University of Maine
B.S. In Cybersecurity
Version 2.0

Prof. George Markowsky
School of Computing & Information Science
University of Maine

April 27, 2015

Contents

List of Figures

List of Tables

1 Background

In 2014, the University of Maine System collectively obtained a designation by the National Security Agency (NSA) as a CAE/IAE- National Centers of Academic Excellence in Information Assurance Education. This was due in large part to Dr. Raymond Albert of the University of Maine at Fort Kent. This gave the University of Maine System an opportunity to offer degrees in Cybersecurity recognized by the NSA as meeting their standards. At this time, this is the highest level of approval for cybersecurity programs. Efforts are under way to create an ABET accreditation for cybersecurity and it is the intent of this group to apply for such accreditation as soon as it becomes available. A copy of the letter is shown in Figure 1.

As a result of the successful application for CAE/IAE status, representatives of the campuses of the University of Maine System began to meet to design a degree program that would provide a much needed option to students of the University of Maine System. The outcome of this effort is contained in a document titled *Bachelor of Science in Cybersecurity Program Proposal* that has been previously circulated. This document provides extensive rationale for this degree program along with a general framework of what is to be covered by the degree. At the same time, it was decided that each campus that participates in this program would offer its own degree and that there would not be a system degree. Ideally, it was felt that we would be able to have courses that would be offered online that could be taken throughout the system. At the same time, it was felt that we wanted to move expeditiously to set up a degree program in a very fast changing field. The campuses have responded positively to the idea of having such a program and all campuses approved an intent to plan.

This document builds on the *Bachelor of Science in Cybersecurity Program Proposal* and shows how we plan to adapt this program to our campus. The goal is to introduce as few new courses as possible, but to modify some of the existing courses so that they fit better into a cybersecurity curriculum. The details of how to do this are in Section 2. We will only reproduce material from the University of Maine System proposal that is most relevant to this document. We invite people to read the University of Maine System program proposal along with this proposal. Table 1 shows the basic curriculum that is being implemented across the campuses of the University of Maine System.

1.1 Evidence of Program Need

The material in this subsection is just a sampling of the material in the University of Maine System B. S. in Cybersecurity proposal. We recommend that people read that report to more fully appreciate the need for this program. We begin with a quote from President Obama (December 19, 2014).

> *In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place...But*

National Centers of Academic Excellence in Information Assurance/Cybersecurity
9800 Savage Road
Ft. Meade, MD 20755-6744

October 24, 2014

University of Maine System
Dr. Raymond Albert
PMD
23 University Drive
Fort Kent, ME 04743

Dr. Albert:

I am pleased to inform you that the National Security Agency and the Department of Homeland Security have designated the University of Maine System as a National Center of Academic Excellence in Information Assurance/Cybersecurity through academic year 2019.

Your ability to meet the increasing demands of the program criteria will serve the nation well in contributing to the protection of the National Information Infrastructure. The Presidents' National Strategy to Secure Cyberspace, February 2003, and the International Strategy for Cyberspace, May 2011, addresses the critical shortage of professionals with these skills and highlights the importance of higher education as a solution to defending America's cyberspace. "Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so." Education is the key to promoting these ideals.

We appreciate your participation in this program and look forward to presenting your certificate to you at a spring 2015 formal recognition event.

Sincerely,

\s\

Karen Leuschner
National CAE Program Manager, NSA

Figure 1: NSA Recognition of the University of Maine System as a Center of Academic Excellence in Information Assurance

Table 1: UMS Cybersecurity Requirements (36 hours)

CYB 100	Introduction to Computer Science	4 hours
CYB 200	Introduction to Information Security	3 hours
CYB 250	Introduction to Programming	3 hours
CYB 300	Computer Programming	3 hours
CYB 330	Networking	3 hours
CYB 340	Cyber Ethics	3 hours
CYB 350	Databases	4 hours
CYB 360	Network Security	4 hours
CYB 370	Operating Systems Security	3 hours
CYB 390	Cybersecurity Internship	3 hours
CYB 400	Cyber Defense (Capstone)	3 hours
	Cybersecurity Portfolio	

> *even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage.*
>
> *This is part of the reason why it's going to be so important for Congress to work with us and get an actual bill passed that allows for the kind of information-sharing we need. Because if we don't put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant.*

The following material comes from the University of Maine System B. S. in Cybersecurity Proposal.

> A recent joint study by the nonprofit Center for Strategic and International Studies (2013) and the computer-security firm McAfee posits a $100 billion annual loss to the U.S. economy and as many as 508,000 U.S. jobs lost as a result of malicious cyber activity (CSIS, 2013). Global losses, it finds, are between $100 billion and $500 billion each year. This new estimate reflects a major revision of McAfee's own previous estimate of $1 trillion (Maass & Rajagopalan, 2012; Vamosi, 2012), which has been cited widely, including by U.S. Government officials. These losses result from cyber-attacks in six categories: the loss of intellectual property, cybercrime, and loss of business information, service disruptions, and the cost of securing networks, and reputational damage to a hacked company.
>
> Market Research Media (MRM) reports that with a cumulative market valued at $65.5 billion between 2013 and 2018, the U.S. Federal Cybersecurity

market will grow steadily at about 6.2

1.1.1 Shortage in Trained Cybersecurity Workers - University of Maine System B. S. in Cybersecurity Proposal

With billions of dollars in global losses due to cybersecurity exploits, the need for trained experts is growing at an astonishing rate. The U.S. Bureau of Labor Statistics is predicting 22% growth in employment in cybersecurity by 2020. The federal government is actively recruiting to fill 10,000 cybersecurity professional positions, of which approximately 5,000 of these positions are at the U.S. Cyber Command. Aggressive growth in training will be critical to the catch- up effort. Such efforts include IBM's Cybersecurity Innovation Program and its new university partnerships around the world, the National Initiative for Cybersecurity Education (NICE), and the strong academic programs at the University of Maryland, the University of Texas at Dallas, the University of Southern California, Purdue University, Northeastern University, and the University of Michigan.

In Maine, there is a need to improve workforce education and development opportunities for the IT community, specifically centered on cybersecurity. IT is one of Maine's high-growth occupations but current conventional training and educational models are not producing enough qualified graduates to meet the demand from IT employers for skilled candidates. This is true throughout Maine but particularly in greater-Portland. Based on information gathered from the University of Maine System (UMS) - Business Computer Science and Information Technology Partnership, as much as 30

The ongoing shortage of qualified cybersecurity IT professionals is creating a set of problems that goes well beyond the immediate security of data and systems. The shortage is also inhibiting the effective adoption of key technologies in the enterprise and the public sector, including mobile, cloud and social applications, among others. And that will, in turn, inhibit enterprise growth and economic expansion (Shaw, 2013). Cyber criminals are well organized and highly skilled yet the U.S.'s cybersecurity workforce is undermanned and under skilled.

1.1.2 National Cybersecurity Workforce Framework - University of Maine System B. S. in Cybersecurity Proposal

An essential step to ensuring that our nation can educate, recruit, train, develop and retain a highly qualified cybersecurity workforce is a common understanding of and lexicon for cybersecurity work. To this end, NICE recently established the National Cybersecurity Workforce Framework, which is for the public, private, and academic sectors using a common taxonomy and lexicon that describe all cybersecurity work and workers irrespective of

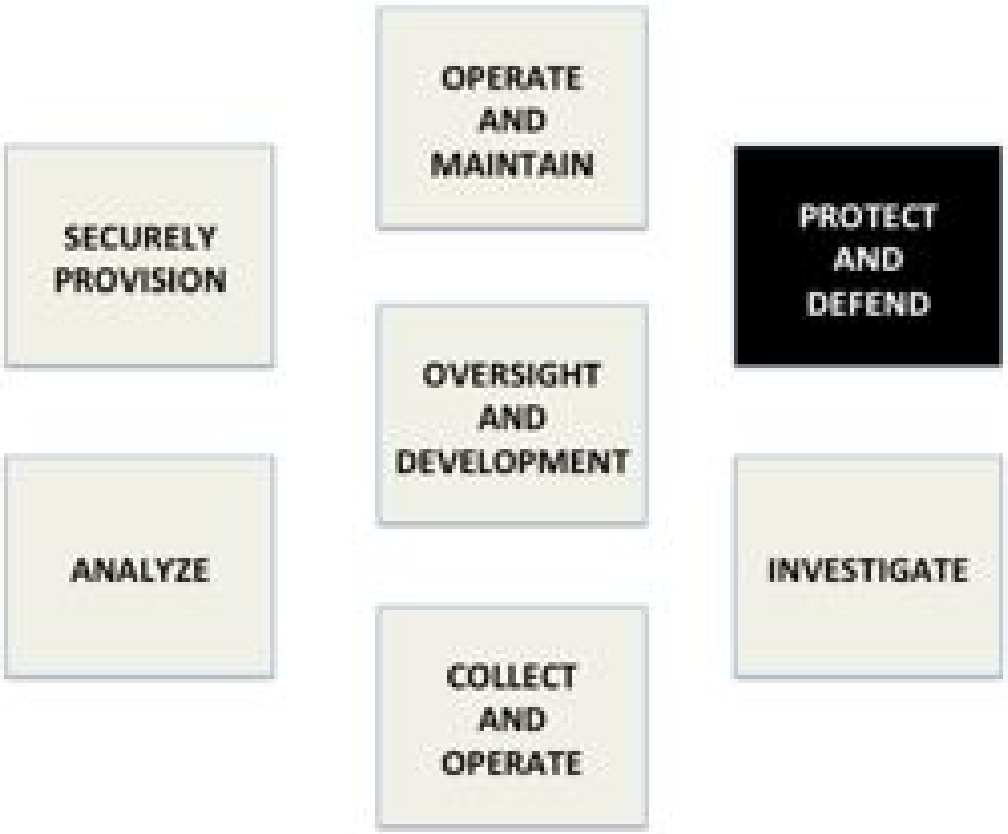


Figure 2: Overarching Cybersecurity Workforce Categories

where or for whom the work is performed. The Framework consists of thirty-one specialty areas organized into seven categories (Figure 2) that serve as an overarching structure for the Framework, grouping related specialty areas together and including each specialty area's requirements for typical tasks and knowledge, skills, and abilities.

The need for skilled practitioners in the cybersecurity field is so great that the federal government has reported continuation of a three-year backlog in unfilled positions. Funding opportunities made available under the auspices of the National Science Foundation have been created to provide full funded scholarships to students who agree to complete graduate degrees in the field and agree to serve as civil servants for a like number of years.

The Department of Defense (DoD) issued in 2008 a directive (Directive 8570) that provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. It affects any full- or part-time military service member, contractor, or local nationals with privileged access to a DoD information system performing information assurance (IA) functions – regardless of job or occupational series. The directive requires:

- 100% of the IA professionals in DoD and DoD contractors must be certified within the next 3 years,
- 40% must be certified by the end of 2008,
- all IA jobs will be categorized as "Technical" or "Management" Level I, II, or III, and to be qualified for those jobs, you must be certified.

Recent reports indicate that only 30% of the approximately 90,000 affected employees have so far met the mandated requirements.

2 The UMaine B. S. in Cybersecurity Curriculum

2.1 Overview

In our proposal we tried to meet the following constraints.

- We wanted to minimize the impact of the program on the School of Computing and Information Science.
- We wanted to make it as compatible as possible with the existing Computer Science B.S. degree program
- We wanted it to meet the needs of its constituents.
- We wanted it to be consistent with the vision of the University of Maine System B. S. in Cybersecurity.
- We wanted to reduce the need for using online courses until the program gets going on all the campuses and we can institute the parameters of inter-campus credit transfers. There is a separate MOU that is under discussion among the Provosts of the different campuses and we will obviously have to abide by whatever agreements are reached.
- We are not requiring faculty to put existing courses online, but we are encouraging them to do so. We plan to make the new COS 330 Introduction to Cybersecurity, COS 336 Cybersecurity Competition 1, COS 337 Cybersecurity Competition 2 and COS 338 Cybersecurity Competition 3 courses available online.
- It should be noted that all the cybersecurity specific courses except for COS 495 Field Experience and COS 497 Computer Science Capstone 2 will be available online for other campuses to utilize. The other required courses for the University of Maine B. S. in Cybersecurity might or might not be available online, but there should be readily available online versions of the courses available from the other campuses in the University of Maine System.
- While the University of Maine System B. S. in Cybersecurity proposal claims that the program can be implemented without additional resources, this does not seem possible in the absence of mechanisms for intercampus cooperation. These are not in place at this time and this proposal is put forward in the hopes of getting the University of Maine B. S. in Cybersecurity started, with the understanding that the program will evolve as intercampus cooperation questions are answered. This topic is pursued further in Section 7, where it is shown that the additional resources needed would be modest before Fall 2019.

Students taking the regular COS B. S. degree can also complete the requirements of the B. S. in Cybersecurity by focusing their electives and taking ECE 331 Unix System Administration. If the School of Computing and Information Science voted to accept

ECE 331 Unix System Administration as an elective for the Computer Science B. S. degree, then students would not need to take any additional courses. Because of the large amount of overlap, there are not enough extra credit hours to qualify as a double major. Perhaps we can explore a way to mark on the diploma that the student has completed all requirements for the B. S. in Cybersecurity along with the requirements for a B. S. in Computer Science.

The proposed University of Maine B. S. in Cybersecurity requires only 40 credits and might be easier for many students to complete than the standard B. S. in Computer Science. It would certainly be easier to have as a double major if they were interested in completing a very attractive major in addition to any other major that they would complete. At this time, other than the NSA certification, there is no professional accreditation available for B. S. in Cybersecurity degrees. As soon as an accreditation is available, we plan to submit the degree for accreditation.

2.2 Requirements for the University of Maine B. S. in Cybersecurity

Here is a quick summary of what the proposed degree would require:

- 120 Credit Hours
- Meet the General Education Requirements
- ENG 101 - 3 cr
- ENG 317 - 3 cr
- MAT (STS) 232 - 3 cr (all the MAT statistics courses are in the process of moving to the STS course designator)
- The following cybersecurity related courses
  - COS 140 Foundations of Computer Science - 3 cr
  - COS 220 Introduction to C++ Programming - 3 cr
  - COS 221 Data Structures in C++ Programming - 3 cr
  - COS 235 Computer Organization - 4 cr
  - COS 330 Introduction to Cybersecurity - 3 cr (this is a redesign of COS 430 Introduction to Cybersecurity)
  - COS 331 Operating Systems - 3 cr
  - ECE 331 Unix System Administration - 3 cr
  - COS 336 Cybersecurity Competition 1 - 1 cr (this is a new course described later)
  - COS 337 Cybersecurity Competition 2 - 1 cr (this is a new course described later)

  - COS 338 Cybersecurity Competition 3 - 1 cr (this is a new course described later)
  - COS 440 Computer Networking I - 3 cr
  - COS 480 Database Management Systems - 3 cr
  - COS 490 Computers, Ethics and Society - 3 cr
  - COS 495 Field Experience - 3 cr (must be a cybersecurity related field experience)
  - COS 497 Computer Science Capstone 2 - 3 cr (we would need to make sure that COS 495 covered the ground covered in COS 397 Capstone 1)

- A Cybersecurity Portfolio.

There are 40 credit hours of cybersecurity related courses required by the program. There is some thought of changing COS 235 Computer Organization to a 3 credit hour course, in which case the University of Maine B. S. in Cybersecurity would require only 39 credit hours. The student's Cybersecurity Portfolio will be an important assessment tool. It will be reviewed by the student's Capstone advisor for evidence of professional development. In particular, students will be required to have in their portfolio links to current developments in the field. They will be expected to be knowledgeable about the links they provide and will need to satisfy their Capstone Advisor that they are professionally engaged.

We intend to implement the Cybersecurity Portfolio using LinkedIn^{TM}. We propose usingLinkedIn^{TM} for several reasons.

- It is almost a requirement for professional people to have a LinkedIn^{TM} profile.
- Most of its features are available for free.
- It helps the program to maintain contact with students once they graduate.
- It seems to be the way that the University of Maine is heading. There is now a University of Maine group on LinkedIn^{TM} with subgroups appearing under the University of Maine umbrella. We plan to establish a Cybersecurity subgroup under the University of Maine group.

The University of Maine B. S. in Cybersecurity would follow all the general degree requirement of the University of Maine. In particular, students will be required to:

1. receive acceptable grades in all required courses and credits, including General Education, college and major courses
2. accumulate the number of degree credits specified by the program in which they are registered (120 credits minimum)
3. achieve a cumulative average of not less than 2.0 in University of Maine courses

Table 2: Sample Program for Fall of Year 1

COURSE	Credit Hours
COS 140 Foundations of Computer Science	3
COS 220 Introduction to C++ Programming	3
MAT Principles of Statistical Inference	3
ENG 101 College Composition	3
General Education Science	3
Total	15

Table 3: Sample Program for Spring of Year 1

COURSE	Credit Hours
COS 221 Data Structures in C++ Programming	3
COS 235 Computer Organization	4
General Education Science	3
Electives	5
Total	15

4. earn a minimum of 30 credits originating from the University of Maine campus at the 300 level or higher over any year of study. There are two exceptions to this policy:

    - students who have already completed three or more years at the University of Maine (minimum of 90 credits of University of Maine courses) when, in the opinion of the student's academic program faculty in consultation with the student's dean, there is sufficient and valid reason to complete the senior year elsewhere
    - students who have completed a minimum of three years of work at the University of Maine and who have been admitted to an accredited professional school of medicine, dentistry, veterinary medicine, or divinity. With the approval of the academic program faculty in consultation with the student's dean, these students may qualify for the appropriate bachelor's degree at the University of Maine upon receipt of the professional degree.

We will discuss the courses and any modifications necessary in much greater detail in Section 3. Tables 2 - 9 display a sample program.

Table 4: Sample Program for Fall of Year 2

COURSE	Credit Hours
COS 330 Introduction to Cybersecurity	3
COS 336 Cybersecurity Competition 1	1
General Education Electives	6
Electives	5
Total	15

Table 5: Sample Program for Spring of Year 2

COURSE	Credit Hours
COS 331 Operating Systems	3
ECE 331 Unix System Administration	3
General Education Electives	6
Electives	3
Total	15

Table 6: Sample Program for Fall of Year 3

COURSE	Credit Hours
ENG 317 Business and Technical Writing	3
COS 337 Cybersecurity Competition 2	1
COS 440 Computer Networking I	3
General Education Elective	3
Electives	5
Total	15

Table 7: Sample Program for Spring of Year 3

COURSE	Credit Hours
COS 480 Database Management Systems	3
General Education Elective	3
Electives	9
Total	15

Table 8: Sample Program for Fall of Year 4

COURSE	Credit Hours
COS 338 Cybersecurity Competition 3	1
COS 490 Computers, Ethics and Society 3	
COS 495 Field Experience	3
Electives	8
Total	15

Table 9: Sample Program for Spring of Year 4

COURSE	Credit Hours
COS 497 Computer Science Capstone 2	3
Electives	12
Total	15

2.3 General Education Requirements

We will now discuss how the proposed University of Maine B. S. in Cybersecurity satisfies the General Education Requirements of the University of Maine. We will summarize the discussion in the following list.

- *Science Requirement:* This will be met by the two General Education Science Electives shown in the Sample Program.
- *Human Values and Social Contexts Requirement:* This will be met by the six General Education Electives shown in the Sample Program.
- *Quantitative Literacy Requirement:* This will be met by the two required courses COS 220 Introduction to C++ Programming and MAT 232 Principles of Statistical Inference.
- *Writing Competency Requirement:* This will be met by ENG 101 College Composition, ENG 317 Business and Technical Writing and COS 490 Computers, Ethics and Society. Additionally, if we adjust matters so that COS 495 Field Experience can take the place of COS 397 Computer Science Capstone 1, then COS 495 Field Experience and COS 497 Computer Science Capstone 2 will also be counted toward this requirement. Since only two courses beyond ENG 101 are required we have this requirement covered even without COS 495 Field Experience and COS 497 Computer Science Capstone 2 and being counted.

