

# CRIM 323 Cybersecurity and the Law-DEAdd-2018-08-13

- The workflow icon is no longer available. Please click on the Page Status after the orange circle icon near the page title. \*

Form Information

 The page you originally access is the global template version. To access the template document that progresses through the workflow, please complete the following steps:

**First Step:** ONLY change the text in the [brackets] so it looks like this: **CRIM 101 Intro to Criminology-CrsRvs-2015-08-10**

- ***If DUAL LISTED list BOTH courses in the page title***

**Second Step:** Click "SAVE" on bottom right

- ***DO NOT TYPE ANYTHING INTO THE FIRST PAGE OTHER THAN THE TEXT IN BRACKETS***
- ***Please be sure to remove the Brackets while renaming the page***

**Third Step:** Make sure the word ***DRAFT*** is in yellow at the top of the proposal

**Fourth Step:** Click on "**EDIT CONTENTS**" (*not EDIT*) and start completing the template. When exiting or when done, click "**SAVE**" (*not Save Draft*) on bottom right

When ready to submit click on the workflow icon and hit approve. It will then move to the chair as the next step in the workflow.

*\*Indicates a required field*

<b>Proposer*</b>	Jennifer Gossett	<b>Proposer Email*</b>	jgossett@iup.edu
<b>Contact Person*</b>	Jennifer Gossett	<b>Contact Email*</b>	jgossett@iup.edu
<b>Proposing Department/Unit*</b>	Criminology	<b>Contact Phone*</b>	724-357-2720

<b>Course Level*</b>	undergraduate-level
----------------------	---------------------

## Distance Education Section

*- Complete this section only if adding Distance Education to a New or Existing Course*

<b>Course Prefix /Number*</b>	CRIM 323
<b>Course Title*</b>	Cyber Security and the Law
<b>Type of Proposal*</b>	<i>See CBA, Art. 42.D.1 for Definition</i> online

<p><b>Brief Course Outline*</b></p>	<p><i>Give an outline of sufficient detail to communicate the course content to faculty across campus. It is not necessary to include specific readings, calendar or assignments</i></p> <p><i>As outlined by the federal definition of a "credit hour", the following should be a consideration regarding student work - For every one hour of classroom or direct faculty instruction, there should be a minimum of two hours of out of class student work.</i></p> <p>Introduction to Cybersecurity</p> <ul style="list-style-type: none"> <li>• Defining cyber security</li> <li>• Introduction and defining key terms in cybersecurity</li> <li>• Demographics of online users</li> </ul> <p>Jurisdiction</p> <ul style="list-style-type: none"> <li>• Traditional principles of jurisdictions</li> <li>• Judicial history of personal jurisdiction</li> <li>• Personal jurisdiction in the online environment</li> <li>• Federal and state jurisdictions</li> </ul> <p>Criminal and Civil Court Issues in Cybersecurity</p> <ul style="list-style-type: none"> <li>• Digital evidence</li> <li>• Cybercrimes</li> <li>• Statutory laws</li> <li>• Intellectual property (copyright, trademarks, patents and trade secrets) theories, practices, cases, and remedies</li> <li>• Use of computers at trial</li> </ul> <p>Laws Relevant to Cybercrimes</p> <ul style="list-style-type: none"> <li>• Digital Millennium Act</li> <li>• Bill of Rights</li> <li>• US Constitution and State Constitutions</li> <li>• Computer Fraud and Abuse Act</li> <li>• First Amendment</li> <li>• US Patriot Act</li> <li>• Application of existing laws</li> <li>• Other current laws</li> </ul> <p>Cybercrimes</p> <ul style="list-style-type: none"> <li>• Espionage</li> <li>• Drug trafficking</li> <li>• Terrorism</li> <li>• Cyberharassment/Cyberstalking</li> <li>• Gambling</li> <li>• Identity theft</li> <li>• Fraud</li> <li>• Child pornography</li> </ul> <p>Cybersecurity Future</p> <ul style="list-style-type: none"> <li>• Global issues</li> <li>• International organizations</li> <li>• Electronic commerce</li> <li>• Law of contracts</li> <li>• Taxation</li> </ul>
-------------------------------------	---

**Rationale for Proposal (Required Questions from CBA)**

<p><b>How is/are the instructor (s) qualified in the Distance Education delivery method as well as the discipline?*</b></p>	<p>Since completing trainings in Blackboard, D2L and Moodle for online delivery, over the years I have taught numerous online classes during the summer, winter and fall/spring sessions at the undergraduate and graduate levels. I also participate in distance education workshops at IUP and online. I have submitted several undergraduate classes for online delivery that were approved, such as CRIM 410 and CRIM 450. I also developed the proposals for many of the MA classes to be delivered online, for the MA online program, such as CRIM 632, CRIM 645, CRIM 791 and CRIM 694.</p> <p>In regard to this specific topics course, I have been teaching cyber security classes since my arrival at IUP. Currently, I am the only faculty member that teaches CRIM 321 and CRIM 323, which are two cyber security classes that are required for Cyber Security majors and minors. I also was a Principle Investigator for an NSF grant entitled 'Cyber Catch', which provided scholarship for students with interest in federal cyber security positions. I am active in cyber security activities and groups across campus, as well as research endeavors with students and colleagues.</p>
---	--

