December 19, 2014

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 an Online Version of the Cybersecurity Option for the Post-Baccalaureate Certificate in Engineering (PCC log no. 14002) and the Master of Engineering (PCC log no. 14003)

At its meeting on October 3, 2014, the Senate Committee on Programs, Curricula, and Courses approved your proposals to establish an online version of the Cybersecurity option for the Post-Baccalaureate Certificate in Engineering and the Master of Engineering. Copies of the approved proposals are attached.

These online versions are effective Spring 2015. Please ensure that these new versions are fully described in the Graduate Catalog and in all relevant descriptive materials, and that all advisors are informed.

MDC/

Enclosure

cc: Gregory Miller, Chair, Senate PCC Committee
    Barbara Gill, Office of Student Financial Aid
    Reka Montfort, University Senate
    Erin Taylor, Division of Information Technology
    Pam Phillips, Institutional Research, Planning & Assessment
    Anne Turkos, University Archives
    Linda Yokoi, Office of the Registrar
    Alex Chen, Graduate School
    William Fournery, A. James Clark School of Engineering
    George Syrmos, Office of Advanced Engineering Education
College/School: ENGR
Please also add College/School Unit Code-First 8 digits: 01320101
Unit Codes can be found at: https://hypprod.umd.edu/Html_Reports/units.htm

Department/Program: OAEE
Please also add Department/Program Unit Code-Last 7 digits: 1322302

Type of Action (choose one):

- Curriculum change (including informal specializations)
- Renaming of program or formal Area of Concentration
- Addition/deletion of formal Area of Concentration
- Suspend/delete program

Italics indicate that the proposed program action must be presented to the full University Senate for consideration.

Summary of Proposed Action:

Creation of an online academic option in Cybersecurity (Z0##) to the existing Post-Baccalaureate Certificate in Engineering program through the Office of Advanced Engineering Education.

APPROVAL SIGNATURES - Please print name, sign, and date. Use additional lines for multi-unit programs.

1. Department Committee Chair
   [Signature]  Jonathan Katz, Director, MC2

2. Department Chair
   [Signature]  George Syrmos, Executive Director, OAEE

3. College/School PCC Chair
   [Signature]  Jenna Bull 4/15/14

4. Dean
   [Signature]  W.J. Foy, nep 4/15/14

5. Dean of the Graduate School (if required)
   [Signature]  W.J. Foy 12/2/14

6. Chair, Senate PCC
   [Signature]  10/5/14

7. University Senate Chair (if required)

8. Senior Vice President and Provost
THE UNIVERSITY OF MARYLAND, COLLEGE PARK
PROGRAM/CURRICULUM/UNIT PROPOSAL

- Please email the rest of the proposal as an MSWord attachment to pcc-submissions@umd.edu.

- Please submit the signed form to the Office of the Associate Provost for Academic Planning and Programs, 1119 Main Administration Building, Campus.

College/School: ENGR
Please also add College/School Unit Code-First 8 digits: 01320101
Unit Codes can be found at: https://hvpprod.umd.edu/Html_Reports/units.htm

Department/Program: OAEE
Please also add Department/Program Unit Code-Last 7 digits: 1322302

Type of Action (choose one):

☐ Curriculum change (including informal specializations)  ☐ New academic degree/award program
☐ Renaming of program or formal Area of Concentration  ☐ New Professional Studies award iteration
☐ Addition/deletion of formal Area of Concentration  ☐ New Minor
☐ Suspend/delete program  ☑ Other

Italics indicate that the proposed program action must be presented to the full University Senate for consideration.

Summary of Proposed Action:

Creation of an online academic option in Cybersecurity (MECY) to the existing Professional Master of Engineering program through the Office of Advanced Engineering Education.

APPROVAL SIGNATURES - Please print name, sign, and date. Use additional lines for multi-unit programs.