Table 10: Possible University of Maine Minor in Cybersecurity

COURSE	Credit Hours
COS 140 Foundations of Computer Science	3
COS 220 Introduction to C++ Programming	3
COS 221 Data Structures in C++ Programming	3
COS 235 Computer Organization	4
COS 330 Introduction to Cybersecurity	3
COS 336 Cybersecurity Competition 1	1
ECE 331 Unix System Administration	3

- *Ethics Requirement:* COS 490 Computers, Ethics and Society covers this requirement.
- *Capstone Experience Requirement:* It is proposed that COS 495 Field Experience and COS 497 Computer Science Capstone 2 cover this requirement.

2.4 Cybersecurity Minor

We feel that we would also have a very attractive Cybersecurity Minor for students wishing to get some credentials in this area. A possible collection of courses for the minor is shown in Table 10

As proposed, the minor would require 20 credit hours. If COS 235 Computer Organization becomes a 3 credit course, the minor would require 19 credit hours.

3 Course Details

This section will illustrate the material that must be covered in each course that is part of the University of Maine B. S. in Cybersecurity. The purpose of this section is to help us understand which courses are most likely to cover which topics. It also tells whether the content of particular courses needs to be adjusted to support the University of Maine B. S. in Cybersecurity. For completeness we have included brief discussions of MAT 232 and ENG 317. It may also be necessary to change the scheduling of some courses to fit the sample program of study. Fortunately, the degree has a very flexible design.

3.1 MAT 232 - Principles of Statistical Inference

Below is the catalog description of MAT 232. It is followed by a discussion of the topics that need to be covered to meet the NSA requirements. We will review these topics with the Mathematics & Statistics faculty to make sure that everything is covered.

MAT 232 - Principles of Statistical Inference
Intended for students who will use statistics as an aid to the comprehension of quantitative work done by others and for students who will follow this course by an intermediate level applied statistics course. An introduction to the language and methods of statistical analysis, probability, graphic and numeric descriptive methods and inference from sample data. NOTE: because of overlap, MAT 232 and MAT 215 cannot both be taken for degree credit.
Satisfies the General Education Quantitative Literacy Requirement.
Prerequisites: Two years of high school math required.
Course Typically Offered: Fall, Spring, Summer
Credits: 3

3.2 NSA Knowledge Units Related to MAT(STS) 232

3.2.1 Requirements from KU Basic Data Analysis - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic abilities to manipulate data into meaningful information.

The following are the relevant topics for MAT(STS) 232

- Problem Solving

The following are the relevant outcomes for MAT(STS) 232

- Students will be able to apply standard statistical inference procedures to draw conclusions from data. This will be done using exams.

3.2.2 Requirements from KU Probability and Statistics - 4 YEAR

The intent of this Knowledge Unit is to provide students with the ability to use basic statistics to analyze and attach meaning to datasets.

The following are the relevant topics for MAT(STS) 232

- Probability Distributions

The following are the relevant outcomes for MAT(STS) 232

- Students will be able to evaluate probabilities to solve applied problems. This will be done using exams and homework.
- Students will be able to describe how basic statistics and statistical methods can be applied in a given situation. This will be done using exams and homework.

3.3 ENG 317 - Business and Technical Writing

There are no special NSA requirements for ENG 317 so we just present its catalog description.

> ENG 317 - Business and Technical Writing
> Supervised practice in the writing of business and technical reports, professional correspondence, and related materials.
> Satisfies the General Education Writing Intensive Requirement.
> Prerequisites: ENG 101 or equivalent and junior standing.
> Course Typically Offered: Fall, Spring, Summer
> Credits: 3

3.4 COS 140 Foundations of Computer Science

No substantive changes are necessary to COS 140. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course.

> COS 140 - Foundations of Computer Science
> Introduces students to the discipline of computer science. Several core areas of computer science (e.g., digital logic, computer organization and architecture, programming languages, operating systems, computer networks, artificial intelligence, and professional ethics) are covered. In each area, particular solutions to fundamental problems in the area are studied in depth. No programming is taught in the course.
> Course Typically Offered: Fall
> Credits: 3

3.5 NSA Knowledge Units Related to COS 140

3.5.1 Requirements from KU Basic Scripting - 2 YEAR

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

The following are the relevant topics for COS 140

- Basic Boolean logic/operations (AND / OR / XOR / NOT)

3.5.2 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant topics for COS 140

- Basic Boolean logic/operations(AND/OR/XOR/NOT).

3.6 COS 220 Introduction to C++ Programming

No substantive changes are necessary to COS 220. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course.

> COS 220 - Introduction to C++ Programming
> Topics include programming techniques with a brief introduction to hardware concepts as they apply to software development. Students are assigned programs emphasizing numerical algorithms for implementation in the C++ language. Assumes knowledge of the Windows operating system, basic word processing, and file and folder management. Some prior experience in programming logic, macros, or scripting is recommended.
> NOTE: Degree credit will not be given for both COS 220 and COS 215.
> General Education Requirements: Satisfies the General Education Quantitative Literacy Requirement.
> Course Typically Offered: Fall & Spring
> Credits: 3

3.7 NSA Knowledge Units Related to COS 220

3.7.1 Requirements from KU Basic Scripting - 2 YEAR

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

The following are the relevant topics for COS 220

- Basic Boolean logic/operations (AND / OR / XOR / NOT)

The following are the relevant outcomes for COS 220

- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL). This will be done using exams and homework.

3.7.2 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant topics for COS 220

- Basic Boolean logic/operations(AND/OR/XOR/NOT).

The following are the relevant outcomes for COS 220

- Students will be able to demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner. This will be done using exams and homework.
- Students will be able to demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web). This will be done using exams, homework and .

3.8 COS 221 Data Structures in C++ Programming

No substantive changes are necessary to COS 221. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course.

COS 221 - Data Structures in C++ This course introduces object-oriented programming techniques and data structures in C++. Topics include class design, dynamic memory management, lists, stacks, queues, trees. STL, algorithm efficiency, searching and sorting algorithms. Prerequisites: COS 220 or ECE 177. Course Typically Offered: Fall Credits: 3

3.9 NSA Knowledge Units Related to COS 221

3.9.1 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant outcomes for COS 221

- Students will be able to demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner. This will be done using exams and homework.
- Students will be able to demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web). This will be done using exams and homework.

3.10 COS 235 Computer Organization

No substantive changes are necessary to COS 235. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course. The online catalog is out of date and only has a course description for COS 335. We include it for reference since the COS 235 description will be similar once the website is updated.

COS 335 - Computer Organization and Architecture
Examines the architecture and organization of the computer including digital logic, the CPU, busses, internal and external memory, computer number representation and arithmetic, computer instructions and some advanced topics (e.g., RISC machines). Particular attention is paid to assembly language as a mechanism for better understanding the architecture, and students will be expected to write significant programs in assembly language.
Prerequisites COS 140 and COS 226.
Credits: 4

3.11 NSA Knowledge Units Related to COS 235

3.11.1 Requirements from KU IT System Components - 2 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

3.11.2 Requirements from KU System Administration - 2 YEAR

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

3.12 COS 330 Introduction to Cybersecurity

This would be a renumbering and redesign of an existing course, COS 430 Introduction to Cybersecurity. It would be designed so that second year students can take it and it would provide a better match with the NSA requirements. It would also include a cyberwar among the students as one of its requirements. The plan is to make this course available online. Also, this course will have to be offered on a regular basis, most likely every year.

COS 430 - Introduction to Cybersecurity
An overview of Cybersecurity as information security, policies, guidelines, and legal issues; the nature of network and computer attacks, system vulnerabilities and defense; implementation issues in Unix/Linux. Projects include system setup, attack, and defense.
Prerequisites: COS 335 and COS 431.
Course Typically Offered: Not Regularly Offered
Credits: 3

3.13 NSA Knowledge Units Related to COS 330

3.13.1 Requirements from KU Basic Scripting - 2 YEAR

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

The following are the relevant outcomes for COS 330

- Students will be able to demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks). This will be done using exams and homework.
- Students will be able to write simple linear and looping scripts. This will be done using exams and homework.

3.13.2 Requirements from KU Cyber Defense - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

The following are the relevant topics for COS 330

- Vulnerability Windows (0-day to patch availability)

The following are the relevant outcomes for COS 330

- Students will be able to describe potential system attacks and the actors that might perform them. This will be done using exams.
- Students will be able to describe cyber defense tools, methods and components. This will be done using exams.
- Students will be able to apply cyber defense methods to prepare a system to repel attacks. This will be done using cyberwar.
- Students will be able to describe appropriate measures to be taken should a system compromise occur. This will be done using exams.

3.13.3 Requirements from KU Cyber Threats - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

The following are the relevant topics for COS 330

- Threat Information Sources (e.g., CERT)

The following are the relevant outcomes for COS 330

- Students will be able to identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk. This will be done using cyberwar.
- Students will be able to describe different types of attacks and their characteristics. This will be done using exams.

3.13.4 Requirements from KU Fundamental Security Design Principles - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

The following are the relevant topics for COS 330

- Usability

The following are the relevant outcomes for COS 330

- Students will be able to list the first principles of security. This will be done using exams.
- Students will be able to describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies. This will be done using exams.
- Students will be able to analyze common security failures and identify specific design principles that have been violated. This will be done using exams and audits.
- Given a specific scenario, students will be able to identify the needed design principle. This will be done using exams and homeworks.
- Students will be able to describe why good human machine interfaces are important to system use. This will be done using exams and homeworks.
- Students will understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms This will be done using cyberwar and audits.

The following are the relevant resources for COS 330

- *The Protection of Information in Computer Systems* (Saltzer and Schroeder, 1975).
- Saltzer and Kaashoek (2009).
- *Computer Security Technology Planning Study* (Anderson Report, introduced the reference monitor concept).
- Bell-LaPadula Model (first multi-level security policy model).

- Biba Integrity Model.
- System Security Analysis/Certification (Clark Weissman, introduced the flaw hypothesis methodology).
- Security Controls for Computer Systems (Ware report, first raised computer security as an issue).
- *The Trusted Computer System Evaluation Criteria* (The "Orange Book").

3.13.5 Requirements from KU IA Fundamentals - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

The following are the relevant topics for COS 330

- Security Mechanisms (e.g., Identification/Authentication, Audit)

The following are the relevant outcomes for COS 330

- Students shall be able to list the fundamental concepts of the Information Assurance / Cyber Defense discipline. This will be done using exams.
- Students will be able to describe how the fundamental concepts of cyber defense can be used to provide system security. This will be done using exams.
- Students will be able to examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed. This will be done using cyberwar.

The following are the relevant resources for COS 330

- *Computer Security Art & Science* by Matt Bishop

3.13.6 Requirements from KU Introduction to Cryptography - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

The following are the relevant topics for COS 330

- Security Functions (data protection, data integrity, authentication)

The following are the relevant outcomes for COS 330

- Students will be able to identify the elements of a cryptographic system. This will be done using exams.
- Students will be able to describe the differences between symmetric and asymmetric algorithms. This will be done using exams.

- Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation. This will be done using exams.
- Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc. This will be done using exams and homeworks.

The following are the relevant resources for COS 330

- *Cryptography: A Very Short Introduction*, Piper and Murphy

3.13.7 Requirements from KU IT System Components - 2 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

The following are the relevant topics for COS 330

- Peripheral Devices/Security Peripherals

The following are the relevant outcomes for COS 330

- Students will be able to describe the hardware components of modern computing environments and their individual functions. This will be done using exams.

3.13.8 Requirements from KU Networking Concepts - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

The following are the relevant topics for COS 330

- Overview of Network Security Issues

The following are the relevant outcomes for COS 330

- Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks. This will be done using exams.
- Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection). This will be done using exams and homeworks.
- Students will be able to use a network monitoring tools (e.g., WireShark). This will be done using exams, homework and cyberwar.
- Students will be able to use a network mapping tool (e.g., Nmap). This will be done using exams, homework and cyberwar.

3.13.9 Requirements from KU Policy, Legal, Ethics, Compliance - 2 YEAR

The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

The following are the relevant outcomes for COS 330

- Students shall be able to describe their responsibilities related to the handling of information about vulnerabilities. This will be done using homework and exams.
- Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it. This will be done using exams and homework.

3.13.10 Requirements from KU System Administration - 2 YEAR

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

The following are the relevant topics for COS 330

- Security Policy Development

The following are the relevant outcomes for COS 330

- Students will be able to apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup. This will be done using cyberwar.

3.13.11 Requirements from KU Databases - 4 YEAR

The intent of this Knowledge Unit is to teach students how database systems are used, managed, and issues associated with protecting the associated data assets.

The following are the relevant topics for COS 330

- Common DBMS vulnerabilities

The following are the relevant outcomes for COS 330

- Students will be able to describe common security models of database management systems. This will be done using exams and homework.
- Students will be able to identify and describe common security concerns in database management systems. This will be done using homework, exams and cyberwar.

3.13.12 Requirements from KU Network Defense - 4 YEAR

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

The following are the relevant topics for COS 330

- Network Attacks (e.g., session hijacking, Man-in-the-Middle)

The following are the relevant outcomes for COS 330

- Students will be able to describe the various concepts in network defense. This will be done using exams and homework.
- Students will be able to apply their knowledge to implement network defense measures. This will be done using cyberwar.
- Students will be able to use a network monitoring tools (e.g., WireShark). This will be done using exams, homework and cyberwar.
- Students will be able to use a network mapping tool (e.g., Nmap). This will be done using exams, homework and cyberwar.

3.13.13 Requirements from KU Networking Technology and Protocols - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

The following are the relevant topics for COS 330

- Remote and Distributed Management

The following are the relevant outcomes for COS 330

- Students will be able to apply their knowledge of network technologies to design and construct a working network. This will be done using cyberwar.
- Students will be able to analyze a trace of packets to identify the establishment of a TCP connection. This will be done using homework.
- Students will be able to demonstrate the use of a network monitor to display packets. This will be done using cyberwar.

3.13.14 Requirements from KU Operating Systems Concepts - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

The following are the relevant topics for COS 330

- Fundamental Security Design Principles as applied to an OS

  - Domain separation, process isolation, resource encapsulation, least privilege

The following are the relevant outcomes for COS 330

- Students will be able to identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems). This will be done using homework and cyberwar.

3.13.15 Requirements from KU Probability and Statistics - 4 YEAR

The intent of this Knowledge Unit is to provide students with the ability to use basic statistics to analyze and attach meaning to datasets.

The following are the relevant outcomes for COS 330

- Students will be able to evaluate probabilities to solve applied problems. This will be done using exams and homework.
- Students will be able to describe how basic statistics and statistical methods can be applied in a given situation. This will be done using exams and homework.

3.13.16 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant outcomes for COS 330

- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL). This will be done using exams and homework.

3.13.17 Requirements from KU Advanced Network Technology & Protocols - Optional KU #1

The intent of this Knowledge Unit is to provide students with an understanding of the latest network technologies and more complex security issues involved in network communications. Examples include (but not limited to): software defined networking, converged voice/data networking.

The following are the relevant topics for COS 330

- Advanced Network Security Topics
  - Secure DNS
  - Network Address Translation
  - Deep Packet Inspection
  - Transport Layer Security

The following are the relevant outcomes for COS 330

- Students will be able to describe current networking technologies and trends. This will be done using exams and homework.
- Students will be able to describe and discuss data network architectures and protocols, to include their advantages and disadvantages, applications, and security issues. This will be done using exams and homework.

3.13.18 Requirements from KU Network Security Administration - Optional KU #2

The intent of this Knowledge Unit is to provide students with knowledge of the methods of analyzing and mitigating threats within a network environment.

The following are the relevant topics for COS 330

- Packet Capture and Analysis

The following are the relevant outcomes for COS 330

- Students will be able to appropriately position network security components within a network architecture to implement a layered defense. This will be done using cyberwar.
- Students will be able to securely configure network devices and services and establish secure communications between networks. This will be done using cyberwar.

3.13.19 Requirements from KU IA Compliance - Optional KU #3

The intent of this Knowledge Unit is to provide students with an understanding of the rules, regulations and issues related to compliance with applicable laws and regulations.

The following are the relevant topics for COS 330

- PCI DSS

The following are the relevant outcomes for COS 330

- Students shall be able to list the applicable laws for compliance in a given situation. This will be done using exams.
- Students shall be able to describe what the laws mandate and where they apply. This will be done using exams and homework.
- Students will be able to conduct audits to determine compliance with laws. This will be done using audits.

3.13.20 Requirements from KU IA Standards - Optional KU #4

The intent of this Knowledge Unit is to provide students with an understanding of the common standards related to information assurance.

The following are the relevant topics for COS 330

- Rainbow Series

The following are the relevant outcomes for COS 330

- Students will be able to describe the impact of legal/regulatory standards on a given system. This will be done using exams and homework.
- Students will be able to describe how standards, such as the Orange Book, may be applied to the requirements for a sub-contractor or customer. This will be done using audits.

3.13.21 Requirements from KU Operating Systems Theory - Optional KU #5

The intent of this Knowledge Unit is to provide students with an understanding of the issues related to the design and implementation of operating system concepts, components and interfaces.

The following are the relevant topics for COS 330

- Clear Interface Semantics

The following are the relevant outcomes for COS 330

- Students will have an understanding of operating systems theory and implementation. They will understand OS internals to the level that they can design and implement significant architectural changes to an existing OS. This will be done using exams and homework.

3.14 COS 331 Operating Systems

No substantive changes are necessary to COS 431. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course. It might also be necessary to schedule this course in the spring in the future.

COS 431 - Operating Systems Study of the structure of current computer operating systems. Topics include I/O management, memory management, multiprogramming, linking loaders, real and virtual systems, batch and time sharing. Prerequisites COS 226, COS 335 or permission. Credits: 3

3.15 NSA Knowledge Units Related to COS 331

3.15.1 Requirements from KU Cyber Defense - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

3.15.2 Requirements from KU Fundamental Security Design Principles - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

3.15.3 Requirements from KU System Administration - 2 YEAR

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

3.15.4 Requirements from KU Operating Systems Concepts - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

The following are the relevant topics for COS 331

- Fundamental Security Design Principles as applied to an OS
  - Domain separation, process isolation, resource encapsulation, least privilege

The following are the relevant outcomes for COS 331

- Students will be able to identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems). This will be done using homework.

3.15.5 Requirements from KU Operating Systems Theory - Optional KU #5

The intent of this Knowledge Unit is to provide students with an understanding of the issues related to the design and implementation of operating system concepts, components and interfaces.

The following are the relevant topics for COS 331

- Clear Interface Semantics

The following are the relevant outcomes for COS 331

- Students will have an understanding of operating systems theory and implementation. They will understand OS internals to the level that they can design and implement significant architectural changes to an existing OS. This will be done using exams and homework.

3.16 ECE 331 Unix System Administration

No substantive changes are necessary to ECE 331. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course.

> ECE 331 - Introduction to Unix Systems Administration
> Topics include hardware and devices, file systems, user management, backup and recovery, application management, and network services such as NFS, NIS, DNS, DHCP, electronic mail and web servers. Problem solving and diagnostic methods, performance tuning, legal and professional issues, ethics and policies and security aspects of hosts on the Internet are discussed. Students gain hands-on experience and complete a project.
> Prerequisites: COS 220 or ECE 177.
> Course Typically Offered: Spring
> Credits: 3

3.17 NSA Knowledge Units Related to ECE 331

3.17.1 Requirements from KU Basic Scripting - 2 YEAR

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

The following are the relevant outcomes for ECE 331

- Students will be able to demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks). This will be done using exams, homework and projects.
- Students will be able to write simple linear and looping scripts. This will be done using exams and homework.

