Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

An Active Learning Approach for Coursework in Information Assurance Ethics and Law

N. Paul Schembari, *East Stroudsburg University of Pennsylvania*

Abstract – Many universities and community colleges with an Information Assurance major or concentration include a course or modules of a course covering the topics of law, ethics, and the affect of information assurance solutions on laws and ethics. In this paper, we discuss how we have applied an active learning approach to our course, "Legal Impacts of Computer Security Solutions" for both undergraduates and graduate students using the traditional classroom as well as an online learning environment.

Index terms – Active Learning, Computer Security Curriculum, Ethics, Information Assurance Curriculum, Information Security Curriculum, Law

I. Introduction

Several colleges and universities are now offering courses in Information Assurance (IA). Some have created undergraduate concentrations or certificates [1], undergraduate majors [2], and others have added this curriculum on the graduate level, offering certificates [3], Master's programs [4], and doctoral programs [5].

One common theme throughout many of these offerings, especially where an IA program is in place (as opposed to a single course), is the existence of a course or modules of one or more courses which cover the areas of law, ethics, and the affect of information assurance solutions on laws and ethics. Throughout this paper, we will use the term "Law and Ethics Course" to indicate such a course or set of modules.

There are two prevailing reasons why Law and Ethics Courses are taught as part of IA programs. First, faculty and industry professionals believe that such curriculum is important for students. The hope is that by having students address legal and ethical issues in advance, the students will not act unethically or illegally in the future. As stated by DeWitt and Cicalese [6]:

> "By assessing the social, legal, and ethical implications associated with using technical skills, an integrative CSIA [computer security and information assurance] curriculum provides students with an increased awareness of how the context influences technical decisions. The resulting appreciation should reduce the likelihood that our students unknowingly become part of the CSIA problem."

A second motivation for Law and Ethics Courses as part of an IA curriculum stems from multiple curriculum standards which require such courses. For example, Cooper, et al [7], give a review of multiple IA curriculum standards, many of which include ethical and legal content. In particular, in Section II below, we consider some IA educational standards and their legal and ethical requirements.

Whether an institution's motivation is pedagogy or standards, it is important for faculty to determine how they will include law and ethics in their curriculum. We at East Stroudsburg University of Pennsylvania (ESU) have taken the approach to include an entire course on these topics for both our undergraduate and graduate (Master's) students. Our first attempt was a lecture-based course for our undergraduates (students with fundamental training in computer science and basic information assurance), but we found this to be less than successful. Hence, we turned to a more active learning approach which we believe is more beneficial for the students. This impression comes from anecdotal discussions with the students and formal student evaluations. This active learning approach is now also included for our graduate students in an online learning environment.

These undergraduate and graduate courses and the active learning approach used will be described in Section III, below. Then, in Section IV, we look at some sample topics covered in the classes. Finally, in Section V, we include student survey results from some of the classes and discuss what we view as our successes, some challenges, and some planned improvements.

N. Paul Schembari is a Professor of Computer Science and the Director of the Computer Security and Information Security Programs at East Stroudsburg University of Pennsylvania.

ISBN 1-933510-99-4

II. A Selection of IA Curriculum Standards With Ethical and Legal Requirements

Many institutions which participate in the Colloquium for Information System Security Education have worked with the National Information Assurance Education and Training Partnership (NIETP), housed in the National Security Agency (NSA). Because of the NIETP requirements, these institutions are familiar with our first six standards, the Committee on National Security System Instructions / National Security Telecommunications and Information Systems Security Instructions (CNSSI / NSTISSI) 4011 – 4016, which have been defined by the US Committee on National Security Systems (CNSS), chaired by the US Department of Defense. We will look at these standards, available from the CNSS Instructions Page [8], and examine some of their ethical and legal requirements. We do not include an exhaustive list of ethical and legal requirements from these standards as this is beyond the scope of this paper.

The CNSS standards are considered "government standards" by many, and so we should also review more academic standards. In this regard, we will examine the ethical and legal requirements for the *Accreditation Board for Engineering and Technology* (ABET) accreditation as well as the educational standards designed by the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) Computer Society. We should also take an industrial view, and so we consider one of the *Information Systems Audit and Control Association* (ISACA) educational "standards" and their ethical and legal requirements. We complete our survey by considering the *Certified Information System Security Professional* (CISSP) industrial certification as a standard.