1. Department Committee Chair
   Jonathan Katz, Director, MC2

2. Department Chair
   George Symos, Executive Director, OAEE

3. College/School PCC Chair
   Jenna Bucci, 4/15/14

4. Dean
   WL Founagy, 4/16/14

5. Dean of the Graduate School (if required)

6. Chair, Senate PCC
   10/3/14

7. University Senate Chair (if required)

8. Senior Vice President and Provost
Proposal for approving an online academic option in Cybersecurity to the existing Professional Master of Engineering and Graduate Certificate in Engineering programs through the Office of Advanced Engineering Education

Revised 09/26/14 to address comments from Academic Planning and Programs.

Established in 1994, the Office of Advanced Engineering Education (OAEE) in the Clark School of Engineering is responsible for lifelong learning programs designed for working engineers and technical professionals. OAEE offers both credit and non-credit programs, but our primary offering is the Master of Engineering degree and the Post-Baccalaureate Certificate. We refer to these programs as the Professional Master of Engineering (ENPM) program and the Graduate Certificate in Engineering (GCEN) program. The Master of Engineering degree is awarded with completion of ten courses (30 credits) and no thesis/research project, scholarly paper, or comprehensive exam are required. Each academic option has its own set of course requirements. The GCEN was developed to serve as a more highly focused area of study. It requires the completion of four specific courses (12 credits) by academic option. There are currently over 600 students in our programs with over 2000 graduates. Students take classes on campus, at regional education centers throughout Maryland, and seven programs are offered online. Enrollments have been averaging 50% on campus and 50% distance/online for the past few years.

OAEE currently offers nineteen academic options under these two programs (http://advancedengineering.umd.edu/degrees-certificates). Academic options were originally versions of the Master of Science programs in each academic department (i.e. Aerospace, Mechanical, Electrical, etc.). However, as the need grew for more interdisciplinary programs, we began working with research institutes and centers in the Clark School to develop and offer programs to meet the needs of the engineering/technology community. We have developed niche academic options in Sustainable Energy Engineering, Project Management, Robotics, Energetics, Software Engineering, and Cybersecurity. In 2003, we began offering these niche programs online to give national and worldwide access to the outstanding programs available at Maryland.

The graduate program in Cybersecurity (PMCY/Z073) began in Fall 2012. It was initiated at the request of the Darryll Pines, Dean of the Clark School of Engineering and the previous Chairs of Computer Science (Larry Davis) and Electrical & Computer Engineering (Pat O'Shea). OAEE worked with faculty and research associates in Engineering and Computer Science to develop the curriculum and maintains a curriculum review committee composed of faculty, research associates, and industry and government experts. The course curriculum was designed to be offered on campus and at regional education centers throughout Maryland via video-teleconferencing and to complete an initial offering within two years. The program would then be offered on campus, at regional education centers in Maryland and online to increase the student population beyond Maryland and the DC metro region. All courses have been taught in the Seigel Learning Center and as of the Spring 2014 semester all but one of the courses in the curriculum have been offered and are available for online delivery. The final course is being offered on campus and at regional education centers in Maryland this summer. The goal is to continue to offer these courses on campus, via VTC at the regional education centers, and now completely online.

The critical demand in Cybersecurity locally and the lack of an equivalent highly technical option available from other top engineering schools nationwide necessitate
offering the PMCY/Z073 online nationally and internationally. There are currently 36 students in the Cybersecurity program, a regional offering. We expect that due to high demand for employment, the strength and reputation of the Maryland Cybersecurity Center, and our highly effective distance learning experience we will provide an outstanding educational option for engineers and technical professionals. In fact, OAEE was recently ranked by US News & World Report as one of the Best Engineering Graduate Programs. Estimating future enrollment is usually a best guess, however based on the trends we’ve seen in enrollment increases from our other online program, we estimate a 66% increase in the number of current students (60 students) in the next two years. OAEE has extensive marketing/recruitment experience and will focus on the Cybersecurity programs technical strengths and outstanding delivery methods.

