**UNIVERSITY OF MARY WASHINGTON -- NEW COURSE PROPOSAL**

Electronically submit this completed form with attachments in one file to the Chair of the College Curriculum Committee.

<table>
<thead>
<tr>
<th>COLLEGE (check one):</th>
<th>Arts and Sciences</th>
<th>Business</th>
<th>X</th>
<th>Education</th>
</tr>
</thead>
</table>

Proposal Submitted By: Kimberley L. Kinsley  
Date Prepared:  

Course Title: Cybersecurity Law  
Department/discipline and course number*: BLAW 300  
Prerequisites: COB Major/Minor or Cybersecurity Major and Junior or Senior Status, or Permission of the COB Associate Dean of Faculty  

*This course number must be approved by the Office of the Registrar before the proposal is submitted.

Number of credits: 3  
Will this course meet for at least 700 contact minutes for each credit hour proposed? **YES**  
Will this be a new, repeatable “special topics” course? (Do you want students to be able to take this new course more than once if the topic changes?) **NO**  

Date of first offering of this new course: **FALL SEMESTER, year** Fall 2019; or Spring 2020  
Proposed frequency of offering of the course: Once/academic year  
Proposed enrollment limit for the course: 35  
List the faculty who will likely teach the course: Kimberley L. Kinsley  
Are ANY new resources required? **YES** Document in attached impact statement  

**The earliest the course may be offered is the fall semester of the academic year FOLLOWING the year in which the course proposal is approved.**

This new course will be (check all that apply):  
Required in the major - Cybersecurity  
Elective in the major – COB  
General Education**  

**AFTER the new course is approved, a separate proposal must be sent to the General Education Committee.**

Catalog Description (suggested length – less than 50 words): Students will examine legal, policy, and ethical challenges stemming from cybersecurity threats involving government and non-government actors. Students will explore the national and international legal frameworks that govern malicious and defensive actions in cyberspace, including laws related to cybercrime, cyberespionage, privacy, and cyberwar. This is a core requirement for a cybersecurity major, and may satisfy the upper level business elective requirement for a business administration major.

COURSE HISTORY:  
Was this course taught previously as a topics or experimental course? **YES**  

<table>
<thead>
<tr>
<th>Course Number and Title of Previous Course</th>
<th>Semester Offered</th>
<th>Enrollment</th>
</tr>
</thead>
</table>

CHECK HERE if the proposed course is to be equated with the earlier topics or experimental offerings. If equated, students who took the earlier “topics” course will only be able to take the new course as a repeat (C- grade or lower).  

NOTE: If the proposed course has not been previously offered as a topics or experimental course, explain in the attached rationale statement why the course should be adopted even though it has not been tried out.

REQUIRED ATTACHMENTS:  
1. Rationale Statement – Why is this course needed? What purposes will it serve?  
2. Credit Hour Justification (if required) – explain how this course will comply with the UMW Credit Hours Policy (D.5.3)  
3. Impact Statement – Provide details about the Library, space, staffing, budget, and technology impacts created by adding this new course. Include supporting statements from the Library, IT Department, etc. Any change that impacts another Department must have a written statement (such as an email) from the Chair(s) agreeing to the change.  
4. Sample Syllabus

Department Chair Approval*: Rachel Graefe-Anderson  
Date: 10/8/18  

CCC Chair Approval: Chris Garcia  
Date: 10/17/18  

New Course Proposal Cover Sheet (July 2018)
1. Rationale Statement – Why is this course needed? What purposes will it serve?

The COB embraces liberal arts tradition and its geographic location. This course furthers the COB Mission by offering a new course that fulfills a requirement for a major in a CAS department, and is relevant to employment and internship opportunities for COB students in the geographic location.

This Washington Post article (noted below [1]) found that job postings in cybersecurity in the Washington area were growing more than in Silicon Valley and in New York City. A recent 2017 report [2] indicated that there were approximately 36,000 open cybersecurity jobs in Virginia alone. While the legal course will focus on regulation, ethics and policy regarding cybersecurity, it offers a critical perspective to the cybersecurity field. In fact, the proposed new course will support the new Bachelors of Computer Science in Cybersecurity as a required course in that major. The Computer Science department within CAS will submit a proposal and rational for the Cybersecurity major which includes this proposed new cybersecurity law and ethics course as a requirement.