A. NSTISSI 4011

NSTISSI 4011, the *National Training Standard for Information Systems Security Professionals* [8], is the basic IA standard from the CNSS. The importance of this standard to academic institutions is shown by the fact that all universities that have been named *National Centers of Academic Excellence in Information Assurance Education* [9] by the US Department of Homeland Security and National Security Agency must meet this standard.

NSTISSI 4011 includes some ethical and legal content. For example, under the section entitled "NSTISS Basics", the following items are part of the standard:

Legal Elements
- fraud, waste and abuse
- criminal prosecution
- evidence collection and preservation
- investigative authorities

B. CNSSI 4012

CNSSI 4012 is the *National Information Assurance Training Standard for Senior System Managers* [8]. Because this standard is meant for senior managers, it includes a much larger legal focus than NSTISSI 4011. For example, Function 3 of the standard requires multiple IA related laws and related issues:

- Copyrights
- Criminal Prosecution
- Evidence Collection and Preservation
- Fraud, Waste, and Abuse
- Electronic Records Management and Federal Records Act
- Federal Managers Financial Integrity Act of 1982
- Federal Property and Administration Service Act
- Etc.

C. CNSSI 4013

CNSSI 4013, the *National Information Assurance Training Standard for System Administrators* [8], also includes some requirements with regard to law and ethics. For example, Function One, covering secure system usage states that system administrators should be able to "Discuss / Explain security policies relating to ethics." In the same function, the standard states that the system administrator should:

- Comply with legal aspects of monitoring
- Ensure legal aspects of monitoring are enforced.

A few other legal points are included in this standard, especially with regard to assisting in legal investigations.

D. CNSSI 4014

CNSSI 4014 is the *National Information Assurance Training Standard for Information Systems Security Officers* [8]. This standard also includes many legal requirements. In fact, in the first Job Function, Develop Certification and Accreditation Posture, under the section on Planning, and entire area is devoted to a "Legal Plan." This area includes subsections on "Criminal Activity Preparedness Planning" as well as a multitude of laws. Indeed, this subsection on laws lists 29 bulleted points, many involving individual laws or groups of laws. These range from the Computer Fraud and Abuse Act to the Digital Millennium Copyright Act to laws on imports and exports.

E. NSTISSI 4015

NSTISSI 4015 is the *National Training Standard for System Certifiers* [8]. Again, we find that ethical and legal issues are important to this government standard. Here, under the very first job function, "Document

Mission Need," the first subsection states that the system certifier must have a

a. Knowledge and/or Awareness of Security Laws

1) identify relevant nation-state security laws, treaties, and/or agreements;
2) interpret nation-state security laws, treaties, and/or agreements in relation to mission accomplishment;
3) relate the identified nation-state security laws, treaties, and/or agreements to the mission needs;
4) discuss identified nation-state security laws, treaties, and/or agreements with involved site personnel.

F. CNSSI 4016

The last CNSS standard is CNSSI 4016, the *National Information Assurance Training Standard for Risk Analysts* [8]. Again, we see ethical and legal emphasis in the standard's requirements. For example, in job function 9, "Training and Awareness Duties," one subsection requires the risk analyst to:

- Identify local application of IA laws, regulations, and policies
- Discuss applicable IA laws, regulations, and policies
- Explain application of IA laws, regulations, and policies.

As the above review has shown, a focus of ethical and especially legal content is present in the CNSS training standards.

G. ABET and ACM / IEEE Standards

"Pure" academic standards for information assurance curriculum are now being created. In fact, Cooper, et al [7], state: "In its exploration of existing government, industry, and academic Information Assurance guidelines and standards, as well as in its discovery of what guidance is being provided for other areas of computing, the working group has developed this paper as a foundation, or a starting point, for creating an appropriate set of guidelines for Information Assurance education." The "working group" refers to a group of IA faculty and professionals from government and industry who have met multiple times to discuss the creation of such academic standards.