In its on-campus form, a student is awarded the Master of Engineering degree - Cybersecurity after having completed ten three-credit courses (six core courses, and four approved technical electives). Cybersecurity courses have been webcast since the Fall 2012 semester via our Distance Education Technology and Services (DETS) Office in the Clark School of Engineering. A student is awarded the GCEN in Cybersecurity (Z073) degree with the completion of four three-credit courses from the core course curriculum. We propose that an online option be added to the existing Professional Master of Engineering program in Cybersecurity (MECY) leading to a Master of Engineering degree and an online option to the existing Graduate Certificate in Engineering program in Cybersecurity (Z0##) leading to a GCEN degree. We will start these fully online options in the Spring 2015 semester by offering a ten course sequence to allow students to complete their degree in two years. The ten courses offer a highly technical course of study that is not found at other institutions in Maryland and give the student the depth and expertise for a successful career in the field of Cybersecurity. Requests by students to substitute courses from other online programs (e.g. Reliability Engineering, Project Management) offered through the Clark School of Engineering will be at the discretion of the Cybersecurity program’s academic advisor, appointment by the Director of the Maryland Cybersecurity Center (MC2).

The faculty who teach for the campus programs will also teach for the online programs. The standards of good practice observed for the on-campus programs will equally apply to the online versions. In particular, faculty support and resources for learning will be provided by the DETS office to our online students.

OAEE provides administrative oversight to all Master of Engineering and Graduate Certificate in Engineering academic options, including student services, faculty support, admissions, and academic outreach. In addition, OAEE works with faculty to develop new courses and programs that meet the needs of the engineering/technology communities. OAEE researches industry needs, meets with private and public sector leaders, attends various professional society and technology conferences to learn about possible program development areas. For each academic option there is an identified academic advisor/content matter expert who advises OAEE and our students on curriculum matters. For the traditional academic options (i.e. aerospace, bioengineering, mechanical, etc.) and advisor is assigned by that department chair. For our interdisciplinary programs, the primary department/research center/institute assigns an academic advisor. These interdisciplinary areas also have curriculum committees that review student and faculty performance, course content, and curriculum development. Like all of the online academic programs offered through OAEE these two new online Cybersecurity academic options will be administered through OAEE making sure that the necessary student services are provided. All content will be overseen by the Maryland
Cybersecurity Center making sure that both commitment to support the programs and academic excellence are in place. Evaluation and assessment of the programs will be performed by both MC2 and OAEE, and their delivery through the DETS Office will ensure a state-of-the-art accessibility of the associated courses.

We recognize that technical experts working in Cybersecurity have diverse academic and professional backgrounds. Therefore, our admissions requirements allow for diversity but also must ensure that qualified students are prepared to succeed in this highly technical academic program. We offer three levels of admission depending upon the academic background, academic performance, and professional experience of the applicant. Please note that three letters of recommendation (preferably professional letters) are required for admission.

- **Prerequisite requirement:** ENEE 150 or equivalent.
- **Further admissions requirements.**
- **Full Admission:** applicants must have a bachelor's degree in Engineering, Computer Science, Applied Mathematics, or Physics, from an accredited institution, with a GPA of 3.0 or better.
- **Provisional Admission:** applicants who have a degree in a closely related field of study (i.e. Information Technology, Information Assurance, Computer Information Systems), and a GPA of 3.0 or better must also possess at least one (1) of the following certifications: CompTIA Security+, GIAC GSEC, or Certified Ethical Hacker certification. Applicants admitted with Provisional Admission will need to complete two core courses with at least a B or better in each course.
- **Advanced Special Student Admission:** applicants with a bachelor’s degree in other fields of study with a minimum 3.0 GPA, one of the above mentioned certifications, and 2+ years work experience in Information Technology or other closely related field. To qualify for this admission, applicants must submit a detailed description of their technical work experience as a personal statement attached to the Applicant Supplement Form (ASF). Applicants admitted as Advanced Special Students will need to complete two core courses with at least a B or better in each course in order to be considered for Provisional Admission later on.

