California State University, San Marcos General Education Program
GENERAL EDUCATION NEW COURSE CERTIFICATION REQUEST
• AREA A3: Critical Thinking
See GE Handbook for information on each section of this form

ABSTRACT

Course Abbreviation and Number: CS 200- **Number of Units: 3**_____	**Course Title:** Critical Thinking about Cyber Security for You and Our Critical Infrastructure	
College or Program: ☐CHABSS ☒CSM ☐CEHHS ☐COBA ☐Other	**Desired term of implementation:** ☐ Fall ☐Spring ☒Summer Year:2016	**Mode of Delivery:** ☒ face to face ☐ hybrid ☐ fully on-line
Course Proposer (please print): **Youwen Ouyang**	**Email:** **ouyang@csusm.edu**	**Submission Date:** **03/11/2016**

1. Course Catalog Description: This course is designed to introduce students to Critical Thinking Skills. The course is also designed to introduce students to Cyber Security with an emphasis on how Cyber Security will affect them personally. Students will be introduced to the key concepts of Cyber Security. Cyber Security-related news reports will be examined using Critical Thinking skills. Examples will include the debate over personal privacy vs. the FBI's need to decrypt smartphones. Students will be asked to reason about the impact a cyber-attack on any of our 16 critical infrastructure sectors. What can students do to defend themselves and their families from cyber security attacks? What should we, as a nation, do "before the lights go out"?
See http://hp.ipviking.com/ to see the attacks that are occurring right now.

2. GE Syllabus Checklist: The syllabi for all courses certified for GE credit must contain the following:

☒	Course description, course title and course number
☒	Student learning outcomes for General Education Area and student learning objectives specific to your course, linked to how students will meet these objectives through course activities/experiences
☒	Topics or subjects covered in the course
☒	Registration conditions
☒	Specifics relating to how assignments meet the writing requirement
☒	Tentative course schedule including readings
☒	Grading components including relative weight of assignments

SIGNATURES

Course Proposer _____ Date _____

Department Chair _____ date _____

Please note that the department will be required to report assessment data to the GEC annually. _____ ***DC Initial***

		Support	Do not support*
Library Faculty _____	Date _____	☐	☐
Impacted Discipline Chair _____	Date _____	☐	☐
Impacted Discipline Chair _____	Date _____	☐	☐

		Approve	Do not Approve
GEC Chair _____	Date _____	☐	☐

California State University, San Marcos General Education Program
GENERAL EDUCATION NEW COURSE CERTIFICATION REQUEST
• AREA A3: Critical Thinking
See GE Handbook for information on each section of this form

Part A: Critical Thinking General Education Learning Outcomes (GELOs) related to course content. [Please type responses into the tables.]

Critical Thinking GELOs this course will address:	**Course content that addresses each GELO.**	**How will these GELOs be assessed?**
A3.1: Distinguish matters of fact from issues of judgment or opinion and derive factual or judgmental inferences from unambiguous statements of knowledge or belief.	Logic Book: An Illustrated Book of Bad Arguments Reasoning Skills Book: Lessons 1 – 3 Cyber Security Book: Ch 1 Stuxnet – The First Cyber Guided Missile Cyber Security Book: Ch 8 Nations at Cyber War Cyber Security Book: Ch 14 Listening In and Going Dark	Students will be asked to participate in both in-class and online discussions on critical Cyber Security related issues such as privacy rights versus government need to protect citizens. This GELO will be assessed based on the quality of student participation in the Discussion Boards. Students will be asked to distinguish facts from opinions and explain how both sides of the debate derive judgment from facts and opinions. Students will be exposed to all of the concepts in the Logic Book – "An Illustrated Book of Bad Arguments" at the beginning of the course. Each week students will be presented with concepts from the Reasoning Skills book. They will then be asked apply these concepts in debating questions derived from the Cyber Security book, as well as other examples that illustrate the point from the other resources. This GELO will also be assessed in the student Essays on Cyber Security-related topics presented in class. In both the Discussion Board debates and the student Essays, the ability to distinguish matters of fact from issues of judgement will be assessed. Students will be required to distinguish between opinions they disagree with and statements meant to be factual. The identification of "Bad Arguments" will be required throughout the course as part of this GELO.
A3.2: Judge the reliability and credibility of sources.	Reasoning Skills Book: Lessons 4 & 5 Cyber Security Book: Ch 12 Big Data – "They" Know Everything about You	This GELO will primarily be assessed in the Student Essays and Student Presentations. Students will be asked to research topics related to cyber security, cyber-attacks and our Critical Infrastructure.