Since we do not have formal IA curriculum standards at this date, we consider the related ABET and ACM / IEEE standards. While ABET does not provide specific content for coursework, it does provide required Program Outcomes. In this regard, the ABET guidelines [10] state that a computing program should enable "students to achieve, by the time of graduation… an understanding of professional, ethical, legal, security and social issues and responsibilities."

The ACM / IEEE computing curriculum standards [11] also include an emphasis on ethics and law. This can be seen by examining the section on "Social and Professional Issues." In this section, some of the key issues include:

- Professional Ethics
- Intellectual Property
- Privacy and Civil Liberties
- Computer Crime

Each of these topics shows an ethical or legal focus. Hence we see that institutions wishing to follow academic computing standards will also need to include ethics and law as part of their curriculum.

H. ISACA Model Curriculum and CISSP Common Body of Knowledge

To consider the industrial standards for IA curriculum, we examine the ISACA Model Curriculum for Information Security Management [12] and the CISSP Common Body of Knowledge (CBK) [13]. The ISACA Model Curriculum actually does not include much in its standard with regard to ethics and law. In fact, we find no recommendation for a study of ethics in this standard. Further, legal considerations are relegated to two somewhat diminutive points. First, under the topic of "Security Governance," one subtopic is: " Scope and charter of information security governance (laws, regulations, policies, assurance process integration, convergence)." Second, under the topic of "Program Development," one subtopic is: " Information infrastructure, architecture, laws, regulations and standards." We recommend an improvement to this standard in that a greater focus in ethics and law must be included. Interestingly enough, even though this standardized curriculum does not have a large ethical focus, ISACA does require its members to adhere to a code of ethics.

As a second industrial example, we consider the CISSP CBK. Here, we find a much stronger emphasis in ethics and law than found in the ISACA Model Curriculum. The CISSP CBK includes one domain entitled "Information Security and Risk Management." In this domain, we find a section entitled "Ethics." Also, the $(ISC)^2$ (the organization with certifies CISSPs) requires that all CISSPs adhere to a code of ethics. Second, the CISSP CBK also includes an entire domain entitled "Legal, Regulations, Compliance, and Investigations." Hence more than one of the ten domains in the CISSP CBK covers the areas of ethics and law.

Our review of IA curriculum standards and recommendations, including governmental, academic, and industrial standards, has shown that any institution wishing to educate students in information assurance must include curriculum covering the topics of IA ethics and law.

III. An Active Learning Approach

Once the decision has been made to include ethics and law in an IA curriculum, one must next decide the methodology. We have decided to create an entire course called "Legal Impacts of Computer Security Solutions." This course is at the senior undergraduate level for our Computer Security students and also available to graduate students in our Information Security program, so students are expected to have some IA background. The undergraduate class is taught as a regular on-campus course, and the graduate class is taught online.

Before we had implemented our graduate program, we taught this course to our undergraduates using a mostly lecture-based approach. With this execution, we lectured and had student discussions on the following topics:

- Introduction to Computer Ethics and the US Legal System
- US Constitution
- Privacy
- Liability
- Encryption
- Cybercrime
- Intellectual Property

While we incorporated some discussion in these course offerings, this was far from an active-learning approach. Also, through interviews with students we found that this method was not very successful for student learning. The students found the material "dry" and did not feel they would retain much of the instruction.

Hence, we decided to have the students take a more active role in the course, hoping for more involvement and interest from the students, leading to better learning. Following the above set of topics as a guide, we created a collection of case studies for the students to analyze. Students are given a case study one week in advance of the required discussion so that they have enough time to research the case. *This is the requirement which forces the student to learn actively.* They must analyze the case and research ethical and legal points on both "sides" of the case – prosecution and defense. The legal points must be drawn from existing laws and actual court cases. The students are required to write a written report on the case study which is due on the day discussion begins.

After this week of research, with their written reports in hand, the students then debate the case studies in class. In the review of the case studies, we use the following schedule each week which consists of three class meetings:

Day 1 - Issues

- Students are broken into multiple groups.
- Each group discusses both sides of the case.
- At the end of the class session, all students are required to present points to the class.