The following schedule of classes lists cybersecurity core and elective courses as well as approved technical electives for the online programs. The courses will be offered in a timeline to allow a student to complete the ten courses in two years.

**ENPM691 Secure Programming in C (3)**
This course teaches the fundamentals of secure programming in C. An in depth discussion on various security vulnerabilities (e.g., buffer overflows) in C applications will be taught with hands-on demo of concepts during the class. Students will learn how a C program runs “under-the-hood”. The course will teach nitty-gritty of C programs by analyzing at the assembly level. The course discusses best practices (e.g., coding standards) and design principles for secure programming so that security can be built-in during design time. In addition to assignments, students are required to present papers related to this course.

*Instructor: Dr. Dharma Ganesan, Ph.D. Computer Science Vrije Universiteit Research Associate, Fraunhofer Center for Experimental Software Engineering, University of Maryland*
ENPM693 Network Security (3)
Prerequisite: An operating systems and/or network protocol course or equivalent.
Formerly: ENPM808N.
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.
Instructor: Dr. Farshad Bahari, Ph.D., Electrical & Computer Engineering, University of Maryland
Research Associate, University of Maryland, Electrical & Computer Engineering

ENPM808A Networks and Protocols (3)
This course provides a deep understanding of TCP/IP protocol suit 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).
Instructor: Dr. Sohraab Soltani, Ph.D., Computer Science, Michigan State University
Senior Research Scientists, Intelligent Automation, Inc.

ENPM808B Secure Operating Systems (3)
Prerequisite: ENPM691 Secure Programming in C, 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.
Instructor: Dr. Atif Memon, Ph.D., Computer Science, University of Pittsburgh
Associate Professor, Computer Science, University of Maryland

ENPM808D Security Tools for Information Security (3)
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.
Instructor: Mr. Robert Maxwell, B.S. Mathematics, Catholic University
Manager, Security Operations, Managing Director, Digital Forensics Lab, University of Maryland
ENPM808E Information Assurance (3)
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.

Instructor & Academic Advisor: Dr. Michel Cukier, Ph.D. Computer Science, National Polytechnic Inst. of Toulouse
Associate Professor, Reliability Engineering, Associate Director, Maryland Cybersecurity Center

ENPM808F Reverse Software Engineering (3)
Prerequisite: ENPM691 Secure Programming in C, CMSC 106 Introduction to C Programming, or permission of the instructor.
This course provides in-depth understanding of reverse software engineering concepts and hands-on training with reverse engineering tools, including disassembler, decompiler, and code analyzer. Students will become familiar with both low-level software and the x86 instruction set through binary reversing sessions. This course also provides insights into many subjects such as system security, source code analysis, software design, and program understanding that will be beneficial in a variety of fields.

Instructor: Dr. Charles Song, Ph.D., Computer Science, University of Maryland
Senior Development Leader, Fraunhofer Center for Experimental Software Engineering, University of Maryland

ENPM808K Secure Software Testing & Construction (3)
Prerequisite: ENPM691 Secure Programming in C, CMSC 106 Introduction to C Programming, or permission of the instructor.
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.

Instructor: Dr. Atif Memon, Ph.D., Computer Science, University of Pittsburgh
Associate Professor, Computer Science, University of Maryland
ENPM808O Intrusion Detection: From Theory to Practice (3)
Intrusion detection systems (IDSs) constitute an essential component of any network security solution package. Underlying IDSs is a great deal of fascinating mathematics mostly taken from various fields such as Probability Theory, Statistic, and Detection Theory. A good understanding of this mathematical background will enable Security Officers to better appreciate the benefits and limitations of IDSs and prepare them to become better practitioners. The goal of this course is two-fold. First, it will provide to students a hands-on exposure to the mathematical principles and techniques used in intrusion detection. Second, students will experiment with the real-life process of going from a theoretical intrusion detection solution to its implementation. The course will proceed by introducing mathematical concepts on an "as needed" basis, motivated by their direct applications to intrusion detection.
Instructor: Dr. Assane Gueye, Ph.D., Electrical Engineering/Computer Science, University of California, Berkeley
Research Associate, NIST Information Technology Laboratory/Electrical & Computer Engineering, University of Maryland

