

UNIVERSITY OF DELAWARE

**MASTER OF SCIENCE IN
CYBERSECURITY**

ACADEMIC PROGRAM APPLICATION

JANUARY, 2015

Table of Contents

PART I	3
UNIVERSITY FACULTY SENATE FORM	3
Master of Science degree in Cybersecurity	4
Routing and Authorization	6
GRADUATE CATALOG LISTING	7
Master of Science in Cybersecurity	8
A. Program Overview	8
B. Requirements For Admission	8
C. Degree Requirements	9
D. Progress Toward the Degree	11
E. Financial Aid	11
PROPOSAL	12
I. Description	12
II. Rationale and Demand	14
A. Demand and Employment Factors	14
A.1. Enrollment projections	14
A.2. Survey of existing programs	14
B. Institutional Factors	16
B.1. Compatibility with university academic priorities	16
B.2. Significant impact on other university programs	16
B.3. Utilization of existing resources	16
B.4. Support of the College of Engineering	17
C. Access to Graduate and Professional Programs	18
III. Program Administration	18
A. Program Direction	18
B. Degree Requirements	18
C. Admissions Criteria	21
D. 4+1 Master's Program	21
APPENDIX A - Course Descriptions	22
APPENDIX B – Relevant Existing Courses	24
APPENDIX C – Letters of Approval and Support	29

PART I

UNIVERSITY FACULTY SENATE FORM

MASTER OF SCIENCE IN CYBERSECURITY

Academic Program Approval

This form is a routing document for the approval of new and revised academic programs. Proposing department should complete this form. For more information, call the Faculty Senate Office at 831-2921.

Submitted by: __ Charles Cotton _____ phone number ____ x 8517 _____

Department: __ Electrical and Computer Engineering _ email address _ ccotton@udel.edu __

Date: _____ 01/05/15 _____

Action: _____ Request for new Master of Science in Cybersecurity (MSCY) _____
(Example: add major/minor/concentration, delete major/minor/concentration, revise major/minor/concentration, academic unit name change, request for permanent status, policy change, etc.)

Effective term ____ 15F _____
(use format 04F, 05W)

Current degree ____ N/A _____
(Example: BA, BACH, BACJ, HBA, EDD, MA, MBA, etc.)

Proposed change leads to the degree of: _____ MS _____
(Example: BA, BACH, BACJ, HBA, EDD, MA, MBA, etc.)

Proposed name: _____ Master of Science in Cybersecurity (MSCY) _____
Proposed new name for revised or new major / minor / concentration / academic unit
(if applicable)

Revising or Deleting:

Undergraduate major / Concentration: _____
(Example: Applied Music – Instrumental degree BMAS)

Undergraduate minor: _____
(Example: African Studies, Business Administration, English, Leadership, etc.)

Graduate Program Policy statement change: _____
(Must attach your Graduate Program Policy Statement)

Graduate Program of Study: _____
(Example: Animal Science: MS Animal Science: PHD Economics: MA Economics: PHD)

Graduate minor / concentration: _____

Note: all graduate studies proposals must include an electronic copy of the Graduate Program Policy Document, highlighting the changes made to the original policy document.

List new courses required for the new or revised curriculum. How do they support the overall program objectives of the major/minor/concentrations)?

(Be aware that approval of the curriculum is dependent upon these courses successfully passing through the Course Challenge list. If there are no new courses enter "None")

CPEG697 Advanced Cybersecurity	CPEG674 SCADA Systems and Security
CPEG670 Web Applications Security	CPEG675 Embedded Computer Systems
CPEG671 Pen Test and Reverse Engineering	CPEG676 Secure Software Design
CPEG672 Applied Cryptography	CPEG869 Master's Thesis
CPEG673 Cloud Computing and Security	

These and other existing courses will form the basis of a Cybersecurity Master's to enable and recognize deeper study in the field.

Explain, when appropriate, how this new/revised curriculum supports the 10 goals of undergraduate education: <http://www.ugs.udel.edu/gened/>

N/A

Identify other units affected by the proposed changes:

(Attach permission from the affected units. If no other unit is affected, enter "None")

Department of Computer and Information Science, approval attached
Department of Accounting and Management Information Systems, approval attached
Department of Business Administration, approval attached
Department of Finance, approval attached

Describe the rationale for the proposed program change(s):

(Explain your reasons for creating, revising, or deleting the curriculum or program.)


Establishing high quality Cybersecurity educational programs is a top national priority as well as a regional imperative. This Master's will be structured to enable professionals to gain advanced training in this field. Unlike other programs that are solely focused on IT security, this program emphasizes the design of secure software and systems, security analytics, and secure business systems. It trains individuals that have a traditional background in engineering, computer science, information systems, or related fields to have strong security skills enabling them to develop *new* secure systems and/or software, to exploit analytics for security purposes, or to develop and manage secure business systems. Thus graduates of this program are skilled in the latest theories and practices required to address the most challenging cybersecurity issues facing the world today.

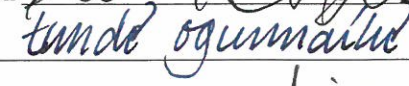
Program Requirements:

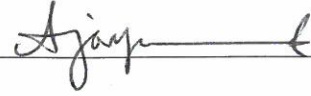
(Show the new or revised curriculum as it should appear in the Course Catalog. If this is a revision, be sure to indicate the changes being made to the current curriculum and **include a side-by-side comparison** of the credit distribution before and after the proposed change.)

(document follows)

ROUTING AND AUTHORIZATION: (Please do not remove supporting documentation.)

Department Chairperson  Date 1-20-15

Dean of College  Date 2/9/2015

Chairperson, College Curriculum Committee  Date 2/10/2015

Chairperson, Senate Com. on UG or GR Studies _____ Date _____

Chairperson, Senate Coordinating Com. _____ Date _____

Secretary, Faculty Senate _____ Date _____

Date of Senate Resolution _____ Date to be Effective _____

Registrar _____ Program Code _____ Date _____

Vice Provost for Academic Affairs & International Programs _____ Date _____

Provost _____ Date _____

Board of Trustee Notification _____ Date _____

Revised 02/09/2009 /khs

GRADUATE CATALOG LISTING

MASTER OF SCIENCE IN CYBERSECURITY

Department of Electrical and Computer Engineering
University of Delaware
info@ece.udel.edu (302) 831-2405

A. PROGRAM OVERVIEW

The 2008 CSIS report¹ “Securing Cyberspace for the 44th Presidency” highlighted the human capital challenge the United States faces in Cybersecurity: “The cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the federal government.” In the 2010 follow-on CSIS report², Evans and Reeder reinforced the need to “Expand cyber education” in their strategy to “Promote and fund the development of more rigorous curriculums in our schools”. Clearly, ensuring the security of the world’s and our own nation’s computers, systems and networks is a key national security challenge. Thus, establishing high-quality Cybersecurity educational programs is a top national priority as well as a regional imperative since Cybersecurity graduates are of critical importance to several large employer groups in this region.

