UNIVERSITY FACULTY SENATE FORMS

Academic Program Approval

This form is a routing document for the approval of new and revised academic programs. Proposing department should complete this form. Detailed instructions for the proposal should be followed. A checklist is available to assist in the preparation of a proposal. For more information, call the Faculty Senate Office at 831-2921.

Submitted by: Stephan Bohacek phone number:302-831-4274

Department: Electrical and Computer Engineering email address_bohacek@udel.edu

Date: September 28, 2015

Action: Add Graduate Certificate in Cyber Security
(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: ASAP, ideally 16S (use format 04F, 05W)

Current degree: None
(Example: BA, BACH, BACJ, HBA, EDD, MA, MBA, etc.)

Proposed change leads to the degree of: Nothing directly. But courses could be applied toward Master's in Cybersecurity (Example: BA, BACH, BACJ, HBA, EDD, MA, MBA, etc.)

Proposed name: Graduate Certificate in Cybersecurity
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:__ Graduate Certificate in Cybersecurity _____
(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, either describing the new program or 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")
None.

Supply support letter from the Library, Dean, and/or Department Chair if needed
(all new majors/minors will need a support letter from the appropriate administrator.)

Supply a resolution for all new majors/programs; name changes of colleges, departments, degrees; transfer of departments from one college to another; creation of new departments; requests for permanent status. **See example of resolutions.**

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

Identify other units affected by the proposed changes:
(This would include other departments/units whose courses are a required part of the proposed curriculum. Attach permission from the affected units. If no other unit is affected, enter "None")

Describe the rationale for the proposed program change(s):
(Explain your reasons for creating, revising, or deleting the curriculum or program.)

As cyber-systems become more integrated into society, the impact of cyber-attack increases, necessitating the need for cybersecurity research and education.

In order to meet the growing needs for improved cybersecurity, the University of Delaware is pursuing a cybersecurity initiative which has led to

- A new undergraduate minor and MS degree in cybersecurity
- The hiring and planned hiring of several faculty to pursue cybersecurity research and education
- The hiring of a director and deputy director of the cybersecurity initiative

A graduate certificate in cybersecurity is next step in this initiative. The educational goal of this certificate are

1. Impart cybersecurity best-practices on professionals working in computing and related areas
2. Act as a first step of students' pursuit of a graduate degree in cybersecurity, enabling them to become cybersecurity professionals
3. Act as a first step of students' pursuit of a Ph.D. in cybersecurity

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.) **See example of side by side.**

Requirements for Admission

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.

3. Applicants must have programming experience in a high level language (e.g. C, C++, java, python) and familiarity with basic networking protocols and operating systems.
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.

Program Description

The Certificate in Cybersecurity requires satisfactory completion of three (3) graduate level courses (9 credits) as detailed below. Each certificate program course must be completed with a grade no lower than a B-; the overall GPA of the Certificate in Cybersecurity courses must be no lower than 3.0.

Course Requirements

Three course selected from the following
CPEG 665 Introduction to Cybersecurity
CPEG 697 Advanced Cybersecurity
CPEG 694 System Hardening & Protection
CPEG 695 Digital Forensics
CPEG 676 Secure Software Design
CPEG 671 Pen Test and Reverse Engineering
CPEG 672 Applied Cryptography

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

Department Chairperson [signature] Date 9-28-15

Dean of College [signature] Date 10/1/2015

(By signing above, the Dean confirms that their college policies and bylaws have been followed correctly during consideration of the request described in this form.

The approval actions that were taken at the college level were (check all that apply) :

_____ college faculty vote; _____ ✓ college curriculum approval _____ college senate approval

Chairperson, College Curriculum Committee [signature] Date 9/30/2015

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 _____

Board of Trustee Notification _____ Date _____

Revised 10/27/2014/khs

UNIVERSITY OF DELAWARE
Department of Electrical & Computer Engineering
OFFICE OF THE CHAIR

Newark, DE 19716-3130
Phone: 302-831-2405
Fax: 302-831-4375

September 23, 2015

Faculty Senate

Regarding: Fundamentals of Cybersecurity Certificate Program

The Department of Electrical and Computer Engineering fully supports the proposed Fundamentals of Cybersecurity Certificate. The proposed certificate program builds on existing courses and the recently established Master's of Science in Cybersecurity degree program, administered by the ECE Department.