3.17.2 Requirements from KU Cyber Defense - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

The following are the relevant outcomes for ECE 331

- Students will be able to apply cyber defense methods to prepare a system to repel attacks. This will be done using exams.
- Students will be able to describe appropriate measures to be taken should a system compromise occur. This will be done using exams.

3.17.3 Requirements from KU Cyber Threats - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

The following are the relevant outcomes for ECE 331

- Students will be able to identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk. This will be done using exams.
- Students will be able to describe different types of attacks and their characteristics. This will be done using exams.

3.17.4 Requirements from KU Fundamental Security Design Principles - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

The following are the relevant topics for ECE 331

- Usability

3.17.5 Requirements from KU IA Fundamentals - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

The following are the relevant topics for ECE 331

- Security Mechanisms (e.g., Identification/Authentication, Audit)

The following are the relevant outcomes for ECE 331

- Students shall be able to list the fundamental concepts of the Information Assurance / Cyber Defense discipline. This will be done using exams.
- Students will be able to describe how the fundamental concepts of cyber defense can be used to provide system security. This will be done using exams.
- Students will be able to examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed. This will be done using projects.

3.17.6 Requirements from KU Introduction to Cryptography - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

3.17.7 Requirements from KU IT System Components - 2 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

The following are the relevant topics for ECE 331

- Peripheral Devices/Security Peripherals

The following are the relevant outcomes for ECE 331

- Students will be able to describe the hardware components of modern computing environments and their individual functions. This will be done using exams.

3.17.8 Requirements from KU Networking Concepts - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

The following are the relevant topics for ECE 331

- Overview of Network Security Issues

The following are the relevant outcomes for ECE 331

- Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks. This will be done using exams.

3.17.9 Requirements from KU System Administration - 2 YEAR

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

The following are the relevant topics for ECE 331

- Security Policy Development

The following are the relevant outcomes for ECE 331

- Students will be able to apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup. This will be done using homework.

3.17.10 Requirements from KU Databases - 4 YEAR

The intent of this Knowledge Unit is to teach students how database systems are used, managed, and issues associated with protecting the associated data assets.

3.17.11 Requirements from KU Network Defense - 4 YEAR

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

The following are the relevant topics for ECE 331

- Network Attacks (e.g., session hijacking, Man-in-the-Middle)

The following are the relevant outcomes for ECE 331

- Students will be able to describe the various concepts in network defense. This will be done using exams and homework.
- Students will be able to apply their knowledge to implement network defense measures. This will be done using homework and projects.
- Students will be able to use a network monitoring tools (e.g., WireShark). This will be done using homework.
- Students will be able to use a network mapping tool (e.g., Nmap). This will be done using homework.

3.17.12 Requirements from KU Networking Technology and Protocols - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

The following are the relevant topics for ECE 331

- Remote and Distributed Management

3.17.13 Requirements from KU Operating Systems Concepts - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

The following are the relevant topics for ECE 331

- Fundamental Security Design Principles as applied to an OS
  - Domain separation, process isolation, resource encapsulation, least privilege

3.17.14 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant outcomes for ECE 331

- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL). This will be done using exams and homework.

3.17.15 Requirements from KU Advanced Network Technology & Protocols - Optional KU #1

The intent of this Knowledge Unit is to provide students with an understanding of the latest network technologies and more complex security issues involved in network communications. Examples include (but not limited to): software defined networking, converged voice/data networking.

The following are the relevant topics for ECE 331

- Advanced Network Security Topics
  - Secure DNS
  - Network Address Translation
  - Deep Packet Inspection
  - Transport Layer Security

3.17.16 Requirements from KU Network Security Administration - Optional KU #2

The intent of this Knowledge Unit is to provide students with knowledge of the methods of analyzing and mitigating threats within a network environment.

The following are the relevant topics for ECE 331

- Packet Capture and Analysis

3.17.17 Requirements from KU IA Standards - Optional KU #4

The intent of this Knowledge Unit is to provide students with an understanding of the common standards related to information assurance.

The following are the relevant outcomes for ECE 331

- Students will be able to describe the impact of legal/regulatory standards on a given system. This will be done using exams and homework.

3.17.18 Requirements from KU Operating Systems Theory - Optional KU #5

The intent of this Knowledge Unit is to provide students with an understanding of the issues related to the design and implementation of operating system concepts, components and interfaces.

The following are the relevant topics for ECE 331

- Clear Interface Semantics

3.18 COS 336-338 Cybersecurity Competitions

COS 336-338 Cybersecurity Competitions would be three 1-credit courses that would be available online. Their goal is to provide some background on topics students encounter in cybersecurity competitions. Initially the courses will work with the National Cyberleague's (`http://www.nationalcyberleague.org/index.shtml`) Cyber Challenge Competition which features both individual and team competitions. Students would be required to compete in both types of competitions. To earn credit for all of COS 336-338 Cybersecurity Competitions students would need to keep performing at an ever more challenging level. For example, the NCL Cyber Challenge has competitions at the Bronze, Silver and Gold levels. Students who want to take COS 337 Cybersecurity Competition 2 must have earned at least Silver level status in COS 336 Cybersecurity Competition 1. Similarly, students who want to take COS 338 Cybersecurity Competition 3 must have attained at least the Gold level of competition in COS 337 Cybersecurity Competition 2. We give more complete course descriptions of COS 336-338 Cybersecurity Competitions in Section 4.

3.19 NSA Knowledge Units Related to COS 336-338

3.19.1 Requirements from KU Cyber Defense - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

3.19.2 Requirements from KU IA Fundamentals - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

3.19.3 Requirements from KU Introduction to Cryptography - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

The following are the relevant topics for COS 336-338

- Security Functions (data protection, data integrity, authentication)

The following are the relevant outcomes for COS 336-338

- Students will be able to identify the elements of a cryptographic system. This will be done using competition.
- Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation. This will be done using debriefing notes.

3.19.4 Requirements from KU IT System Components - 2 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

The following are the relevant topics for COS 336-338

- Peripheral Devices/Security Peripherals

3.19.5 Requirements from KU Networking Concepts - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

The following are the relevant topics for COS 336-338

- Overview of Network Security Issues

The following are the relevant outcomes for COS 336-338

- Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection). This will be done using competition.
- Students will be able to use a network monitoring tools (e.g., WireShark). This will be done using competition.
- Students will be able to use a network mapping tool (e.g., Nmap). This will be done using competitions.

3.19.6 Requirements from KU System Administration - 2 YEAR

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

3.19.7 Requirements from KU Databases - 4 YEAR

The intent of this Knowledge Unit is to teach students how database systems are used, managed, and issues associated with protecting the associated data assets.

The following are the relevant topics for COS 336-338

- Common DBMS vulnerabilities

The following are the relevant outcomes for COS 336-338

- Students will be able to describe common security models of database management systems. This will be done using competitions.

3.19.8 Requirements from KU Network Defense - 4 YEAR

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

The following are the relevant topics for COS 336-338

- Network Attacks (e.g., session hijacking, Man-in-the-Middle)

The following are the relevant outcomes for COS 336-338

- Students will be able to use a network monitoring tools (e.g., WireShark). This will be done using competitions.
- Students will be able to use a network mapping tool (e.g., Nmap). This will be done using competitions.

3.19.9 Requirements from KU Networking Technology and Protocols - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

The following are the relevant topics for COS 336-338

- Remote and Distributed Management

3.19.10 Requirements from KU Operating Systems Concepts - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

3.19.11 Requirements from KU Advanced Network Technology & Protocols - Optional KU #1

The intent of this Knowledge Unit is to provide students with an understanding of the latest network technologies and more complex security issues involved in network communications. Examples include (but not limited to): software defined networking, converged voice/data networking.

The following are the relevant topics for COS 336-338

- Advanced Network Security Topics
  - Secure DNS
  - Network Address Translation
  - Deep Packet Inspection
  - Transport Layer Security

3.19.12 Requirements from KU Network Security Administration - Optional KU #2

The intent of this Knowledge Unit is to provide students with knowledge of the methods of analyzing and mitigating threats within a network environment.

The following are the relevant topics for COS 336-338

- Packet Capture and Analysis

3.19.13 Requirements from KU Operating Systems Theory - Optional KU #5

The intent of this Knowledge Unit is to provide students with an understanding of the issues related to the design and implementation of operating system concepts, components and interfaces.

The following are the relevant topics for COS 336-338

- Clear Interface Semantics

3.20 COS 440 Computer Networking I

No substantive changes are necessary to COS 440 Computer Networking I. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course. Note that the COS 440 Computer Networking I course description needs to be update at least as far as requiring COS 331 Operating Systems and not COS 431.

COS 440 - Computer Networks I Covers data and computer communications using ISO model. Discussion of physical media, communication protocols, and network architectures including wide area and local area networks. Includes examples of networks currently in use. Prerequisites: COS 431 or permission. Course Typically Offered: Fall Credits: 3

3.21 NSA Knowledge Units Related to COS 440

3.21.1 Requirements from KU Cyber Defense - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

3.21.2 Requirements from KU Cyber Threats - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

3.21.3 Requirements from KU Fundamental Security Design Principles - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

The following are the relevant topics for COS 440

- Usability

3.21.4 Requirements from KU IA Fundamentals - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

3.21.5 Requirements from KU Introduction to Cryptography - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

3.21.6 Requirements from KU IT System Components - 2 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

The following are the relevant topics for COS 440

- Peripheral Devices/Security Peripherals

The following are the relevant outcomes for COS 440

- Students will be able to describe the hardware components of modern computing environments and their individual functions. This will be done using exams.

3.21.7 Requirements from KU Networking Concepts - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

The following are the relevant topics for COS 440

- Overview of Network Security Issues

The following are the relevant outcomes for COS 440

- Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks. This will be done using exams.
- Students will be able to describe a basic network architecture given a specific need and set of hosts/clients. This will be done using projects.

- Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection). This will be done using exams and homeworks.
- Students will be able to use a network monitoring tools (e.g., WireShark). This will be done using exams and homework.
- Students will be able to use a network mapping tool (e.g., Nmap). This will be done using exams and homework.

3.21.8 Requirements from KU System Administration - 2 YEAR

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

3.21.9 Requirements from KU Network Defense - 4 YEAR

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

The following are the relevant topics for COS 440

- Network Attacks (e.g., session hijacking, Man-in-the-Middle)

The following are the relevant outcomes for COS 440

- Students will be able to describe the various concepts in network defense. This will be done using exams and homework.
- Students will be able to use a network monitoring tools (e.g., WireShark). This will be done using homework.
- Students will be able to use a network mapping tool (e.g., Nmap). This will be done using exams and homework.

3.21.10 Requirements from KU Networking Technology and Protocols - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

The following are the relevant topics for COS 440

- Remote and Distributed Management

The following are the relevant outcomes for COS 440

- Students will be able to apply their knowledge of network technologies to design and construct a working network. This will be done using projects.
- Students will be able to analyze a trace of packets to identify the establishment of a TCP connection. This will be done using homework.

3.21.11 Requirements from KU Operating Systems Concepts - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

3.21.12 Requirements from KU Advanced Network Technology & Protocols - Optional KU #1

The intent of this Knowledge Unit is to provide students with an understanding of the latest network technologies and more complex security issues involved in network communications. Examples include (but not limited to): software defined networking, converged voice/data networking.

The following are the relevant topics for COS 440

- Advanced Network Security Topics
  - Secure DNS
  - Network Address Translation
  - Deep Packet Inspection
  - Transport Layer Security

The following are the relevant outcomes for COS 440

- Students will be able to describe current networking technologies and trends. This will be done using exams and homework.
- Students will be able to describe and discuss data network architectures and protocols, to include their advantages and disadvantages, applications, and security issues. This will be done using exams and homework.

3.21.13 Requirements from KU Network Security Administration - Optional KU #2

The intent of this Knowledge Unit is to provide students with knowledge of the methods of analyzing and mitigating threats within a network environment.

The following are the relevant topics for COS 440

- Packet Capture and Analysis

The following are the relevant outcomes for COS 440

- Students will be able to appropriately position network security components within a network architecture to implement a layered defense. This will be done using projects.
- Students will be able to securely configure network devices and services and establish secure communications between networks. This will be done using exams and homework.

3.22 COS 480 Database Management Systems

This course currently requires COS 350 as a prerequisite. Perhaps this can be changed. It might also be possible to redesign the course and perhaps move it to the 300 level, maybe even a COS 380. In any event, there needs to be some discussion on how to best utilize this course in the new program.

COS 480 - Database Management Systems Covers database management systems from the perspective of database designers and database application programmers. Topics include Entity-Relationship modeling, relational databases, transactions and isolation, and Web-database applications. Includes both individual programming assignments and semester-long group projects culminating in demonstrations of substantial database application. Prerequisites: COS 350 or permission. Course Typically Offered: Fall Credits: 3

3.23 NSA Knowledge Units Related to COS 480

3.23.1 Requirements from KU Databases - 4 YEAR

The intent of this Knowledge Unit is to teach students how database systems are used, managed, and issues associated with protecting the associated data assets.

The following are the relevant topics for COS 480

- Common DBMS vulnerabilities

The following are the relevant outcomes for COS 480

- Students will be able to describe common security models of database management systems. This will be done using exams.
- Students will be able to identify and describe common security concerns in database management systems. This will be done using exams.
- Students will be able to apply security principles to the design and development of database systems and database structures. This will be done using homework.

3.23.2 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant outcomes for COS 480

- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL). This will be done using exams and homework.

3.24 COS 490 Computers, Ethics and Society

No substantive changes are necessary to COS 431. It is necessary to double check that the NSA requirements attributed to this course are actually covered by the course.

COS 490 - Computers, Ethics and Society Consideration of human and social consequences of technological development and application of computers, ethical questions of computer use, professional ethics. General Education Requirements: Satisfies the General Education Ethics and Writing Intensive Requirements. Prerequisites: COS 431, ENG 317. Course Typically Offered: Fall Credits: 3

3.25 NSA Knowledge Units Related to COS 490

3.25.1 Requirements from KU Cyber Threats - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

3.25.2 Requirements from KU Policy, Legal, Ethics, Compliance - 2 YEAR

The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

The following are the relevant topics for COS 490

- Americans with Disabilities Act, Section 508

The following are the relevant outcomes for COS 490

- Students shall be able to list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data. This will be done using exams and papers.
- Students shall be able to describe their responsibilities related to the handling of information about vulnerabilities. This will be done using papers.
- Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it. This will be done using papers.

3.25.3 Requirements from KU IA Compliance - Optional KU #3

The intent of this Knowledge Unit is to provide students with an understanding of the rules, regulations and issues related to compliance with applicable laws and regulations.

The following are the relevant topics for COS 490

- PCI DSS

The following are the relevant outcomes for COS 490

- Students shall be able to list the applicable laws for compliance in a given situation. This will be done using exams.
- Students shall be able to describe what the laws mandate and where they apply. This will be done using exams and papers.

3.25.4 Requirements from KU IA Standards - Optional KU #4

The intent of this Knowledge Unit is to provide students with an understanding of the common standards related to information assurance.

The following are the relevant topics for COS 490

- Rainbow Series

3.26 COS 495 Field Experience

COS 495 would need to be added to the program with the stipulation that the Field Experience would have to be in a cybersecurity setting. Students could work for the university, government or commercial sectors. COS 495 would need to incorporate the aspects of COS 397 (shown below) to make sure that it integrates with COS 497. We would need approval for the COS 495 and COS 497 sequence to count as a Capstone Experience and be an alternative to the COS 397 and COS 497 sequence. To adapt this to the Cybersecurity requirements we would have to require that it be in a position that was primarily in cybersecurity. Most likely we would need to revise the statement that it be in a commercial environment since government and university environments would be suitable as well. Finally, I would like to argue that participating in a high level and intensive event such as the Northeast Collegiate Cyber Defense Competition be eligible. This would require turning the team preparation into a course.

COS 495 - Field Experience
A pre-planned work experience of no less than ten and preferably more weeks in a commercial environment, with faculty supervision. Normally a paid work experience. A presentation open to interested faculty, staff and students might be required at the completion of the project. May be repeated for a maximum of 3 credit hours. (Pass/Fail Grade Only.)
General Education Requirements: Satisfies the General Education Capstone Experience Requirement.
Prerequisites: Normally a student must complete COS 301, COS 420, COS 431 and preferably COS 350, with at least a grade of "C" and permission.
Course Typically Offered: Not Regularly Offered
Credits: 1-3

COS 397 - Computer Science Capstone 1
The first of a two-course sequence, designed to guide students in proposing the Capstone project in either an independent study, group project, or field experience format. The focus is on the early stages of project work, including finding a suitable topic and project advisor, investigating related work, and writing a thorough project proposal. The relevant skills are covered and practiced by studying a collection of classic and topical papers.
General Education Requirements: Upon completion of the two course sequence (COS 397 & COS 497), satisfies the General Education Writing Intensive and Capstone Experience Requirements.
Prerequisites: COS Majors with at least Junior standing and permission.
Course Typically Offered: Fall
Credits: 3

3.27 NSA Knowledge Units Related to COS 495

3.27.1 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant outcomes for COS 495

- Students will be able to demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web). This will be done using employer evaluation.

3.28 COS 497 Computer Science Capstone 2

COS 497 usually pairs with COS 397 to provide the Capstone Experience for CS majors. We propose that a sequence of a redesigned COS 495 and COS 497 be accepted as an alternative Capstone Experience.

COS 497 - Computer Science Capstone 2
The second of a two-course sequence, designed to guide students in completing the Capstone project in either an independent study, group project, or field experience format. The focus is on the later stages of project work, including completing the programming tasks, evaluating the implemented systems, documenting all work in a project report, demonstrating the work in action, and making a public oral presentation. The relevant skills are covered and practiced by studying a collection of classic and topical papers.
General Education Requirements: Upon completion of the two course sequence (COS 397 & COS 497), satisfies the General Education Writing Intensive and Capstone Experience Requirements.
Prerequisites: COS Majors with Senior standing, COS 397, and permission.
Course Typically Offered: Spring
Credits: 3

We would need to make sure that the COS 495 Field Experience (in Cybersecurity) would serve as an adequate substitute for COS 397 Computer Science Capstone 1.

3.29 NSA Knowledge Units Related to COS 497

3.29.1 Requirements from KU Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

The following are the relevant outcomes for COS 497

- Students will be able to demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web). This will be done using the final project evaluation.

4 Course Proposals and Modifications

4.1 COS 330 Introduction to Cybersecurity- Modification

The COS 330 Introduction to Cybersecurity course modification form is on the following pages.

THE UNIVERSITY OF MAINE

Modification Form

DEPARTMENT: CIS
COURSE DESIGNATOR: COS 430
COURSE TITLE: Introduction to Cybersecurity

COLLEGE: CLAS
PROPOSED COURSE #: COS 330
EFFECTIVE SEMESTER: Fall 2015

Requested Action: **Note: A complete Syllabus is required for all new courses, including travel-study courses offered through CED or Summer Session and for the addition General Education and/or travel-study to an existing course. Please be sure that all elements required for a syllabus at the University of Maine are present. We recommend you work closely with the syllabus check list found at www.umaine.edu/upcc.**

Please check all that apply *(Please note if you are making a substantial modifications you may want to consider creating a new course)*

Designator Change		Credit Change	
Cross Listing		Number Change	X
Title Change		Description Change	
Prerequisite Change		Travel Study	
Addition of Elec. Learning Component	X	Conversion of an existing onsite Course to an online Course	
Other (Please Explain)		Addition of Gen Ed (Complete Section 2. Please see additional information on www.umaine.edu/upcc)	

ENDORSEMENTS *(Please Print and Sign Name)* **DATE**

Leader, Initiating Department/Unit(s)

College(s) Curriculum Committee Chair(s)

Dean(s)

Associate Provost for Undergraduate Education

CURRENT CATALOG DESCRIPTION (Include designator, number, title, prerequisites, credit hours):
COS 430 - Introduction to Cybersecurity

An overview of Cybersecurity as information security, policies, guidelines, and legal issues; the nature of network and computer attacks, system vulnerabilities and defense; implementation issues in Unix/Linux. Projects include system setup, attack, and defense.