Day 2 – Teams Chosen

- The class is randomly broken into 2 teams – each team is randomly given a side to defend.
- Each group picks 4 major topics to debate. The group must also prepare possible counterpoints to the arguments which may be devised by the opposing team.
- With a few minutes left in class, a subgroup of students is selected from each group to act as jury. The remaining students plan their selection of topics to discuss or summarize.
- Each student should be on the jury about once every few weeks.

Day 3 - Debate

- Each team presents a topic for approximately 5 minutes, and the other team then has 1 minute to counter. Eight topics are covered overall.
- The jury is required to write up their decision by the next class – this must be based on evidence presented by their peers and not their opinion.

We have used this debate approach in three different course offerings, two undergraduate classes in a traditional classroom, and one graduate class in an online environment. We report on the results of these offerings in Section V.

In terms of grading, we evaluate students on their written case study analyses as well as their debate skills and participation. Here are rubrics that we have used with success:

Written Report Grading

- Did the student argue both sides of the case
- Each side must include ethics / logic, law, and case law, whenever possible
- References must be included
- Grammar and written presentation is important

Debate Grading

- Was the presentation well organized?
- Was the presentation well defended? This should include sources (expert witnesses), law, and case law.

- Did the student anticipate counter arguments?
- Was the presentation interesting?

For classroom participation, students are penalized if they are absent or do not participate in classroom discussions. For the online version of the course, we have used forums as a replacement for the oral debates.

IV. Sample Topics for IA Ethics and Law

In this section, we provide three examples of case studies that we have used in our Legal Impacts of Computer Security Solutions course. Each of these case studies has been attempted multiple times with good results. It should be noted that some of the case studies are taken from real news stories and cases, so some of the quotes in this section are real and some are fictitious.

A. Case Study Example: Microsoft v. Schembechler

Professor Pablo Schembechler is a Michigan university faculty who performs computing research. Dr. Schembechler has discovered a vulnerability in Microsoft Windows Vista Home Premium, a product which he purchased during August 2009. By providing the correct set of characters to "Windows Help", Dr. Schembechler can cause a "Blue Screen of Death." He claims that he found this vulnerability and attack using black-box experimentation alone. He also claims that since he has not looked at any source code, he is not sure of the exact cause of the vulnerability, but has a theory concerning the reason. He intended to publish a paper with his theory and results on this vulnerability and attack, and post the paper on his web site. He also planned to present his paper at a computer science conference.

Microsoft has found out about Dr. Schembechler's work and has had a court ruling made against him – because of the court order Dr. Schembechler is not allowed to publish any research concerning any Microsoft vulnerabilities or attacks against Microsoft products in any way. One of Microsoft's claims is that publishing the vulnerability will give away important trade secret information about a Microsoft product. Prof. Schembechler now wants to appeal this court ruling.

B. Case Study Example: US v. Clean

The federal government has asked a U.S. District Court in Pennsylvania to order a man to type a password that would unlock files on his computer, despite his claim that doing so would constitute self-incrimination. The suspect, John Clean, is believed to have child pornography on his laptop. However, part of his computer is encrypted with "LockedDrive."

Criminals and terrorists are using "relatively inexpensive, off-the-shelf encryption products," said John Miller, the FBI's assistant director of public affairs. "When the intent . . . is purely to hide evidence of a crime . . . there needs to be a logical and constitutionally sound way for the courts" to allow law enforcement access to the evidence, he said.

The case began March 17, when Clean was using his laptop in a speeding car. When the driver was pulled over, the police officer saw a file on the laptop entitled "Two-year-old being *** during diaper change." The officer asked Clean to show the file contents, but Clean stated that they were stored on an encrypted portion of the laptop – the Z drive. Clean was arrested and charged with possession of child pornography.

FBI agents seized the laptop and copied its contents. But the investigator could not get access to the drive Z content because it was protected by LockedDrive. LockedDrive is a product which creates virtual drives and encrypts them. Access to the drives requires a password for decryption. A grand jury subpoenaed Clean to enter his password to allow access to the files on the laptop. Clean moved to quash the subpoena on the grounds that it violates his Fifth Amendment right against self-incrimination.

