methods of building security in from the beginning of development and testing the resulting software to ensure security vulnerabilities are detected. The course will use a mixture of textbook principles and research papers to cover the concepts. Students will also complete a course project.

**ENPM 808 Security Tools for Information Security (3 credits)** Prerequisites: familiarity with Linux and Windows operating systems, as well as TCP/IP and basic networking concepts. Students will perform host- and network-based security tasks relating to
security, investigation, compliance verification and auditing using a wide selection of commonly used tools on both Windows and Linux platforms, with emphasis on open source tools.

**ENPM 808 Digital Forensics and Incidence Response** (3 credits) Prerequisites: intermediate Windows and Linux skills, familiarity with file system concepts. Students will implement a robust incident response methodology, including proper forensic handling of evidence, and cover legal aspects of national and international law regarding forensics. The bulk of the course covers evidence acquisition, preservation, analysis and reporting on multiple platforms.

**ENEE 808 Reverse Software Engineering** (3 credits) This course provides in-depth, hands-on training for reverse engineering tools, including the IDA Pro disassembler, the Wireshark network protocol analyzer, debuggers, and binary tools. Students will become familiar with the x86 instruction set through both assembly programming and disassembly. Class exercises include revealing back doors and exploiting buffer overflows. Each student will develop a network-based application and in turn reverse engineer and exploit one of their peer's completed applications.