Prerequisites: COS 335 and COS 431.

Course Typically Offered: Not Regularly Offered

Credits: 3

PROPOSED CATALOG DESCRIPTON (Include designator, number, title prerequisites, credit hours):
COS 330 - Introduction to Cybersecurity

An overview of Cybersecurity as information security, policies, guidelines, and legal issues; the nature of network and computer attacks, system vulnerabilities and defense; implementation issues in Unix/Linux. Projects include system setup, attack, and defense.

Prerequisites: COS 220 and COS 235.

Course Typically Offered: Fall

Credits: 3

REASON FOR COURSE MODIFICATION:
This course needs to move earlier to be used in the University of Maine B. S. in Cybersecurity. It is important that this course be taken before COS 331 Operating Systems and ECE 331 Unix System Administration. It can also be taken earlier by students in the regular B. S. program. Also, we are planning to offer our cybersecurity oriented courses online to support the University of Maine System B. S. in Cybersecurity initiative.

INSTRUCTOR: Dr. George Markowsky

Does this change in course prefix, number/or credit hours affect any prerequisite? If yes, please list course(s):
COS 430 is not a prerequisite for any course and COS 330 will also not be a prerequisite for any course.

For Addition of Electronic Learning Component:

If adding an electronic component to a regularly scheduled, on site course, please indicate the following:

FirstClass Conferencing	
Blackboard	*Yes*
Other Course Management Software/Online Delivery Platform	

Broadband Connection Necessary to Access Course Materials? Yes No

PLEASE CHECK ALL THOSE THAT APPLY:

Adobe Connect	
Skype	
Polycom	
Video Conferencing	
Other	X

REAL TIME PARTICIPATION EXPECTED/REQUIRED?
The class will be offered onsite and an audio feed will be provided to offsite students. They will have access to all the materials that will be presented in class. There will also be a variety of items that all students will have to do online.

PERCENTAGE OF COURSE TO BE DELIVERED ELECTRONICALLY? 50% - 100%?
The material will be presented in-class to the extent that it makes sense. Activities such as the cyberwars will be done using cloud services so all students will have to learn to use those services. This would be done in the natural evolution of cybersecurity. In some sense all the material will be available both in class and online.

49% or LESS?

IF CONVERTING AN EXISTING ON SITE COURSE TO AN ONLINE COURSE, PLEASE INDICATE THE PEDAGOGICAL CHANGES EMPLOYED TO ADAPT YOUR COURSE TO AN ONLINE FORMAT:

The course will make extensive use of cloud-based resources which it would do even if it were not being modified for the B. S. in Cybersecurity.

4.2 COS 336-338 Cybersecurity Competitions - New Courses

One new course form covers all three courses. The idea is that so much of the material is already online and the cyber competitions are completely online so the students will be enrolled at the level that is appropriate for the student. All students taking the competition the first time will be enrolled in COS 336. Those who have completed COS 336 and reached at least the second level of competition (typically called Silver) will be allowed to register for COS 337. Only those students who reach the third level of competition (typically called Gold) will be allowed to register for COS 338. The new course form is on the subsequent pages followed by the syllabus.

4.2.1 COS 336-338 Cybersecurity Competitions New Course Proposal

The following pages include the new course proposal for COS 336-338 Cybersecurity Competitions.

New Course Proposal

DEPARTMENT: CIS
COLLEGE: CLAS
COURSE DESIGNATOR: COS 336, COS 337, COS 338
PROPOSED COURSE #: COS 336, COS 337, COS 338
COURSE TITLE: Cybersecurity Competition 1, 2 and 3
EFFECTIVE SEMESTER: FALL 2015

Requested Action: Note: A complete Syllabus is required for all new courses, including travel-study courses offered through CED or Summer Session and for the addition General Education and/or travel-study to an existing course. Please be sure that all elements required for a syllabus at the University of Maine are present. We recommend you work closely with the syllabus check list found at www.umaine.edu/upcc.

NEW COURSE: (check all that apply and complete Section 1):

_X_ New Course ___ One-time course w/GenEd ___ New Course/GenEd (Complete Section 2)

___ One-time Course ___ Experimental ____ Travel Study Course

ENDORSEMENTS *(Please Print and Sign Name)* DATE
Leader, Initiating Department/Unit(s)

College(s) Curriculum Committee Chair(s)

Dean(s)

Associate Provost for Undergraduate Education

Section 1

If more writing space is required please staple additional pages to the end of this document

** When determining the number of credit hours for your course please note the Definition of an Undergraduate Student Credit Hour as published in the Undergraduate Catalog:

Definition of an Undergraduate Student Credit Hour: The University of Maine defines a Student Credit Hour in an undergraduate program as an expectation, on average, of approximately 45 clock hours of student academic engagement per credit hour per course. Student Academic Engagement in a course can take many forms including, but not limited to: class time, testing, reading, writing, studying, discussion group time, laboratory work, internships, practica, practicing, performing or otherwise working on course content. **

PROPOSED CATALOG DESCRIPTION (INCLUDE DESIGNATOR, NUMBER, TITLE, PREREQUISITES, CREDIT HOURS):

COS 336 Cybersecurity Competition 1
This course prepares the student for competition in the National Cyberleague Cyber Challenge Competition of some similar competition. Topics include cryptography, network scanning, packet capturing and analysis, system configuration, and team formation. Student must be available for all the scheduled competitions which might involve participating on the weekend. The critical dates will be available at the time of registration. Students will be responsible for the registration fees which typically range from $20-$30.

Prerequisites: COS 221 and a co-requisite of COS 330, or permission.

Course Typically Offered: Fall

Credits: 1

COS 337 Cybersecurity Competition 2
This course prepares the student for competition in the National Cyberleague Cyber Challenge Competition of some similar competition. Topics include cryptography, network scanning, packet capturing and analysis, system configuration, and team formation. Student must be available for all the scheduled competitions which might involve participating on the weekend. The critical dates will be available at the time of registration. Students will be responsible for the registration fees which typically range from $20-$30.

Prerequisites: COS 336 and the ability to compete at an intermediate level (Silver) or permission.

Course Typically Offered: Fall

Credits: 1

COS 338 Cybersecurity Competition 3
This course prepares the student for competition in the National Cyberleague Cyber Challenge Competition of some similar competition. Topics include cryptography, network scanning, packet capturing and analysis, system configuration, and team formation. Student must be available for all the scheduled competitions which might involve participating on the weekend. The critical dates will be available at the time of registration. Students will be responsible for the registration fees which typically range from $20-$30.

Prerequisites: COS 337 and the ability to compete at the top level (Gold) or permission.

Course Typically Offered: Fall

Credits: 1

REASON FOR NEW COURSE (Elective?, Free Elective? Part of Core Curriculum? How will this course be used as part of your departments curriculum?)
These courses are a required part of the B. S. in Cybersecurity that has been proposed and for which an extensive course proposal is available.

COMPONENTS (TYPE OF COURSE/USED BY STUDENT RECORDS FOR MaineStreet)
Please check ONLY ONE box unless the proposed course will have multiple non-graded components:

Applied Music		Lecture	
Clinical		Recitation	
Field Experience/Internship		Research	
Independent Study		Seminar	
Laboratory		Studio	

IF CREATING A NEW DISTANCE LEARNING COURSE USING ANY COMBINATION OF ONSITE, SYNCHRONOUS, or ASYNCHRONOUS DELIVERY, PLEASE DESCRIBE CLEARLY:

Synchronous:

Asynchronous:

Hybrid Course: *There will be classroom lectures to which students can connect remotely. There will be many online laboratories and the competitions will all be online.*

Location Offered: *University of Maine*

Mode(s) of Delivery: *Lecture and online.*

Technology Required: *Students will have to have access to a personal computer.*

OTHER SPECIFIC INFORMATION:

Can this course be repeated for credit? Yes No (If no please skip the next two questions)

If YES, total number of credits allowed: _____ If YES, total number of completions allowed: _____

Can students enroll multiple times in term? Yes No

When will this course typically be offered? (Please Choose One)

Alternative Years		Spring Semesters (odd numbered years)	
Every Year		Spring Semesters	
Fall Semesters	x	Spring and Summer Semesters	
Fall Semesters (even numbered years)		Summer Semesters	
Fall Semesters (odd numbered years)		Summer Semesters (even numbered years)	
Fall and Summer Semesters		Summer and Fall Semesters (odd numbered years)	
Fall, Spring and Summer Semesters		Summer and Fall Semesters (even numbered years)	
Not Regularly Offered		Variable	
Spring Semesters (even numbered years)		Other (Please Describe)	

TEXT(s) PLANNED FOR USE: (if more room is needed please attach a separate page)
The course will use the extensive battery of online laboratories and exercises as well as the current competition. There will be suggested references provided, most of which will be available online at little of no cost.

COURSE INSTRUCTOR: (Include name, position and teaching load)
Prof. George Markowsky

DOES THE COURSE ADDITION REQUIRE ADDITIONAL DEPARTMENT OR INSTITUTIONAL FACILITIES, SUPPORT AND/OR RESOURCES, e.g. NEW LAB FACILIITES, COMPUTER SUPPORT AND SERVICES< STAFFING or LIBRARY SUBSCRIPTIONS AND RESOURCES?

_____ No. The department will not request additional resources for this course, now or in the future, unless the request is accompanied by an explanation of how the increased funding or other support is to be provided.

__X__ Yes. Please list additional resources required and note how they will be funded or supported
The idea is that COS 336, COS 337 and COS 338 could be taught as a single 1-credit course. The actual labs would be tailored to the skill level of the student. This course might be part of someone's regular load or it might require section funding for a 1-credit course.

DOES THE CONTENT OF THIS COURSE OVERLAP SIGNIFICANTLY WITH OTHER UNIVERSITY COURSES? IF SO, LIST THE COURSES, EXPLAIN THE OVERLAP, AND JUSTIFY THE NEED FOR THE PROPOSED COURSE

NO

WHAT OTHER DEPARTMENTS/PROGRAMS ARE AFFECTED? HAVE AFFECTED DEPARTMENTS/PROGRAMS BEEN CONSULTED? ANY CONCERNS EXPRESSED? Please Explain.
No other departments are affected.

WILL ANY COURSE(S) BE DROPPED OR OFFERED LESS FREQUENTLY TO ACCOMMODATE THE PROPOSED COURSE IN THE SCHEDULE? IF SO, EXPLAIN.

No. This will be an additional course that will need to be covered.

WILL OFFERING THIS COURSE RESULT IN OVERLOAD SALARY PAYMENTS, EITHER THROUGH THE COLLEGE OR CED, EITHER TO THE INSTURCTOR OF THIS COURSE OR TO ANYONE ELSE AS A RESULT OF REARRANGING TEACHING ASSIGNMENTS? IF YES, PLEASE EXPLAIN:

This was already covered above.

4.2.2 COS 336-338 Cybersecurity Competitions Syllabi

The following pages include the syllabi for COS 336-338 Cybersecurity Competitions. This will be customized each time the course will be offered since the competition and the laboratories are likely to change. They will also have to be tailored to the competition levels announced for the particular competition season.

COS 336-338 CYBERSECURITY COMPETITIONS

George Markowsky
Computer Science Department
University of Maine

GOALS

1. To provide you with the background to compete in the National Cyberleague Cyber Challenge Competition or similar competition.
2. To make sure that you know how to use some of the standard tools of cybersecurity such as Nmap and Wireshark that will be used in the competition.
3. To help you better understand the nature of cyber defense and cyber attack.
4. To give you some experience in team competition and cooperation.

PREREQUISITES

COS 220 and COS 235, or permission for COS 336.

COS 336 and the ability to compete at the intermediate (Silver) level for COS 337.

COS 337 and the ability to compete at the top (Gold) level for COS 338.

GRADING

Cheating has become all too common in contemporary academic settings. I am very much opposed to it because it keeps people from acquiring the skills that are taught in the course. Furthermore, as you will see, cybersecurity depends on trusting individuals to protect cyber-assets. It should be clear that people who cheat in their cybersecurity course are not worthy of passing the course since they are not developing the skills that they need and are not demonstrating the high level of integrity that is necessary to be effective in this area. Cheating will be dealt with severely in this course.

1. I will use +/- grading in the class. The grades will be assigned on the basis of your **final class average** based on the following ranges:

A	90 or above	C	70 to 72
A-	85 to 89	C-	65 to 69
B+	83 or 84	D+	63 or 64
B	80 to 82	D	60 to 62
B-	75 to 79	D-	55 to 59
C+	73 or 74	E	54 or below

2. The grade will be based on the number of laboratories completed and the results achieved on the competitions. More details will be supplied each semester when it becomes clear what labs are available and exactly how the competitions will be scored that semester.

3. All numbers are rounded and the letter grades are assigned according the scale mentioned in 1.

OFFICE HOURS

TBD

If you have problems with this course and need help come in to see me immediately. Don't fool around until the end of the semester and then try to learn all the material in a week.

TEACHING ASSISTANT

TBD – It might be possible to run this course without a teaching assistant.

TEXTBOOKS

Online laboratories and materials.

COS 336-338 SCHEDULE

This course will most likely be scheduled once a week in the evening for 3 hours each time. There will only be 5 lectures and then the competitions.

Lecture 1: Introduction to the competition, the range of problems to be considered, introduction and review of common protocols.

Lecture 2: Introduction to Nmap and Wireshark. Packet capturing and analysis. Essential network security.

Lecture 3: Encoding and encryption, password cracking, recognition of encoding and decoding schemes.

Lecture 4: Reconnaissance of computer sites, threats and vulnerabilities, review of past problems.

Lecture 5: Team formation and operation, access control and identity management, firewall configuration, final preparation for the competitions.

There will be opportunities for informal debriefings between competitions. These will be set up based on the interests and availability of the students.

4.2.3 COS 336-338 Cybersecurity Competitions Supporting Material - CompTIASecurity+^{TM} Syllabus

The two syllabi presented on the following pages along with the NSA required topics motivated the proposed syllabus for COS 336-338 Cybersecurity Competitions.

The National Cyber League – Where Cybersecurity is a Passion

National Cyber League
CompTIA Security+™ Syllabus

Note to Faculty

This NCL Syllabus is intended as a supplement to courses that are based on the CompTIA Security+™ curriculum/exam, or courses that include similar knowledge and skills.

A primary goal of the NCL is to seamlessly integrate hands-on lab exercises and challenging cybersecurity games into higher education curriculum. The NCL uses a game analogy to describe our events because we believe that we are providing a fun environment that allow students (AKA **players**) to test their knowledge and skills against other players - just like a game!

This NCL Syllabus is not intended as a replacement to an existing course, but can provide supplemental hands-on lab exercises aligned with the NCL games. We encourage college faculty (AKA **coaches**) to look at ways to include this syllabus as part of the lab component of their course(s). While CompTIA Security+™ and EC-Council Certified Ethical Hacker (CEH)™ performance-based exam objectives are the foci of the 2014 NCL Fall Season, faculty and students in related security courses can also benefit from adding hands-on labs and NCL games as part of their course assignments. As educators, we understand the importance of aligning exercises to an academic calendar (e.g., semesters). We welcome feedback to help us to best support faculty and their instructional goals.

Network Development Group (NDG) collaborated with the Center for Systems Security and Information Assurance (CSSIA) to create a series of lab exercises intended to support the Security+™ curriculum. As an NDG partner, the NCL is able to take full advantage of this collaboration and offer these excellent hands-on labs to all NCL players and coaches.

The National Cyber League – Where Cybersecurity is a Passion

We suggest that faculty use the lab assignments in this syllabus as ungraded homework for students, and the NCL games as graded assignments.

Through the NCL, college faculty will be able to infuse virtual lab exercises into their courses and be better prepared to coach competitive cyber teams. Please contact Casey W. O'Brien, NCL Commissioner (info@nationalcyberleague.org) if you have questions about using the labs and games in your fall courses.

2014 Fall Season

The 2014 NCL Fall Season will be will partially based on the Security+™ performance-based objectives, a widely recognized and adopted curriculum and certification - the 2014 NCL Fall Season also includes objectives for the EC-Council Certified Ethical Hacker™ exam.

Akin to conditioning in athletics, or practicing layups and free throws in the gym, the NCL will host 20 virtual preparatory Security+™ lab exercises in Cyber Gymnasiums across the country, which students can use to develop and practice hands-on skills for the NCL games and the Security+™ certification exam.

Players will be participating in a type of computer security game called a *Capture-the-Flag* (CTF). In CTF games, players race to answer security-related challenges, often searching for digital "flags" hidden on servers, in encrypted text, or in applications. Challenges within the CTF are open-ended and require expertise and skills in a wide range of security-related topics: computer forensics, cryptography, network penetration testing, web security, and system/network administration. When a player submits a flag, they receive points for solving the challenge. The player or team with the highest cumulative score at the end of the game wins.

The National Cyber League – Where Cybersecurity is a Passion

The NCL will also host a Regular Season, comprised of a mandatory Pre-Season assessment (September 27-October 4), two Regular Season games, optimized for individuals (October 18 and November 1), and a game for teams - NCL National Championship (November 15-22).

These games will be created and optimized for individuals and teams and are designed to provide hands-on experiences and challenges to help students to develop and improve cybersecurity skills and problem-solving abilities. All games will be conducted remotely, in a virtual Cyber Stadium (powered by iSIGHT Partner's ThreatSPACE), equally accessible to all.

Who Can Participate?

- Individuals currently enrolled as a student at an U.S. accredited 2- or 4-year college/university
- All teams must have a faculty/mentor coach
- Registration fee is $20 per individual participant and $25 per participating team
- Players are expected to commit to the entire season
- There are no prerequisite skills for participation, but successful Bronze-level players will have completed the preparatory exercises; Silver- and Gold-level players a cross-section of intermediate knowledge and skills in computer science, networking, systems administration, and information security

NCL Recommended Text

The syllabus topics provided below are based on the following textbook:

Security+ Guide to Network Security Fundamentals, 4e
Author: Mark Ciampa
Publisher: Course Technology
ISBN-10: 1111640122
ISBN-13: 9781111640125

The National Cyber League – Where Cybersecurity is a Passion

NCL Syllabus Topics

- Introduction to Security
- Malware and Social Engineering Attacks
- Application and Network Attacks
- Vulnerability Assessment and Mitigating Attacks
- Host, Application, and Data Security
- Network Security
- Administering a Secure Network
- Wireless Network Security
- Access Control Fundamentals
- Authentication and Account Management
- Basic Cryptography
- Advanced Cryptography
- Business Continuity
- Risk Mitigation

The table below lists the domain areas measured by the Security+™ examination and the approximate extent to which they are represented in the exam:

The National Cyber League – Where Cybersecurity is a Passion

CompTIA Security+™ Domain	% of Examination
1.0 Network Security	21%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	21%
4.0 Application, Data and Host Security	16%
5.0 Access Control and Identity Management	13%
6.0 Cryptography	11%
Total	**100%**

Within these six domains are the following Security+™ performance-based exam objectives:

- **1.0 Network Security**:
  - Objective 1.2: Apply and implement secure network administration principles
  - Objective 1.4: Implement and use common protocols
  - Objective 1.6: Implement wireless network in a secure manner
- **2.0 Compliance and Operational Security**:
  - Objective 2.2: Carry out appropriate risk mitigation strategies
  - Objective 2.3: Execute appropriate incident response procedures
  - Objective 2.7: Execute disaster recovery plans and procedures
- **3.0 Threats and Vulnerabilities**:
  - Objective 3.1: Analyze and differentiate among types of malware

- Objective 3.2: Analyze and differentiate among types of attacks
- Objective 3.5: Analyze and differentiate among types of application attacks
- Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques
- Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities

- **4.0 Application, Data and Host Security**:
  - Objective 4.2: Carry out appropriate procedures to establish host security

- **5.0 Access Control and Identity Management**:
  - Objective 5.3: Implement appropriate security controls when performing account management

- **6.0 Cryptography**:
  - Objective 6.2: Use and apply appropriate cryptographic tools and products
  - Objective 6.4: Implement PKI, certificate management and associated components

Lab Exercises

There are 20 remote lab exercises, available in the NCL Gym, designed to:

- Reinforce the concepts covered in the Security+™ performance-based exam objectives
- Help prepare students for the NCL games
- Help students prepare for the CompTIA Security+™ exam
- Provide supplemental lab exercises for faculty teaching CompTIA Security+™ and Network Security-related classes

The National Cyber League – Where Cybersecurity is a Passion

The lab exercises can be completed anytime, anyplace, via the virtual NCL Cyber Gym. Instructions for accessing these lab exercises will be made available separately.