The Master of Science in Cybersecurity program is administered through the Department of Electrical and Computer Engineering.

The cybersecurity master’s program is structured to enable professionals to gain advanced training in this field. Unlike other programs that are solely focused on IT security, this program emphasizes design of secure software and systems, security analytics, and secure business systems. It will train individuals that have a traditional background in engineering, computer science, information systems, or related fields to have strong security skills enabling them to develop *new* secure systems and/or software, to exploit analytics for security purposes, or to develop and manage secure business systems. Thus graduates of this program will be skilled in the latest theories and practices required to address the most challenging cybersecurity issues facing the world today.

B. REQUIREMENTS FOR ADMISSION

The requirements for admission to the Master of Science in Cybersecurity are the following:

1. Applicants must hold a bachelor’s degree from an accredited four-year college or university with a minimum grade point average of 3.0 on a 4.0 system.
2. Applicants must have undergraduate degrees in electrical engineering, computer engineering, computer science, mathematics, physics, or related disciplines. Applicants with degrees in other disciplines may be admitted with provisional status and may be required to complete

¹ J. A. Lewis, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, Washington, DC, 2008.

² K. Evans and F. Reeder, "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters," Center for Strategic and International Studies, Washington, DC, 2010.

prerequisite courses that are deemed necessary for appropriate preparation for courses in the program.

3. All applicants must take the Graduate Record Examination. The following GRE scores are competitive: Quantitative: 150, Verbal + Quantitative: 300. No GRE subject test is required.
4. International applicants must demonstrate a satisfactory level of proficiency in the English language if English is not their first language. The University requires an official TOEFL score of at least 550 on paper-based, 213 on computer-based, or 79 on Internet-based tests. TOEFL scores more than two years old cannot be considered official. Alternatively, IELTS can be accepted in the place of the TOEFL. The minimum IELTS score is 6.5 overall with no individual sub-score below 6.0.

Applications are accepted according to the standard University of Delaware deadlines. Admission to the graduate program is competitive. Those who meet the stated requirements are not guaranteed admission, and those who fail to meet all requirements are not necessarily precluded from admission if they offer other appropriate strengths.

C. DEGREE REQUIREMENTS

The Master's program requires 30 credit hours in either a thesis or non-thesis option. The non-thesis option requires all 30 credits to be completed through coursework, while the thesis-option requires 24 credit hours of coursework and six credits of master's thesis (CPEG 869). The curriculum requirements for the thesis and non-thesis options are:

- 15 credits of Fundamentals of Cybersecurity courses
- 15 credits of elective courses in a chosen Concentration Area.
 - Concentration Areas are: (I) Secure Software, (II) Secure Systems, (III) Security Analytics, and (IV) Security Management.
 - Elective courses are to be taken primarily from a single chosen Concentration Area, with a maximum of six (6) credits taken from an alternative Concentration Area or as additional Fundamentals of Cybersecurity courses.
 - In the thesis option, six (6) credits of master's thesis are to be completed in lieu of six (6) Concentration Area elective credits.

Fundamentals of Cybersecurity and Concentration Area courses are listed below. Note that individual courses are typically three (3) credits, i.e., the 30 credit hours required for the master's non-thesis degree typically equates to 10 courses (or eight (8) courses and a thesis for the thesis option).

Fundamentals of Cybersecurity

Students must complete 15 credits, or five (5) courses, of Fundamentals of Cybersecurity. Courses designated as Fundamentals of Cybersecurity are:

CPEG 665 Introduction to Cybersecurity (CYBER I)
CPEG 697 Advanced Cybersecurity (CYBER II)
CPEG 694 System Hardening & Protection (DEFENSE)

CPEG 695 Digital Forensics
CPEG 676 Secure Software Design
CPEG 671 Pen Test and Reverse Engineering
CPEG 672 Applied Cryptography

Concentration Areas

Students must complete 15 credits, or five (5) courses, of electives. Elective courses are to be taken primarily from a single chosen Concentration Area. Of these five (5) elective courses, a maximum of two (2) can be taken outside the single Concentration Area (from one of the other Concentration Areas or from the set of Fundamentals of Cybersecurity courses). The Concentration Areas and courses within each area are listed below.

Secure Software

The Secure Software concentration is designed for a professional responsible for developing secure software systems. Secure Software electives are:

CPEG 670 Web Applications Security
CISC 621 Algorithm Design and Analysis
CISC 663 Operating Systems
CISC 672 Compiler Construction or CPEG 621 Compiler Design
CISC 675 Software Engineering Principles and Practices
CISC 611/CPEG 611 Software Process Management
CISC 612/CPEG 612 Software Design
CISC 613/CPEG 613 Software Requirements Engineering
CISC 614/CPEG 614 Formal Methods in Software Engineering
CISC 615/CPEG 615 Software Testing and Maintenance
CPEG 676 Secure Software Design

Secure Systems

The Secure Systems concentration is designed for a professional responsible for secure systems that can include wireless and network communication systems, embedded systems, and related physical systems. Secure Systems electives are:

ELEG 635 Digital Communication
ELEG 658 Advanced Mobile Services
ELEG 617 The Smart Grid
CPEG 696 Topics in Cybersecurity (Simulation-based Cybersecurity)
ELEG 812 Wireless Digital Communication
CPEG 675 Embedded Computer Systems
CISC 650 / ELEG 651 Computer Networks
CISC 853 Network Management
CPEG 673 Virtualization and Cloud Security
CISC 886 Multi-Agent Systems
CPEG 674 SCADA Systems and Security

CPEG 853 Computer System Reliability

Security Analytics

The Security Analytics concentration is designed for a professional responsible for utilizing big data, analytics, and statistical learning methods to identify and characterize anomalous behavior and security risks. Security Analytics electives are:

- ELEG 815 Analytics I - Statistical Learning
- ELEG 817/FASN 817 Large Scale Machine Learning
- CISC 683 Introduction to Data Mining
- CISC 637 Database Systems
- CPEG 657 Search and Data Mining
- CISC 681 Artificial Intelligence
- CISC 684 Introduction to Machine Learning
- CISC 689 TPCS: Artificial Intelligence: Machine Learning
- ELEG 630 Information Theory

Security Management

The Security Management concentration is designed for a professional responsible for instituting and managing security controls within an enterprise. Security Management electives are:

- MISY 850 Security and Control
- FINC 855 Financial Institutions & Markets
- BUAD 840 Ethical Issues in Domestic and Global Business Environments
- MISY 840 Project Management and Costing
- ACCT 806 Systems Analysis and Design
- BUAD 870 Leadership and Organizational Behavior
- BUAD 877 Skills for Change Agents
- MISY 810 Telecommunications and Networking

D. PROGRESS TOWARD THE DEGREE

Maintaining steady, reasonable progress towards the degree is the responsibility of the student. In accordance with the Graduate Student Probation Policy, a cumulative GPA of 3.00 must be maintained in coursework for each semester. A normal course load for full-time students is 12 credits in the fall semester, 12 credits in the spring semester, and six credits in the summer.