The COB does not currently offer an undergraduate legal and ethical course targeted to address cybersecurity regulations, ethics and policy; yet, state and federal government, as well as federal contractors, increasingly seek graduates to fill cybersecurity positions, and to have a basic understanding of, and an appreciation for, the cybersecurity legal framework. Additionally, the course will offer business administration majors an additional upper level business elective required for graduation. Currently, the only other upper level BLAW course is Commercial Law which does not include cybersecurity content.


2. Impact Statement – Provide details about the Library, space, staffing, budget, and technology impacts created by adding this new course. Include supporting statements from the Library, IT Department, etc. This proposal has no resource impact. The library indicates no resource impact verbally at the COB CC meeting on October 8. IT indicates no resource impact through email (available if required). The department recognizes that, should the Cybersecurity Major become large enough, this course could require additional instructors, but will have no staff impact in the meantime.

3. Sample Syllabus:
BLAW 300 (01) Cybersecurity Law - 3 credits  
Fall 2019, MWF 1-1:50 PM; Room 149 Woodard

Instructor: Kimberley Kinsley, J.D., M.A., C.I.P.P.  
Office: Woodard 253  
Office Phone: (540) 654-1453  
E-Mail: kkinsley@umw.edu

Office Hours  
- Monday 11:25-12:55  
- Wednesday 11:55-12:55  
- Wednesday 2:50 – 4:50  
- Friday 12:15 – 12:45

UMW Technology Help Desk: 540-654-2255; http://technology.umw.edu/helpdesk/  

Students must use UMW e-mail or Canvas when communicating with the instructor in this course, and have access to Canvas.

The Office of Disability Resources has been designated by the University as the primary office to guide, counsel, and assist students with disabilities. If you receive services through the Office of Disability Resources and require accommodations for this class, be sure to inform me of your accommodation needs, and provide me a copy of the accommodation letter, at least one week prior to an examination, and at least two weeks prior to the final examination. I will hold any information you share with me in strictest confidence unless you give me written permission to do otherwise. If you have not made contact with the Office of Disability Resources and need accommodation(s) (note taking assistance, extended time for tests, etc.) then, contact the Office of Disability Resources. The office will require appropriate documentation of disability.

Contact information for the Office of Disability Resources: Tel#: 540-654-1266; Location: Lee Hall 401; Email: odr@umw.edu – Website: http://academics.umw.edu/disability/.

Title IX Statement

University of Mary Washington faculty are committed to supporting students and upholding the University’s Policy on Sexual and Gender Based Harassment and Other Forms of Interpersonal Violence. Under Title IX and this Policy, discrimination based upon sex or gender is prohibited. If you experience an incident of sex or gender-based discrimination, we encourage you to report it. While you may talk to me, understand that as a “Responsible Employee” of the University, I MUST report to UMW’s Title IX Coordinator what you share. If you wish to speak to someone confidentially, please contact the below confidential resources. They can connect you with support services and help you explore your options. You may also seek assistance from UMW’s Title IX Coordinator. Please visit http://diversity.umw.edu/title-ix/ to view UMW’s Policy on Sexual and Gender Based Harassment and Other Forms of Interpersonal Violence and to find further information on support and resources.

Resources  
Confidential Resources

On-Campus  
Tiffany W. Oldfield, J.D.  
Title IX Coordinator  
Office of Title IX  
Fairfax House  
540-654-5656  
toldfiel@umw.edu  

Talley Center for Counselling Services – Lee Hall 106  
Student Health Center  
Lee Hall 112

Off-Campus  
Myranda Thomson  
Title IX Deputy for Students  
Area Coordinator  
540-654-1184  
mthomson@umw.edu

Empowerhouse  
RCASA 540-371-1666

New Course Proposal Cover Sheet (July 2018)
THE COURSE AND ITS PURPOSE:
Students will examine legal, policy and ethical challenges stemming from cybersecurity threats involving government and non-government actors. This course will explore the national and international legal frameworks that govern malicious and defensive actions in cyberspace, including laws related to cybercrime, cyberespionage, privacy, and cyberwar. This is a core requirement for a cybersecurity major, and may satisfy the upper level business elective requirement for a business administration major. The purpose of the course is to introduce the student to regulations, court opinions, policy and ethics in cybersecurity.