The lab exercises listed as follows are mapped to the appropriate Security+™ domain and performance-based exam objective:

- **1.0 Network Security**:
  - Objective 1.2: Apply and implement secure network administration principles:
    - **Lab Exercise 1**: *Network Devices and Technologies - Capturing Network Traffic*
    - **Lab Exercise 2**: *Secure Network Administration Principles - Log Analysis*
    - **Lab Exercise 7:** *Configuring the pfSense Firewall*
  - Objective 1.4: Implement and use common protocols:
    - **Lab Exercise 3**: *Protocols and Default Network Ports - Transferring Data Using TCP/IP*
    - **Lab Exercise 4**: *Protocols and Default Network Ports - Connecting to a Remote System*
  - Objective 1.6: Implement wireless network in a secure manner:
    - **Lab Exercise 5**: *Secure Implementation of Wireless Networking*

- **2.0 Compliance and Operational Security**:
  - Objective 2.3: Execute appropriate incident response procedures:
    - **Lab Exercise 6**: *Incident Response Procedures*
    - **Lab Exercise 8**: *Configuring Backups*

- **3.0 Threats and Vulnerabilities**:
  - Objective 3.1: Analyze and differentiate among types of

malware
    - **Lab Exercise 9**: *Analyze and Differentiate Types of Malware*
  - Objective 3.2: Analyze and differentiate among types of attacks:
    - **Lab Exercise 10**: *Analyze and Differentiate Types of Attacks Using Window Commands*
  - Objective 3.5: Analyze and differentiate among types of application attacks:
    - **Lab Exercise 11**: *Analyze and Differentiate Types of Application Attacks*
  - Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques:
    - **Lab Exercise 12**: *Mitigation and Deterrent Techniques - Anti Forensics*
    - **Lab Exercise 13**: *Mitigation and Deterrent Techniques - Password Cracking*
  - Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities:
    - **Lab Exercise 14**: *Discovering Security Threats and Vulnerabilities*

- **4.0 Application, Data and Host Security**:
  - Objective 4.2: Carry out appropriate procedures to establish host security:
    - **Lab Exercise 15**: *Importance of Data Security - Data Theft*
    - **Lab Exercise 16**: *Importance of Data Security - Securing Data Using Encryption Software*

- **5.0 Access Control and Identity Management**:
  - Objective 5.3: Implement appropriate security controls when performing account management:

The National Cyber League – Where Cybersecurity is a Passion

- **Lab Exercise 17**: *Authentication, Authorization and Access Control*
- **Lab Exercise 18**: *Access Controls*

- **6.0 Cryptography**:
  - Objective 6.2: Use and apply appropriate cryptographic tools and products:
    - **Lab Exercise 16**: *Importance of Data Security - Securing Data Using Encryption Software*
    - **Lab Exercise 19**: *General Cryptography Concepts*
    - **Lab Exercise 20:** *Cryptography*

Learning Objectives:

Upon successfully completing the course, students will be able to:

- Articulate why information security is essential in today's computing environments;
- Identify the goals of information security;
- Describe common security threats and attacks, their ramifications and how to safeguard against them;
- Determine the factors involved in developing strong information security strategies, policies, and procedures;
- Identify and explain how various security-related technologies work (e.g., Intrusion Detection/Prevention Systems);
- Differentiate between the various cryptographic concepts;
- Differentiate between physical security, disaster recovery, and business continuity;
- Describe computer forensics and its role in information security;
- Demonstrate ethical behavior appropriate to security-related technologies
- Discuss measures to secure remote access users, Email, web services, wireless networks, and operating systems; and
- Work in virtualized environments.

The National Cyber League – Where Cybersecurity is a Passion

Suggested Schedule

The following suggested schedule maps the *Security+ Guide to Network Security Fundamentals, 4e* textbook chapters with the corresponding NCL lab exercise(s) and NCL games.

The Preseason Game will be held on 9/27-10/04. This game is mandatory for all players and requires no prerequisite knowledge.

Suggested Schedule (game dates subject to change)
-**Chapter 1**: Introduction to Security
-**Chapter 2**: Malware and Social Engineering Attacks
-**Chapter 3**: Application and Network Attacks --***Lab 10****: Analyze and Differentiate Types of Attacks Using Windows Commands* --***Lab 9****: Analyze and Differentiate Types of Malware* --***Lab 11****: Analyze and Differentiate Types of Application Attacks (Tasks 2-4)* --***Lab 14****: Discovering Security Threats and Vulnerabilities (Task 3)* --***Lab 15****: Importance of Data Security - Data Theft* --***Lab 6****: Incident Response Procedures (Task 1)*\ ***--Lab 7:*** *Configuring the pfSense Firewall*
-**Chapter 4**: Vulnerability Assessment and Mitigating Attacks --***Lab 14****: Discovering Security Threats and Vulnerabilities (Tasks 1-2)* --***Lab 12****: Mitigation and Deterrent Techniques - Password Cracking* --***Lab 1****: Network Devices and Technologies - Capturing Network Traffic*
-**Chapter 5**: Host, Application, and Data Security --***Lab 12****: Mitigation and Deterrent Techniques - Anti-Forensics* --***Lab 2****: Secure Network Administration Principles - Log Analysis*
-**Chapter 6**: Network Security

The National Cyber League – Where Cybersecurity is a Passion

-**Chapter 7**: Administering a Secure Network --***Lab 3***: *Protocols and Default Network Ports - Transferring Data Using TCP/IP* --***Lab 4***: *Protocols and Default Network Ports - Connecting to a Remote System* --***Lab 11***: *Analyze and Differentiate Types of Application Attacks (Task 1)*
10/18/14 Regular Season: Game #1 **(Prerequisite: Mandatory Preseason 09/27-10/04)**
-**Chapter 11**: Basic Cryptography --***Lab 19***: *General Cryptography Concepts*
-**Chapter 12**: Advanced Cryptography --***Lab 16***: *Importance of Data Security - Securing Data Using Encryption Software* --***Lab 20***: *Cryptography*
-**Chapter 8**: Wireless Network Security --***Lab 5***: *Secure Implementation of Wireless Networking*
11/01/14 Regular Season: Game #2 **(Prerequisite: Mandatory Preseason and Regular Season Game #1)**
-**Chapter 9**: Access Control Fundamentals --***Lab 17***: *Authentication, Authorization, and Access Control* --***Lab 20***: *Access Controls*
11/15-11/22 Post Season: NCL Championship **(Prerequisite: Mandatory Preseason and Regular Season Games #1 & #2)**
-**Chapter 13**: Business Continuity
-**Chapter 14**: Risk Mitigation --***Lab 6***: *Incident Response Procedures (Tasks 2-3)*

4.2.4 COS 336-338 Cybersecurity Competitions Supporting Material - EC-COuncil Certified Ethical Hacker (CEH)^{TM} Syllabus

The National Cyber League – Where Cybersecurity is a Passion

National Cyber League
Certified Ethical Hacker (CEH)™ Syllabus

Note to Faculty

This NCL Syllabus is intended as a supplement to courses that are based on the EC-Council Certified Ethical Hacker™ (CEHv8) exam, or courses that include similar knowledge and skills.

A primary goal of the NCL is to seamlessly integrate hands-on lab exercises and challenging cybersecurity games into higher education curriculum. The NCL uses a game analogy to describe our events because we believe that we are providing a fun environment that allow students (AKA **players**) to test their knowledge and skills against other players - just like a game!

This NCL Syllabus is not intended as a replacement to an existing course, but can provide supplemental hands-on lab exercises aligned with the NCL games. We encourage college faculty (AKA **coaches**) to look at ways to include this syllabus as part of the lab component of their course(s). While CompTIA Security+™ and EC-Council Certified Ethical Hacker (CEH)™ performance-based exam objectives are the foci of the 2014 NCL Fall Season, faculty and students in related security courses can also benefit from adding hands-on labs and NCL games as part of their course assignments. As educators, we understand the importance of aligning exercises to an academic calendar (e.g., semesters). We welcome feedback to help us to best support faculty and their instructional goals.

Network Development Group (NDG) collaborated with the Center for Systems Security and Information Assurance (CSSIA), a co-founding member of the NCL, to create a series of lab exercises intended to support the CEH curriculum. As an NDG partner, the NCL is able to take full advantage of this collaboration and offer these excellent hands-on labs to all NCL players and coaches.

The National Cyber League – Where Cybersecurity is a Passion

We suggest that faculty use the lab assignments in this syllabus as ungraded homework for students, and the NCL games as graded assignments.

Through the NCL, college faculty will be able to infuse virtual cyber lab exercises into their courses and be better prepared to coach competitive cyber teams. Please contact Casey W. O'Brien, NCL Commissioner (info@nationalcyberleague.org) if you have any questions about using the labs and games in your fall courses.

2014 Fall Season

The 2014 NCL Fall Season will be will partially based on the CEH™ performance-based exam objectives, a widely recognized and adopted curriculum and certification - the 2014 NCL Fall Season also includes objectives for the Security+™.

Akin to conditioning in athletics, or practicing layups and free throws in the gym, the NCL will host 19 virtual preparatory CEH™ lab exercises in Cyber Gymnasiums across the country, which students can use to develop and practice hands-on skills for the NCL games and the CEH™ certification exam.

Players will be participating in a type of computer security game called a *Capture-the-Flag* (CTF). In CTF games, players race to answer security-related challenges, often searching for digital "flags" hidden on servers, in encrypted text, or in applications. Challenges within the CTF are open-ended and require expertise and skills in a wide range of security-related topics: computer forensics, cryptography, network penetration testing, web security, and system/network administration. When a player submits a flag, they receive points for solving the challenge. The player or team with the highest cumulative score at the end of the game wins.

The National Cyber League – Where Cybersecurity is a Passion

The NCL will also host a Regular Season, comprised of a mandatory Pre-Season assessment (September 27-October 4), two Regular Season games, optimized for individuals (October 18 and November 1), and a Post Season game for teams – the NCL National Championship (November 15-22).

These games will be created and optimized for individuals and teams and are designed to provide hands-on experiences and challenges to help students to develop and improve cybersecurity skills and problem-solving abilities. All games will be conducted remotely, in a virtual Cyber Stadium (powered by iSIGHT Partner's ThreatSpace), equally accessible to all.

Who Can Participate?

- Individuals currently enrolled as a student at an U.S. accredited 2- or 4-year college/university
- All teams must have a faculty/mentor coach
- Registration fee is $20 per individual participant and $25 per participating team
- Players are expected to commit to the entire season
- There are no prerequisite skills for participation, but successful Bronze-level players will have completed the preparatory exercises; Silver- and Gold-level players a cross-section of intermediate knowledge and skills in computer science, networking, systems administration, and information security

NCL Recommended Books

The syllabus topics provided below are based on the following textbooks:

Official Certified Ethical Hacker Review Guide
Author: Steven DeFino
ISBN-10: **1435488539**
ISBN-13: **978-1435488533**

The National Cyber League – Where Cybersecurity is a Passion

Hands-On Ethical Hacking and Network Defense, Second Edition
Author: Michael T. Simpson
ISBN-10: **1435486099**

Ethical Hacking & Countermeasures: Attack Phases
Author: EC-Council
ISBN-10: **143548360X**
ISBN-13: **978-1435483606**

Ethical Hacking and Countermeasures: Linux, Macintosh & Mobile Systems
ISBN-10: **1435483642**
ISBN-13: **978-1435483644**

Ethical Hacking & Countermeasures: Secure Network Infrastructures
Author: EC-Council
ISBN-10: **1435483650**
ISBN-13: **978-1435483651**

Ethical Hacking & Countermeasures: Threats & Defense Mechanisms
Author: EC-Council
ISBN-10: **1435483618**
ISBN-13: **978-1435483613**

Ethical Hacking & Countermeasures: Web Applications & Data Servers
Author: EC-Council
ISBN-10: **1435483626**
ISBN-13: **978-1435483620**

The National Cyber League – Where Cybersecurity is a Passion

NCL Syllabus Topics

- Background knowledge needed for CEH™v8
- Analysis and Assessment
- Security
- Tools/Systems/Programs
- Procedures/Methodology
- Regulation/Policy
- Ethics

The table below lists sections and content of the CEH™ exam and the approximate extent to which they are represented in the exam: (from EC-Council http://www.eccouncil.org/Certification/exam-information/ceh-exam-312-50):

CEH Section	% of Exam	# of Questions
Background	4%	5
Analysis/Assessment	13%	16
Security	25%	31
Tools/Systems/Programs	32%	40
Procedures/Methodology	20%	25
Regulation/Policy	4%	5
Ethics	2%	3

The National Cyber League – Where Cybersecurity is a Passion

The above-mentioned 7 sections include the following CEH™ exam content knowledge:

- **Background**
  - Networking technologies
  - Web technologies (e.g. web 2.0, Skype)
  - Systems technologies
  - Communication protocols
  - Malware operations
  - Mobile technologies (e.g. smart phones)
  - Telecommunication technologies
  - Backups and archiving (e.g. local, network)

- **Analysis/Assessment**
  - Data analysis
  - Systems analysis
  - Risk assessments
  - Technical assessment methods

- **Security**
  - Systems security controls
  - Application / file server
  - Firewalls
  - Cryptography
  - Network security
  - Physical security
  - Threat modeling
  - Verification procedures (e.g. false positive / negative validation
  - Social engineering (human factors manipulation)
  - Vulnerability scanners
  - Security policy implications
  - Privacy / confidentiality (with regard to engagement)

- Biometrics
- Wireless access technology (e.g. networking, RFID, Bluetooth)
- Trusted networks
- Vulnerabilities

- **Tools/Systems/Programs**
  - Network- / host- based intrusion
  - Network / wireless sniffers (e.g. Wireshark, Airsnort)
  - Access control mechanisms (e.g. smartcards)
  - Cryptography techniques (e.g. IPsec, SSL ,PGP)
  - Programming languages (e.g. C++, Java, C#, C)
  - Scripting languages (e.g. PHP, Java script)
  - Boundary protection appliances (e.g. DMZ)
  - Network topologies
  - Subnetting
  - Port Scanning (e.g. NMAP)
  - Domain name system (DNS)
  - Routers / modems / switches
  - Vulnerability scanner (e.g. Nessus, Retina)
  - Vulnerability management and protection systems (e.g. Foundstone, Ecora)
  - Operating environments (e.g. Linux, Windows, Mac)
  - Antivirus systems and programs
  - Log analysis tools
  - Security models
  - Exploitation tools
  - Database structures

- **Procedures/Methodology**
  - Cryptography
  - Public Key Infrastructure (PKI)
  - Security Architecture (SA)

- Service Oriented Architecture (SOA)
- Information security incident management
- N-Tier application design
- TCP/IP networking (e.g. network routing)
- Security testing methodology

- **Regulation/Policy**
  - Security policies
  - Compliance regulations (e.g. PCI)

- **Ethics**
  - Professional code of conduct
  - Appropriateness of hacking activities

Lab Exercises

There are 19 remote lab exercises, available in the NCL Cyber Gym, designed to:

- Reinforce the concepts covered in the CEH™ content knowledge with hands-on activities
- Help prepare students for the NCL games
- Help students prepare for the CEH™ certification exam
- Provide supplemental lab exercises for faculty teaching CEH™ and related course(s) and content

The following lab exercises can be completed anytime, anyplace, via the virtual NCL Cyber Gym. Instructions for accessing these lab exercises will be made available separately:

Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

- Introduction to Ethical Hacking
- Scanning Networks
- Enumeration
- Sniffers

The National Cyber League – Where Cybersecurity is a Passion

Lab 2: Conducting Active and Passive Reconnaissance Against a Target
- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Social Engineering

Lab 3: Using the SYSTEM account
- System Hacking

Lab 4: Poison Ivy – Remote Access Trojan
- System Hacking
- Trojans and Backdoors
- Viruses and Worms

Lab 5: Using the SHARK Remote Administration Tool
- System Hacking
- Trojans and Backdoors
- Viruses and Worms

Lab 6: Utilizing Malware - Dark Comet
- System Hacking
- Trojans and Backdoors
- Viruses and Worms

Lab 7: Breaking Windows Passwords
- System Hacking

Lab 8: Using John the Ripper to Crack Linux Passwords
- System Hacking

Lab 9: Using Spear Phishing to Target an Organization
- System Hacking
- Social Engineering

- Session Hijacking

Lab 10: Breaking WEP and WPA Encryption
- Hacking Wireless Networks

Lab 11: Using Metasploit to Attack a Remote System
- Scanning Networks
- Enumeration
- Sniffers
- Evading IDS, Firewalls, and Honeypots

Lab 12: Using Armitage to Attack the Network
- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- System Hacking
- Penetration Testing

Lab 13: Exploitation with IPv6
- System Hacking

Lab 14: Creating MSFPAYLOADS
- System Hacking
- Trojans and Backdoors
- Viruses and Worms
- Penetration Testing

Lab 15: Abusing SYSTEMS
- Denial of Service

Lab 16: SQL Injection
- Hacking Webservers
- Hacking Web Applications
- SQL Injection

The National Cyber League – Where Cybersecurity is a Passion

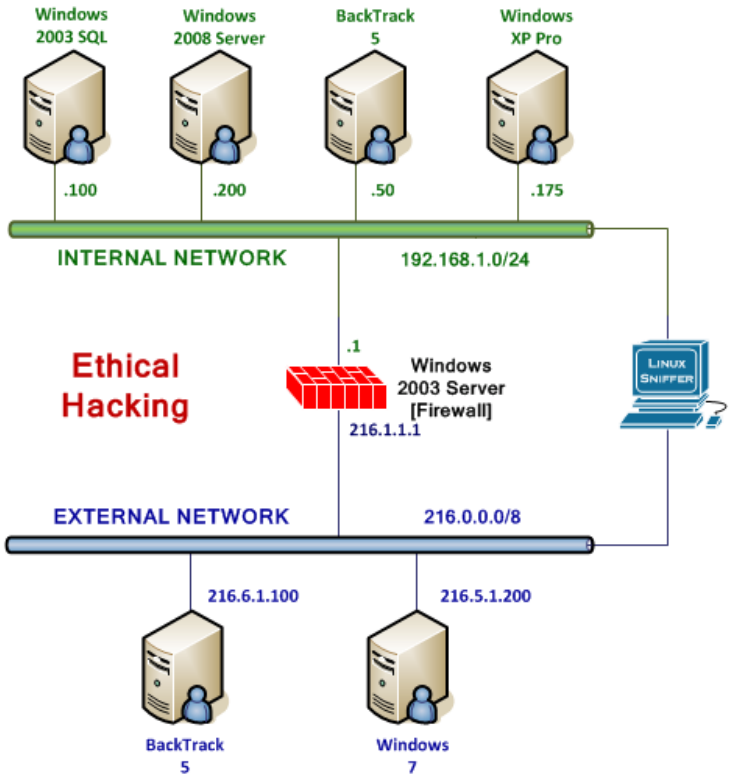
Lab 17: Launching a Buffer Overflow
- System Hacking
- Buffer Overflow

Lab 18: Intrusion Detection
- Evading IDS, Firewalls, and Honeypots

Lab 19: Using Certificates to Encrypt Email
- Cryptography

Lab Topology for Virtual Lab Exercises (available in the NCL Cyber Gym)

The National Cyber League – Where Cybersecurity is a Passion



(From http://www.netdevgroup.com/content/cybersecurity/labs/ethical_hacking.html)

Learning Objectives

Upon successfully completing the course, students will be able to:

- Utilize various information security tools given different target systems in different environments
- Discuss how the tools interrelate with each other in an overall penetration testing process

The National Cyber League – Where Cybersecurity is a Passion

- Implement countermeasures for various types of attacks
- Apply a common ethical hacking methodology to carry out a penetration test
- Analyze how penetration testing and ethical hacking fit into a comprehensive enterprise information security program
- Demonstrate ethical behavior appropriate to security-related technologies

Suggested Schedule

The following suggested schedule maps the *Official Certified Ethical Hacker Review Guide* chapters with the corresponding NCL lab exercise(s) and NCL games. The Preseason Game will be held on 9/27 - 10/4. This game is mandatory for all players and requires no prerequisite knowledge.