E. FINANCIAL AID

Students enrolled in the Master of Science in Cybersecurity are responsible for all tuition, fees, and living expenses associated with participation in the program.

PROPOSAL

I. DESCRIPTION

The 2008 CSIS report³ “Securing Cyberspace for the 44th Presidency” highlighted the human capital challenge the United States faces in Cybersecurity: “The cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the federal government.” In the 2010 follow-on CSIS report⁴, Evans and Reeder reinforced the need to “Expand cyber education” in their strategy to “Promote and fund the development of more rigorous curriculums in our schools”. Clearly, ensuring the security of the world’s and our own nation’s computers, systems and networks is a key national security challenge. Thus, establishing high-quality Cybersecurity educational programs is a top national priority as well as a regional imperative since trained Cybersecurity graduates are of critical importance to several large employer groups in this region.

The objective of the Master of Science in Cybersecurity is to use an integrated collaborative approach to train scientists and engineers to analyze and address the most challenging Cybersecurity issues. While a wide range of topics will be covered, the Cybersecurity curriculum emphasizes design of secure software and systems, security analytics, and secure business systems. This objective distinguishes the proposed program from other programs that are solely focused on IT security. The Cybersecurity curriculum will encompass multiple subject areas critical in addressing modern cybersecurity challenges: the principles and practice of network and computer security, the secure design and implementation of software systems, the analysis of artifacts found in modern systems and protection mechanisms, the study of modern complex systems and protocols, and targeted critical infrastructure and industry domains (e.g., financial services). It will train individuals that have a traditional background in engineering, computer science, information systems, or related fields to have strong security skills enabling them to develop *new* secure systems and/or software, to exploit analytics for security purposes, or to develop and manage secure business systems. Thus graduates of this program will be skilled in the latest theories and practices required to address the most challenging cybersecurity issues facing the world today.

This program offers a thesis or non-thesis option. The non-thesis Cybersecurity MS degree targets professionals who want to update their skills through full-time or part-time study. To accommodate the working schedules of part-time students, an emphasis will be placed on scheduling courses at the end of the day, developing online and distance versions of courses, and offering courses on-site (e.g., on the Army Post at the Aberdeen Proving Ground).

The Cybersecurity master’s program will prepare graduates to work in cybersecurity through a comprehensive curriculum that requires a group of Fundamental courses followed by in-depth courses in a particular chosen Concentration. It requires 30 credit hours in either a thesis or

³ J. A. Lewis, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, Washington, DC, 2008.

⁴ K. Evans and F. Reeder, "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters," Center for Strategic and International Studies, Washington, DC, 2010.

non-thesis option. The non-thesis option requires all 30 credits be completed through coursework, while the thesis-option requires 24 credit hours of coursework and six (6) credits of master's thesis. The Fundamentals of Cybersecurity portion of the curriculum requires five (5) of the following courses (or 15 credits):

- CPEG 665 Introduction to Cybersecurity (CYBER I)
- CPEG 697 Advanced Cybersecurity (CYBER II)
- CPEG 694 System Hardening & Protection (DEFENSE)
- CPEG 695 Digital Forensics
- CPEG 676 Secure Software Design
- CPEG 671 Pen Test and Reverse Engineering
- CPEG 672 Applied Cryptography

Five (5) elective courses, or 15 credits, primarily in one area of concentration are also required. For the thesis option, two (2) of these courses, or 6 credits, are thesis credits. The concentrations available are Secure Software, Secure Systems, Security Analytics, and Security Management. The courses under each concentration are given in Section IIIB. The courses are described in Appendices A and B.

This program leverages multiple existing efforts already in place at the University. In addition to several in-depth courses in computer and network security offered periodically since at least 2001, courses in both the ECE and CIS departments have long reinforced the need for deeper systems knowledge of complex computer, software, and communications systems.

Since 2010, the University, fellow state educational institutions, and the State of Delaware have organized and sponsored a yearly summer week-long college and graduate-level cybersecurity camp. Delaware leads the nation in the evolution of these camps from an outreach perspective. It was the first in 2012 to introduce high cyber knowledgeable high school students. Then again it was the first in 2014 to introduce security participants from industry and government into the camp who trained and worked on student teams to provide students with the opportunity to work with cyber professionals. This also gave potential employers access to bright cybersecurity students. The camp, often visited by Delaware's Congressional delegation and Governor (particularly at the graduation ceremony), had 61 participants in the fifth annual camp held at the University of Delaware in the summer of 2014.

In 2012, faculty from the ECE and CIS departments were awarded a four-year NSF cybersecurity capacity building grant to help bootstrap formal programs in cybersecurity at the University (NSF-1241711, "Collaborative Project: A Regional Cybersecurity Education Initiative"). Collaborating with a cross-University faculty team, the grant PIs have created and launched five new well-received cybersecurity courses with over 90 students, from five different majors, registered for cybersecurity classes in the Spring of 2015. A Cybersecurity Minor was also formally introduced this year (September, 2014).

The introduction of a Master of Cybersecurity at the University of Delaware will further strengthen Delaware's ability to supply cybersecurity knowledgeable graduates to public and government sector employers such as Northern Delaware's financial services industry and the east coast cyber corridor, including the information assurance organizations at the Army's Communications-Electronics

Research, Development and Engineering Center (CERDEC) R&D facility at Aberdeen Proving Grounds in northern Maryland.

II. RATIONALE AND DEMAND

A. DEMAND AND EMPLOYMENT FACTORS

Trained Cybersecurity graduates are of critical importance to several large employer groups in this region, notably the Financial Services industry, centered in Northern Delaware, and the recently relocated Army Research, Development, and Electronics Command (RDECOM), and its supporting government contractors, now located at Aberdeen Proving Ground (APG) in northern Maryland.

A.1. ENROLLMENT PROJECTIONS

As part of a series of ongoing meetings with industrial partners (e.g., finance, industry, government) under the NSF cyber capacity building grant, we have collected feedback on what a viable program should entail as well as what the potential student pool will be. External demand from currently employed "professional" master's students appears strong. Existing classes are already attracting these types of students. Internal demand from existing engineering, computer science, and MIS students has also been strong, with enrollments in cyber classes given Spring 2013 through Spring 2015 totaling 292 undergraduate and graduate students across 5 majors. This degree, along with the minor, and the 4+1 offering should produce a healthy yearly Master's cohort within two years of the planned Fall 2015 introduction (e.g., cohort sizes of 20+ students).

A.2. SURVEY OF EXISTING PROGRAMS

The emergence of dedicated degree programs (Bachelor's, Minor, Master's) in the information security/assurance, computer & network security, and cybersecurity fields is fairly new, but these disciplines are rapidly growing. The earliest programs, typically Information Assurance (IA), were less technical and oriented toward technology management and risk assessment. As cyber threats became increasingly technically complex, programs evolved into more engineering and computer science oriented, and they focused on Computer and Network Security (CNS) topics. Most programs today have adopted the Cybersecurity name to better reflect the most common term used at large today in industry, government, media and the public. Even graduate programs that have kept their historic degree names are aggressively marketing their programs as cybersecurity programs. Most programs are designated as Master of Science (MS) degrees.