On Nov. 29, Magistrate Judge Gerald George ruled that compelling Clean, a 30-year-old drywall installer, to enter his password into his laptop would violate his Fifth Amendment right against self-incrimination. "If Clean does know the password, he would be faced with the forbidden trilemma: incriminate himself, lie under oath, or find himself in contempt of court," the judge said.

In his ruling, George said forcing Clean to enter his password would be like asking him to reveal the combination to a safe. The government can force a person to give up the key to a safe because a key is physical, not in a person's mind. But a person cannot be compelled to give up a safe combination because that would "convey the contents of one's mind," which is a "testimonial" act protected by the Fifth Amendment.

"The consequence of this decision being upheld is that the government would have to find other methods to get this information," said Marc Rotenberg, executive director of the Electronic Privacy Information Center. "But that's as it should be. That's what the Fifth Amendment is intended to protect."

Orin S. Kerr, an expert in computer crime law at George Washington University, said that Clean lost his Fifth Amendment privilege when he admitted that it was his computer and that he stored images in the encrypted part of the hard drive. "If you admit something to the government, you give up the right against self-

incrimination later on," said Kerr, a former federal prosecutor.

The government appealed the case and won. In its submission on appeal, the Government stated that it does not in fact seek the password for the encrypted hard drive, but requires Clean to produce the contents of his encrypted hard drive in an unencrypted format by opening the drive before the grand jury. In oral argument and post-argument submissions, the Government stated that it intends only to require Clean to provide an unencrypted version of the drive to the grand jury. Judge Duce, hearing the appeal, stated that: "Because Clean cannot refuse to provide a grand jury with evidence, his motion to quash the subpoena is denied. Clean is directed to provide an unencrypted version of the Z drive. The Government may not make use of Clean's act of production to authenticate the unencrypted Z drive or its contents either before the grand jury or a petit jury. The Government's appeal of the Magistrate Judge's opinion and order is sustained."

Clean has not produced the unencrypted version of drive Z and has asked for a Supreme Court review of the case.

C. Case Study Example: US v. Hackstop

HackStop, Inc. is a provider of network-based intrusion prevention systems and services for enterprises. Because of its control of the Robinson botnet, the US Department of Justice has charged HackStop with conspiracy to intentionally damage a protected computer, with intentionally causing or intending to cause damage to a protected computer, and with the use of malicious software to intercept Internet communications.

Before HackStop became involved, the Robinson botnet had infected tens of thousands of PCs. Researchers at HackStop decided to study the malware, and they noticed that on start-up machines controlled by Robinson ran through a pre-arranged list of domains as they searched for a functioning command-and-control server. If no C&C server could be found, the botnet would then register the next domain on the list and set up a new command server. The bots in the network ran through the list until they came to the new domain and simply began taking commands from that machine.

Using this feature, HackStop registered some domains in the Robinson list and emulated a C&C server. The phony server then received connection requests from Robinson-infected PCs around the Internet, adding up to nearly 1 million in a one-week period. Hence, the HackStop researchers had the ability to control these bots in the Robinson army. With that control, the researchers sent the infected PCs new binaries that disinfected the Robinson bots.

In its charges, the US states that while the HackStop research *may have* had non-malicious intent, the fact is that they controlled thousands of US citizens' computers, intercepting information as desired. The DOJ believes that these actions went beyond the typical norm for computer security research and reached a level of vigilantism.

V. Results and Lessons Learned

As we stated earlier, Computer Science and Security students do not typically have a good response to lectures on ethics and law. For this reason, we have created an active learning environment for our Legal Impacts of Computer Security Solutions class. We now discuss the some of the successful points and some challenges we have faced.

A. General Issues and Lessons Learned

We first give a few general impressions that come from teaching our Legal Impacts of Computer Security Solutions class three different times using the above described approach. After these general impressions, we include more specific recommendations.

