Course Syllabus and Policy Requirement Statement

Accessing the course implies that you completed the following:

- You have read, understood, and will comply with the policies and procedures listed in the class syllabus, and that you have acquired the required textbook(s).
- You have read, understood, and will comply with class policies and procedures as specified in the online Student Handbook.
- You have read, understood, and will comply with computer and software requirements as specified with Browser Test.
- You have familiarized yourself with how to access course content in Blackboard using the Student Quick Reference Guide or CSS Student Orientation Course.

BOR/ISSA 6350 Cyber Vulnerability

Course Description/Overview

Cyber vulnerabilities pose potentially devastating consequences to the U.S. critical infrastructure systems such as water systems, power lines, transportations, communications systems, agriculture, and others. There are over 18 different national critical systems in the U.S. and protecting these critical systems is a paramount job for all cybersecurity stakeholders involved. We discuss many of these cyber vulnerabilities throughout the course to recognize the current cyber vulnerabilities as well as any future attacks.

As a Graduate Seminar, the students will essentially determine the flow of the course through their participation in discussions and writing requirements.

Prerequisite Knowledge

There is no specific prerequisite knowledge for this course; however, it is recommended that students have some security knowledge in protecting national security and describing computer vulnerability.

Online Course Access

The student will complete all required course activities through the University online course site. Upon registration the student will be provided with the course access in Blackboard Leaning System. The student is advised to contact the school administrator if the registered courses are unavailable.

Required Technical Skills

Students are expected to possess technical skills in computer use and collaborate in the online course activities in a weekly basis. Students are required to access the online course and participate in the required discussion forums.

Course Required Textbooks:


VitalSource
Course Objectives/Learning Outcomes

Objectives: This course will introduce the need for a national cyber security program to protect critical infrastructure. The ten components of this program, which make up the remaining chapters of the textbook, are introduced as well.

After completing this course, the student will be able to:

1. Identify cyber threats and vulnerabilities to national critical infrastructure.
2. Analyze cyber threats and vulnerabilities to critical infrastructure.
3. Evaluate recommended solutions to cyber threats to national critical infrastructure.
4. Apply cybersecurity best practices to a practical application.

Grading Policies

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Percent of Grade</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation in the Discussion Board</td>
<td>30%</td>
<td>Initial posts due at the end of each week on Friday no later than 11:59 P.M. Peer responses are due no later than 11:59 P.M the following Monday. The next discussion board week begins on Tuesday.</td>
</tr>
<tr>
<td>Midterm</td>
<td>30%</td>
<td>Construct a 5-7 page essay that identifies specific cyber vulnerabilities associated with one of the 18 DHS critical infrastructure sectors. The essay should provide a narrative of a hypothetical cyber-attack against your selected sector. You may only use open source and unclassified sources to develop your scenario. Identify these cyber vulnerabilities and explain why you would launch a cyber-attack against one or more of these vulnerabilities. Do not detail how you would conduct such an attack. Please cite your sources using Chicago, APA, or MLA style guides. Your paper should be double spaced and use 11 or 12 pitch. The midterm essay is due by 11:59 P.M. Central Daylight Time</td>
</tr>
</tbody>
</table>
Final

40%

Construct a 5-7 page essay that analyzes specific cyber threats and identifies specific countermeasures, preventive policies, or responses to a cyber-vulnerability associated with one of the 18 DHS critical infrastructure sectors. The essay should provide a concise narrative of a hypothetical preventive policy and/or response strategy to an assigned sector. You may only use open source and unclassified sources to develop your strategy/policy. Do not detail specific cyber capabilities or procedures in your response. Please cite your sources using Chicago, APA, or MLA style guides. Your paper should be double spaced and use 11 or 12 pitch. The midterm essay is due by 11:59 P.M. Central Daylight Time on Thursday of week five. There is no discussion board during this week.

Essays:

The purpose of the midterm and final paper is to assess your ability to think critically, write effectively, and to analyze complex security issues at the graduate level. Formal academic writing uses standardized styles and citation formats. To access the APA writing guidelines go to this link: http://owl.english.purdue.edu/owl/resource/560/01/. Should you wish to use CHICAGO style that will be acceptable. The Chicago Style guide can be found at http://www.chicagomanualofstyle.org.

Check the discussion board regularly. Many student questions are applicable to the class as a whole, as are the responses. You may be surprised how many of your classmates have the same questions and concerns as you. I may simply post your particular question on the discussion board and allow your classmates to provide the answer through their own posts.

**Date and Time of Final Essay.** This is an online course. Students submit a cyber vulnerability essay assigned during week eight. Students are concurrently asked to complete end of course surveys and provide feedback.