In the development of this proposal, Cybersecurity Master's programs were reviewed at a number of top-ranked or otherwise noteworthy institutions, including: University of Texas at San Antonio (UTSA), Syracuse University, Carnegie Mellon University (CMU), George Mason University (GMU), Johns Hopkins University (JHU), University of Maryland College Park (UMD), and Drexel University.

For roughly equivalent four semester 30 credit programs, the curriculum typically combines two or more of these three knowledge areas:

1. core cybersecurity topics
2. core engineering & computer science
3. risk and technology management

IA programs typically mix these three areas evenly under degree requirements. CNS and Cybersecurity programs tend to mix the first two areas. The following table better illustrates this mix of topics (numbers represent required courses in each area).

Program	Engr / CIS core	Cyber core	Risk & Tech Mgt.	Complex Systems	Secure Software	Analytics & Big Data
USTA	2	6	2		+	
Syracuse	4	4	2			
CMU		5	5		+	
JHU	4	6				
GMU	2	4.5	3			
UMD	4	6			+	
Drexel	5.5	3.5		+		
UD	see rt. 4 columns	5	concentr. 5	concentr 5	concentr. 5	concentr. 5

The development of the Cybersecurity program at the University of Delaware has produced a unique program with many strengths and a flexibility not usually found in other leading programs. This program includes:

- A strong and deep core cybersecurity emphasis similar to CMU, UMD, and JHU;
- An ability for students to focus on secure software (CMU, UTSA, UMD) and/or complex systems (Drexel);
- An ability for students to focus on modern big data and analytics topics.

The use of concentrations allows the Delaware program to more intensively cover areas that are included in many of the other leading programs but treated somewhat superficially in several of them. The software and systems concentrations allow the Delaware program to better cover two of the most challenging security issues facing industry today. And the Delaware analytics concentration enables students to focus on one of the most promising future cybersecurity technologies needed to deal with a problem space buried by overwhelming quantities of data.

In the core engineering, computer science, and technology management topics, the Delaware program incorporates companion graduate courses that reinforce the fundamentals of cybersecurity. New cybersecurity courses will further promote a "T" shaped educational program, allowing both broad coverage with selective depth for key subject areas — broad knowledge and depth in key

areas are critical requirements for a modern cybersecurity professional. The core cybersecurity courses have been designed to cover current cybersecurity challenges as well as to follow NIST NICE and DHS knowledge area coverage recommendations.

Moreover, as increasingly seen nationally in technology-focused Master's programs, the UD Cybersecurity MS program will seek to offer many of its cyber foundation courses in an online format to better accommodate the professional part-time student.

B. INSTITUTIONAL FACTORS

B.1. COMPATIBILITY WITH UNIVERSITY ACADEMIC PRIORITIES

A strong educational program in Cybersecurity will contribute to the scholarly and educational missions of the University—to *disseminate scientific, humanistic, and social knowledge for the benefit of the larger society* and to produce graduates who *are prepared to contribute to a global society, addressing the critical needs of the state, nation and global community*.

B.2. SIGNIFICANT IMPACT ON OTHER UNIVERSITY PROGRAMS

The proposed Master of Science in Cybersecurity will not compete with any existing program at the University of Delaware but will complement several. We anticipate the following positive impacts:

- It will **strengthen interactions with local, national, and global industry**.
- It will create and offer new courses at UD that can be used as electives to enhance current graduate and undergraduate degree programs that will increasingly need to incorporate knowledge of security into their programs.
- Its new curriculum will likely spawn a series of new texts that cover and organize the subject.
- It will grow the number of highly qualified graduate students at UD who take elective classes and participate in and potentially enhance graduate student life on campus.
- It represents a new source of income for the University .

B.3. UTILIZATION OF EXISTING RESOURCES

This program will benefit from an integrated collaborative approach, both within the University and with collaborating institutions. Within the University, it builds on the close intellectual and programmatic collaborations that exists across the ECE and CIS departments. The two departments have a long history of jointly offered courses and complementing degree programs, such as the jointly administered Software Engineering degree. The majority of the courses in the proposed program are taught by the ECE and CIS departments. The ECE and CIS departments are also the principles within the College of Engineering that partner with the College of Business and Economics on the cross disciplinary Financial Services Analytics (FSA) PhD program. Core courses in the FSA program are included in the Cybersecurity MS, particularly in the Security Analytics concentration. Additional Business courses are included in the Security Management concentration.

Partnerships with collaborating institutions and utilization of existing resources created through those partnerships are also critical to the success of the Cybersecurity MS program. The NSF Cybersecurity capacity building grant is a partnership of the University of Delaware (UD), Delaware Technical & Community College (DTCC), Harford Community College (HCC; Bel Air, MD) and leading local government and industrial partners, namely the US Army at APG (RDECOM), SAIC/LEIDOS, and JP Morgan Chase (JPMC). The academic institutions are establishing articulation agreements to facilitate student transfers from two-year to four-year programs, are jointly administering summer programs and K-12 outreach activities, and are aligning curriculum efforts — all in the Cybersecurity area. Complementing the academic efforts, government and industrial partners are providing students with Cybersecurity-focused internships, are sponsoring research projects, are providing faculty exchanges, and are assisting with instruction through adjunct faculty with Cybersecurity expertise.

JPMC has developed a partnership with UD focusing on financial systems operations and analytics. This partnership prepares UD students for careers in financial systems operations and analytics, and enables UD researchers to focus on related challenges, such as enterprise computing and data centers. Cybersecurity is an area of particular interest to JPMC. A central tenant of the JPMC-UD partnership is introducing UD researchers to the critical problems facing JPMC specifically, and facing large data and enterprise computing in general. To this end, JPMC funds collaborative research projects, sends personnel to present their challenges at UD seminars, and provides opportunities and funding for UD students and faculty to visit JPMC, ranging from a day of job shadowing to extended internships/sabbaticals. These initiatives will be extended to include a Cybersecurity focus, enabling UD students and faculty to bridge the gap between academic approaches and real-world financial enterprise Cybersecurity methods and challenges.

B.4. SUPPORT OF THE COLLEGE OF ENGINEERING

As described in the accompanying letter of support, the College of Engineering and the University administration have been very supportive of broadening Cybersecurity efforts at UD. This support has included hiring a leading national expert, Dr. Starnes Walker, as the Founding Director of the University of Delaware Cybersecurity Initiative (UDCSI), a new ECE Professor, Dr. Haining Wang, specializing in cybersecurity to enhance research and instruction efforts, and a full-time CNTT Professor of Practice, Dr. Charles Cotton, to teach needed courses, secure and assist adjunct faculty members, and administer and develop needed courses and programs. The College is also committed to providing the resources for the successful start of this Master's degree program, including an additional CNTT position to help support the new courses proposed under the program, administrative support necessary as the program grows, and teaching assistants required to support fully subscribed courses, especially those offered in alternative formats (e.g., online courses).