The Fundamentals of Cybersecurity Certificate is earned by completing three of the courses designated as Cybersecurity Fundamentals in the Cybersecurity MS degree. The seven fundamentals courses 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

The ECE Department is committed to regularly offering these fundamental courses. Additionally, the ECE faculty unanimously voted to approve the Fundamentals of Cybersecurity Certificate Program. All departmental policies and bylaws were followed in the generation and approval of this Certificate Program.

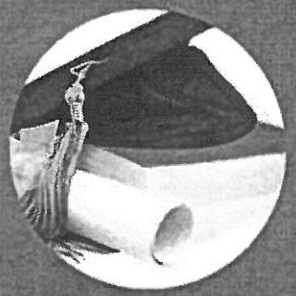
Please feel free to contact me if I can provide additional information or assistance.

Sincerely,

Kenneth E. Barner
Professor & Chair

UNIVERSITY *of* DELAWARE

Cybersecurity Initiative

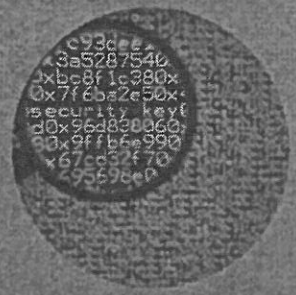


Educational Programs

- Certificate Program
- Minor Degree
- Masters Degree
- 4+1 Program
- 2+2 Program

Partnerships

- Corporate & Government
  - SWIFT, SAIC, JPMC, US Army (APG), DE DTI, DE NG Network Warfare Squad.
- Academic
  - Del Tech, Harford CC, DSU



