LSC Use Only
Number:
Submission Date:
Action-Date:

FEB 28 2002

UWUCC USE Only
Number: 01-57g
Submission Date:
Action-Date: UWUCC Appr - 4/16/02
Senate Appr 5/7/02

CURRICULUM PROPOSAL COVER SHEET
University-Wide Undergraduate Curriculum Committee

I. CONTACT

Contact Person DENNIS GIEVER Phone X 7-5600

Department CRIMINOLOGY

MAR 14 2002 LIBERAL STUDIES

II. PROPOSAL TYPE (Check All Appropriate Lines)

____ COURSE

Suggested 20 character title

__X__ New Course* CRIM 323 CYBERSECURITY AND THE LAW
Course Number and Full Title

____ Course Revision
Course Number and Full Title

____ Liberal Studies Approval+ for new or existing course
Course Number and Full Title

____ Course Deletion
Course Number and Full Title

____ Number and/or Title Change
Old Number and/or Full Old Title

New Number and/or Full New Title

APR - 1 2002

____ Course or Catalog Description Change
Course Number and Full Title

____ PROGRAM: ____ Major ____ Minor ____ Track

____ New Program*
Program Name

____ Program Revision*
Program Name

____ Program Deletion*
Program Name

____ Title Change
Old Program Name

New Program Name

III. Approvals (signatures and date)

Department Curriculum Committee — Department Chair

College Curriculum Committee — College Dean 11/14/2001

+Director of Liberal Studies (where applicable) — *Provost (where applicable)

SYLLABUS OF RECORD

I. Catalog Description

CRIM 323 Cybersecurity and the Law
Prerequisite: CRIM 101 or CRIM 102

3 lecture hours
0 lab hours
3 semester hours
(3c-0l-3sh)

Examines the scope of cybercrime and its impact upon today's system of criminal justice. Topics to be studied include: Cybercrime and the Bill of Rights, computer-based economic crime, electronic commerce, ethical challenges, and the Computer Fraud and Abuse Act. Included will be an analysis of the legal considerations facing law enforcement and cybersecurity professionals who deal with the problem of discovering, investigating, and prosecuting cybercrime.

II. Course Objectives

Students will:

Gain knowledge about the way in which cybersecurity, and the computer itself, has affected - and has been affected by - the criminal justice system, law enforcement professionals, and the community-at-large.

More specifically, it is expected that each student will:

- Become conversant with terminology of the world of "cyberspace," with emphasis on terms and concepts pertinent to the application of computerization within the criminal justice system.
- Be able to discuss the impact that specific security issues related to cybertechnology have had on the criminal justice system in particular, and upon modern society in general, in the context of past, present, and future developments.
- Be able to identify and analyze provisions of the United States Constitution, with special emphasis on The Bill of Rights, which underlie the basis upon which the criminal justice system must deal with "cybercrime," and those who commit such criminal acts.
- Be able to distinguish the particular attributes of a computer-based economic system which tend to facilitate fraud and other criminal acts by those with criminal intent.
- Be able to compare and contrast and, more significantly, understand those efforts undertaken by the Legislative and Executive branches of both state and federal government to thwart crimes facilitated by or, in some instances, only made possible by the use of computers.

- ❖ Be able to trace the history of development of the law enforcement community's efforts at policing the unlawful use of computers.

- ❖ Be able to identify the ethical challenges to be considered by those within the law enforcement field who are working to thwart cybertech crime.

- ❖ Be able to anticipate changes in laws and legal procedures that may likely occur as the criminal justice system attempts to forestall further incursions by deviants into the world of cybertech security.

III. Detailed Course Outline

This course is comprised of seven (7) units of study. The units begin with a study of the fundamental concepts relative to the study of Cybersecurity and the Law. The units follow a pattern of progression which introduces students to the positive applications of Cybertechnology by Law Enforcement and other Criminal Justice entities, and then focuses on the respective agencies whose job it is to impede Cybercrime. The use of computer technology to carry out crimes of a more traditional nature is followed by the study of criminal offenses which are peculiar to the Cybertech world. Methods of, and the problems inherent in, locating, securing, seizing and analyzing "Cyber Evidence" is then discussed.