C. ACCESS TO GRADUATE AND PROFESSIONAL PROGRAMS

Graduates of the master's in cybersecurity are expected to re-join or obtain cybersecurity jobs in industry or government. In cases where students are exceptionally talented, they may be encouraged to apply to the PhD program in Electrical and Computer Engineering or related disciplines at the University of Delaware.

III. PROGRAM ADMINISTRATION

A. PROGRAM DIRECTION

The master's program will be administered by the Department of Electrical and Computer Engineering (ECE). An Executive Committee, led by the program Director, will oversee administration of the degree. The Executive Committee will include a member from each of the key collaborating units, namely the CIS Department and the College of Business and Economics. UD's broader Cybersecurity Initiative and its external Advisory Board will provide additional feedback and guidance to the program.

The responsibilities of the Director will be to direct and administer the program under supervision of the Chairperson. This will include providing and overseeing core programmatic instruction (including the recruitment and monitoring of any necessary adjunct faculty), admissions, and student advisement. Administrative support for the program will be provided by the College of Engineering in conjunction with the Department of Electrical and Computer Engineering.

B. DEGREE REQUIREMENTS

The Master's program requires 30 credit hours in either a thesis or non-thesis option. The non-thesis option requires all 30 credits to be completed through coursework, while the thesis-option requires 24 credit hours of coursework and six credits of master's thesis (CPEG 869). The curriculum requirements for the thesis and non-thesis options are:

- 15 credits of Fundamentals of Cybersecurity courses
- 15 credits of elective courses in a chosen Concentration Area.
 - Concentration Areas are: (I) Secure Software, (II) Secure Systems, (III) Security Analytics, and (IV) Security Management.
 - Elective courses are to be taken primarily from a single chosen Concentration Area, with a maximum of six (6) credits taken from an alternative Concentration Area, or as additional Fundamentals of Cybersecurity courses.
 - In the thesis option, six (6) credits of master's thesis are to be completed in lieu of six (6) Concentration Area elective credits.

Fundamentals of Cybersecurity and Concentration Area courses are listed below. Note that individual courses are typically three (3) credits, i.e., the 30 credit hours required for the master's degree typically equates to 10 courses (or eight (8) courses and a thesis for the thesis option).

Fundamentals of Cybersecurity

Students must complete 15 credits, or five (5) courses, of Fundamentals of Cybersecurity. Courses designated as Fundamentals of Cybersecurity are:

- CPEG 665 Introduction to Cybersecurity (CYBER I)
- CPEG 697 Advanced Cybersecurity (CYBER II)
- CPEG 694 System Hardening & Protection (DEFENSE)
- CPEG 695 Digital Forensics
- CPEG 676 Secure Software Design
- CPEG 671 Pen Test and Reverse Engineering
- CPEG 672 Applied Cryptography

Concentration Areas

Students must complete 15 credits, or five (5) courses, of electives. Elective courses are to be taken primarily from a single chosen Concentration Area. Of these five (5) elective courses, a maximum of two (2) can be taken outside the single Concentration Area (from one of the other Concentration Areas or from the set of Fundamentals of Cybersecurity courses). The Concentration Areas and courses within each area are listed below.

Secure Software

The Secure Software concentration is designed for a professional responsible for developing secure software systems. Secure Software electives are:

- CPEG 670 Web Applications Security
- CISC 621 Algorithm Design and Analysis
- CISC 663 Operating Systems
- CISC 672 Compiler Construction or CPEG 621 Compiler Design
- CISC 675 Software Engineering Principles and Practices
- CISC 611/CPEG 611 Software Process Management
- CISC 612/CPEG 612 Software Design
- CISC 613/CPEG 613 Software Requirements Engineering
- CISC 614/CPEG 614 Formal Methods in Software Engineering
- CISC 615/CPEG 615 Software Testing and Maintenance
- CPEG 676 Secure Software Design

Secure Systems

The Secure Systems concentration is designed for a professional responsible for secure systems that can include wireless and network communication systems, embedded systems, and related physical systems. Secure Systems electives are:

ELEG 635 Digital Communication
ELEG 658 Advanced Mobile Services
ELEG 617 The Smart Grid
CPEG 696 Topics in Cybersecurity (Simulation-based Cybersecurity)
ELEG 812 Wireless Digital Communication
CPEG 675 Embedded Computer Systems
CISC 650 / ELEG 651 Computer Networks
CISC 853 Network Management
CPEG 673 Virtualization and Cloud Security
CISC 886 Multi-Agent Systems
CPEG 674 SCADA Systems and Security
CPEG 853 Computer System Reliability

Security Analytics

The Security Analytics concentration is designed for a professional responsible for utilizing big data, analytics, and statistical learning methods to identify and characterize anomalous behavior and security risks. Security Analytics electives are:

ELEG 815 Analytics I - Statistical Learning
ELEG 817/FASN 817 Large Scale Machine Learning
CISC 683 Introduction to Data Mining
CISC 637 Database Systems
CPEG 657 Search and Data Mining
CISC 681 Artificial Intelligence
CISC 684 Introduction to Machine Learning
CISC 689 TPCS: Artificial Intelligence: Machine Learning
ELEG 630 Information Theory

Security Management

The Security Management concentration is designed for a professional responsible for instituting and managing security controls within an enterprise. Security Management electives are:

MISY 850 Security and Control
FINC 855 Financial Institutions & Markets
BUAD 840 Ethical Issues in Domestic and Global Business Environments
MISY 840 Project Management and Costing
ACCT 806 Systems Analysis and Design
BUAD 870 Leadership and Organizational Behavior
BUAD 877 Skills for Change Agents
MISY 810 Telecommunications and Networking

C. ADMISSIONS CRITERIA

The requirements for admission to the Master of Science in Cybersecurity are the following:

1. Applicants must hold a bachelor's degree from an accredited four-year college or university with a minimum grade point average of 3.0 on a 4.0 system.
2. Applicants must have undergraduate degrees in electrical engineering, computer engineering, computer science, mathematics, physics, or related disciplines. Applicants with degrees in other disciplines may be admitted with provisional status and may be required to complete prerequisite courses that are deemed necessary for appropriate preparation for courses in the program.
3. All applicants must take the Graduate Record Examination. The following GRE scores are competitive: Quantitative: 150, Verbal + Quantitative: 300. No GRE subject test is required.
4. International applicants must demonstrate a satisfactory level of proficiency in the English language if English is not their first language. The University requires an official TOEFL score of at least 550 on paper-based, 213 on computer-based, or 79 on Internet-based tests. TOEFL scores more than two years old cannot be considered official. Alternatively, IELTS can be accepted in the place of the TOEFL. The minimum IELTS score is 6.5 overall with no individual sub-score below 6.0.