Faculty are encouraged to supplement with the more comprehensive information in the five CEH™ textbooks:

Suggested Schedule (game dates subject to change)
Chapter 1: Ethical Hacking Basics
Chapter 3: Reconnaissance Information Gathering for the Ethical Hacker • **Lab 2:** Conducting Active and Passive Reconnaissance Against a Target -- Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, Social Engineering • **Lab 12:** Using Armitage to Attack the Network -- Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, System Hacking, Penetration Testing
Chapter 4: Scanning and Enumeration • **Lab 1:** Using Active and Passive Techniques to Enumerate Network Hosts - Introduction to Ethical Hacking, Scanning Networks, Enumeration, Sniffers • **Lab 11:** Using Metasploit to Attack a Remote System - Scanning Networks,

Enumeration, Sniffers, Evading IDS, Firewalls, and Honeypots
Chapter 5: Hacking Through the Network Sniffers and Evasion
Chapter 6: Attacking a System • **Lab 3:** Using the SYSTEM account -- System Hacking • **Lab 18:** Intrusion Detection -- Evading IDS, Firewalls, and Honeypots
Chapter 8: Web-Based Hacking Servers and Applications • **Lab 13:** Exploitation with IPv6 -- System Hacking • **Lab 15:** Abusing SYSTEMS -- Denial of Service • **Lab 16:** SQL Injection -- Hacking Webservers, Hacking Web Applications, SQL Injection • **Lab 17:** Launching a Buffer Overflow-- System Hacking, Buffer Overflow
10/18/14 Regular Season: Game #1 **(Prerequisite: Mandatory Pre-Season 09/27-10/4)**
Chapter 2: Cryptography 101 • **Lab 7:** Breaking Windows Passwords -- System Hacking • **Lab 8:** Using John the Ripper to Crack Linux Passwords -- System Hacking • **Lab 19:** Using Certificates to Encrypt Email -- Cryptography
Chapter 9: Wireless Networking Hacking • **Lab 10:** Breaking WEP and WPA Encryption -- Hacking Wireless Networks
11/01/14 Regular Season: Game #2 **(Prerequisite: Mandatory Pre-Season and Regular Season Game #1)**
-**Chapter 10**: Trojans and Other Attacks • **Lab 4:** Poison Ivy (Remote Access Trojan) -- System Hacking, Trojans and Backdoors, Viruses and Worms • **Lab 5:** Using the SHARK Remote Administration Tool -- System Hacking, Trojans and Backdoors, Viruses and Worms • **Lab 6:** Utilizing Malware (Dark Comet) -- System Hacking, Trojans and

The National Cyber League – Where Cybersecurity is a Passion

Backdoors, Viruses and Worms • **Lab 14:** Creating MSFPAYLOADS -- System Hacking, Trojans and Backdoors, Viruses and Worms, Penetration Testing
-**Chapter 7**: Low Tech: Social Engineering and Physical Security • **Lab 9:** Using Spear Phishing to Target an Organization -- System Hacking, Social Engineering, Session Hijacking
11/15-11/22 Post Season: NCL Championship **(Prerequisite: Mandatory Preseason and Regular Season Games #1 & #2)**

4.3 COS 480 Database Management Systems - Modification

The COS 480 Database Management Systems course modification form is on the following pages.

THE UNIVERSITY OF MAINE

Modification Form

DEPARTMENT: CIS
COLLEGE: CLAS
COURSE DESIGNATOR: COS 480
PROPOSED COURSE #:
COURSE TITLE: Database Management Systems
EFFECTIVE SEMESTER: Fall 2015

Requested Action: Note: A complete Syllabus is required for all new courses, including travel-study courses offered through CED or Summer Session and for the addition General Education and/or travel-study to an existing course. Please be sure that all elements required for a syllabus at the University of Maine are present. We recommend you work closely with the syllabus check list found at www.umaine.edu/upcc.

Please check all that apply *(Please note if you are making a substantial modifications you may want to consider creating a new course)*

Designator Change		Credit Change	
Cross Listing		Number Change	
Title Change		Description Change	
Prerequisite Change	X	Travel Study	
Addition of Elec. Learning Component		Conversion of an existing onsite Course to an online Course	
Other (Please Explain)		Addition of Gen Ed (Complete Section 2. Please see additional information on www.umaine.edu/upcc)	

ENDORSEMENTS *(Please Print and Sign Name)* DATE
Leader, Initiating Department/Unit(s)

College(s) Curriculum Committee Chair(s)

Dean(s)

Associate Provost for Undergraduate Education

CURRENT CATALOG DESCRIPTION (Include designator, number, title, prerequisites, credit hours):
COS 480 - Database Management Systems

Covers database management systems from the perspective of database designers and database application programmers. Topics include Entity-Relationship modeling, relational databases, transactions and isolation, and Web-database applications. Includes both individual programming assignments and semester-long group projects culminating in demonstrations of substantial database application.

Prerequisites: COS 350 or permission.

Course Typically Offered: Fall

Credits: 3

PROPOSED CATALOG DESCRIPTON (Include designator, number, title prerequisites, credit hours):
COS 480 - Database Management Systems

Covers database management systems from the perspective of database designers and database application programmers. Topics include Entity-Relationship modeling, relational databases, transactions and isolation, and Web-database applications. Includes both individual programming assignments and semester-long group projects culminating in demonstrations of substantial database application.

Prerequisites: COS 331 or COS 350 or permission.

Course Typically Offered: Spring

Credits: 3

REASON FOR COURSE MODIFICATION:
We are moving COS 480 to the Spring to better fit the recommended schedule for the B. S. in Cybersecurity. Also, since the students in the Cybersecurity Program do not typically take COS 350 or the courses that are prerequisites for COS 350, we needed to have an alternative prerequisite. Dr. Chawathe said he had been thinking about changing the prerequisites to make it easier for students to take the course. He is quite satisfied that once the students complete COS 331 they would be ready for COS 480.

INSTRUCTOR: Dr. Sudarshan Chawathe

Does this change in course prefix, number/or credit hours affect any prerequisite? If yes, please list course(s):
COS 480 is not a prerequisite for any course. We have already presented the rationale for modifying the prerequisites for COS 480.

4.4 COS 495 Field Experience - Modification

The COS 495 Field Experience course modification form is on the following pages.

THE UNIVERSITY OF MAINE

Modification Form

DEPARTMENT: CIS
COURSE DESIGNATOR: COS 495
COURSE TITLE: Field Experience

COLLEGE: CLAS
PROPOSED COURSE #:
EFFECTIVE SEMESTER: Fall 2015

Requested Action: Note: A complete Syllabus is required for all new courses, including travel-study courses offered through CED or Summer Session and for the addition General Education and/or travel-study to an existing course. Please be sure that all elements required for a syllabus at the University of Maine are present. We recommend you work closely with the syllabus check list found at www.umaine.edu/upcc.

Please check all that apply *(Please note if you are making a substantial modifications you may want to consider creating a new course)*

Designator Change		Credit Change	
Cross Listing		Number Change	
Title Change		Description Change	X
Prerequisite Change	X	Travel Study	
Addition of Elec. Learning Component		Conversion of an existing onsite Course to an online Course	
Other (Please Explain)		Addition of Gen Ed (Complete Section 2. Please see additional information on www.umaine.edu/upcc)	X

ENDORSEMENTS *(Please Print and Sign Name)* DATE
Leader, Initiating Department/Unit(s)

College(s) Curriculum Committee Chair(s)

Dean(s)

Associate Provost for Undergraduate Education

CURRENT CATALOG DESCRIPTION (Include designator, number, title, prerequisites, credit hours):
COS 495 - Field Experience

A pre-planned work experience of no less than ten and preferably more weeks in a commercial environment, with faculty supervision. Normally a paid work experience. A presentation open to interested faculty, staff and students might be required at the completion of the project. May be repeated for a maximum of 3 credit hours. (Pass/Fail Grade Only.)

General Education Requirements: Satisfies the General Education Capstone Experience Requirement.

Prerequisites: Normally a student must complete COS 301, COS 420, COS 431 and preferably COS 350, with at least a grade of "C" and permission.

Course Typically Offered: Not Regularly Offered

Credits: 1-3

PROPOSED CATALOG DESCRIPTON (Include designator, number, title prerequisites, credit hours):
COS 495 - Field Experience

A pre-planned work experience of no less than ten and preferably more weeks in a production environment, with faculty supervision. Students will be expected to file regular progress reports and to write a substantial project proposal. A presentation open to interested faculty, staff and students will be required at the completion COS 497. (Pass/Fail Grade Only.)

General Education Requirements: *Upon completion of the two course sequence (COS 495 \& COS 497), satisfies the General Education Writing Intensive and Capstone Experience Requirements.*

Prerequisites: CS B.S. majors must complete COS 301, COS 331 and COS 420 and preferably COS 350, with at least a grade of "C" and permission. Cybersecurity B.S. majors must complete COS 330 and COS 301 with at least a grade of "C" and permission.

Course Typically Offered: Fall

Credits: 3

REASON FOR COURSE MODIFICATION:
The new description permits COS 495 to function as an alternative to COS 397 as the first part of the capstone experience. It also brings it into line with the expectations of a writing intensive course. It removes the flexibility of offering it as a 1-credit course, an option that was hardly, if ever, used.

INSTRUCTOR: *A suitable instructor will be assigned to this course.*

Does this change in course prefix, number/or credit hours affect any prerequisite? If yes, please list course(s):
The prerequisites for this course have changed and it will now be part of the Capstone Experience.

For Addition of Electronic Learning Component:

If adding an electronic component to a regularly scheduled, on site course, please indicate the following:

FirstClass Conferencing	
Blackboard	
Other Course Management Software/Online Delivery Platform	

Broadband Connection Necessary to Access Course Materials? Yes No

PLEASE CHECK ALL THOSE THAT APPLY:

Adobe Connect	
Skype	
Polycom	
Video Conferencing	
Other	

REAL TIME PARTICIPATION EXPECTED/REQUIRED?

PERCENTAGE OF COURSE TO BE DELIVERED ELECTRONICALLY? 50% - 100%?

49% or LESS?

IF CONVERTING AN EXISTING ON SITE COURSE TO AN ONLINE COURSE, PLEASE INDICATE THE PEDAGOGICAL CHANGES EMPLOYED TO ADAPT YOUR COURSE TO AN ONLINE FORMAT:

Section 2

THIS SECTION MUST BE COMPLETED FOR GENERAL EDUCATION APPROVALS:

CHECK ALL AREAS FOR WHICH A COURSE IS PROPOSED- Max. 2

Quantitative Literacy	
Lab Science	
Science Applications	
Western Cultural Tradition	
Population & Environment	
Cultural Diversity or International Perspectives	
Artistic & Creative Expressions	
Social Context & Institutions	
Ethics	
Writing Intensive	X
Capstone Experience	X

PLEASE PROVIDE RATIONAL FOR ASSIGNING A GEN ED TO THIS COURSE:
This course will provide a field experience introduction to COS 497. It is actually the field experience version of COS 397 and will adhere to all the requirements of COS 397, which is currently approved for Gen Ed credit as Writing Intensive and Part of the Capstone Experience. The current description of COS 397 permits a field experience format. Using COS 495 for this variant makes it clear that the student has taken field experience as required by the UMS B. S. in Cybersecurity Proposal.

PLEASE EXPLAIN HOW STUDENT LEARNING OUTCOMES FOR THE COURSE AS PRESENTED IN THE COURSE SYLLABUS, ALIGN WITH THE STUDENT LEARNING OUTCOMES FOR THE PROPOSED GENERAL EDUCATION CATEGORY OR CATORIES:
This course will follow all the requirements of COS 397 which has already been approved for Writing Intensive and Capstone Experience.

FOR EACH AREA PROPOSED, DESCRIBE EVIDENT OF STUDENT ACHIEVEMENT THAT HAS BEEN AND/OR WILL BE USED TO MEASURE LEARNER OUTCOMES AND DESCRIBE HOW THIS INFORMATION WILL BE USED TO IMPROVE LEARNING. INDICATED WHERE THE SYLLABUS EXPLAINS THESE ASSESSMENT MEASURES FOR STUDENTS:
This course will follow all the requirements of COS 397 which has already been approved for Writing Intensive and Capstone Experience.

FOR EACH AREA PROPOSED, DESCRIBE PLANS FOR REVIEWING THE DATA/INFORMATION FROM ASSESSMENT OF STUDENT OUTCOMES AND INDICATED HOW IT WILL BE USED TO IMPROVE LEARNER OUTCOMES AND/OR REVISE COURSE CONTENT AND INSTRUCTION:
This course will follow all the requirements of COS 397 which has already been approved for Writing Intensive and Capstone Experience.

4.5 COS 497 Computer Science Capstone2

The COS 497 Computer Science Capstone 2 course modification form is on the following pages.

THE UNIVERSITY OF MAINE

Modification Form

DEPARTMENT: CIS
COLLEGE: CLAS
COURSE DESIGNATOR: COS 497
PROPOSED COURSE #:
COURSE TITLE: Computer Science Capstone 2
EFFECTIVE SEMESTER: Fall 2015

Requested Action: Note: A complete Syllabus is required for all new courses, including travel-study courses offered through CED or Summer Session and for the addition General Education and/or travel-study to an existing course. Please be sure that all elements required for a syllabus at the University of Maine are present. We recommend you work closely with the syllabus check list found at www.umaine.edu/upcc.

Please check all that apply *(Please note if you are making a substantial modifications you may want to consider creating a new course)*

Designator Change		Credit Change	
Cross Listing		Number Change	
Title Change		Description Change	X
Prerequisite Change	X	Travel Study	
Addition of Elec. Learning Component		Conversion of an existing onsite Course to an online Course	
Other (Please Explain)		Addition of Gen Ed (Complete Section 2. Please see additional information on www.umaine.edu/upcc)	

ENDORSEMENTS *(Please Print and Sign Name)* DATE

Leader, Initiating Department/Unit(s)

College(s) Curriculum Committee Chair(s)

Dean(s)

Associate Provost for Undergraduate Education

CURRENT CATALOG DESCRIPTION (Include designator, number, title, prerequisites, credit hours):
COS 497 - Computer Science Capstone 2

The second of a two-course sequence, designed to guide students in completing the Capstone project in either an independent study, group project, or field experience format. The focus is on the later stages of project work, including completing the programming tasks, evaluating the implemented systems, documenting all work in a project report, demonstrating the work in action, and making a public oral presentation. The relevant skills are covered and practiced by studying a collection of classic and topical papers.

General Education Requirements: Upon completion of the two course sequence (COS 397 \& COS 497), satisfies the General Education Writing Intensive and Capstone Experience Requirements.

Prerequisites: COS Majors with Senior standing, COS 397, and permission.

Course Typically Offered: Spring

Credits: 3

PROPOSED CATALOG DESCRIPTON (Include designator, number, title prerequisites, credit hours):
COS 497 - Computer Science Capstone 2

The second of a two-course sequence, designed to guide students in completing the Capstone project in either an independent study, group project, or field experience format. The focus is on the later stages of project work, including completing the programming tasks, evaluating the implemented systems, documenting all work in a project report, demonstrating the work in action, and making a public oral presentation. The relevant skills are covered and practiced by studying a collection of classic and topical papers.

General Education Requirements: Upon completion of the two course sequence (COS 397 \& COS 497) or (COS 495 \& COS 497), satisfies the General Education Writing Intensive and Capstone Experience Requirements.

Prerequisites: CS Majors or Cybersecurity Majors with Senior standing, COS 397 or COS 495, and permission.

Course Typically Offered: Spring

Credits: 3

REASON FOR COURSE MODIFICATION:
To provide a capstone experience to students in the B. S. in Cybersecurity program. This does not require a change to the course, just to the prerequisites.

INSTRUCTOR: *This course will be taught by whoever is assigned to teach the Capstone 2 course.*

Does this change in course prefix, number/or credit hours affect any prerequisite? If yes, please list course(s):
COS 497 is not a prerequisite for any other course. This modification does not change that.

For Addition of Electronic Learning Component:

If adding an electronic component to a regularly scheduled, on site course, please indicate the following:

FirstClass Conferencing	
Blackboard	
Other Course Management Software/Online Delivery Platform	

Broadband Connection Necessary to Access Course Materials? Yes No

PLEASE CHECK ALL THOSE THAT APPLY:

Adobe Connect	
Skype	
Polycom	
Video Conferencing	
Other	

REAL TIME PARTICIPATION EXPECTED/REQUIRED?

PERCENTAGE OF COURSE TO BE DELIVERED ELECTRONICALLY? 50% - 100%?

49% or LESS?

IF CONVERTING AN EXISTING ON SITE COURSE TO AN ONLINE COURSE, PLEASE INDICATE THE PEDAGOGICAL CHANGES EMPLOYED TO ADAPT YOUR COURSE TO AN ONLINE FORMAT:

5 Program Level Assessment

So far we have focused on assessment and discussion of individual courses. The University of Maine System B. S. in Cybersecurity includes some program level outcomes. George Markowsky met with Brian Doore to ensure that the program level assessment would be in step with the University of Maine's overall assessment program. The assessment questions are the same questions being used by Brian Doore in his work with assessing programs at the University of Maine. We begin by presenting the program outcomes that are presented in the University of Maine System B. S. in Cybersecurity proposal.

5.1 Student Learning Outcomes

Cybersecurity program graduates will be able to:

1. Apply knowledge of computing and information technologies and use software development and security analysis tools to produce effective designs and solutions for specific cybersecurity problems within a variety of computing platforms and employing an approved secure systems development process model.

2. Identify, analyze, and synthesize scholarly and professional literature relating to the fields of cybersecurity, information security, or information assurance, to help solve specific problems and to stay abreast of the rapidly changing security context.