Formal academic writing uses standardized styles and citation formats. The preferred format is the Chicago Manual of Style style (CMOS). To access the CMOS and APA writing guidelines go to this link: http://owl.english.purdue.edu/owl/resource/560/01/.

The CMOS guide can also be found at http://www.chicagomanualofstyle.org.

**Participation & Communication**
In this class everyone brings something to the table. Your ideas and thoughts do count, not only to me, but the entire class. Feel free to ask questions either via e-mail or the discussion board. Check the discussion board regularly. Many student and instructor questions are applicable to the class as a whole, as are the responses. You may be surprised how many of your classmates have the same questions and concerns as you.

**Courtesy and Respect**

Courtesy and respect are essential ingredients to this course. We respect each other’s opinions and respect their point of view at all times while in our class sessions. The use of profanity & harassment of any form is strictly prohibited (Zero Tolerance), as are those remarks concerning one’s ethnicity, life style, race (ethnicity), religion, etc.. Violations of these rules will result in immediate dismissal from the course.

**Date and Time of Final Essay**

This is an online course. Students submit the cyber vulnerability essays IAW posted guidance. Students are concurrently asked to complete end of course surveys.

**Office Hours and/or hours of outside-of class contact**

This is an online course. The professor will provide contact information and availability times for direct discussion in the Instructor Information section on Blackboard.

Angelo State University employs a letter grade system. Grades in this course are determined on a percentage scale:

- A = 90 – 100%
- B = 80 – 89%
- C = 70 – 79%
- F = 69% and below.

**Course Organization:**

### Lesson 1: Introduction Cyber Vulnerabilities

This lesson introduces the need for a national cyber security program to protect the national critical infrastructure systems. The lesson covers threats to national infrastructure and components of a national cybersecurity methodology. In addition, the lesson will discuss different attack modes against the critical infrastructure targets.

Chapter 1 - Introduction.

### Lesson 2: Diversity's Role in Cybersecurity

This lesson discusses the concept of diversity and will discuss the role it plays in a cybersecurity program. Further, the lesson introduces the concept of diversity and will discuss the role it plays in a cybersecurity program. How diversity can stop worm propagation is discussed, as are various methods of diversifying a system. The concept of diversity will be introduced with its importance in stopping malicious attacks.

Chapter 2 – Deception
Chapter 3 - Separation

### Lesson 3: Discretionary Tactics

This lesson discusses the concept of discretion — when it is effective and when it is not. The
discussion begins with the idea of a trusted computing base, continues through ways to share information, and concludes with methods of obscuring and compartmentalizing information.

Chapter 4 – Diversity

Lesson 4: Cybersecurity Protection Depth and Discretion
This lesson discusses the concept of commonality and depth. The cybersecurity protection measures deployed in depth and discretion will be discussed in detail.

Chapter 5 – Commonality
Chapter 6 – Depth

Lesson 5: Cybersecurity Protection Discretion and Collection/Midterm Essay Due
This lesson discusses the concepts of discretion and collection. The cybersecurity protection measures deployed in discretion and collection will be discussed.

Chapter 7 – Discretion
Chapter 8 – Collection

Lesson 6: Cybersecurity Protection and Correlation
This lesson describes the cybersecurity concept of correlation. Cyber correlation can be used defensively by the internal stakeholders and offensively by adversaries.

Chapter 9 – Correlation

Lesson 7: Cybersecurity Protection and Awareness
This lesson describes cybersecurity awareness program and the cybersecurity incident response program.

Chapter 10 – Awareness
Chapter 11 – Response

Lesson 8: Feedback and Final Paper
This week is the final week of the course. We ask you for feedback on the Cyber Vulnerability course. Students complete and submit their final essays.

Communication

Office Hours/Contacting the Instructor
See the Instructor Information section for contact information.

University Policies

Academic Integrity
Angelo State University expects its students to maintain complete honesty and integrity in their academic pursuits. Students are responsible for understanding and complying with the university Academic Honor Code and the ASU Student Handbook.
Accommodations for Disability

ASU is committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs or activities of the university, or be subjected to discrimination by the university, as provided by the Americans with Disabilities Act of 1990 (ADA), the Americans with Disabilities Act Amendments of 2008 (ADAAA), and subsequent legislation.

Student Affairs is the designated campus department charged with the responsibility of reviewing and authorizing requests for reasonable accommodations based on a disability, and it is the student's responsibility to initiate such a request by emailing studentservices@angelo.edu, or by contacting:

Office of Student Affairs
University Center, Suite 112
325-942-2047 Office
325-942-2211 FAX

Student absence for religious holidays

A student who intends to observe a religious holy day should make that intention known in writing to the instructor prior to the absence. A student who is absent from classes for the observance of a religious holy day shall be allowed to take an examination or complete an assignment scheduled for that day within a reasonable time after the absence.