<p><b>For each outcome in the course, describe how the outcome will be achieved using Distance Education technologies.*</b></p>	<p>Course outcomes:</p> <ol style="list-style-type: none"> <li>1. <i>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.</i> Concepts will be introduced through powerpoint presentations and required readings. Threaded discussion questions, writing assignments and exams will evaluate knowledge of key concepts.</li> <li>2. <i>Discuss the impact that specific security issues related to cyber technology have had on the criminal justice system in particular, and upon modern society in general, in the context of past, present, and future developments.</i> Course readings and videos will provide insight into how the criminal justice system responds to cyber technology. Discussion questions, assignments and exams will measure this outcome.</li> <li>3. <i>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 "cyber crime," and those who commit such criminal acts.</i> Reading relevant legal cases related to cyber crimes will expose students to these issues. Writing assignments, such as a case analysis, and threaded discussions of specific cases will evaluate student understanding of this outcome.</li> <li>4. <i>Distinguish the particular attributes of a computer-based economic system which tend to facilitate fraud and other criminal acts by those with criminal intent.</i> Videos and newspaper accounts, as well as textbook reading, will allow for critical thinking of current criminal acts in cyber space. Writing assignments and exams will ensure this outcome has been met.</li> <li>5. <i>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.</i> Reading specific cases, such as Supreme Court decisions, will provide students a context to compare and contrast government branches, as well as text book chapter material. Discussion questions, writing assignments and exams will measure student success for this outcome.</li> <li>6. <i>Trace the history of development of the law enforcement community's efforts at policing the unlawful use of computers.</i> Videos and historical articles will provide students information they can process in understanding the evolution of law enforcement and computers. Writing assignments and exams will allow students to show their ability to relate time periods to law enforcement protocols with computers.</li> <li>7. <i>Identify the ethical challenges to be considered by those within the law enforcement field who are working to thwart cyber tech crime.</i> News accounts and other readings will give students information about ethical considerations in cyber security. Scenarios provided in threaded discussions, writing assignments and exams will measure this outcome.</li> <li>8. <i>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 cyber tech security.</i> Current events, legal cases and cyber security related reports will give students information to consider in future events. Writing assignment, threaded discussions and exams will allow students to show their thoughts on further changes in cyber security and cyber crimes.</li> </ol>
<p><b>How will the instructor-student and student-student interaction take place?*</b> <b>(if applicable)</b></p>	<p>Instructor-student interactions will occur in several ways. Forums with threaded discussions will occur weekly. Email and 'live' office hours will be held each week to allow for various interaction options. Student assignment feedback also allows for instructor-student dialogue. Phone calls can be used, if necessary.</p> <p>Student-student interactions will occur in weekly threaded discussions, as well as feedback exercises. Small group exercises and critical reviews of peer assignments can also create interactions between students.</p>
<p><b>How will student achievement be evaluated?</b></p>	<p>Student achievement will be evaluated through graded threaded discussions, writing assignments, and exams. The threaded discussions ask students to process their thoughts on the various questions and submit them in a discussion, which allows their peers to respond. This dialogue allows for a 'conversation' about the topics and a gauge in how well students understand course material. Writing assignments allow for flexibility in using current events, which is relevant to the evolution of cyber security. From online scavenger hunts, court case analysis, journaling, to research papers, allows students to showcase their critical thinking, application and knowledge of required material. Exams help to ensure students are staying current with course materials and making efforts to process and apply information to cyber security. Exams also provide a gauge of student success in understanding course topics and concepts.</p>
<p><b>How will academic honesty for tests and assignments be addressed?*</b></p>	<p>Academic honesty will be addressed with the option of timed exams and/or application (essay) exams that require students to explain and justify their points through essay writing. The instructor will participate in threaded discussions to confirm appropriate and relevant dialogue between students, as well as gain exposure to student participation. Assigned papers will include an 'honor code' statement to ensure students are aware of the consequences of not maintaining academic integrity. Also, the instructor can submit papers through plagiarism software programs for additional assessment of borrowed work.</p>

Please scroll to the top and click the Page Status if you are ready to take action on the workflow.

Please submit an ihelp if you have any questions <http://ihelp.iup.edu>