ENPM808P Digital Forensics and Incidence Response (3)
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.
Instructor: Mr. Robert Maxwell, B.S. Mathematics, Catholic University
Manager, Security Operations, Managing Director, Digital Forensics Lab, University of Maryland
## OAEE Cybersecurity Proposed Course Schedule

### Iteration 1 - Courses offered on-campus and via DETS

<table>
<thead>
<tr>
<th>SEMESTER</th>
<th>CYBERSECURITY CORE COURSES</th>
<th>CYBERSECURITY ELECTIVES</th>
<th>OTHER ELECTIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fall 2012</td>
<td>ENPM 691 Secure Programming in C - D. Ganesan, Fraunhofer Inst.</td>
<td></td>
<td>ENPM 611 Software Engineering</td>
</tr>
<tr>
<td></td>
<td>ENPM 693 Network Security - F. Bahari, UMCP</td>
<td></td>
<td>ENPM 613 Software Design &amp; Implementation</td>
</tr>
<tr>
<td></td>
<td>ENPM 808A Networks and Protocols - S. Soltani</td>
<td></td>
<td>ENPM 641 Systems Concepts, Issues and Processes</td>
</tr>
<tr>
<td></td>
<td>ENPM 808E Information Assurance - M. Cukier, UMCP</td>
<td></td>
<td>ENPM 614 Software Testing &amp; Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ENPM 642 Systems Req., Design &amp; Trade-Off Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ENPM 808 Advanced TCP/IP Networking</td>
</tr>
<tr>
<td></td>
<td>ENPM 693 Network Security - F. Bahari, UMCP</td>
<td></td>
<td>ENPM 613 Software Design &amp; Implementation</td>
</tr>
<tr>
<td></td>
<td>ENPM 808A Networks and Protocols - S. Soltani</td>
<td></td>
<td>ENPM 641 Systems Concepts, Issues and Processes</td>
</tr>
<tr>
<td></td>
<td>ENPM 808E Information Assurance - M. Cukier, UMCP</td>
<td></td>
<td>ENPM 614 Software Testing &amp; Maintenance</td>
</tr>
<tr>
<td></td>
<td>ENPM 808B Secure Operating Systems - A. Memon, UMCP</td>
<td></td>
<td>ENPM 642 Systems Req., Design &amp; Trade-Off Analysis</td>
</tr>
</tbody>
</table>

Courses in red require ENPM 691 Secure Programming in C as a prerequisite.