Significant attention - through analysis of pertinent case law - is directed to how the court system has dealt with both the innovative concepts inherent in Cybersecurity, and also how computerization has affected more traditional concepts of Criminal Law, Criminal Procedure, and Constitutional Law. Specifically, decisions from both the federal and state court systems will be read, reviewed, and discussed.

A survey of statutory law enacted both by Congress and respective state legislatures follows as a demonstration of the type of legislative initiatives that have been directed at enhancing Cybersecurity, thwarting Cybercrime, and punishing those who would seek to use such modern technology for criminal purposes.

The course concludes with a "look ahead" to the future; what can be expected when Cybersecurity is confronted by even more technological innovations.

The major substantive areas are as follows:

Unit I (1 week)

Introduction to Cybersecurity
- Safeguarding Computers
- Concept of "Digital Evidence"
- Definitions Relating to Cybersecurity
- The Language of Cybersecurity
- Turning Technology Against the Perpetrators

Forensic Science Applications
Computer Systems Security
Evidence Gathering
Use of Computers at Trial

Unit II (1 week)

Applying Forensic Science to Computers
Law Enforcement Use of Computers
Law Enforcement Agencies with Active Computer Search and Seizure Groups
Digital Evidence on Computer Networks
Digital Evidence on the Internet

Unit III (2 weeks)

Traditional Substantive Offenses Subject to Cybertechnology Implications
Espionage
Drug trafficking
Terrorism
Cyberstalking
Violence, or Threat of Violence, Against Others
Gambling on the Web
Money Laundering
R.I.C.O.
Offenses Against Children

Unit IV (1 week)

Where to Look for the "Smoking Gun" of Stored or Transmitted Digital Evidence
Digital Evidence at the Transport and Network Layers
Digital Evidence on the Data-Link and Physical Layers
Using Digital Evidence and Behavioral Evidence Analysis in an Investigation

Unit V (1 week)

Computer "Crackers"
Computer Intrusion
Fraud
Cyberstalking
Digital Evidence as Alibi
Methods and Legal Challenges of Ensuring Security

MIDTERM

Unit VI (2 weeks)

Cybertechnology and the Courts:
- Digital Evidence as Alibi
- Statutory Law
- Copyrights
  - Copyright Act of 1976
- Theories of Liability for Copyright Infringement
- Limitations on Copyright Owner's Exclusive Rights
- Remedies for Copyright Infringement

Unit VII (2 weeks)

Jurisdiction for Investigation and Prosecution Cases
- Traditional Principles of Jurisdictions
- Judicial History of Personal Jurisdiction
- Personal Jurisdiction in the Online Environment
- Federal Jurisdictions
- State Jurisdictions

Unit VIII (2 weeks)

Implications of the U.S. Constitution and Bill of Rights
Privacy
- Sources of the Right to Privacy
- Common Law Torts for Invasion of Privacy
- First Amendment Protection – Freedom of Expression
  - Government Regulation of Cyberporn
  - Child Pornography
  - Employees and Workplace Access to Adult Web Sites
  - Global Issues: Obscenity on the Internet

Unit XI (2 weeks)

A Look Ahead: "What's in the Future For Cybersecurity?"
Global Issues
- International Organizations
- Jurisdictions
- Choice of Law
- Substantive Laws Affecting Electronic Commerce
- The Law of Contracts
- Regulation of the International Movement of Capital
- Taxation of International Electronic Commerce

IV. Course Evaluation Methods

30% QUIZZES - There will be three (3) quizzes during the semester (each of these will be valued at maximum of 10 %). Two (2) of these will be objective quizzes. All of the objective quiz questions will be based upon previously assigned reading material, as well as prior class discussions.

25% MID-TERM EXAM. This will be an essay-type exam. It will consist of an in-class writing exercise answering specific questions that relate to the assigned readings. The focus will be on analysis, understanding, and utilization of the substantive content of prior reading assignments to fashion an appropriate response to questions involving topics covered to date.