LEARNING OBJECTIVES:
(1) to acquaint the student with the legal framework in which cybersecurity actors operate
(2) to encourage the student to reflect on legal ethics and related scenarios that may occur in cybersecurity work
(3) to contextualize cybersecurity threats and responses to them in a domestic and international law framework, while also recognizing the limits of current law, the need for further policy evolution, and the real-world impacts of different legal and policy options

SCOPE:
The study will cover but not be limited to the following areas:
- Cybersecurity Law and Its Sources
- Federal, State and International Cybersecurity Legal Framework
- Employment law considerations in Cybersecurity
- Privacy Law as it relates to Cybersecurity
- Legal Ethics
- Domestic and International Policy relevant to Cybersecurity

CONDUCT OF COURSE:
The material will be covered through lectures, discussions, group and team case solving, tests, and a final exam. Students will be required to analyze key legislation and court opinions.

GRADE: 100 points possible for the semester. There is no extra credit in this course.

Three exams (25; 25 and 25): 75 points
Research Paper: 10 points
Presentation: 5 points – due no later than 12/6 (submit hard copy or digitally in Canvas)
Classroom Participation (Jigsaw based Home Group and Expert Team Work) 10 points

Letter grades will be on the following scale: (Based as a percentage of total points.)

<table>
<thead>
<tr>
<th>Grade</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>93-100</td>
</tr>
<tr>
<td>A-</td>
<td>90-92</td>
</tr>
<tr>
<td>B+</td>
<td>87-89</td>
</tr>
<tr>
<td>B</td>
<td>83-86</td>
</tr>
<tr>
<td>B-</td>
<td>80-82</td>
</tr>
<tr>
<td>C+</td>
<td>77-79</td>
</tr>
<tr>
<td>C</td>
<td>73-76</td>
</tr>
<tr>
<td>C-</td>
<td>70-72</td>
</tr>
<tr>
<td>D+</td>
<td>67-69</td>
</tr>
<tr>
<td>D</td>
<td>60-66</td>
</tr>
<tr>
<td>F</td>
<td>0-59</td>
</tr>
</tbody>
</table>

A grade of "F" will be awarded for failure to take the final exam.

A mid-semester grade of "U" may be awarded for a grade of less than 70 at that time.

TEXT AND REFERENCE MATERIAL:

New Course Proposal Cover Sheet (July 2018)
GENERAL POLICIES:

(1) Make-up examinations will not be permitted except for extraordinary circumstances, which shall be solely determined by the instructor.

(2) Quizzes may be given at the sole option of the instructor. These quizzes may be announced or unannounced. The format, timing, and number of points to be awarded for any quiz is determined solely by the instructor.

(3) It is the responsibility of each student to complete the reading and homework outside the class. The instructor will work on the assumption that all reading has been completed when items are reviewed in class.

(4) Assignments – 3 exams (to include the final exam); paper and presentation; Jigsaw based home group and expert team assessments

(5) **HONOR CODE POLICY** -- The following is in expression of my support of the Honor System and is offered as a reminder to the Students:

"Study groups are encouraged for chapter coverage and problem solving. Each student is expected to turn in their own product and not copy verbatim solutions from any source. Unpledged work will not be graded."

(6) This syllabus may be changed at any time by the instructor in her sole discretion. If UMW closes for any reason (for example inclement weather) and it impacts the tentative schedule, the instructor may require an online assignment to be submitted by students as a “make-up” in lieu of class.

(7) Be sure to check Canvas prior to class for announcements, updates and reading assignments for selected cases.

GUIDELINES FOR RESEARCH PAPER – See Canvas for detailed instructions and rubric

Students “may” format the research paper by adopting the style that is depicted in law review articles found on Lexis-Nexis (see UMW’s online library database). This format is titled, The Bluebook: A Uniform System of Citation, a style guide, prescribes the most widely used legal citation system in the United States style of referencing sources (as generally found in law review articles). Students, however, may also utilize APA, MLA or Chicago style. There are many online sources for how to adopt these formats.

The paper and presentation rubric is located in Module One in Canvas. Module One contains an example of the basic format requirements, and “content” requirements that must be delivered in the paper and presentation. Please direct questions pertaining to format and substantive distinctions to me. Cases must be cited completely the first time that the case is referenced in a report or in the presentation and in the paper. For example, the first time that the Fero case is cited it must be a complete legal citation: Fero v. Excellus Health Plain, Inc., 2017 U.S. Dist. LEXIS 25471 (W.D.N.Y. Feb. 22, 2017). Notice that the case citation is in italics, this is the correct method of citing a case. After citing the case thoroughly when it
is first referenced, the subsequent citations may simply appear as: *Fero, p.* (if a quotation); or, *Fero, 2017* will work for purposes of this course. Hence, if the court’s opinion is quoted, then: first parties name, page number where information is drawn from; or – if it is not an exact quotation, first parties name, year.