Applications are accepted according to the standard University of Delaware deadlines. Admission to the graduate program is competitive. Those who meet the stated requirements are not guaranteed admission, and those who fail to meet all requirements are not necessarily precluded from admission if they offer other appropriate strengths.

D. 4+1 MASTER'S PROGRAM

The College of Engineering offers a 4+1 master's program that allows students to satisfy the degree requirements for both a Bachelor's degree and Master of Science in Cybersecurity degree. Establishing a 4+1 program requires a separate approval by the Undergraduate Senate Committee. After establishing the Master of Science in Cybersecurity program, we plan to formally establish a 4+1 program. Under this program, University of Delaware students will be able to enroll in up to six (6) credits of approved courses during their first four years that satisfy both the Bachelor's degree and the Master of Science in Cybersecurity.

APPENDIX A - COURSE DESCRIPTIONS

CPEG/ELEG/CISC/MISY 665 Introduction to Cybersecurity (CYBER I)

Introduction to computer and network security covers the foundation security policies and methods to provide confidentiality, integrity, and availability, as well as cryptography, auditing, and user security. Topics are reinforced with hands-on exercises run in a virtual machine environment.

CPEG694 System Hardening and Protection

Practical treatment of the defensive techniques used to harden computer systems to make them less vulnerable to cyber-attacks. Defect management, configuration/hardening, account control, logs/auditing, and risk assessment are covered and reinforced with hands-on exercises run in a virtual machine environment.

CPEG695 Digital Forensics

Introduction to digital forensics as used to analyze criminal evidence in computer systems and digital media. Forensic tools and techniques for storage and memory analysis of windows/linux, network traffic, and documentation are covered and reinforced with hands-on exercises run in a virtual machine environment.

CPEG696 Topics in Cybersecurity

Examine varied topics in cybersecurity that coincide with interests of the students and current faculty. Potential topics include: (1) applications, web or cloud security, (2) risk management and incident response, (3) malware and reverse engineering, and (4) wireless, smartphone, or SCADA security.

CPEG697 Advanced Cybersecurity

This seminar course explores areas in advanced computer and network security not covered in introductory cybersecurity classes. Course provides insight into realistic complex defensive and offensive cybersecurity topics such as DoS attacks, DNS security, Email spam, On-line Authentication, Phishing, Cloud Security, Malware, and Web security.

CPEG670 Web Applications Security

This seminar-style cybersecurity course covers one specific discipline of information security known as application security. This discipline (APPSEC) refers to the development of software that can continue to function correctly even under constant scrutiny and attack by determined adversaries.

Prerequisites: Programming experience in a high level language (e.g., C, C++, java, python).

CPEG671 Pen Test and Reverse Engineering

This cybersecurity course introduces techniques used (1) to identify strengths and exploit weaknesses in networked systems or hosts, and (2) to reverse engineer programs of unknown origin and identify their function to classify them as malware and highlight the level of risk that they represent.

Prerequisites: CPEG465/CPEG665 or CPEG494/CPEG694. Programming experience in assembly language (CISC260, CPEG222, or equivalent).

CPEG672 Applied Cryptography

This cybersecurity course explores modern Cryptography covering algorithms and cryptosystems, cryptanalysis, and best practices for application and implementation of crypto in software systems.

Prerequisites: CPEG465/CPEG665 or MATH549 or equivalent.

CPEG673 Cloud Computing and Security

This cybersecurity course introduces the virtualization and cloud computing technologies used in most modern online services. The unique and conventional security issues related to protecting these types of systems are addressed and reinforced with hands-on exercises run in a virtual machine environment.

Prerequisites: CPEG/ELEG/CISC/MISY 465/665 or CPEG/ELEG 494/694 or experience with virtualization and computer networking.

CPEG674 SCADA Systems and Security

This cybersecurity course introduces SCADA (Supervisory Control And Data Acquisition) industrial control systems widely used in manufacturing, infrastructure, utilities, and control of buildings, ships, etc. Types of SCADA, use in critical infrastructure, use of communications, vulnerabilities, and best security practices and design will be addressed.

Prerequisites: CPEG465/CPEG665 or CPEG494/CPEG694

CPEG675 Embedded Computer Systems

This course explores the practice of embedding computers and software in most modern devices - appliances, games, phones, vehicles, etc. Covers engineering issues as well as best cybersecurity practices so that the resulting device does not become a target of attack for its owner.

Prerequisites: CPEG465/CPEG665 or CPEG494/CPEG694

CPEG676 Secure Software Design

This cybersecurity course introduces the theory and practices used to help make a computer program secure and provides the skills needed to implement programs that are free from vulnerabilities.

Prerequisites: Programming experience in a high level language (e.g., C, C++, java, python).

CPEG869 Master's Thesis

Independent and laboratory study conducted for the purpose of contributing new data and theory to some field of Cybersecurity in which information is lacking. Although supervised, the work will be independent in character to encourage the development of initiative.

APPENDIX B – RELEVANT EXISTING COURSES

ACCT806 Systems Analysis, Design and Implementation

Explores the management, organizational and technical challenges of developing systems. Analyzes business processes within a data-driven development methodology. Students will elicit requirements, weigh alternatives and design and implement solutions. Data, process and object modeling will be covered.

Prerequisites: ACCT804

BUAD840 Ethical Issues in Domestic and Global Business Environments

Topics include ethics in organizations, and problems and challenges dealing with external environment demands including global issues.

BUAD870 Leadership and Organizational Behavior

Develops a knowledge base and requisite skills for managing individual, group, and organizational processes through the use of diagnostic models, cases, and/or simulated exercises.

BUAD877 Skills for Change Agents

Develops skills and abilities for driving change at the individual, team, and organization levels. Team development skills, leadership skills, and negotiation skills are emphasized through simulation exercises.

CISC/CPEG 611 Software Process Management

Software management studies processes and concepts for planning and monitoring all software life-cycle phases. Topics include management models and structures, project planning including scheduling, effort estimation and risk management, project personnel and organization, project control (monitoring, measurement, correction and performance standards), software configuration management, and process description languages and tools.

CISC/CPEG 612 Software Design

Key software design concepts are introduced. Topics include basic design concepts, principles of good design, design strategies, software architecture and styles of architectural design, and design and architectural notations and languages. Detailed design, including design patterns and component design are also covered. Implementation issues that affect the design, including design support tools and tools for analyzing designs, are discussed.

CISC/CPEG 613 Software Requirements Engineering

Rigorous methods to elicit, analyze, and specify the requirements of a software system. The tasks range from identifying stakeholders and their goals to producing a precise software specification document. Topics may include data flow diagrams, use cases, UML sequence and collaboration diagrams, finite state machines, requirements for real-time and concurrent systems, entity-relationship diagrams, and logic-based specifications, as well as the analysis of specifications for consistency and completeness.