15% PAPER - This exercise, an original writing of no more than five, double-spaced typewritten or computer-printed pages will be on a topic chosen by the student and approved in advance by the instructor. Recommended topics can include any drawn from the assigned readings, or from class. The completed paper will be due three (3) weeks before the final exam.

25% FINAL EXAMINATION. This objective exam will consist of multiple choice, true-false, and "fill in the blank" questions. For this exam, students will be responsible for the materials covered in the reading assignments, and for those matters that were the subject of discussion. Computer scoring will be used for this exam, and it will be taken using "bubble sheets."

5% CLASS PARTICIPATION. A subjective evaluation by the instructor of overall classroom performance of each student. Preparedness for class, as evidenced by a demonstrated understanding of the content of reading assignments, will be graded along with the exhibited level of participation in class discussions. The overall evaluation will involve equal consideration of these three areas: (1) class attendance; (2) the volunteering of pertinent comments and/or answers; and, (3) correct responses to questions asked by the instructor - that is, exhibiting evidence of BEING PREPARED FOR CLASS! In addition, the first portion of each class will be used to identify and discuss <u>current</u> cases and incidents in the news which involve either or both of the principal subjects of this course, "Cybertechnology" and the "Criminal Justice System." Therefore, each student should come to class fully prepared to discuss any such contemporary matters appearing in the media which relate to either or both of those topics and, more specifically, how such current issues in the news relate to the totality of the subject matter being covered by the course.

100% Total

GRADING SCALE:

A.....90 % - 100 % B.....80 % - 89 % C.....70% - 79%

D.....60 % - 69 % F.....Below 60 %

V. Textbooks and Other Required Readings

The course text is:
Casey, Eoghan (2000). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* San Diego, CA: Academic Press.

Additional assigned readings will be available on reserve at the library and posted online, and will include the following:

Articles to be read for class discussion: [The following selections are similar to those which will be included in the final Syllabus - however, others may be substituted which may be more current to the time at which the course is actually offered].

1. "Computer-crime treaty evokes criticism from U.S. tech firms," MSNBC, 26 October 2000.
2. "E-Signatures Become Valid," New York Times, 2 October 2000.
3. "Ex-NSA expert warns of concealed backdoors," ZDNet News UK, 25 September 2000 (reported by GJ Halfond).
4. "Experts see rash of hack attacks coming; recent costly hits show 'more brazen' criminals preying on companies," USA Today, 27 September 2000.
5. "Microsoft Says Hackers Broke Into Its Network," Washington Post, 27 October 2000.
6. "Mideast hackers may strike U.S. sites," FBI warns, Cnet, 2 November 2000.
7. "Report finds risk but supports Carnivore email surveillance," CNet, 21 November 2000.
8. "Scarfo case could test cyber-spying tactic," Philadelphia Inquirer, 4 December 2000 (suggested by William GJ Halfond).
9. "Sonic: another self-updating Internet -worm has been discovered 'in the wild'," Net Security, 2 November 2000.
10. "The Risks of Touch-Screen Balloting," San Francisco Chronicle, 4 December 2000.
11. "The Nexus of Privacy and Security," New York Times, 8 December 2000. Report on SafeNet conference sponsored by Microsoft.
12. "U.S., European Union move toward cybercrime treaty," USA Today, 27 September 2000.

VI. Special Resources Requirements

None

VII. Bibliography

1. "Computer-crime treaty evokes criticism from U.S. tech firms," MSNBC, 26 October 2000.
2. Computer Crime: A Crimefighter's Handbook (Computer Security), Icove, David J., *et al*, O'Reilly and Associates, (1996) ISBN 1565921062.