No instructor assigned.
<table>
<thead>
<tr>
<th>SEMESTER</th>
<th>CYBERSECURITY CORE COURSES</th>
<th>CYBERSECURITY ELECTIVES</th>
<th>OTHER ELECTIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fall 2014</td>
<td>ENPM 691 Secure Programming in C - D. Ganesan, Fraunhoffer Inst.</td>
<td></td>
<td>ENPM 611 Software Engineering</td>
</tr>
<tr>
<td></td>
<td>ENPM 693 Network Security - F. Bahari, UMCP</td>
<td></td>
<td>ENPM 613 Software Design &amp; Implementation</td>
</tr>
<tr>
<td></td>
<td>ENPM 808A Networks and Protocols - S. Soltani</td>
<td></td>
<td>ENPM 641 Systems Concepts, Issues and Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENPM 808F Reverse Software Engineering - C. Song, Fraunhoffer Inst.</td>
<td>ENPM 808 TCP/IP Networking</td>
</tr>
<tr>
<td>Spring 2015</td>
<td>ENPM 691 Secure Programming in C - D. Ganesan, Fraunhoffer Inst.</td>
<td></td>
<td>ENPM 612 System &amp; Software Requirements</td>
</tr>
<tr>
<td></td>
<td>ENPM 808E Information Assurance - M. Cukier, UMCP</td>
<td></td>
<td>ENPM 614 Software Testing &amp; Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENPM 808P Digital Forensics and Incidence Response - R. Maxwell, UMCP</td>
<td>ENPM 642 Systems Req., Design &amp; Trade-Off Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ENPM 808 Advanced TCP/IP Networking</td>
</tr>
<tr>
<td></td>
<td>ENPM 693 Network Security - F. Bahari, UMCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ENPM 808A Networks and Protocols - S. Soltani</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fall 2015</td>
<td>ENPM 691 Secure Programming in C - D. Ganesan, Fraunhoffer Inst.</td>
<td></td>
<td>ENPM 611 Software Engineering</td>
</tr>
<tr>
<td></td>
<td>ENPM 693 Network Security - F. Bahari, UMCP</td>
<td></td>
<td>ENPM 613 Software Design &amp; Implementation</td>
</tr>
<tr>
<td></td>
<td>ENPM 808A Networks and Protocols - S. Soltani</td>
<td></td>
<td>ENPM 641 Systems Concepts, Issues and Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENPM 808K Secure Software Testing &amp; Construction - A. Memon, UMCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ENPM 808B Secure Operating Systems - A. Memon, UMCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ENPM 808E Information Assurance - M. Cukier, UMCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summer 2016</td>
<td>ENPM 808 Intrusion Detection: From Theory to Practice - A. Gueye</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENPM 808F Reverse Software Engineering - C. Song, Fraunhoffer Inst.</td>
<td></td>
</tr>
</tbody>
</table>

Courses in red require ENPM 691 Secure Programming in C as a prerequisite.

no instructor assigned
ASSessment methods, criteria & results  Graduate Certificate in Engineering (GCEN)

For Time Period: Academic Year

Program Contact: Dr. George Syrmos  Phone: 301-405-3633  E-mail: syrmos@umd.edu

Date submitted to Academic Unit Head: ____________________________

<table>
<thead>
<tr>
<th>Student Learning Outcomes for assessments that will occur during the academic year</th>
<th>Assessment Methods &amp; Criteria</th>
<th>Assessment Results</th>
<th>Impact of Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Demonstrate knowledge of advanced principles in engineering.</td>
<td><strong>Criterion:</strong> All ENPM courses offered during any given semester. The final exam in all these courses will include a question specifically tailored to demonstrate understanding of a fundamental principle in engineering. <strong>Measure:</strong> At least 70% of the students in every ENPM course offered during any given semester would be expected to successfully answer this question posed on the final exam.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Demonstrate knowledge of advanced principles in engineering.  

| 2. Demonstrate knowledge of advanced principles in engineering. | **Criterion:** 90% of the Graduate Certificate in Engineering students should have a GPA equal or greater than 3.0  

**Measure:** GPA | | |

3. Demonstrate continued retention of students and progress towards degree completion.  

<p>| 3. Demonstrate continued retention of students and progress towards degree completion. | <strong>Criterion:</strong> 80% enrollment by existing students each semester. | | |</p>
<table>
<thead>
<tr>
<th></th>
<th>Measure: Registrar's Enrollment Records.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Demonstrate completion of degree program.</td>
</tr>
<tr>
<td></td>
<td><strong>Criterion</strong>: 80% graduation rate of students within the five year limit for Graduate Certificate in Engineering students.</td>
</tr>
<tr>
<td></td>
<td><strong>Measure</strong>: Registrar's Graduation Records.</td>
</tr>
<tr>
<td>5.</td>
<td>Point-of-graduation survey. The survey is web based. Graduating students, prior to the end of the semester, are sent the web site in which to fill in the appropriate information and submit the survey electronically. The survey seeks to ascertain a student's experiences in the GCEN Program regarding the quality of courses, the general program, faculty, and staff. The survey also collects information on employment (position, salary, etc.) at graduation.</td>
</tr>
<tr>
<td></td>
<td><strong>Criterion</strong>: 50% response rate by graduating students.</td>
</tr>
<tr>
<td></td>
<td><strong>Measure</strong>: Graduation Survey.</td>
</tr>
</tbody>
</table>
### Student Learning Outcomes for assessments that will occur during the academic year

