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

FEB 28 2002

UWUCC USE Only
Number: 01-57f
Submission Date: _____
Action-Date: UWUCC App 3/19/02
Senate App 5/7/02

# CURRICULUM PROPOSAL COVER SHEET
University-Wide Undergraduate Curriculum Committee

## I. CONTACT

Contact Person DENNIS GIEVER Phone X 7-5600

Department CRIMINOLOGY

## II. PROPOSAL TYPE (Check All Appropriate Lines)

_____ **COURSE** _____
Suggested 20 character title

__X__ New Course* CRIM 321 CYBERSECURITY AND LOSS PREVENTION
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

____ 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

RECEIVED MAR 14 2002 LIBERAL STUDIES

RECEIVED APR - 1 2002

## III. Approvals (signatures and date)

James L. Martin
Department Curriculum Committee

Kevin Grieve
Department Chair

R. Royce Smith
College Curriculum Committee

11/14/2001
College Dean

+Director of Liberal Studies (where applicable)

*Provost (where applicable)

## SYLLABUS OF RECORD

### I. Catalog Description

CRIM 321 Cybersecurity and Loss Prevention — 3 lecture hours
Prerequisite: CRIM 101 or CRIM 102 — 0 lab hours
3 semester hours
(3c-0l-3sh)

Addresses the cybersecurity threat from a more comprehensive standpoint. Students will be challenged to recognize and understand security concerns from multiple perspectives, ranging from the insider threat to threats involving the actual physical components. Exposure to a design methodology, associated system components modules, and basic security principles are featured in this course. Students will also be exposed to the private and public responses to computer security problems, including the insider threat, domestic and foreign terrorism, and a number of unique computer crimes and solutions to deal with these crimes. The importance of a sound security policy in the overall management of any organization will be addressed.

### II. Course Objectives

Upon completion of the course students will:

- Possess an understanding of physical security system design and evaluation.
- Gain an understanding of the process of evaluating existing or proposed physical protection systems.
- Understand the policies and procedures needed to protect an organization and its computer resources from insiders who might do harm.
- Recognize the threat from domestic and foreign terrorism.
- Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

### III. Detailed Course Outline

A. Design and Evaluation of Physical Protection Systems **(2 Weeks)**

Facility Characterization
Threat Definitions
Target Identification

B. Physical Protection System Design (3 Weeks)

The Outsider Threat
- Exterior Intrusion Sensors
- Interior Intrusion Sensors
- Alarm Assessment
- Alarm Communication and Display
- Entry Control
- Access Control
- Access Delay
- Response

The Insider Threat

C. Analysis and Evaluation (2 Weeks)

Computer Model for Analysis
Risk Assessment

MIDTERM

D. Terrorism (4 Weeks)

History
Federal Response
Weapons of Mass Effect
- Chemical
- Biological
- Cyber
- Radiation
- Explosives

Crime Scene Operation

E. Cyber Crime (3 Weeks)

Digital Evidence
CyberStalking
Computer Crackers
Forensic Science and Computers

## IV. Course Evaluation Methods

| | |
|---|---|
| Midterm Examination | 20% |

| | |
|---|---|
| Final Examination | 20% |
| Review Essays | 20% |
| Final Problem Solution | 30% |
| Attendance | 10% |
| Total | 100% |

Grading Scale:
90% – 100% . . . A
80% – 89% . . . . B
70% – 79% . . . . C
60% – 69% . . . . D
Below 60% . . . . F

Examinations: There will be two examinations in this class, a midterm and a final. Both will cover material from the books, readings placed on reserve, guest lectures, films and class presentations.

Attendance Policies: Students are expected to attend class regularly, and to prepare for class by reading the scheduled assignments. Since students will be working in groups and sharing their ideas with fellow students, class participation is very important. Students who fail to come to class prepared or have more than 3 hours of unexcused absence can expect to have points automatically deducted from this part of their grade. Students can expect to loss points equivalent to 1% of their final grade per class hour missed due to unexcused absences (remember this is after 3 class hours are missed). If it becomes apparent that a student is unprepared for class, it will be treated as an unexcused absence. Class attendance and participation will be worth up to 10% of your final grade.

Review Essays: Students will be assigned two research essays during the semester. These two research essays will deal with computer security issues within an organization. Students are to critique the article and, utilizing knowledge gained from this class, address a more appropriate method of minimizing the threat.

Final Problem Solution: The final requirement for this class will be a problem solution comprised of two parts – an in class presentation of your system design (10% of your final grade) and a 30 page (minimum) paper describing the new design (20% of your final grade). Students will work in teams assigned by the instructor.

## V. Textbooks and Other Required Readings

Garcia, Mary Lynn (2001). *The Design and Evaluation of Physical Protection Systems.* Boston, MA: Butterworth-Heinemann.

Maniscalco, Paul M. & Christen, Hank T. (2001). *Understanding Terrorism and Managing the Consequences.* Upper Saddle River, NJ: Prentice Hall.

Material placed on reserve in the library.

## VI. Special Resources Requirements

Existing Cybersecurity Laboratory – Purchased with NSF Grant # 0113533

## VII. Bibliography


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

Cooper, Paul (1996). *Introduction to the Technology of Explosives (2nd Ed.).* New York, NY: Wiley.

Dr. K (2000). *A Complete Hacker's Handbook: Everything You Need To Know About Hacking in the Age of the Web.* London, UK: Carlton.

Fennelly, Lawrence J. (1996). *Handbook of Loss Prevention and Crime Prevention (3rd Ed.).* Boston, MA: Butterworth-Heinemann.

Hudson, David (1997). *Rewired: A Brief (and Opinionated) Net History.* Indianapolis, IN: Macmillan Technical Publishing.

Moore, James (2001). *Very Special Agents: The Inside Story of America's Most Controversial Law Enforcement Agency – The Bureau of Alcohol, Tobacco, and Firearms.* Urbana, IL: University of Illinois Press.

Nichols, Randall K., Ryan, Daniel J., Ryan, Julie J. C. H. & Coviello, Arthur W. Jr. (1999). *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves.* New York, NY: McGraw-Hill.

Pipkin, Donald L. (2000). *Information Security: Protecting the Global Enterprise.* Upper Saddle River, NJ: Prentice-Hall.

Power, Richard (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace.* Indianapolis, IN: QUE.

Rubin, Aviel D. (2001). *White-Hat Security Arsenal: Tackling the Threats.* Boston, MA: Addison-Wesley.

Simonsen, Clifford E. & Spindlove, Jeremy R. (2000). *Terrorism Today: The Past, The Players, The Future.* Upper Saddle River, NJ: Prentice Hall.

## 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.**

None that we are aware of.

**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.**

Universities are being encouraged to develop programs in information assurance by the federal government. This interdisciplinary minor is our unique approach to this initiative.

## 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**

***Equipment**

***Laboratory Supplies and other Consumable Goods**

***Library Materials**

***Travel Funds**

Funds for equipment and laboratory supplies are provided for by an NSF grant.

**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?**

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.**

We plan to accommodate 30 students in each section offered.
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.**