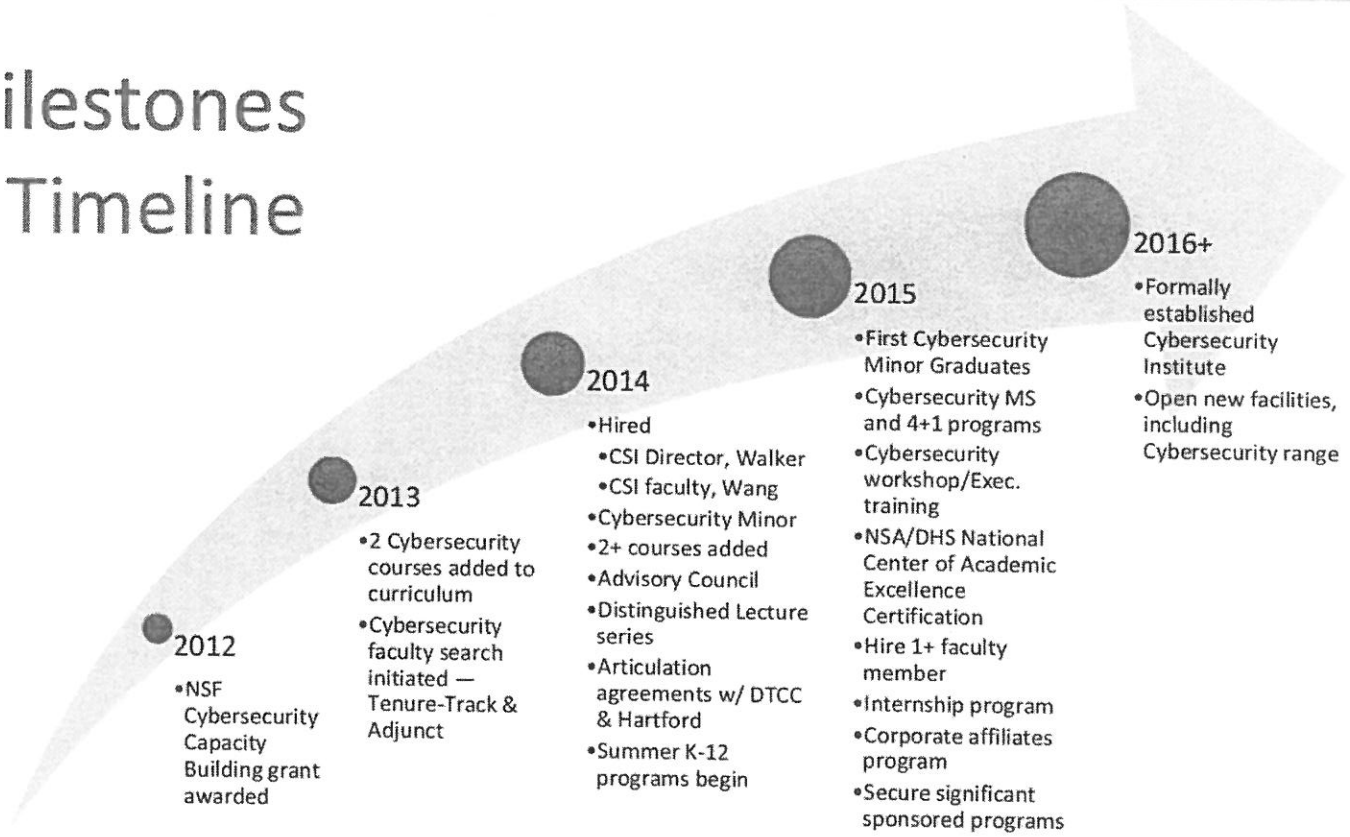
Research

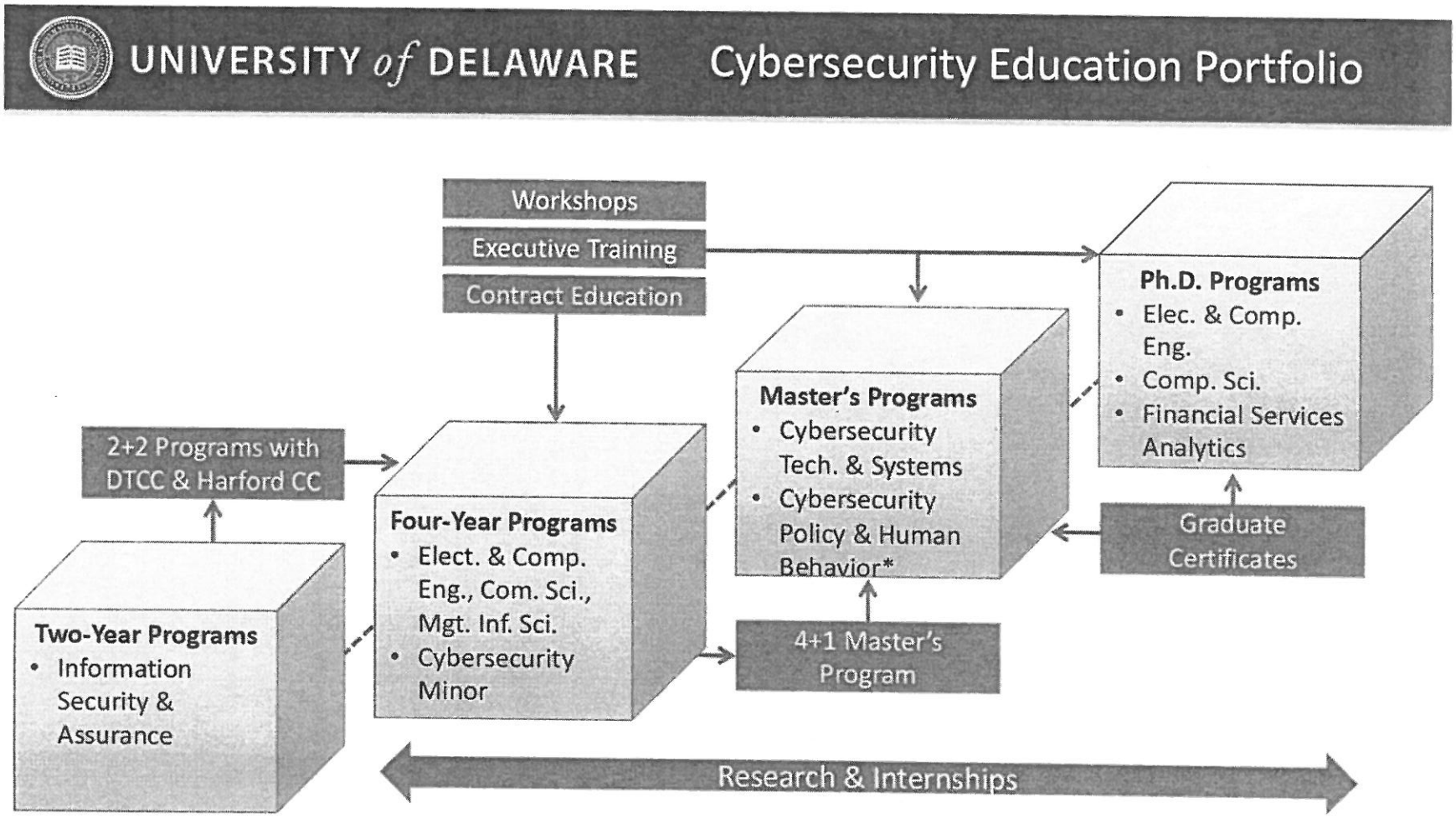
- Fundamental Research
  - Network, Computer & Systems Security
  - Information Assurance
  - Cyber Defense and Offense
  - Behavioral Analysis
- Classified Research