<table>
<thead>
<tr>
<th>Outcome</th>
<th>Assessment Methods &amp; Criteria</th>
<th>Assessment Results</th>
<th>Impact of Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Demonstrate knowledge of advanced principles in engineering.</strong></td>
<td><strong>Criterion:</strong> All ENPM courses offered during any given semester. The final exam in all these courses will include a question specifically tailored to demonstrate understanding of a fundamental principle in engineering. <strong>Measure:</strong> At least 70% of the students in every ENPM course offered during any given semester would be expected to successfully answer this question posed on the final exam.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><strong>Demonstrate knowledge of advanced principles in engineering.</strong></td>
<td><strong>Criterion:</strong> 90% of the Master of Engineering students should have a GPA equal or greater than 3.0 <strong>Measure:</strong> GPA</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><strong>Demonstrate continued retention of students and progress towards degree completion.</strong></td>
<td><strong>Criterion:</strong> 80% enrollment by existing students each semester. <strong>Measure:</strong> Registrar’s Enrollment Records.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **4. Demonstrate completion of degree program.** | **Criterion:** 80% graduation rate of students within the five year limit for Master of Engineering students.  
**Measure:** Registrar's Graduation Records. |
| **5. Point-of-graduation survey.** The survey is web based. Graduating students, prior to the end of the semester, are sent the website in which to fill in the appropriate information and submit the survey electronically. The survey seeks to ascertain a student's experiences in the ENPM Program regarding the quality of courses, the general program, faculty, and staff. The survey also collects information on employment (position, salary, etc.) at graduation. | **Criterion:** 50% response rate by graduating students.  
**Measure:** Graduation Survey. |
Proctoring Agreement

STUDENT

You have registered for an online course that requires a proctor for its exams. A proctored exam is administered by an individual who supervises the student while he/she is taking the exam. The proctor’s function is to ensure the integrity and security of the exam. Information regarding the University of Maryland Honor Pledge can be found at http://shc.umd.edu/SHC/HonorPledgeInformation.aspx.

Choosing a Proctor

The proctor may be any disinterested third party. A member of the HR/Training staff within your company would qualify to serve in this position. Students have used hotel concierges, librarians, religious leaders (i.e. pastors), and military education officers when an HR/Training staff member is unavailable. The proctor cannot be any person with a vested interest in your success, such as another student in the program, a friend/colleague, family member, supervisor, or subordinate.

Scheduling Exams

Professors (not the OAEE) determine the date range for exams. You must tell OAEE the date and time of your scheduled exam at least one week in advance. You are not required to take the exam in the evening on the day it is scheduled; you can take it at any time that day, unless specified by your professor.

If you are unable to take the exam during this range, you must discuss an alternative date with your professor. If an alternative date is approved, you must provide the professor’s written permission to the OAEE to ensure that the materials are sent to your proctor on time. If you miss your scheduled exam time, your professor may give you a zero on the exam.

The OAEE must receive this completed Agreement from you within two weeks of the semester’s start date. Please note: If you do not return the Agreement to the OAEE by this deadline, you will be at risk of jeopardizing your course grade for failure to make proctor arrangements. This Agreement must be completed and re-submitted each semester in which you register for an online course that requires a proctor. The OAEE reserves the right to deny any proctor or assign proctors to students as necessary.