3. Participate as an active and effective member of a project team engaged in achieving specific computer-based results or solutions.

4. Communicate, both orally and in writing, and negotiate with colleagues and other stakeholders including employees, managers, and executives. Negotiation and communication skills should also extend to all relevant external persons and organizations.

5. Demonstrate sensitivity to and sound judgment on ethical issues as they arise in information security and cyber defense and will adhere to accepted norms of professional responsibility.

6. Integrate knowledge from other disciplines, such as economics, management science, psychology and human factors, with their technical expertise to arrive at practical solutions that work successfully in real organizations.

7. Use appropriate tools to prevent, detect, react, and recover from attacks.

5.2 Assessment Questions

The two key assessment questions are given below. In subsequent sections we will illustrate how we intend to get answers to these questions in assessing each of the Student Learning Outcomes described in the preceding subsection.

- *Question 1:* Other than grades, what data/evidence were used to determine that students have achieved the stated outcome for the degree? Direct evidence is required, while indirect evidence is optional. Provide:

  1. Type of data/evidence
  2. Sample details including # of students sampled, which semesters, where in curriculum the outcome was assessed.

- *Question 2:*What methods or processes were used to evaluate student work? Provide:

  1. Evaluation instruments.
  2. Expected level of student achievement of the outcome.
  3. Who applied the evaluation tool.
  4. Who interpreted the results of the assessment process.

5.3 Outcome 1 - Application of Knowledge

Apply knowledge of computing and information technologies and use software development and security analysis tools to produce effective designs and solutions for specific cybersecurity problems within a variety of computing platforms and employing an approved secure systems development process model.

We expect this outcome to be assessed in COS 330 Introduction to Cybersecurity, COS 336-338 Cybersecurity Competitions, COS 495 Field Experience and COS 497 Computer Science Capstone 2. In COS 330 assessment will be based on the results of the individual cyberwars that will be held as part of that course and the specific course outcomes discussed in Section 3.

In COS 331 assessment will be based on the performance levels defined by the competition and by the national ranking of the competitors. In particular, the expectation is that any graduate of the University of Maine B. S. in Cybersecurity program would be able to achieve at least the Gold level of performance by the end of the program. We also expect students to place in the top half of competitors nationally.

In COS 495 assessment will be based on a self-report by the student and by an assessment of the student's outside manager. This will provide a valuable outside reference point for assessing the student's ability to apply knowledge.

In COS 497 assessment will be based on a report by the Capstone Advisor and by the response of external viewers of the Capstone presentation. In the past we have had members of the External Advisory Board review the Capstone projects.

We will expect the various assessments to deal explicitly with this outcome. We expect to do this assessment for all students.

5.4 Outcome 2 - Using Resources and Staying Current

Identify, analyze, and synthesize scholarly and professional literature relating to the fields of cybersecurity, information security, or information assurance, to help solve specific problems and to stay abreast of the rapidly changing security context.

This outcome will be accessed in COS 330 Introduction to Cybersecurity, COS 336-338 Cybersecurity Competitions, COS 497 Computer Science Capstone 2 and in review of the student's Cybersecurity Portfolio. In COS 330 students will be competing against each other and they will be evaluated on how much originality and knowledge they can bring to the competitions. National cybersecurity competitions are constantly being updated to include new aspects of the cybersecurity landscape. Through participation in these competitions in COS 331 and doing well, a student can demonstrate being current.

Similarly, we can have a specific question about whether the Capstone project demonstrates current thinking on a subject or not. In particular, we will ask a student's Capstone advisor to review the student's Cybersecurity Portfolio when becoming the advisor and at the end of the student's tenure to ensure that the portfolio continues to be updated in a timely manner.

5.5 Outcome 3 - Teamwork

Participate as an active and effective member of a project team engaged in achieving specific computer-based results or solutions.

COS 330 Introduction to Cybersecurity, COS 336-338 Cybersecurity Competitions and COS 495 Field Experience all feature teamwork. In COS 330 there will be specific instruction on team formation and team functioning. Students will have to respond to questions on homeworks and exams on the basic theories of team formation. They will also be evaluated during the COS 330 team cyberwar activities which involve teams providing reports on their activities and assessments of how well students performed as team members.

COS 331 will feature a team round every semester that it is offered and there will be assessments of how well students performed as team members. In COS 495 the student's external manager will be asked to assess the student's performance as a team member.

5.6 Outcome 4 - Oral Communication, Written Communication and Negotiation Skills

Communicate, both orally and in writing, and negotiate with colleagues and other stakeholders including employees, managers, and executives. Negotiation and communication skills should also extend to all relevant external persons and organizations.

This outcome will be formally assessed in COS 330 Introduction to Cybersecurity through various reports and presentations that the students have to give both during the individual cyberwars and during the team cyberwars. We will also ask the external manager to assess the student's communication skills during COS 495 Field Experience.

We will rely on the COS 495 assessment to give insight into whether the student is able to negotiate well.

5.7 Outcome 5 - Ethical Conduct

Demonstrate sensitivity to and sound judgment on ethical issues as they arise in information security and cyber defense and will adhere to accepted norms of professional responsibility.

We will assess this outcome in three courses: COS 330 Introduction to Cybersecurity, COS 490 Computers, Ethics and Society and COS 495 Field Experience. In COS 330 and COS 490 the assessment will be primarily through class work that presents scenarios that involve ethical issues. In COS 495 we have the possibility of getting an ethics review by the student's outside manager.

5.8 Outcome 6 - Interdisciplinary Knowledge

Integrate knowledge from other disciplines, such as economics, management science, psychology and human factors, with their technical expertise to arrive at practical solutions that work successfully in real organizations.

Many aspects of cybersecurity do not readily interconnect with other disciplines. At the same time, social engineering is a powerful technique for compromising systems. Social engineering will be covered extensively in COS 330 Introduction to Cybersecurity and we will design instruments for measuring how much interdisciplinary knowledge each student is able to marshall in support of cybersecurity activities.

5.9 Outcome 7 - Dealing with Cyber Attacks

Use appropriate tools to prevent, detect, react, and recover from attacks.

We expect to be able to assess this outcome based on activities in COS 330 Introduction to Cybersecurity and COS 495 Field Experience. In COS 330 there are both individual and team cyberwars and each student will need to understand how to prevent, detect, react and recover from cyber attacks. COS 336-338 Cybersecurity Competitions is of limited use in this regard, because the emphasis there is on offensive, rather than defensive activities. Some cybersecurity competitions such as the National Collegiate Cyber Defense competitions are either completely defensive or are at least partially defensive. Should students engage in such competitions we will use the results of these competitions to assess this outcome.

Table 11: Comparison of the UMS and UM Versions of the B. S. in Cybersecurity

CYB 100	Introduction to CS	4 cr	COS 140	Foundation of CS	3 cr
CYB 200	Intro to Info Security	3 cr	COS 330	Intro Cybersecurity	3 cr
CYB 250	Intro to Programming	3 cr	COS 220	Intro to C++	3 cr
CYB 300	Comp Programming	3 cr	COS 221	Intermediate C++	3 cr
CYB 330	Networking	3 cr	COS 440	Networking I	3 cr
CYB 340	Cyber Ethics	3 cr	COS 490	Comps, Ethics & Soc	3 cr
CYB 350	Databases	4 cr	COS 480	Databases	3 cr
CYB 360	Network Sec	4 cr	COS 336	Cyber Competition 1	1 cr
			COS 337	Cyber Competition 2	1 cr
			COS 338	Cyber Competition 3	1 cr
CYB 370	OS Security	3 cr	ECE 331	Intro Unix Sys Adm	3 cr
CYB 390	Cyber Internship	3 cr	COS 495	Field Exp	3 cr
CYB 400	Cyber Def Cap	3 cr	COS 497	Capstone 2	3 cr
			COS 235	Computer Organization	4 cr
			COS 331	Operating Systems	3 cr
	Cybersecurity Portfolio			LinkedIn^{TM} Portfolio	
	Total Credit Hours	36 cr		Total Credit Hours	40 cr

6 Comparision to the UMS Degree

Table 11 gives a quick comparison between the University of Maine System B. S. in Cybersecurity and the University of Maine B. S. in Cybersecurity. Overall, they mesh fairly well. There are three 4 credit courses in the University of Maine System B. S. in Cybersecurity program, while there is only one 4 credit course in the University of Maine B. S. in Cybersecurity program. The University of Maine System program totals to 36 credit hours while the University of Maine program totals to 40 credit hours. If COS 235 becomes a 3 credit course, the University of Maine program would total to 39 credit hours. COS 235 was included in the University of Maine program because it is a required course for many other courses. COS 431 was included to cover some of the operating systems concepts in the NSA requirements. While the courses do not match exactly, the arrangement is quite similar and quite a few courses have a direct translation into one of the University of Maine System courses. We feel that the University of Maine B. S. in Cybersecurity proposal is very much in the spirit of the University of Maine System B. S. in Cybersecurity proposal and is a good starting point. We expect that once the various campuses begin their programs there will be many discussions and evolution will most likely lead to a greater convergence across the programs.

7 Impact on UMaine

This proposal for a University of Maine B. S. in Cybersecurity degree was designed to minimize negative impact on the University of Maine. For the most part it uses existing courses and calls for some topic realignment and some harmonization of the curriculum. At this time there is great interest and demand for cybersecurity programs. It is important that the University of Maine be in a position to respond to this demand. In particular, we do not want to lose students to other institutions which can offer such a program. Because of the strength of the current offering in Computer Science, we are able to offer a potential very popular program with a relatively minor realignment of our current offerings.

The University of Maine System B. S. in Cybersecurity Proposal says that no new resources are necessary for this program. We do not think that we would be able to do this at the University of Maine. In particular, there are no mechanisms in place for using courses from other campuses in our programs here at the University of Maine. While these mechanisms might be developed, it will probably take some time to develop them. Delay in implementing the University of Maine B. S. in Cybersecurity will disadvantage the many students who have shown an interest in the degree.

There will be some scheduling issues and also some updating of course numbers, revision of curriculum and the creation of three completely new courses, COS 336-338 Cybersecurity Competitions. We note that these courses can be taught simultaneously since they differ primarily in the skill level of the student. Since these courses will use many online materials, they can be taught as one course but students enrolled in COS 336 Cybersecurity Competition 1, COS 337 Cybersecurity Competition 2 or COS 338 Cybersecurity Competition 3 depending on the level at which they will be competing.

Figure 3 was supplied by Dr. Max Egenhofer, Director of the School of Computing and Information Science. It shows the number of course sections that will need staffing over the next several years. Ideally, the demand can be met by adding adjuncts and/or faculty to the School of Computing and Information Science since we could more easily guarantee that the courses taught would mesh with the other courses in the program. Alternatively, we might be able to use courses supplied by one of the other campuses of the University of Maine System providing that cooperative agreements are in place.

A few words of explanation are in order for Figure 3. The sections in red are the ones that would need coverage. First, note that COS 336-338 Cybersecurity Competitions are listed as three 1-credit courses, but they could be taught in a single section with students registering for the level that is appropriate for them. Thus, it would need to be covered as a 1-credit course while the other courses would need to be covered as 3-credit courses. That is why the a+b notation, where the first number shows how many 3-credit courses need to be covered and the second number shows how many 1-credit courses need to be covered. Many semesters the shortfall is just a single course. The most problematic semester is Fall 2019, but there are a few years during which we can get ready for this semester.

In a fast changing discipline like Computer Science it is important that the Univer-

	F 2015	S 2016	F 2016	S 2017	F 2017	S 2018	F 2018	S 2019	F 2019	S 2020
COS 140	x		x		x		x		x	
COS 220	x		x		x		x		x	
COS 221		x		x		x		x		x
COS 235		x		x		x		x		x
COS 330			x		x		x		x	
COS 331				x		x		x		x
COS 336-8 1 cr			x		x		x		x	
COS 440					x		x		x	
COS 480						x		x		x
COS 490							x		x	
COS 495							x		x	
COS 497								x		x
Not Covered		1	0+1	1	2+1	2	1+1	1	3+1	2

Figure 3: Projecting the Shortages in Covering Sections for the University of Maine B. S. in Cybersecurity

sity of Maine is able to offer relevant degree programs. The B. S. in Cybersecurity is extremely relevant and will benefit the University of Maine and students.

The library and computing resources are adequate to support this new program and no large expenditures are needed for equipment. We expect the program to be successful in soliciting support for various projects. The Cybersecurity Program has successfully raised over $60,000 to support the Northeast Collegiate Cyber Defense Competition which was held at the University of Maine in 2010 and 2013. We believe this University of Maine B. S. in Cybersecurity program also has the potential of attracting out-of-state students. Finally, since the credit hour requirements of the University of Maine B. S. in Cybersecurity are substantially less than that of the University of Maine B. S. in Computer Science, it is probably an easier degree for many students to complete and an easier degree to have if a person is interested in double majoring.

Finally, the Computer Science B. S. program has historically had a substantial dropout rate. We believe that many of the students who dropout do so because of their difficulties with the more mathematical and theoretical courses. Since the University of Maine B. S. in Cybersecurity does not require these courses, we believe that many of the students who currently drop out of the Computer Science program might find the University of Maine B. S. in Cybersecurity compelling enough to remain in the program. We believe that this degree can be a significant retention tool for the School of Computing and Information Science.

8 Coverage of the NSA Knowledge Units

8.1 Basic Data Analysis - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic abilities to manipulate data into meaningful information.

8.1.1 Topics

- Summary Statistics. This topic is covered in MAT(STS) 232
- Graphing / Charts. This topic is covered in MAT(STS) 232
- Spreadsheet Functions. This topic is covered in MAT(STS) 232
- Problem Solving. This topic is covered in MAT(STS) 232

8.1.2 Outcomes

- Students will be able to apply standard statistical inference procedures to draw conclusions from data.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In MAT(STS) 232 this outcome is evaluated using exams.

8.2 Basic Scripting - 2 YEAR

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

8.2.1 Topics

- Basic Security (Bounds checking, input validation). This topic is covered in COS 220
- Program Commands. This topic is covered in COS 220
- Program Control Structures. This topic is covered in COS 220
- Variable Declaration. This topic is covered in COS 220
- Debugging. This topic is covered in COS 220
- Scripting Language (e.g. PERL, Python, BASH, VB Scripting, PowerShell). This topic is covered in COS 330 and ECE 331
- Basic Boolean logic/operations (AND / OR / XOR / NOT). This topic is covered in COS 140 and COS 220

8.2.2 Outcomes

- Students will be able to demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In ECE 331 this outcome is evaluated using exams, homework and projects.
- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 220 this outcome is evaluated using exams and homework.
- Students will be able to write simple linear and looping scripts.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In ECE 331 this outcome is evaluated using exams and homework.

8.3 Cyber Defense - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

8.3.1 Topics

- Network mapping (enumeration and identification of network components). This topic is covered in COS 330, COS 336-338 and COS 440
- Network security techniques and components (access controls, flow control, cryptography, firewalls, intrusion detection systems, etc.). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Applications of Cryptography. This topic is covered in COS 330 and COS 336-338
- Malicious activity detection / forms of attack. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Appropriate Countermeasures. This topic is covered in COS 330, ECE 331 and COS 440
- Trust Relationships. This topic is covered in COS 330

- Defense in Depth (Layering of security mechanisms to achieve desired security). This topic is covered in COS 330, ECE 331 and COS 440
- Patching (OS and Application Updates). This topic is covered in COS 330, ECE 331 and COS 331
- Vulnerability Scanning. This topic is covered in COS 330, ECE 331, COS 331 and COS 440
- Vulnerability Windows (0-day to patch availability). This topic is covered in COS 330

8.3.2 Outcomes

- Students will be able to describe potential system attacks and the actors that might perform them.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
- Students will be able to describe cyber defense tools, methods and components.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
- Students will be able to apply cyber defense methods to prepare a system to repel attacks.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.
  - In ECE 331 this outcome is evaluated using exams.
- Students will be able to describe appropriate measures to be taken should a system compromise occur.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In ECE 331 this outcome is evaluated using exams.

8.4 Cyber Threats - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

8.4.1 Topics

- Adversaries and targets. This topic is covered in COS 330
- Motivations and Techniques. This topic is covered in COS 330
- The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access). This topic is covered in COS 330
- Attack Timing (within x minutes of being attached to the net). This topic is covered in COS 330
- Types of attacks. This topic is covered in COS 330 and ECE 331
  - Password guessing/cracking. This topic is covered in COS 330 and ECE 331
  - Backdoors/Trojans/viruses. This topic is covered in COS 330 and ECE 331
  - Sniffing/spoofing/session hijacking. This topic is covered in COS 330 and ECE 331
  - Denial of service/distributed DOS/BOTs. This topic is covered in COS 330 and ECE 331
  - MAC spoofing /web app attacks /0-day exploits. This topic is covered in COS 330 and ECE 331
- Social Engineering. This topic is covered in COS 330
- Events that indicate an attack is/has happened. This topic is covered in COS 330, ECE 331 and COS 440
- Legal Issues. This topic is covered in COS 330 and COS 490
- Attack surfaces/vectors. This topic is covered in COS 330
- Attack trees. This topic is covered in COS 330
- Insider Problem. This topic is covered in COS 330
- Covert Channels. This topic is covered in COS 330
- Threat Information Sources (e.g., CERT). This topic is covered in COS 330

8.4.2 Outcomes

- Students will be able to identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.

  - In ECE 331 this outcome is evaluated using exams.

- Students will be able to describe different types of attacks and their characteristics.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.

  - In COS 330 this outcome is evaluated using exams.
  - In ECE 331 this outcome is evaluated using exams.

8.5 Fundamental Security Design Principles - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

8.5.1 Topics

- Separation (of domains). This topic is covered in COS 330, ECE 331 and COS 440
- Isolation. This topic is covered in COS 330, ECE 331 and COS 440
- Encapsulation. This topic is covered in COS 330, ECE 331 and COS 440
- Least Privilege. This topic is covered in COS 330, ECE 331 and COS 440
- Simplicity (of design). This topic is covered in COS 330 and ECE 331
- Minimization (of implementation). This topic is covered in COS 330 and ECE 331
- Fail Safe Defaults/Fail Secure. This topic is covered in COS 330 and ECE 331
- Modularity. This topic is covered in COS 330 and ECE 331
- Layering. This topic is covered in COS 330, ECE 331, COS 331 and COS 440
- Least Astonishment. This topic is covered in COS 330
- Open Design. This topic is covered in COS 330 and COS 440
- Usability. This topic is covered in COS 330, ECE 331 and COS 440

8.5.2 Outcomes

- Students will be able to list the first principles of security.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.

  - In COS 330 this outcome is evaluated using exams.

- Students will be able to describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
- Students will be able to analyze common security failures and identify specific design principles that have been violated.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and audits.
- Given a specific scenario, students will be able to identify the needed design principle.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homeworks.
- Students will be able to describe why good human machine interfaces are important to system use.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homeworks.
- Students will understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar and audits.