1. Preparation of Case Studies

Preparation of the Case Studies is a very time consuming task. First, we began by choosing a list of topics – this was gathered from our earlier lecture-based course. Then, for each topic, a scenario with interesting legal twists should be developed. Often we have found that real news stories can help motivate a Case Study, so it is important to keep track of current events in IA and keep track of references. Some very good sources for this type of material are the Electronic Frontier Foundation [14] and Bruce Schneier's Website / Blog [15].

2. Debates Can Be Challenging

For those of us used to the lecture style of teaching, debates can be challenging. It's important to allow the students to explore ideas, but at the same time this must be balanced with restricting the waste of time. It can be difficult to control some students who may want to make sure their chosen points are highly emphasized, while other students hardly participate at all. Also, keeping students on track can be an issue.

3. Meeting Standards Requirements

In Section II of this paper, we listed a variety of IA standards. If an instructor is trying to meet any of these standards, especially the CNSS standards, then using this approach also requires some supplemental instruction or

delivery of material. This is because of the fact that it is impossible to cover all the laws in the standards and allow students to explore their own legal points. Our solution has been to create a web page which lists the laws in the CNSS certificates offered by ESU with links to various sources [16].

B. Using the Debate Approach Depends on the Class

We have offered this style of class twice to our undergraduates in a traditional classroom environment. We consider the first offering successful and the second offering a bit less successful. This impression stems from the fact that the second class offered less participation than the first. We believe this is because of the make-ups of the classes - the first class consisted of approximately 20 students, many of whom have outgoing personalities. Instead, the second class consisted of about 10 students with only a few outgoing individuals. Because of this, the few outgoing individuals in the second class became the de facto group leaders each week. The smaller size of the second class may have also played a role in this issue.

C. Using the Debate Approach is Challenging if Students Are Frequently Absent

In the second offering of the class, mentioned above, we also had an issue with attendance. Two to three of the ten students would often miss class without warning. If these students were responsible for a particular debate topic or were jury members, it became difficult to resolve their absence. Fortunately, in the first class offering, almost all 20 students attended almost every class. The attendance policy (with penalties for missing classes) was instituted because of the issues in this second class.

D. Challenges with the Online Version of the Class

We also tried to implement this approach in an online learning environment, offered once. Our idea was to have the students submit their written reports, and then transmit these reports to the entire class as our "discussion." Then, using an online forum, the students could have a debate. We again ran into issues with tardiness – if a student submitted his or her report late, then their points were not part of the original discussion. Then, with the forums, students were required to include points and counter other students' points. However if a student was late with his or her original point, how could another student counter this point on time?

We tried to solve these issues by having the students participate in forums first and write their reports second. The forums would act as a discussion so that the students could collect the best ideas, and then write a report based on those best ideas. We found that, instead, students would post to the forum and submit the same written report as their forum post with no additions.

We will try to correct these issues the next time this course is offered in an online environment (next scheduled for Fall 2011). In the meantime, the author would gladly accept any suggestions from the reader to help with improvements.

E. Student Reviews

Even with the above mentioned challenges, we believe this active learning approach with debate is better than the traditional lecture-based, passive student approach. We have evidence in the form of student evaluations to suggest that students view this type of course as beneficial.

For example, in the second undergraduate offering, which we viewed as less successful than the first, the students were asked: "Please rate this class on a scale of 0 – 10 (0 = horrible, 10 = great)." The average score for the eight students who responded was 8.5. Here we have received a good overall score even when the class was not viewed as being very successful by the instructor. As a point of reference, the first offering of this class lead to an average score of 7.93 on the same question [N=15].

The student evaluations also included the question: "Here is a list of Case Studies covered in the class. Which need improvement? Why?" [We leave out a full list of case studies for the sake of brevity.] The student responses for this question addressed two major points:

- Some case studies were considered one-sided.
- Some case studies needed more details to make them more realistic.

The third question on the student evaluations was: "The course followed the following schedule each week [with a description of the weekly schedule as given above]. Can this method be improved?" Five of the nine respondents gave positive remarks. The others commented on the following points:

- Choose teams at the end of the first day to allow for more planning.
- All laws and cases should be posted no later than the second day to allow both sides to research. [This was a response to the practice of one student who would often introduce cases and laws on debate day even though they had not been mentioned before.]