Name: ___________________________ UID: ___________________________
Course(s): ___________________________ Email Address: ___________________________
(ex. ENPM 600) ___________________________ Phone Number: ___________________________
Semester: Spring 2014

Select all that apply. It is permissible for you to have more than one proctor, as long as the OAEE receives a separate Proctoring Agreement for each person and you indicate which proctor will be used for each of your exams. If you have a last-minute proctor conflict, you must find a substitute from one of the options below and submit a new Proctoring Agreement to the OAEE (preferably at least one week before your scheduled exam). You are responsible for contacting and confirming each proctor.

☐ Off-Campus Proctor (completion of page 2 required)
☐ On-Campus Proctor
☐ In-class: You must contact the professor for permission to take the exam with the on-campus students. If the professor approves, inform the OAEE so we can ensure that a seat is reserved for you.
☐ The OAEE proctors exams during regular business hours (8:30 AM – 5:00 PM, Monday-Friday).
☐ The Distance Education Technology & Services (DETS) office proctors exams after-hours (5:00 PM – 9:00 PM, Monday-Thursday, in 2125 J.M. Patterson).
☐ The Engineering Library in the Math building can proctor exams on Friday evenings and weekends. To request proctoring services here, please contact Pat Delauberfels at 301-405-9143 or marta@umd.edu.

By signing below, I certify that I have read and understood the above statements, will abide by the OAEE and University proctoring and academic policies, and am responsible if the proctor does not adhere to the regulations as stated herein.

Signature ___________________________________________ Date __________

Return this form via: mail Office of Advanced Engineering Education
email oaeestudent@umd.edu
Attn: Proctoring fax 301-405-3305
The University of Maryland College Park
2105 J.M. Patterson Building
College Park, MD 20742
Proctoring Agreement

PROCTOR

As the student's approved proctor, your responsibility is to administer the student's exam(s) for the duration of the semester. You will receive the exam instructions, Honor Pledge, exam, and any supplementary exam materials by email from the OAAE one business day before the exam is to be administered. (If the University is closed due to unforeseen circumstances [i.e. weather-related], the OAAE will send you the exam when the University reopens. All closures will be posted on the University of Maryland Police Department's website, www.umdnews.umd.edu.) Exams cannot be administered in a home office.

Print all pages and provide them, along with scrap paper, to the student at the beginning of the testing period. Give the student a 15-minute warning before the exam time ends and then stop the student when the time is up. Then, scan and email or fax the exam and any supplementary notes/pages to the OAAE. Once you have the OAAE's written confirmation that the electronic materials were successfully received, then send all pages by regular mail to the OAAE (including the address line “Attn: Proctoring”).

Name: ____________________________
Title: ____________________________
Company: ________________________
Email Address: ____________________
Phone Number: ____________________
Fax Number: ______________________
Business Address: __________________
Relationship to Student: _______________

Please initial the following statements:

_____ I will inform the student if he/she is required to pay any fees for testing at my facility.

_____ I will inform the student if he/she is required to provide a stamped, addressed envelope for me to return the original exam materials back to the OAAE.

_____ I will ensure that the student adheres to all exam instructions (regarding duration of time to take the exam and usage of outside materials and electronics).

_____ I will not permit the student to leave the proctoring facility with any original or copied exam materials.

_____ I will immediately return the exam materials to the OAAE, either by fax or as an email attachment, upon the student’s completion of the exam.

_____ If I choose to email the exam to the OAAE, I will not include the student as a recipient.

_____ I will NOT mail out the hard copy of the exam until I have received written confirmation from the OAAE that the electronic file was successfully received.

_____ I will delete the electronic file of the exam once it has been administered.

By signing below, I certify that I have read and understood the above statements and that I will abide by the OAAE and University proctoring and academic policies.

Signature ____________________________ Date ________________

Return this form via mail Office of Advanced Engineering Education email oaae.student@umd.edu
Attn. Proctoring fax 301-405-3305
The University of Maryland College Park
2105 J.M. Patterson Building
College Park, MD 20742