		Students will write essays based on their research and include discussions of the reliability and credibility of the sources selected for use in their essays. This GELO will be assessed by Students' ability to identify credible sources vs sources that might just be seeking to "sell" a Cyber Security solution or service.
A3.3: Effectively argue a point of view by clarifying the issues, focusing on the pertinent issues, and staying relevant to the topic.	Logic Book: An Illustrated Book of Bad Arguments Reasoning Skills Book: Lessons 2, 7, 8 Cyber Security Book: Ch 18: Looking Forward – What Does the Future Hold?	When stating their point of view regarding cyber security policies and practices, students will be asked to focus on selected problems and keep their argument relevant to the topic. This GELO will primarily be assessed in the Student Essays and Student Presentations on Cyber Security topics – where students have time to fully argue a point of view. This GELO will be assessed to a lesser extent in the debate in the Discussion Boards on Cyber Security-related questions (as well as other examples that illustrate the point from the other resources).
A3.4: Understand the nature of inductive and deductive reasoning, identify formal and informal fallacies of reasoning, and employ various methods for testing the strength, soundness, and validity of different argument forms.	Reasoning Skills Book: Lessons 11 - 15 Cyber Security Book: Ch 12 Big Data – "They" Know Everything about You Cyber Security Book: Ch 14 Listening In and Going Dark Logic Book: An Illustrated Book of Bad Arguments	Students will be asked to evaluate examples of cyber events to determine whether such event post a threat to cyber security using inductive and deductive reasoning. Students will also be asked to assess potential errors in inductive and deductive reasoning presented by news reports on cyber-attacks. Students will be asked apply sound reasoning (avoid "Bad Arguments") when writing their essays, and when stating their views. This GELO will be assessed in classroom discussions and in the debate in the Discussion Boards on Cyber Security-related questions (as well as other examples that may more clearly illustrate the point from the other resources (e.g., the Reasoning Skills book or the Logic Book)). This GELO will also be assessed in the Essays and student presentations

		on Cyber Security topics.
A3.5: Understand the basic concepts of meaning (sense, reference, connotation, etc.) and identify different methods of word definition.	Reasoning Skills Book: Lesson 5 – 10 Additional Resources: Cybersecurity Awareness Training Version 2.0 This is Cybersecurity training to explain the Cyber Security concepts in an interactive, audio, video, and kinetic (AVK) way. http://cdsetrain.dtic.mil/cybersecurity/	This GELO will be assessed in Chapter Reviews, where student understanding of the concepts, their relevance locally, nationally and internationally will be exercised and evaluated. This GELO will be assessed in classroom discussions and in the debate in the Discussion Boards. This GELO will also be assessed in the Essays and student presentations on Cyber Security topics. The course is designed to introduce students to Cyber Security with an emphasis on how Cyber Security will affect them personally. The Cybersecurity Awareness Training includes a printable certificate which can serve as evidence that a student completed the course. Students will be asked to submit the printed certificate to the instructor as evidence of completion. Students will demonstrate a practical understanding of the meaning (sense, reference, and connotation) of Cyber Security terms using this practical interactive, audio, video, and kinetic (AVK) hands-on assignment. This GELO will also be assessed in the Essays and student presentations on Cyber Security topics.
A3.6: Understand logic and its relationship to language by identifying the basic components of reasoning, including the propositional content of statements, the functions of premises and conclusions in the makeup of	Reasoning Skills Book: Lesson 5 – 10 Logic Book: An Illustrated Book of Bad Arguments Cyber Security Book: Ch 7 Hacktivists and Insurgency	This GELO will be assessed in Chapter Reviews, where students will be asked to identify the form of argument and language being presented in the Cyber Security Book. This GELO will also be assessed in the debate in the Discussion Boards on examples that illustrate elements of Logic from the Reasoning Skills Book and the Logic Book – An Illustrated Book of Bad Arguments. Students will be asked to identify the basic components of reasoning. This GELO will also be assessed in the Student Essays and Student