CISC/CPEG 614 Formal Methods in Software Engineering

Formal approaches to the specification, verification, and design of software systems. Topics include representing programs as transition systems; liveness and safety properties; state space reachability; explicit, symbolic and automata-based model checking; temporal logics; symbolic execution; automated theorem-proving; and relational calculus. Learn to use state-of-the-art tools based on these methods, such as the model checker Spin.

CISC/CPEG 615 Software Testing and Maintenance

Study of software testing and maintenance methodologies for modern software. Topics include approaches to automatic test case generation, test oracles, test coverage analysis, regression testing, program understanding, and software maintenance tools. A primary focus will be automation in software testing and maintenance approaches.

CISC621 Algorithm Design and Analysis

Emphasis on developing expertise in the design and analysis of algorithms. Equal importance given to techniques and specific algorithms. Particular topics include advanced data structures, graph algorithms, disjoint set manipulation, sorting and selection, amortized analysis, NP-completeness, and matrix and polynomial multiplication.

Prerequisites: Undergraduate algorithms and discrete math courses

CISC637 Database Systems

Physical and logical organization of databases. Data retrieval languages, relational database languages, security and integrity, concurrency, and distributed databases.

Prerequisites: CISC220 and CISC304 or equivalent

CISC650 / ELEG651 Computer Networks II

Foundation principles, architectures, and techniques employed in computer and communication networks. Focuses on mechanisms used in TCP/IP protocol suite. Topics include connection management, end-to-end reliable data transfer, sliding window protocols, quality of service, flow control, congestion control, routing, LANs, framing, error control, analog versus digital transmission, packet versus circuit switching, and multiplexing.

Prerequisites: An undergraduate level course in computer architecture and operating systems.

CISC663 Operating Systems

Comparison and analysis of strategies for the management of memory, processors, I/O devices and file systems.

Prerequisites: CISC260 or equivalent

CISC672 Compiler Construction

Advanced design and implementation of programming language translators. Emphasis on parsing methods, run-time, storage management techniques, code generation and optimization.

Prerequisites: CISC320 or equivalent, and CISC601 recommended

CISC675 Software Engineering Principles and Practices

Understand and apply a complete modern software engineering process. Topics include requirements analysis, specification, design, implementation, verification, and project management. Real-life team projects cover all aspects of software development lifecycle, from requirements to acceptance testing. Use of formal methods in the specification, design, and verification of software will be explored.

CISC681 Artificial Intelligence

Programming techniques for problems not amenable to algorithmic solutions. Problem formulation, search strategies, state spaces, applications of logic, knowledge representation, planning and application areas.

CISC683 Introduction to Data Mining

Concepts, techniques, and algorithms for mining large data sets to discover structural patterns that can be used to make subsequent predictions. Emphasis on practical approaches and empirical evaluation. Use of a workbench of data mining tools, such as the Weka toolkit.

CISC684 Introduction to Machine Learning

Development of methods to learn to solve a task using examples. Explore different machine learning algorithms/techniques and discuss their strengths and weaknesses and situations they are or are not suited for.

CISC689 Topics: Artificial Intelligence

Contents vary to coincide with the interests of students and faculty.

Prerequisites: CISC681

CISC853 Network Management

Introduction to network management concepts. Network management architectures and protocols: the Internet and OSI frameworks, management functionalities, management domains and objects, protocols and services (SNMP, CMIS/P). Design of management agents and clients. Concepts of performance management, fault management, configuration management and other management applications.

Prerequisites: CISC650

CISC886 Multi-Agent Systems

Introduction to the field of Multi-Agent Systems, examining issues that arise when groups of self-interested or cooperating autonomous agents interact to solve shared problems. Issues include reasoning about the knowledge and beliefs of other agents, communication and negotiation, computational organization, coordination and control.

Prerequisites: CISC681 or equivalent.

CPEG621 Compiler Design

Introduction to compiler design, syntax and semantics, code generation and optimization. Design of high performance computers together with high performance optimizing compilers as an integral

unit. Software/hardware tradeoffs in pipelined computers, super-scalar computers and computers embedded in other systems.

Prerequisites: CPEG323 and CISC361 or equivalent.

CPEG657 Search and Data Mining

With the increasing amount of textual information, it is important to develop effective search engines, such as Google, to help users manage and exploit the information. Examine the underlying technologies of search engines and get hands-on project experience. Requires good programming skills.

CPEG853 Computer System Reliability

Introduction to reliability challenges in computer systems, including permanent, transient, and intermittent faults. Various types of redundancy for fault tolerant computing will be studied. Hardware/software approaches for reliability enhancement in various computer systems will be examined, emphasizing tradeoffs involving performance, power, and reliability.

ELEG617 The Smart Grid

This course will examine not just the smart grid technologies, but the transformational impacts of the smart grid on the industry. Students in this course will learn the fundamentals of the smart grid: its purpose and objectives, its technologies, its architectures, and its management.

ELEG630 Information Theory

Information theory establishes the theoretical limits that can be achieved in communications systems, and provides insights about how to achieve these limits in practical systems. Covers lossless and lossy compression, and studies the maximum information rate achievable in communications over noisy channels.

Prerequisites: Undergraduate course in probability.

ELEG635 Digital Communication

The theory and applications of digital communications including modulation, pulse shaping, and optimum receiver design for additive white Gaussian noise and bandlimited channels.

Prerequisites: Undergraduate course in probability, signals and linear systems

ELEG658 Advanced Mobile Services

Foundations for the creation of successful advanced mobile services, including the interplay of business and technology evolution, methodologies, architectures and paradigm shifts that accompany the development of converged user centric intelligent telecommunication services from location sensitive and navigation services to social networking and remote sensing.

ELEG812 Wireless Digital Communications

Fundamentals and current techniques in wireless digital communications, including propagation, modem design, fading countermeasures, and multiple access techniques, such as FDMA, TDMA, and CDMA.

Prerequisites: Probability and linear systems

ELEG815 Analytics I: Statistical Learning

Introduction to the mathematics of data analysis. Bayes estimation, linear regression and classification methods. The singular value decomposition and the pseudo-inverse. Statistical models for inference and prediction in finance, marketing, and engineering applications. Regularization methods and principles of sparsity priors are applied. Streaming solutions. High dimensional problems. Concepts reinforced in R programming experiments.

Prerequisites: First course in linear algebra. First course in probability and statistics (ELEG310 or equivalent). Basic programming skills.

ELEG/FASN 817 Large Scale Machine Learning

Introduction to the analysis and processing of massive high-dimensional data. Massive data sets generally involve growth not only in the number of individuals represented but also in the number of descriptive parameters of the individuals, leading to exponential growth in the number of hypotheses considered. New approaches to address these problems exploit sparsity prior concepts from optimization theory, signal processing, statistics, and machine learning.

Prerequisites: ELEG815.

FINC855 Financial Institutions and Markets

Examines the nature, purpose, and management of financial institutions and markets.

Prerequisites: FINC850

MISY810 Telecommunications and Networking

Leadership skills in information technology, telecommunications and internet technology for technology management. Introduces concepts in data and image compression, digital audio and digital cellular telephony. Provides fundamental knowledge of transmission and storage technology and a system-level understanding of computer networks and the internet.

