Course Syllabus and Policy Requirement Statement

To minimize disruptions for you in this course, your self-compliance should include doing 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 familiarize yourself with how to access course content in Blackboard using the Student Quick Reference Guide or CSS Student Orientation Course.

BOR 6350 Cyber Vulnerability

Course Description/Overview

Cyber vulnerabilities pose 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 participations in discussions and preparation of cryptography project that will be practically useful in the current technology.

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.

Contributing Course Creator's Biography

Charles Pak earned his Ph.D. in Information Security from Nova Southeastern University, an M.S. in Network Security from Capitol College, and a B.S. in Electrical Engineering from Penn State University. He has taught Information Systems (IS) courses for over 25 years as an IS practitioner and professor. He has managed U.S. Federal Government data centers for over 20 years, including personnel. He has

designed, tested, implemented, and maintained many of these enterprise network sites (largest in the world) that encompasses distributed sites across the U.S. as well as the international sites. He has managed state-of-the art systems for military and federal government missions for which he was deployed.

His research topics include Cyber Security, Critical Infrastructure Protection (CIP), PKI, Cyber Counter Terrorism, and Risk Assessment & Management. He has published several research papers in Information Security. As a practitioner, he holds several industry certifications: CISM, CRISC, CISSP, ITIL, SSCP, MCSE, MCT, Security +, and CCNA.

Recent Publications:

- Pak, C. (2011). Near Real-time Risk Assessment Using Hidden Markov Models. Nova Southeastern University, ProQuest Dissertations and Theses,ISBN:9781124992945.
- Pak, C. & Cannady, J. (2010). Risk Forecast Using Hidden Markov Models. Research in Information Technology (RIT), ACM, SIGITE, 7(2), 4-15.
- Pak, C. & Cannady, J. (2009). Asset Priority Risk Assessment Using Hidden Markov Models. Proceedings of the 10th ACM SIGITE, Fairfax, Virginia, 2009, 65-73.
- Pak, C. (2008). The near real time statistical asset priority driven (nrtsapd) risk assessment. Proceedings of the 9th ACM SIGITE, Cincinnati, Ohio, 2008, 105-112.

Course Required Textbooks:

Amoroso, E. (2013). *Cyber Attacks: Protecting National Infrastructure*. Elsevier. ISBN-978-0-12-391855-0. VitalSource

Course Objectives/Learning Outcomes

Objectives: This lesson 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.

As a result of completing this course, the student will be able to:

1. Demonstrate a comprehensive knowledge of threats to national critical infrastructure.
2. Demonstrate critical reading and writing skills developed through the cyber vulnerability.
3. Apply cybersecurity best practices to a practical application.

Grading Policies

Assignment	**Percent of Grade**	**Due**
Participation in the Discussion Board	30%	Weekly **at the end of each week on Saturday at 11:59 P.M.**

		Central Standard Time.
Research Papers	70%	**1 - 7 Due Weekly at the end of each week on Sunday at 11:59 P.M. Central Standard Time**.

Research Papers

The purpose of these short papers is for you to demonstrate the ability to take the knowledge you have gained about encryption technology and its application. This is not intended to be a thesis, but a cryptography technique that can be implemented in your business, agency, or local community for a specific security requirement that you have identified.

These paper should be ***1 page, inclusive of the references***. It will be prepared as an academic paper along the guidelines provided in the APA writing style manuals. Feel free to ask your professor for assistance, clarification, or guidance at any time.

Formal academic writing uses standardized styles and citation formats. The preferred format is the APA style. 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.

Rubrics

Discussion forums and writing assignments will be graded using a standardized rubric. It is recommended that you be familiar with these grading criteria and keep them in mind as you complete the writing assignments. There are two rubrics. Click the link to download the PDF document:

Discussion Rubric
Writing Assignment Rubric

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 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.

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 Exam

This is an online course. In lieu of a final exam, students submit the cyber vulnerability research papers

throughout in the course. Students are concurrently asked to complete end of course surveys and provide an end of program analysis.

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 %
D = 60 – 69 %
F = 59 % 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's effective and when it isn't. 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 details.

Chapter 5 – Commonality

Chapter 6 – Depth

Lesson 5: **Cybersecurity Protection Discretion and Collection**

This lesson discusses the concept 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: **Feedbacck**

This week is the final week of the course. We ask you for feedback on the Cyber Vulnerability course. Students complete their critical analysis of other student(s) Emergency Planning proposals.

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.