Outreach

- Student Internships
- Summer K-12 Camps
- Bridge Programs
- Workshops & Seminars
- Business Cooperative Extension

Milestones & Timeline




UNIVERSITY of DELAWARE
Cybersecurity Education Portfolio
Workshops
Executive Training
Contract Education
Ph.D. Programs
• Elec. & Comp. Eng.
• Comp. Sci.
• Financial Services Analytics
Master's Programs
• Cybersecurity Tech. & Systems
• Cybersecurity Policy & Human Behavior*
2+2 Programs with DTCC & Harford CC
Four-Year Programs
• Elect. & Comp. Eng., Com. Sci., Mgt. Inf. Sci.
• Cybersecurity Minor
Graduate Certificates
Two-Year Programs
• Information Security & Assurance
4+1 Master's Program
Research & Internships

UNIVERSITY *of* DELAWARE

Cybersecurity MS Courses

Fundamentals of Cybersecurity

Introduction to Cybersecurity; Advanced Cybersecurity; System Hardening & Protection; Digital Forensics; Secure Software Design; Pen Test and Reverse Engineering; Applied Cryptography

Secure Software

Web applications Security; Operating System; Compiler Construction; Software Engineering Principles and Practices; Software Process Management; Software Design; Software Requirements Engineering; Formal Methods in Software Engineering; Software Testing and Maintenance; Secure Software Design

Secure Systems

Digital Communication; Advanced Mobile Services; The Smart Grid; Simulation-Based Cybersecurity; Wireless Digital Communications; Embedded Systems; Computer Networks; Network Management; Virtualization and Cloud Security; Multi-Agent Systems; SCADA Systems and Security; Computer Systems Reliability

Security Analytics

Analytics I - Statistical Learning; Large Scale Machine Learning; Introduction to Data Mining; Database Systems; Search and Data Mining; Artificial Intelligence; Artificial Intelligence and Machine Learning; Information Theory; Introduction to Machine Learning

Security Management

Security and Control; Financial Institutions and Market; Ethical Issues in Domestic and Global Business Environments; Project Management and Costing; System Analysis and Design; Leadership and Organizational Behavior; Skills for Change Agents; Telecommunications and Networking

UNIVERSITY *of* DELAWARE

MASTER'S IN CYBERSECURITY
GRADUATE CERTIFICATE IN CYBERSECURITY

Foundations of Cybersecurity – Computer & Network Security	Certificate: 9 credits Master's: 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
Master's Concentration Areas - 15 credits (5 courses; a max of 2 courses can be taken from an alternative concentration area or cyber fundamentals)	
Secure Software 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 ELEG 635 Digital Communication ELEG 658 Advanced Mobile Services ELEG 617 The Smart Grid CPEG 696 Topics in Cybersecurity (Sim-based Cybersecurity) ELEG 812 Wireless Digital Communications	CPEG 675 Embedded 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 Systems Reliability
Security Analytics ELEG 815 Analytics I - Statistical Learning ELEG 817 / FSAN 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 ELEG 630 Information Theory CISC 684 Introduction to Machine Learning CISC 689 TPCS: Artificial Intelligence: Machine Learning
Security Management 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