It is expected that written assignments will be clear, concise, complete and free of grammatical errors—if not, points will be deducted. Before submitting a final report, students “may” submit a draft of it to the Writing Center and have them review the work. Do not wait until the last minute; schedule an appointment at least one week in advance.

*Warning:* I do have the ability and means to check for authenticity in student submissions. In fact, when I grade written reports, I routinely check all references, sources and citations for content and citation accuracy.

**Tentative Schedule**

**Important UMW Dates:** [https://academics.umw.edu/calendar/fall-2019-2/](https://academics.umw.edu/calendar/fall-2019-2/)

Material will be delivered via Lecture and Group/Expert Team Assignments

<table>
<thead>
<tr>
<th>Date</th>
<th>Chapters/Topics</th>
<th>Cases/Pages (See Canvas for more details)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1:</td>
<td>Ch 1</td>
<td>Course Requirements; begin Data Security Laws and Enforcement Action</td>
</tr>
<tr>
<td>Week 2:</td>
<td>Ch. 1-2</td>
<td>Data Security Laws and Enforcement Action; Cybersecurity Litigation</td>
</tr>
<tr>
<td>Week 3:</td>
<td>Ch. 2-3 Handout #1 – Group and Team Experts</td>
<td>Cybersecurity Litigation; begin Cybersecurity Requirements for Specific Industries</td>
</tr>
<tr>
<td>Week 4:</td>
<td>Ch. 3-4</td>
<td>Cybersecurity Requirements for Specific Industries;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Begin Cybersecurity and Corporate Governance</td>
</tr>
<tr>
<td>Week 5:</td>
<td>Ch. 4-5</td>
<td>Cybersecurity and Corporate Governance; begin Anti Hacking Laws</td>
</tr>
<tr>
<td></td>
<td>[Exam 1 covers chapters 1-2-3-4; Ethics essay]</td>
<td></td>
</tr>
<tr>
<td>Week 6:</td>
<td>Ch. 5-6</td>
<td>Anti-Hacking Laws; begin Public and Private Cybersecurity Partnerships</td>
</tr>
<tr>
<td>Week 7:</td>
<td>Ch. 6-7</td>
<td>Public and Private Cybersecurity Partnerships; begin Surveillance and Cyber</td>
</tr>
<tr>
<td>Week 8:</td>
<td>Ch. 7</td>
<td>FALL BREAK (12th – 15th); Surveillance and Cyber, continued</td>
</tr>
<tr>
<td>Week 9:</td>
<td>Ch 8</td>
<td>Handout #2: Group and Team Experts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Begin Cybersecurity and Federal Government Contractors</td>
</tr>
<tr>
<td>Week 10:</td>
<td>Ch. 8</td>
<td>Cybersecurity and Federal Government Contractors</td>
</tr>
<tr>
<td></td>
<td>[Exam 2 covers chapters 5-6-7-8; and Ethical essay]</td>
<td></td>
</tr>
<tr>
<td>Week 11:</td>
<td>Ch. 9</td>
<td>Privacy Laws; Guest Speaker</td>
</tr>
<tr>
<td>Week 12:</td>
<td>Ch 10</td>
<td>begin International Cybersecurity Laws</td>
</tr>
<tr>
<td>Week 13:</td>
<td>Ch 10</td>
<td>Thanksgiving Break (Nov 27th – Dec 1st) International Cybersecurity Laws;</td>
</tr>
<tr>
<td>Week 14:</td>
<td>Presentations</td>
<td>Presentation week</td>
</tr>
<tr>
<td>Week 15:</td>
<td></td>
<td>Discuss cumulative final exam; Handout #3: Group and Team Experts;</td>
</tr>
<tr>
<td></td>
<td>Paper due in Canvas on 12/6</td>
<td></td>
</tr>
<tr>
<td>Week 16:</td>
<td><strong>Final Exam:</strong> Exam covers course materials, lectures, and group work; Day/time: TBD</td>
<td></td>
</tr>
</tbody>
</table>

New Course Proposal Cover Sheet (July 2018)