

BCJ 355

Homeland Security



925 North Spurgeon Street, Santa Ana, CA 92701
Phone: 714-547-9625 Fax: 714-547-5777
www.calcoast.edu

Rev. 01/17

Tracking Your Academic Activities

Verifying an accurate course completion time is essential for accreditation. To meet both accreditation requirements and award academic credit, educational institutions must document the total number of hours students spend completing designated academic activities related to their coursework.

The total hours are then translated into academic credit based on a prescribed method of measuring educational attainment known as the Carnegie Unit. 90 hours of student preparation time and 45 hours of student engagement time are required for a 3 credit hour course.

Using the attached form as an example, keep track of the time you spend on each lesson, pre-test, self-test, unit test, writing assignment, reading assignment, outside reading, final examination, etc. You will not be required to turn in the worksheet; however, at the end of the course you will receive a Student Course Survey and the final question will ask how long it took you to complete the course. Your assistance in completing this requirement and providing the university with this valuable data is greatly appreciated.

As you fill out the worksheet, please keep in mind that your **Academic Engagement Activities** should total approximately 45 hours. Some examples of this type of activity may include:

Lesson Review Exercises
Key Term Reviews
Analysis
Study Guide Review
Writing Assignments
Review Grading Rubric

Unit Examinations
Proctored Final Examination
Course Academic Online Discussions
Student/Instructor Interaction
Documents/Student Resources

As you fill out the **Academic Preparation Activities**, please keep in mind that these should total approximately 90 hours. Some examples of this type of activity may include:

Pre-Test
Reading Assignments
Key Term Reviews
Studying for Examinations
Writing Assignments

Review Grading Rubric
Study Lesson Review Exercises
Internet/Web Research
Reading Websites
Suggested Outside Reading

Sample Worksheet for Tracking Your Academic Activities

This worksheet was developed to help you track your time. You are not required to turn it in.

Upon completion of this course, you will be asked to complete a survey. The last question on the survey will ask you the number of hours it took to complete the course. Course credit is based on the Carnegie Unit - a prescribed method of measuring educational attainment. For each 3 unit semester course, students will complete a variety of academic activities including:

45 hours of Academic Engagement and 90 hours of Academic Preparation = 135 hours in total.

	Time to Complete Unit 1	Time to Complete Unit 2	Time to Complete Unit 3	Time to Complete Unit 4	Time to Complete Final	Total Time Spent
Academic Engagement Activities						
Lesson Review Exercises						
Key Term Review Exercises						
Study Guide Review						
Student Resources						
Review Grading Rubric						
Case Studies/Critical Analysis						
Writing Assignments						
Complete Unit Examinations						
Course Academic Online Discussions						
Student/Instructor Interactions						
Total Academic Engagement required for a 3 unit course = 45 hours					Total =	

Academic Preparation Activities						
Pre-Test						
Reading Assignments						
Review Case Studies/Critical Analysis						
Key Term Review Exercises						
Study for Examinations						
Suggested Outside Readings						
Web Research						
Review Writing Assignments						
Review Completed Examinations						
Review Grading Rubric						
Reading Websites						
Study Lesson Review Exercises						
Total <u>Academic Preparation</u> required for a 3 unit course = 90 hours					Total =	
Total hours: <u>Academic Engagement</u> and <u>Academic Preparation</u> related to this course.					Grand Total	

Other Activities/Comments - (Please note all time for additional course related activities):

Pre-test Instructions

Thank you for taking the time to complete the required pre-test. The purpose of the pre-test is to measure your knowledge of the subject matter at the beginning of each course.

Please be assured, your score on the pre-test will not be part of your course grade. We do not want you to try to study for it or be worried about doing well on the pre-test. It is simply a measure of your “starting place,” that will be used for improving course content and to meet accreditation requirements.

If you receive your course materials online:

- Please log-in to your Coast Connection student portal to complete your pre-test.

If you receive your course materials by mail:

- You will receive your answer sheets for the pre-test by mail.
- Once you have completed your pre-test, please mail or fax your answer sheet to the University at:

California Coast University
925 N. Spurgeon Street
Santa Ana, CA 92701
Fax: 714-547-1451

If you have any questions, please feel free to contact the Student Services Department. Thank you for your cooperation.