arguments, the linkage between evidence and inference, and the rules of inference and logical equivalence.		Presentations on Cyber Security topics. Students will be asked to present analyses of news reports based on logic and draw conclusions about the relative importance of a cyber-attack on different Critical Infrastructure sectors. Students will also be asked to reason about the cyber attacks that are occurring daily, and to determine the potential for serious cyber attacks in the future. Students will be asked to discuss, as an example, whether corporations that are being cyber-attacked can (and should) counter-attack? Should the US Government protect them? How? Students will be asked to reason about, as an example, the activities of Hacktivists like the group "Anonymous". Are their actions justified? Do they help the situation or make it worse?

Part B: General Education Learning Outcomes required of all GE courses related to course content:

GE Outcomes required of <u>all</u> Courses	**Course content that addresses each GE outcome?**	**How will these GELOs be assessed?**
Students will communicate effectively in writing to various audiences. (writing)	Cyber Security Book: Ch 1 – 17 Logic Book: An Illustrated Book of Bad Arguments	This GELO will be assessed in evaluating the Student Essays. Students will be asked to write several essays, and to present several topics to the class. Students will select topics of interest to them from the options provided during the course. Students will also be asked to debate (in writing) Course Topics in the Discussion Board after each Session. Many of the topics of this course do not lend themselves to one word or symbolic answers, but require explanations and personal judgements.

California State University, San Marcos General Education Program
GENERAL EDUCATION NEW COURSE CERTIFICATION REQUEST
• AREA A3: Critical Thinking
See GE Handbook for information on each section of this form

		Some of the Chapter Review questions may require lengthy written answers.
Students will think critically and analytically about an issue, idea or problem. (critical thinking)	Do not complete. This information is provided in Part A.	Do not complete. This information is provided in Part A.
Students will find, evaluate and use information appropriate to the course and discipline. (Faculty are strongly encouraged to collaborate with their library faculty.)	This course identifies a number of additional resources to start students in the right direction. Additional Resources: Critical Infrastructure Sectors This resource identifies the Critical Infrastructure Sectors that we will be discussing in class and writing about in essays. http://www.dhs.gov/critical-infrastructure-sectors Additional Resources: Cybersecurity Awareness Training Version 2.0 This is Cybersecurity training to explain the Cyber Security concepts in an interactive, audio, video, and kinetic (AVK) way. http://cdsetrain.dtic.mil/cybersecurity/ Students will be encouraged to use the Library resources to find additional authoritative sources to round out their perspective.	Students will be asked to research topics related to cyber security, cyber-attacks and our Critical Infrastructure. Authoritative sources such as the Department of Homeland Security and cyber security-related firms will be accessed. This GELO will be assessed primarily with the evaluation of the sources selected for the Essays and Student Presentations on Cyber Security. The Cybersecurity Awareness Training includes a printable certificate which can serve as evidence that a student completed the course. Students will be asked to submit the printed certificate to the instructor.

Part C: GE Programmatic Goals: The GE program aligns with CSUSM specific and LEAP Goals. All A3 courses must meet at least one of the LEAP Goals.