8.5.3 Resources

- *The Protection of Information in Computer Systems* (Saltzer and Schroeder, 1975). will be used in the following courses.
  - COS 330
- Saltzer and Kaashoek (2009). will be used in the following courses.
  - COS 330
- *Computer Security Technology Planning Study* (Anderson Report, introduced the reference monitor concept). will be used in the following courses.
  - COS 330

- Bell-LaPadula Model (first multi-level security policy model). will be used in the following courses.
  - COS 330
- Biba Integrity Model. will be used in the following courses.
  - COS 330
- System Security Analysis/Certification (Clark Weissman, introduced the flaw hypothesis methodology). will be used in the following courses.
  - COS 330
- Security Controls for Computer Systems (Ware report, first raised computer security as an issue). will be used in the following courses.
  - COS 330
- *The Trusted Computer System Evaluation Criteria* (The "Orange Book"). will be used in the following courses.
  - COS 330

8.6 IA Fundamentals - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

8.6.1 Topics

- Threats and Adversaries. This topic is covered in COS 330 and ECE 331
- Vulnerabilities and Risks. This topic is covered in COS 330 and ECE 331
- Basic Risk Assessment. This topic is covered in COS 330
- Security Life-Cycle. This topic is covered in COS 330
- Intrusion Detection and Prevention Systems. This topic is covered in COS 330, ECE 331 and COS 440
- Cryptography. This topic is covered in COS 330 and COS 336-338
- Data Security (in transmission, at rest, in processing). This topic is covered in COS 330, COS 336-338 and COS 440
- Security Models. This topic is covered in COS 330, COS 336-338 and COS 440

- Access Control Models (MACS, DAC, RBAC). This topic is covered in COS 330 and ECE 331
- Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, and Privacy. This topic is covered in COS 330 and ECE 331
- Security Mechanisms (e.g., Identification/Authentication, Audit). This topic is covered in COS 330 and ECE 331

8.6.2 Outcomes

- Students shall be able to list the fundamental concepts of the Information Assurance / Cyber Defense discipline.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In ECE 331 this outcome is evaluated using exams.
- Students will be able to describe how the fundamental concepts of cyber defense can be used to provide system security.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In ECE 331 this outcome is evaluated using exams.
- Students will be able to examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.
  - In ECE 331 this outcome is evaluated using projects.

8.6.3 Resources

- *Computer Security Art & Science* by Matt Bishop will be used in the following courses.
  - COS 330

8.7 Introduction to Cryptography - 2 YEAR

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

8.7.1 Topics

- Symmetric Cryptography (DES, Twofish). This topic is covered in COS 330 and COS 336-338
- Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3). This topic is covered in COS 330 and COS 336-338
- Public Key Cryptography. This topic is covered in COS 330 and COS 336-338
  - Public Key Infrastructure. This topic is covered in COS 330 and COS 336-338
  - Certificates. This topic is covered in COS 330 and COS 336-338
- Digital Signatures (Authentication). This topic is covered in COS 330 and COS 336-338
- For integrity. This topic is covered in COS 330 and COS 336-338
  - For protecting authentication data. This topic is covered in COS 330 and COS 336-338
  - Collision resistance. This topic is covered in COS 330 and COS 336-338
- Key Management (creation, exchange/distribution). This topic is covered in COS 330 and COS 336-338
- Cryptographic Modes (and their strengths and weaknesses). This topic is covered in COS 330 and COS 336-338
- Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.). This topic is covered in COS 330 and COS 336-338
- Common Cryptographic Protocols. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Evolution from DES to AES. This topic is covered in COS 330
- Security Functions (data protection, data integrity, authentication). This topic is covered in COS 330 and COS 336-338

8.7.2 Outcomes

- Students will be able to identify the elements of a cryptographic system.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In COS 336-338 this outcome is evaluated using competition.

- Students will be able to describe the differences between symmetric and asymmetric algorithms.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
- Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In COS 336-338 this outcome is evaluated using debriefing notes.
- Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homeworks.

8.7.3 Resources

- *Cryptography: A Very Short Introduction*, Piper and Murphy will be used in the following courses.
  - COS 330

8.8 IT System Components - 2 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

8.8.1 Topics

- Workstations. This topic is covered in COS 330
- Servers. This topic is covered in COS 330 and ECE 331
- Network Storage Devices. This topic is covered in COS 235, COS 330, COS 336-338 and ECE 331
- Routers/Switches/Gateways. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Guards/CDSes/VPNs/Firewalls. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

- IDSes, IPSes. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Mobile Devices. This topic is covered in COS 330
- Peripheral Devices/Security Peripherals. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

8.8.2 Outcomes

- Students will be able to describe the hardware components of modern computing environments and their individual functions.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In ECE 331 this outcome is evaluated using exams.
  - In COS 440 this outcome is evaluated using exams.

8.9 Networking Concepts - 2 YEAR

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

8.9.1 Topics

- Overview of Networking (OSI Model). This topic is covered in COS 330, ECE 331 and COS 440
- Network Media. This topic is covered in COS 330, ECE 331 and COS 440
- Network architectures (LANs, WANs). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Devices (Routers, VPNs, Firewalls). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Services. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Protocols (TCP/IP, HHTP, DNS, SMTP). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Topologies. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Overview of Network Security Issues. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

8.9.2 Outcomes

- Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In ECE 331 this outcome is evaluated using exams.
  - In COS 440 this outcome is evaluated using exams.
- Students will be able to describe a basic network architecture given a specific need and set of hosts/clients.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 440 this outcome is evaluated using projects.
- Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homeworks.
  - In COS 336-338 this outcome is evaluated using competition.
  - In COS 440 this outcome is evaluated using exams and homeworks.
- Students will be able to use a network monitoring tools (e.g., WireShark).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams, homework and cyberwar.
  - In COS 336-338 this outcome is evaluated using competition.
  - In COS 440 this outcome is evaluated using exams and homework.
- Students will be able to use a network mapping tool (e.g., Nmap).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams, homework and cyberwar.
  - In COS 336-338 this outcome is evaluated using competitions.
  - In COS 440 this outcome is evaluated using exams and homework.

8.10 Policy, Legal, Ethics, Compliance - 2 YEAR

The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

8.10.1 Topics

- HIPAA/FERPA. This topic is covered in COS 490
- Computer Security Act. This topic is covered in COS 490
- Sarbanes – Oxley. This topic is covered in COS 490
- Gramm – Leach – Bliley. This topic is covered in COS 490
- Privacy (COPPA). This topic is covered in COS 490
- Payment Card Industry Data Security Standard (PCI DSS). This topic is covered in COS 490
- State, US and international standards / jurisdictions. This topic is covered in COS 490
- Laws and Authorities. This topic is covered in COS 490
- US Patriot Act. This topic is covered in COS 490
- BYOD issues. This topic is covered in COS 330 and COS 490
- Americans with Disabilities Act, Section 508. This topic is covered in COS 490

8.10.2 Outcomes

- Students shall be able to list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 490 this outcome is evaluated using exams and papers.
- Students shall be able to describe their responsibilities related to the handling of information about vulnerabilities.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using homework and exams.
  - In COS 490 this outcome is evaluated using papers.
- Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In COS 490 this outcome is evaluated using papers.

8.11 System Administration - 2 YEAR

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

8.11.1 Topics

- OS Installation. This topic is covered in COS 330, ECE 331 and COS 331
- User accounts/management. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Password Policies. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Authentication Methods. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Command Line Interfaces. This topic is covered in COS 235, COS 330, COS 336-338, ECE 331 and COS 331
- Configuration Management. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Updates and patches. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Access Controls. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Logging and Auditing (for performance and security). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Managing System Services. This topic is covered in COS 330, ECE 331 and COS 331
- Virtualization. This topic is covered in COS 330 and COS 331
- Backup and Restoring Data. This topic is covered in COS 330, ECE 331 and COS 331
- File System Security. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Network Configuration (port security). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Host (Workstation/Server) Intrusion Detection. This topic is covered in COS 330, COS 336-338 and COS 440
- Security Policy Development. This topic is covered in COS 330 and ECE 331

8.11.2 Outcomes

- Students will be able to apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.
  - In ECE 331 this outcome is evaluated using homework.

8.12 Databases - 4 YEAR

The intent of this Knowledge Unit is to teach students how database systems are used, managed, and issues associated with protecting the associated data assets.

8.12.1 Topics

- Relational Databases. This topic is covered in COS 330, COS 336-338 and COS 480
- No SQL Databases. This topic is covered in COS 330 and COS 480
- Object Based vs. Object Oriented. This topic is covered in COS 480
- Overview of Database Vulnerabilities. This topic is covered in COS 330 and COS 480
- Overview of Database topics/issues (indexing, inference, aggregation, polyinstantiation). This topic is covered in COS 480
- Hashing and Encryption. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 480
- Database access controls (DAC, MAC, RBAC, Clark-Wilson). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 480
- Information flow between databases/servers and applications. This topic is covered in COS 480
- Database security models. This topic is covered in COS 330, COS 336-338 and COS 480
- Security issues of inference and aggregation. This topic is covered in COS 480
- Common DBMS vulnerabilities. This topic is covered in COS 330, COS 336-338 and COS 480

8.12.2 Outcomes

- Students will be able to describe common security models of database management systems.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In COS 336-338 this outcome is evaluated using competitions.
  - In COS 480 this outcome is evaluated using exams.
- Students will be able to identify and describe common security concerns in database management systems.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using homework, exams and cyberwar.
  - In COS 480 this outcome is evaluated using exams.
- Students will be able to apply security principles to the design and development of database systems and database structures.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 480 this outcome is evaluated using homework.

8.13 Network Defense - 4 YEAR

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

8.13.1 Topics

- Implementing IDS/IPS. This topic is covered in COS 330 and ECE 331
- Implementing Firewalls and VPNs. This topic is covered in COS 330 and ECE 331
- Defense in Depth. This topic is covered in COS 330, ECE 331 and COS 440
- Honeypots and Honeynets. This topic is covered in COS 330
- Network Monitoring. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Traffic Analysis. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Minimizing Exposure (Attack Surface and Vectors). This topic is covered in COS 330, ECE 331 and COS 440

- Network Access Control (internal and external). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- DMZs / Proxy Servers. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Hardening. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Mission Assurance. This topic is covered in COS 330
- Network Policy Development and Enforcement. This topic is covered in COS 330 and ECE 331
- Network Operational Procedures. This topic is covered in COS 330 and ECE 331
- Network Attacks (e.g., session hijacking, Man-in-the-Middle). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

8.13.2 Outcomes

- Students will be able to describe the various concepts in network defense.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In ECE 331 this outcome is evaluated using exams and homework.
  - In COS 440 this outcome is evaluated using exams and homework.
- Students will be able to apply their knowledge to implement network defense measures.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.
  - In ECE 331 this outcome is evaluated using homework and projects.
- Students will be able to use a network monitoring tools (e.g., WireShark).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams, homework and cyberwar.
  - In COS 336-338 this outcome is evaluated using competitions.
  - In ECE 331 this outcome is evaluated using homework.
  - In COS 440 this outcome is evaluated using homework.

- Students will be able to use a network mapping tool (e.g., Nmap).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams, homework and cyberwar.
  - In COS 336-338 this outcome is evaluated using competitions.
  - In ECE 331 this outcome is evaluated using homework.
  - In COS 440 this outcome is evaluated using exams and homework.

8.14 Networking Technology and Protocols - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

8.14.1 Topics

- Network Architectures. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Networks Infrastructure. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Services. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Protocols (TCP/IP – v4 and v6, DNS, HTTP, SSL, TLS). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Address Translation and Sub-netting. This topic is covered in COS 330, ECE 331 and COS 440
- Network Analysis/Troubleshooting. This topic is covered in COS 330, ECE 331 and COS 440
- Network Evolution (Change Management, BYOD). This topic is covered in ECE 331 and COS 440
- Remote and Distributed Management. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

8.14.2 Outcomes

- Students will be able to apply their knowledge of network technologies to design and construct a working network.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.

  - In COS 440 this outcome is evaluated using projects.

- Students will be able to analyze a trace of packets to identify the establishment of a TCP connection.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.

  - In COS 330 this outcome is evaluated using homework.
  - In COS 440 this outcome is evaluated using homework.

- Students will be able to demonstrate the use of a network monitor to display packets.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.

  - In COS 330 this outcome is evaluated using cyberwar.

8.15 Operating Systems Concepts - 4 YEAR

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

8.15.1 Topics

- Privileged and non-privileged states. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Processes and Threads (and their management). This topic is covered in COS 330 and COS 331
- Memory (real, virtual, and management). This topic is covered in COS 330 and COS 331
- Files Systems. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Virtualization/Hypervisors. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Access Controls (Models and Mechanisms). This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
  - Access control lists. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- How does the an OS protect itself from attack?. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

- Fundamental Security Design Principles as applied to an OS. This topic is covered in COS 330, ECE 331 and COS 331
  - Domain separation, process isolation, resource encapsulation, least privilege. This topic is covered in COS 330, ECE 331 and COS 331

8.15.2 Outcomes

- Students will be able to identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using homework and cyberwar.
  - In COS 331 this outcome is evaluated using homework.

8.16 Probability and Statistics - 4 YEAR

The intent of this Knowledge Unit is to provide students with the ability to use basic statistics to analyze and attach meaning to datasets.

8.16.1 Topics

- Probability as a concept. This topic is covered in MAT(STS) 232
- Random variables/events. This topic is covered in MAT(STS) 232
- Odds of an event happening. This topic is covered in MAT(STS) 232
- Data Interpretation. This topic is covered in MAT(STS) 232
- Statistical Problem Solving. This topic is covered in MAT(STS) 232
- Probability Distributions. This topic is covered in MAT(STS) 232

8.16.2 Outcomes

- Students will be able to evaluate probabilities to solve applied problems.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In MAT(STS) 232 this outcome is evaluated using exams and homework.
  - In COS 330 this outcome is evaluated using exams and homework.
- Students will be able to describe how basic statistics and statistical methods can be applied in a given situation.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.

  - In MAT(STS) 232 this outcome is evaluated using exams and homework.
  - In COS 330 this outcome is evaluated using exams and homework.

8.17 Programming - 4 YEAR

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

8.17.1 Topics

- Programming Language, such as: C. This topic is covered in COS 220 and COS 221
- Programming constructs and concepts variables, strings, assignments, sequential execution, loops, functions.. This topic is covered in COS 220 and COS 221
- Security issues, such as type checking and parameter validation.. This topic is covered in COS 220 and COS 221
- Basic Boolean logic/operations(AND/OR/XOR/NOT).. This topic is covered in COS 140 and COS 220

8.17.2 Outcomes

- Students will be able to demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 220 this outcome is evaluated using exams and homework.
  - In COS 221 this outcome is evaluated using exams and homework.
- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In ECE 331 this outcome is evaluated using exams and homework.
  - In COS 480 this outcome is evaluated using exams and homework.
- Students will be able to demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web).. The following list describes the courses that this outcome is measured in and the instruments used to measure it.

  - In COS 220 this outcome is evaluated using exams, homework and .
  - In COS 221 this outcome is evaluated using exams and homework.
  - In COS 495 this outcome is evaluated using employer evaluation.
  - In COS 497 this outcome is evaluated using the final project evaluation.

8.18 Advanced Network Technology & Protocols - Optional KU #1

The intent of this Knowledge Unit is to provide students with an understanding of the latest network technologies and more complex security issues involved in network communications. Examples include (but not limited to): software defined networking, converged voice/data networking.

8.18.1 Topics

- Routing algorithms and protocols. This topic is covered in COS 440
- IPv6 Networking Suite. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Software Defined Networking. This topic is covered in COS 440
  - Principles, protocols, implications. This topic is covered in COS 440
- BGP. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Quality of Service. This topic is covered in COS 440
- Network Services. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Social Networks. This topic is covered in COS 330
- Network Topologies. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Voice over IP (VoIP). This topic is covered in COS 330 and COS 440
- Multicasting. This topic is covered in COS 440
- Advanced Network Security Topics. This topic is covered in COS 330 and COS 440
  - Secure DNS. This topic is covered in COS 330, COS 336-338 and COS 440
  - Network Address Translation. This topic is covered in COS 330, COS 336-338 and COS 440
  - Deep Packet Inspection. This topic is covered in COS 330, COS 336-338 and COS 440
  - Transport Layer Security. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

8.18.2 Outcomes

- Students will be able to describe current networking technologies and trends.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In COS 440 this outcome is evaluated using exams and homework.
- Students will be able to describe and discuss data network architectures and protocols, to include their advantages and disadvantages, applications, and security issues.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In COS 440 this outcome is evaluated using exams and homework.

8.19 Network Security Administration - Optional KU #2

The intent of this Knowledge Unit is to provide students with knowledge of the methods of analyzing and mitigating threats within a network environment.

8.19.1 Topics

- Network Components. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Protocols. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Security Devices. This topic is covered in COS 330 and COS 440
- Network Security Services. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Protection of Communicated Data. This topic is covered in COS 330, COS 336-338 and COS 440
- Network Configuration. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Security Automation. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440
- Network Security Policies. This topic is covered in COS 330, ECE 331 and COS 440
- Packet Capture and Analysis. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 440

8.19.2 Outcomes

- Students will be able to appropriately position network security components within a network architecture to implement a layered defense.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.
  - In COS 440 this outcome is evaluated using projects.
- Students will be able to securely configure network devices and services and establish secure communications between networks.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using cyberwar.
  - In COS 440 this outcome is evaluated using exams and homework.

8.20 IA Compliance - Optional KU #3

The intent of this Knowledge Unit is to provide students with an understanding of the rules, regulations and issues related to compliance with applicable laws and regulations.

8.20.1 Topics

- HIPAA. This topic is covered in COS 330 and COS 490
- Sarbanes Oxley. This topic is covered in COS 330 and COS 490
- FERPA. This topic is covered in COS 330 and COS 490
- Data Breach Disclosure Laws. This topic is covered in COS 330 and COS 490
- FISMA. This topic is covered in COS 330 and COS 490
- Gramm Leach Bliley. This topic is covered in COS 330 and COS 490
- PCI DSS. This topic is covered in COS 330 and COS 490

8.20.2 Outcomes

- Students shall be able to list the applicable laws for compliance in a given situation.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams.
  - In COS 490 this outcome is evaluated using exams.

- Students shall be able to describe what the laws mandate and where they apply.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In COS 490 this outcome is evaluated using exams and papers.
- Students will be able to conduct audits to determine compliance with laws.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using audits.

8.21 IA Standards - Optional KU #4

The intent of this Knowledge Unit is to provide students with an understanding of the common standards related to information assurance.

8.21.1 Topics

- HIPAA. This topic is covered in COS 330 and COS 490
- FERPA. This topic is covered in COS 330 and COS 490
- Sarbanes-Oxley. This topic is covered in COS 330 and COS 490
- Understanding appropriate commercial standards. This topic is covered in COS 330 and COS 490
- Knowing which standards apply to specific situations. This topic is covered in COS 330 and COS 490
- Rainbow Series. This topic is covered in COS 330 and COS 490

8.21.2 Outcomes

- Students will be able to describe the impact of legal/regulatory standards on a given system.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In ECE 331 this outcome is evaluated using exams and homework.
- Students will be able to describe how standards, such as the Orange Book, may be applied to the requirements for a sub-contractor or customer.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using audits.

8.22 Operating Systems Theory - Optional KU #5

The intent of this Knowledge Unit is to provide students with an understanding of the issues related to the design and implementation of operating system concepts, components and interfaces.

8.22.1 Topics

- Privilege States. This topic is covered in COS 330, COS 336-338 and COS 331
- Processes & Threads, Process/Thread Management. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Memory Management, Virtual Memory. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Inter-process Communications. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Concurrency and Synchronization, Deadlocks. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- File Systems. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Input/Output. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Real-time operating systems/security issues. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Distributed OS architectures & security issues. This topic is covered in COS 331
- Race Conditions. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Buffer Overflows. This topic is covered in COS 330 and COS 331
- Virtualization. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331
- Clear Interface Semantics. This topic is covered in COS 330, COS 336-338, ECE 331 and COS 331

8.22.2 Outcomes

- Students will have an understanding of operating systems theory and implementation. They will understand OS internals to the level that they can design and implement significant architectural changes to an existing OS.. The following list describes the courses that this outcome is measured in and the instruments used to measure it.
  - In COS 330 this outcome is evaluated using exams and homework.
  - In COS 331 this outcome is evaluated using exams and homework.