The last question of the student evaluations was: "Please suggest any other improvements to the class." The responses are summarized as follows:

- Clarify the format of the paper [written report].
- Student presenters should use visual aids.

- Either all students or none should have Internet access. [A few students brought laptops to class.]
- Students should be limited in their "talking time."
- Penalize for ad hominem attacks.
- Reduce the number of privacy case studies.
- Try to make the case studies less one-sided.

As we can see from these reviews, especially the results of the first question, the students enjoy the active-learning debate approach, while also asking for some improvements. These improvements will be made in the next course offering. Also note that none of the responses have asked for more lecturing by the instructor. The question of whether or not the students would prefer a lecture format course will be asked in the next set of student evaluations.

We will continue to offer our *Legal Impacts of Computer Security Solutions* course using an active learning, student debate, approach. Of course, we plan to make improvements based on the challenges described above. We believe that the presented student debate method is much more valuable to the student because he or she must actively analyze the material, and write a written report, in advance of the classroom discussion and debate. Our hope is that this will lead to students with a better understanding of Information Assurance Ethics and Law.

VI. References

[1] Polytechnic Institute of New York University, Information Systems and Internet Security Lab. "Curriculum Page." Retrieved on March 14, 2010 from http://isis.poly.edu/index.php?page=3.

[2] Schembari N. P. "A bachelor of science degree in computer security: The experiences of a national center of academic excellence in information assurance education." *Proceedings of the Ninth Colloquium for Information Systems Security Education*, 2005, pp. 6-11.

[3] University at Buffalo School of Management. "Information Assurance Concentration." Retrieved on March 14, 2010 from http://mgt.buffalo.edu/programs/mba/academics/curriculum/assurance.

[4] Dakota State University. "Master of Science in Information Assurance." Retrieved on March 14, 2010 from http://www.dsu.edu/msia/.

[5] Perdue University, Center for Education and Research in Information Assurance and Security. "Infosec Graduate Program." Retrieved on March 14, 2010 from http://www.cerias.purdue.edu/site/education/graduate_program/#interdisciplinaryphd.

[6] Dewitt J. and Cicalese C. "Contextual Integration: A Framework for Presenting Social, Legal, and Ethical Content Across the Computer Security and Information Assurance Curriculum." *Proceedings of the Third Annual Conference on Information Security Curriculum Development*, 2006, pp. 30-40.

[7] Cooper S., et al. " An exploration of the current state of information assurance education." *ACM SIGCSE Bulletin* 41, 4 (Dec. 2009), pp. 109-125.

[8] Committee on National Security Systems. "Instructions Page." Retrieved on March 14, 2010 from http://www.cnss.gov/instructions.html.

[9] National Security Agency Central Security Service. "National Centers of Academic Excellence." Retrieved on March 14, 2010 from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

[10] Accreditation Board for Engineering and Technology, Computing Accreditation Commission. "Criteria For Accrediting Computing Programs." Retrieved on March 14, 2010 from http://www.abet.org/Linked%20Documents-UPDATE/Criteria%20and%20PP/C001%2010-11%20CAC%20Criteria%2011-16-09.pdf.

[11] ACM/ IEEE Computer Society Interim Review Task Force. "Computer Science Curriculum 2008: An Interim Revision of CS 2001." Retrieved on March 14, 2010 from http://www.acm.org//education/curricula/ComputerScience2008.pdf

[12] Information Systems Audit and Control Association. " ISACA Model Curriculum for Information Security Management." Retrieved on March 14, 2010 from http://www.isaca.org/Template.cfm?Section=Model_Curriculum&CONTENTID=46950&TEMPLATE=/ContentManagement/ContentDisplay.cfm

[13] Tipton H. F. *Official (ISC)2 Guide to the CISSP CBK*. Auerbach Publications, 2006.

[14] Electronic Frontier Foundation. "Home Page." Retrieved on April 8, 2010 from http://www.eff.org.

[15] Schneier B. "Schneier on Security." Retrieved on April 8, 2010 from http://www.schneier.com/.

[16] Schembari N. P. "Legal Resources." Retrieved on April 8, 2010 from http://www.esu.edu/compusec/legalResources.html.