GE Programmatic Goals	***Course addresses this LEAP Goal:***
LEAP 1: Knowledge of Human Cultures and the Physical and Natural World.	☐ *No* ☒ *Yes*
LEAP 2: Intellectual and Practical Skills	☐ *No* ☒ *Yes*
LEAP 3: Personal and Social Responsibility	☐ *No* ☒ *Yes*
LEAP 4: Integrative Learning	☐ *No* ☒ *Yes*
CSUSM Specific Programmatic Goals	**Course content that addresses the following CSUSM goals. Please explain, *if applicable.***
CSUSM 1: Exposure to and critical thinking about issues of diversity.	☐ *No* ☒ *Yes (please describe):Students will be asked to evaluate the actions of several diverse groups in terms of their disaster preparedness.*

California State University, San Marcos General Education Program
GENERAL EDUCATION NEW COURSE CERTIFICATION REQUEST
• AREA A3: Critical Thinking

See GE Handbook for information on each section of this form

CSUSM 2: Exposure to and critical thinking about the interrelatedness of peoples in local, national, and global contexts.	☐*No* ☒***Yes (please describe):Students will be asked to look at the impact of our Critical Infrastructure (e.g., the power grid) and see how it would impact the whole US. Also the global nature of cyber security and cyber-attacks will be addressed.***

Part D: Course requirements to be met by the instructor.

Course Requirements:	**How will this requirement be met by the instructor?**
Course meets the All-University Writing requirement: A minimum of 2500 words of writing shall be required for 3+ unit courses.	The instructor will assign the following: Students will be asked to write two (2) 1,250 word essays / student presentations on topics related to cyber security and our critical infrastructure.
Critical thinking may be taught in the context of a subject area, by including specific attention to general principles of critical thinking and applying them to examples and exercises in the subject area.	The instructor will guide the students through the areas of concern for Cyber Security and our Critical Infrastructure segments.
The course proposals will demonstrate the application of information literacy to the course materials.	The instructor will show the relationship between computers, Cyber Security and the various Critical Infrastructure Sectors.
All critical thinking courses will be open to all students regardless of their majors; therefore, the basic reasoning skills listed in the above objectives must be explicitly covered.	*The instructor will address the fundamentals of Cyber Security and relate it to common areas of knowledge and practical experience (e.g., the electrical power grid). Cyber Security with an emphasis on how Cyber Security will affect students personally.*

Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare

Professor Paul Rosenzweig

http://www.audible.com/pd/Nonfiction/Thinking-about-Cybersecurity-From-Cyber-Crime-to-Cyber-Warfare-Audiobook/B00DL152XU/ref=a_search_c4_1_1_srTtl?qid=1456895991&sr=1-1

1. **Stuxnet—The First Cyber Guided Missile**

Your introduction to the fascinating—and fascinatingly dangerous—world of cybersecurity begins with the story of "Stuxnet." Learn how this unique piece of malware, which shut down a uranium enrichment facility in Iran, signaled the dawn of a new age in which viruses and other cyber threats can manipulate the physical world.

2. **The Incredible Scope of Cyberspace**

What makes the Internet so vulnerable is its ability to connect, and to be connected to, anyone and almost anything. Here, explore how cyberspace works. You'll learn what goes on behind the scenes of a simple Internet search, how a simple TCP/IP system functions, the five layers of connections that make up a conceptual "map" of cyberspace, and more.

3. **The Five Gateways of Internet Vulnerability**

Take a closer look at the cyber domain's inherent vulnerability to cyber threats. Professor Rosenzweig explains the five key gateways to this vulnerability, including the Internet's ability to destroy time and space; allow users to act in ways they can't in the physical world; and operate without international boundaries.

4. **Of Viruses, Botnets, and Logic Bombs**

Learn about some of the most dangerous ways people can exploit the Internet's vulnerabilities, including DDoS attacks (which flood websites with connection requests), "Trojans" (malware hidden inside an innocent piece of information), and "botnets" (which control computers like puppets). Then, investigate some common defense mechanisms that help pinpoint and capture these threats. x

5. **The Problem of Identity on the Network**

Identification is perhaps the single most profound challenge for cybersecurity today. In this lecture, delve into the question of network anonymity and identity. Who maintains domain names? How can people obscure their identities for malicious purposes? How are network designers fighting back against this threat? What are the ethical problems involved in this issue?