Multiple Choice Questions (Circle the correct answer)

1. James Lee Witt became the director of FEMA during which President's administration?
 - a. Ronald Reagan
 - b. George H.W. Bush
 - c. Bill Clinton
 - d. George W. Bush

 2. Which incident can be described as an act of domestic terrorism?
 - a. the 1993 attack on World Trade Center
 - b. the events of September 11, 2001
 - c. Aimal Kasi's attack
 - d. the Oklahoma City bombing

 3. Roughly how big is the United States' northern border with Canada?
 - a. 2,800 miles
 - b. 4,000 miles
 - c. 6,000 miles
 - d. 5,000 miles

 4. Which of the following is not typically considered to be a type of terrorism?
 - a. group
 - b. religious
 - c. single-issue
 - d. left-wing/right-wing

 5. Which of the following Federal Statutes were amended by the USA PATRIOT Act?
 - a. Bank Holding Company Act of 1956
 - b. Fair Credit Reporting Act
 - c. Federal Wiretap Statute
 - d. all of the above

 6. Which Presidential Executive Order created the Public Alert and Warning System?
 - a. 13311
 - b. 13356
 - c. 13407
 - d. none of the above
-

7. In terms of size, where does the DHS rank, compared to all federal cabinet-level departments?
- third
 - first
 - seventh
 - fifth
8. Which part of DHS oversees the integrity of the nation's financial infrastructure ?
- Secret Service
 - FBI
 - US-CERT
 - ICE
9. The Critical Infrastructure and Key Resources (CIKR) Asset Protection Technical Assistance Program (CAPTAP) is part of which DHS major mission area?
- preparedness and response
 - security of U.S. borders
 - counter-terrorism
 - protection of cyberspace
10. Which agency/department generally handles domestic Human Intelligence (HUMINT)?
- Federal Bureau of Investigation
 - National Security Agency
 - Department of Defense
 - Customs and Immigration
11. Which agency/department is in charge of developing map-based intelligence solutions?
- National Geospatial-Intelligence Agency
 - National Security Agency
 - National Reconnaissance Office
 - Defense Intelligence Agency
12. Prior to 9/11, most U.S. counterterrorism resources were dedicated to what?
- airline safety
 - weapons of mass destruction
 - right- and left-wing extremists
 - foreign targets
-

13. Which of the following best describes President George W. Bush's first approach to counter-terrorism after 9/11?
 - a. the War on Terror
 - b. multilateralism
 - c. Bush Doctrine
 - d. none of the above

 14. Strengthening the workforce with training, programs for employee health, and increased workforce diversity were recommendations of which document?
 - a. National Strategy (2007)
 - b. National Response Plan (2004)
 - c. National Response Framework (2008)
 - d. Strategic Plan (2012)

 15. Which of the following can be considered an initiative related to the "Intelligence and Warning" mission described in the National Strategy?
 - a. implementation of the Homeland Security Advisory System
 - b. enhancement of the analytic capabilities of the FBI
 - c. utilization of dual-use analysis to prevent attacks
 - d. all of the above

 16. What biological agent was used in an attack against the United States in the days shortly after 9/11?
 - a. anthrax
 - b. small pox
 - c. ricin
 - d. mustard gas

 17. Which weapon is generally the most conventional?
 - a. anthrax
 - b. fertilizer bomb
 - c. dirty bomb
 - d. nuclear

 18. Which entity plays the biggest role in providing technical and financial support for emergency and disaster recovery?
 - a. state governments
 - b. private industry
 - c. federal government
 - d. local governments
-

19. Community recovery efforts are primarily overseen by what?
- a. local law enforcement
 - b. Incident Command System
 - c. domestic preparedness office
 - d. Joint Field Office
20. Which level of government would typically not employ the Incident Command System (ICS)?
- a. state
 - b. federal
 - c. international
 - d. tribal
21. Which ICS management characteristic allows differing agencies to work together effectively?
- a. manageable span of control
 - b. chain of command
 - c. unified command
 - d. dispatch/deployment
22. The Court Security Improvement Act was passed by which Congress?
- a. 109th
 - b. 110th
 - c. 108th
 - d. 107th
23. Which President Obama executive order optimized biological agent and toxin security in the U.S.?
- a. Executive Order 13539
 - b. Executive Order 13491
 - c. Executive Order 13456
 - d. Executive Order 13553
24. In which Supreme Court case did the court effectively sidestep the constitutional issues surrounding the Jose Padilla case?
- a. Rumsfeld v. Padilla
 - b. Hamden v. Rumsfeld
 - c. Boumediene v. Bush
 - d. Hamdi v. Rumsfeld
-

25. Which organization challenged the “No-Fly Watch List”?

- a. FBI
- b. TSA
- c. ACLU
- d. UN

BCJ 355

Homeland Security

Text: ***Introduction to Homeland Security: Policy, Organization, and Administration***

1st Edition, 2015

ISBN-13: 9781284045833

Author(s): Willard M. Oliver, Nancy E. Marion, Joshua B. Hill

Publisher: Jones & Bartlett



925 North Spurgeon Street, Santa Ana, CA 92701

Phone: 714-547-9625 Fax: 714-547-5777

www.calcoast.edu

Rev. 01/17

All rights reserved. No part of this may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system without written permission, except for the inclusion of brief quotation in review.