MISY840 Project Management and Costing

Provides the technical knowledge and skills needed to successfully plan, execute and evaluate IT projects. Strong emphasis on the costing of IT projects.

MISY850 Security and Control

Considers state-of-the-art technological and organizational approaches to enhancing the security and integrity of corporate information resources in a cost-effective manner.

APPENDIX C – LETTERS OF APPROVAL AND SUPPORT

College of Engineering

1. Dr. Babatunde A. Ogunnaike, Dean, College of Engineering
and William L. Friend Chaired Professor of Chemical Engineering
2. Dr. Errol Lloyd, Chair, Department of Computer & Information Sciences

Alfred Lerner College of Business & Economics

2. Dr. Scott K Jones, Chair, Department of Accounting & Management Information Systems
3. Dr. Stewart Shapiro, Chair, Department of Business Administration
4. Dr. Helen Bowers, Department of Finance



College of Engineering
OFFICE OF THE DEAN

University of Delaware
102 du Pont Hall
Newark, DE 19716-3101
Phone: 302.831.2401
Fax: 302.831.8179

January 5, 2015

Kenneth Barner
Professor & Chair
Department of Electrical and Computer Engineering
Re: Master of Science in Cybersecurity

Dear Prof. Barner:

I am pleased to write in strong support of the proposed Master of Science degree program in Cybersecurity. This is the kind of innovative program that can provide the University of Delaware and the College of Engineering a platform for great visibility and leadership in a critical field of endeavor, with significant implications for national and international impact.

In the interest of launching the program and allowing for a reasonable period to establish its visibility, the College will, for the first three years, provide salary and fringe benefit support for one non-tenure-track faculty position, part-time administrative support, one month of summer support for the program Director, and appropriate levels of TA support when enrollment meets thresholds requiring such support. Support will be continued beyond the indicated time frame pending assessment of the program's performance in educational accomplishments as well as in recruiting and retention statistics.

I wish you the best of luck in this important initiative.

Sincerely,

Sincerely,

Babatunde A. Ogunnaike
Dean, and
William L. Friend Chaired Professor of Chemical Engineering

cc: C. E Cook



January 18, 2015

Kenneth Barner, Professor and Chair
Department of Electrical and Computer Engineering

Re: Master's of Science in Cybersecurity

Dear Prof. Barner:

The Department of Computer and Information Sciences strongly supports the proposed Master's of Science in Cybersecurity degree program. The proposed Cybersecurity MS builds on existing department, college, and university efforts in the area and establishes UD leadership in this critical discipline.

The Department of Computer and Information Sciences is happy to support the inclusion of departmental courses as options within the program, including:

- CISC 611/CPEG 611 Software Process Management
- CISC 612/CPEG 612 Software Design
- CISC 613/CPEG 613 Software Requirements Engineering
- CISC 614/CPEG 614 Formal Methods in Software Engineering
- CISC 615/CPEG 615 Software Testing and Maintenance
- CISC 621 Algorithm Design and Analysis
- CISC 637 Database Systems
- CISC 650/ELEG 651 Computer Networks
- CISC 853 Network Management
- CISC 663 Operating Systems
- CISC 672 Compiler Construction or CPEG 621 Compiler Design
- CISC 675 Software Engineering Principles and Practices
- CISC 683 Introduction to Data Mining
- CISC 684 Introduction to Machine Learning
- CISC 689 TPCS: Artificial Intelligence: Machine Learning
- CISC 861 Artificial Intelligence
- CISC 886 Multi-Agent Systems

I certify that all departmental policies and bylaws were followed in obtaining CIS department support for the inclusion of these courses as options in the program.

We in CIS look forward to supporting ECE in building this exciting new MS program.

Sincerely,

Errol Lloyd
Professor and Chair



Alfred Lerner College of Business & Economics

DEPARTMENT OF ACCOUNTING & MIS

January 8, 2015

Kenneth Barner,
Professor & Chair
Department of Electrical and Computer Engineering

Re: Master's of Science in Cybersecurity

Dear Prof. Barner:

The Department of Accounting and Management Information Systems (MIS) enthusiastically supports the proposed Master's of Science in Cybersecurity degree program. The proposed Cybersecurity MS builds on existing department, college, and university efforts in the area and establishes UD leadership in this critical discipline.

The Department of Accounting and MIS supports the inclusion of departmental courses as options within the program, including:

- MISY 810 Telecommunications and Networking
- MISY 840 Project Management and Costing
- MISY 850 Security and Control
- ACCT 806 Systems Analysis and Design

Please note that all departmental policies and bylaws were followed in making this collaborative commitment.

Sincerely,

A handwritten signature in black ink, appearing to read 'Scott K. Jones', written over a horizontal line.

Scott K. Jones
Professor & Chair



Alfred Lerner College
of Business & Economics
DEPARTMENT OF BUSINESS ADMINISTRATION

Newark, DE 19716-2710
Phone: 302-831-2555
Fax: 302-831-4196

*Dr. Stewart Shapiro
Chair, Department of Business Administration
Professor of Marketing
Lerner College of Business & Economics
University of Delaware
Newark, DE 19716*

*Phone: (302) 831-2516
Fax: (302) 831-4196
Email: sshapiro@udel.edu*

January 5, 2015

Kenneth Barner,
Professor & Chair
Department of Electrical and Computer Engineering

Re: Master's of Science in Cybersecurity

Dear Prof. Barner:

The Department of Business Administration supports the proposed Master's of Science in Cybersecurity degree program. The proposed Cybersecurity MS builds on existing department, college, and university efforts in the area and establishes UD leadership in this critical discipline.

The Department of Business Administration supports the inclusion of departmental courses as options within the program, including:

- BUAD 840 Ethical Issues in Domestic and Global Business Environments
- BUAD 870 Leadership and Organizational Behavior
- BUAD 877 Skills for Change Agents

Please note that all departmental policies and bylaws were followed in making this collaborative commitment.

Sincerely,

Stewart Shapiro
Professor & Chair

www.lerner.udel.edu



**Alfred Lerner College
of Business & Economics**

DEPARTMENT OF FINANCE

306 Purnell Hall
Newark, DE 19716-2712
Phone: 302-831-1484
Fax: 302-831-3061

TO: Kenneth Barner, Professor & Chair
Department of Electrical and Computer Engineering

FROM: Helen Bowers, Associate Professor and Chair
Department of Finance

Helen Bowers

DATE: January 9, 2015

RE: Letter of support for the proposed MS in Cybersecurity

The Department of Finance strongly supports the proposed MS in Cybersecurity.

We understand that FINC855 Financial Institutions and Markets is part of the curriculum. The Department of Finance agrees to make this course available to students in the MS in Cybersecurity program who have met the prerequisites. Please note that all departmental policies and bylaws were followed in making this collaborative commitment.

We appreciate the opportunity to work with you on offering the MS in Cybersecurity.