6. **Cyber Fraud, Theft, and Organized Crime**

Professor Rosenzweig leads you on an examination of all-too-common instances of cybercrime that involve fraud and identity theft. You'll encounter crimes that mimic real-world ones (with a computer as the "weapon") and "computer crimes" that are only possible in the cyber world. Then, find out how law enforcement authorities are fighting back against organized, international cyber criminals.

7. **Hacktivists and Insurgency**

Enter the netherworld of hacktivism, or the use of computer hacking methods to stage protests and make political statements. In this lecture, learn to identify and distinguish the "good guys" from the "bad guys" by exploring real-world examples that illustrate the three major types of hacktivists: political activists, cyber insurgents, and mischief makers.

8. Nations at Cyber War

Turn now to the highest level of cyber conflict: a cyber war between nation-states. What is meant by the term "cyber war"? How does one fight a battle in cyberspace? What do the enemies look like? Do traditional international rules of armed conflict apply? How do we counter such an attack—and should we?

9. Government Regulation of Cyberspace

Join the debate about government regulation of cyberspace with this lecture that considers both sides of the issue. By looking at the debate in America over government oversight of cybersecurity (and whether we even need it at all), you'll be better informed about a topic that has serious ramifications for how you use the Internet.

10. International Governance and the Internet

Continue exploring rules and regulations about the Internet, this time on the international level. First, Professor Rosenzweig discusses existing Internet governance and the dynamics leading to change. Then, he assesses some of the barriers to effective international governance of the Internet. Is the current structure, with all of its flaws, better than the alternatives?

11. The Constitution and Cyberspace

Return to American policies on cybersecurity, this time focusing on the idea of government monitoring of the Internet. Start by learning all about how on-network monitoring systems work. After that, step back and examine how government monitoring is enforced and limited—but not prohibited—by the Constitution.

12. Big Data—"They" Know Everything about You

In the first of two lectures on personal data tracking and privacy, ponder the problem of "Big Data"—where your Internet searches can be tracked, your cellphone can broadcast your geographical location instantly, and your online purchases can be catalogued. It's a frightening aspect of cybersecurity, and one that, unfortunately, is here to stay.

13. Privacy for the Cyber Age

It appears our current conceptions of privacy in cyberspace will disappear. So what can we do about it? By exploring how the government and private sector use "Big Data"—and how "Big Data" can keep the government honest—you'll discover insights into how we can evolve our privacy laws while embracing new technologies.

14. Listening In and Going Dark

Learn how encryption and wiretapping work in cyberspace, and how both methods are becoming increasingly frustrating for law enforcement and national security officials. This "going dark"

phenomenon, as you'll find in this eye-opening discussion, brings benefits and causes problems—and the solutions seem to bring problems of their own.

15. The Devil in the Chips—Hardware Failures

Hardware-based threats are one of the most vexing problems in the entire cybersecurity domain. How do we know that our machines will actually do what we tell them to do? Why is compromised hardware such a critical threat to cybersecurity? What are some possible solutions for dangers hidden in computer chips?

16. Protecting Yourself in Cyberspace

Get practical tips on how to reduce your own risk of danger online in your professional and personal life. You'll find out how to choose the most effective passwords, how to set up the most effective personal computer security systems, how to encrypt and erase personal data and documents, and much more.

17. Critical Infrastructure and Resiliency

Take an alternate approach to cybersecurity, this time focusing on resiliency and recovery. There may be good reason to think that creating a system that isn't immune to failure but is less likely to be attacked—and better able to operate even while under attack—is the best course of action.

18. Looking Forward—What Does the Future Hold?

Finish the course with a helpful summary of the main issues and arguments involved in the current state of cybersecurity throughout the world. Then, take an intriguing peek into the future to explore