3. Computer Law, Blackstone, Chris Reed, Editor, Blackstone Press Ltd, London, (1993) ISBN 1-85431-227-8.
4. Crime, Deviance and the Computer, Hollinger, Richard C., Ashgate Publishing Company, (1997) ISBN 1855214679.
5. Cybercrime: How To Protect Yourself from Computer Criminals, Quarantiello, Laura E., Tiare Publications, (1996) ISBN 0936653744.
6. Definitive Guide to Criminal Justice and Criminology on the World Wide Web. CJ Distance Learning Consortium, Prentice Hall, (1999) ISBN 0-13-096251-1.
7. "E-Signatures Become Valid", New York Times, 2 October 2000.
8. "Ex-NSA expert warns of concealed backdoors" - ZDNet News UK, 25 September 2000 (reported by GJ Halfond).
9. "Experts see rash of hack attacks coming; recent costly hits show 'more brazen' criminals preying on companies," USA Today, 27 September 2000.
10. Halting the Hacker: A Practical Guide to Computer Security, Pipkin, Donald L., Prentice Hall, (1996) ISBN 013243718X.
11. "Microsoft Says Hackers Broke Into Its Network," Washington Post, 27 October 2000.
12. "Mideast hackers may strike U.S. sites," FBI warns, Cnet, 2 November 2000.
13. "Report finds risk but supports Carnivore email surveillance," CNet, 21 November 2000.
14. "Scarfo case could test cyber-spying tactic," Philadelphia Inquirer, 4 December 2000 (suggested by William GJ Halfond).
15. "Sonic: another self-updating Internet -worm has been discovered 'in the wild'," Net Security, 2 November 2000.
16. "The Risks of Touch-Screen Balloting," San Francisco Chronicle, 4 December 2000.
17. "The Nexus of Privacy and Security," New York Times, 8 December 2000. Report on SafeNet conference sponsored by Microsoft.
18. "U.S., European Union move toward cybercrime treaty," USA Today, 27 September 2000.

COURSE ANALYSIS QUESTIONNAIRE

Section A: Details of the Course

A1 How does this course fit into the programs of the department? For what students is the course designed? (majors, students in other majors, liberal studies).

This course is designed as one of nine required courses for an interdisciplinary minor in cybersecurity. It will most likely be restricted to students enrolled in the minor.

A2 Does this course require changes in the content of existing courses or requirements for a program? If catalog descriptions of other courses or department programs must be changed as a result of the adoption of this course, please submit as separate proposals all other changes in courses and/or program requirements.

No.

A3 Has this course ever been offered at IUP on a trial basis (e.g. as a special topic)? If so, explain the details of the offering.

No.

A4 Is this course to be a dual-level course? If so, what is the approval status at the graduate level?

No.

A5 If this course may be taken for variable credit, what criteria will be used to relate the credits to the learning experience of each student? Who will make this determination and by what procedures?

This course cannot be taken for variable credit.

A6 Do other higher education institutions currently offer this course? If so, please list examples.

The concept of an interdisciplinary program which explores the legal ramifications of Cybersecurity at the undergraduate level has been virtually unknown previously. Although there have been certain limited efforts in pursuit of such a multi-disciplinary approach to such inter-related issues – as an example, those which were pioneered by Daniel J. Ryan of the Wyndrose Technical Group whose inroads have generally been directed toward security professionals in both the private and public sectors – no other institution of higher learning has yet attempted to integrate such specific studies within the context of an entire academic track for undergraduate university students.

A7 Is the content, or are the skills, of the proposed course recommended or required by a professional society, accrediting authority, law or other external agency? If so, please provide documentation. Explain why this content or these skills cannot be incorporated into an existing course.

No.

Section B: Interdisciplinary Implications

B1 Will this course be taught by one instructor or will there be team teaching? If the latter, explain the teaching plan and its rationale.

This course will be taught by one instructor.

B2 What is the relationship between the content of this course and the content of courses offered by other departments? Summarize your discussions (with other departments) concerning the proposed changes and indicate how any conflicts have been resolved. Please attach relevant memoranda from these departments which clarify their attitudes toward the proposed change(s).

This course ties directly to the content of other courses in the interdisciplinary minor.

B3 Will seats in this course be made available to students in the School of Continuing Education?

Yes.

Section C: Implementation

C1 Are faculty resources adequate? If you are not requesting or have not been authorized to hire additional faculty, demonstrate how this course will fit into the schedules of current faculty. What will be taught less frequently or in fewer sections to make this possible?

Yes. This course will be taught as part of our electives package. As such, this new course will replace an existing section of another criminology elective class.

C2 What other resources will be needed to teach this course and how adequate are the current resources? If not adequate, what plans exist for achieving adequacy? Reply in terms of the following:

***Space**
One conventional classroom.
***Equipment**
Access to POWERPOINT, overhead projectors, and a VCR/TV.
***Laboratory Supplies and other Consumable Goods**
None.
***Library Materials**
Reserve materials available through the internet.
***Travel Funds**
None anticipated at this time.

C3 Are any of the resources for this course funded by a grant? If so, what provisions have been made to continue support for this course once the grant has expired? (Attach letters of support from Dean, Provost, etc.)

Yes. Start up money for course development was provided by an NSF grant.

C4 How frequently do you expect this course to be offered? Is this course particularly designed for or restricted to certain seasonal semesters?

At least once yearly, but as demand increases we may offer this course once a semester.

C5 How many sections of this course do you anticipate offering in any single semester?

Initially, one.

C6 How many students do you plan to accommodate in a section of this course? Is this planned number limited by the availability of any resources? Explain.

Thirty (30); the anticipated regular interaction between the instructor and the respective students proscribes any larger number.
No.

C7 Does any professional society recommend enrollment limits or parameters for a course of this nature? If they do, please quote from the appropriate documents.

No.

Section D: Miscellaneous

Include any additional information valuable to those reviewing this new course proposal.

None.

Indiana University of Pennsylvania

Department of Special Education and Clinical Services
Davis Hall, Room 203
570 South Eleventh Street
Indiana, Pennsylvania 15705-1087

724-357-2450
Fax: 724-357-7716
Internet: *http://www.iup.edu*

November 13, 2001

To Whom It May Concern:

As Chairperson of the University Senate of the Indiana University of Pennsylvania, I am often consulted on curriculum matters, as an ex officio member of our curriculum committees. In the role, I am aware of the efforts of the Criminology and Computer Science departments in preparing a program in the area of CyberSecurity. I believe that our departments are uniquely qualified to offer such a program, and I strongly support the concept. As they proceed through the curriculum approval process, I am sure there will be appropriate input from all levels to optimize the quality of such a program.

Sincerely,

Richard C. Nowell, Chair
IUP University Senate

MEMORANDUM

TO: Gary Buterbaugh

FROM: Rich Nowell

RE: CyberSecurity Program

DATE: 11/13/01

Gary:

I don't have any power as Chair of the Senate to make any recommendations on curriculum approval, but I am attaching a letter of support, for what it's worth. I am sure the committee will give it a quick review to provide the necessary signature from them. Let me know if there is anything else I can do. I will be out of the country the rest of the week, but I'll be available after the holiday, and by e-mail in the interim, I hope.

Indiana University of Pennsylvania

Department of Management Information Systems
The Eberly College of Business and Information Technology
664 Pratt Drive, Room 203
Indiana, Pennsylvania 15705-1087

724-357-2929
Fax: 724-357-4831
Internet: *http://www.eberly.iup.edu/im/*

Date: December 10, 2001

To: Dr. William Oblitey
Computer Science Department

From: Dr. Louise Burky
MIS & Decision Sciences Department

RE: MIS Minor

Dear Bill,

Please consider this a letter of approval for your Cybersecurity/Information Assurance minor which would be available to our majors. At the present time, I can only commit to one course in that area, namely IFMG 382 Auditing for EDP Systems. I could offer it once every two or three semesters. If we are able to hire more faculty, and that is a big if, other possibilities may come into being.

Along with this, is my implied approval for your entire endeavor along the lines of cybersecurity.

Sincerely,

Louise Burky

Louise Burky, Chair
MIS and Decision Sciences Department

cc: Mary Micco

Statement Of Support For
Joint Minor In Cyber Security
Cyber Track in the BS Degree in Computer Science
APSCUF

IUP-APSCUF believes that should this proposal clear the curriculum committee as written, IUP-APSCUF would allow the proposal to be forwarded to the IUP Council of Trustees.

Approved: Patricia I. Heilman
Signature

Patricia I. Heilman
Printed Name

President, IUP-APSCUF
Title

12-10-01
Date