Copyright ©2020 by California Coast University

Welcome to California Coast University. I hope you will find this course interesting and useful throughout your career.

This course was designed to meet the unique needs of students like you who are both highly motivated and capable of completing a degree program through distance learning.

Our faculty and administration have been involved in distance learning for over forty years and understand the characteristics common to successful students in this unique educational environment.

This course was prepared by CCU faculty members who are not only outstanding educators but who have real world experience. They have prepared these guidelines to help you successfully complete your educational goals and to get the most from your distance learning experience.

Again, we hope that you will find this course both helpful and motivating. We send our best wishes as you work toward the completion of your program.

Sincerely,

Thomas M. Neal
President

Course Number	BCJ 355
Course Title	Homeland Security
Course Description	<i>Homeland Security</i> reviews basic issues of homeland security, the history and context of the field, and what the future of the field might hold. Central issues surrounding homeland security including policy concepts and political and legal responses will be covered.
Units of Credit	3 Units of Credit
Course Objectives	Upon successful completion of this course, students will be able to: • Analyze common themes of homeland security as found through the homeland security bureaucracy, concepts, strategy, mission, goals, and areas of emphasis. • Examine the components of terrorism and what differentiates it from regular crime. • Examine the passage of the USA PATRIOT Act and the myriad laws it contained. • Assess how the intelligence and security communities interact with the criminal justice system. • Examine the different types of threats (chemical, biological, radiological, nuclear, and explosives) facing the United States. • Analyze the challenges faced by homeland security in the future.
Learning Resources	Textbook: <i>Introduction to Homeland Security: Policy, Organization, and Administration</i> 1st Edition, 2015 Oliver, Marion, and Hill Jones & Bartlett ISBN-13: 9781284045833 All course examinations are based on the contents of the textbook required for this course. To successfully complete the examinations, you will need the textbook. You may rent the textbook from the CCU rental library or you may purchase the textbook from another source.

Although this study guide is developed by California Coast University, it does contain materials provided by the publisher of the textbook.

The Study Guide

The study guide was designed to help you further understand the materials in the textbook and master the course content. Each study guide chapter corresponds to a chapter in the textbook.

Additional Readings and Online Resources

When reading your textbook, you may notice images/references/links to additional text materials. If so, these images/references/links may be part of the publisher's "pay-for-access" online platform. Our courses are not designed to incorporate these additional resources and you will NOT need to purchase these additional features to be successful in this course.

For other relevant, helpful resources and learning activities designed to enhance your understanding of the topics in this course, simply log into your student portal.

The Library Information and Resources Network, Inc. (LIRN)

Students are provided access to the Library and Information Resources Network, Inc. (LIRN). LIRN provides a centralized management of electronic information resources that allow students to access multiple research databases through one portal. Detailed information on the Library and Information Resources Network, Inc. is available on the California Coast University website under the Resources tab. For additional information on using the network, LIRN provides a User Guide to help students search for the needed information. This helpful resource is available on the LIRN website. For information on accessing LIRN, please contact California Coast University - library@calcoast.edu or (714) 547-9625.

Your Course Grade

Your grades on course examinations are determined by the percentage of correct answers. The university uses the following grading system:

- A = 90% – 100% correct
- B = 80% – 89% correct
- C = 70% – 79% correct
- D = 60% – 69% correct
- F = 59% and below correct

Your grade in this course will be based on the number of points you earn. Grades are based on the percentage of points you earned out of a total of 500 points:

Four Unit Examinations

100 points each 400 points total 80% of your grade

Final Examination

100 points 100 points total 20% of your grade

Mastering the Course Content

In order to successfully complete this course, we recommend that you do the following before beginning:

- Be sure that you have the correct edition of the course textbook. Check the ISBN number of your textbook with the ISBN number listed on the cover page of this study guide.
- Review the Table of Contents at the end of this syllabus.
You will only be responsible for the chapters in the textbook that are listed in the Table of Contents.

Each study guide contains several components selected and developed by the faculty to help you master the content of the course. Each chapter in the study guide corresponds to a chapter in the textbook. Study guides vary depending on the course, but most will include:

Learning Objectives
Overviews
Self-Tests
Summaries
Key Terms

The most efficient way to complete this course is to read the material in both the study guide and textbook in the sequence in which it appears, generally from beginning to end.

Read the Overviews and Summaries

Before reading a chapter of your textbook, review the corresponding learning objectives, overview, key terms and summary sections in the study guide. These were prepared to give you a preview of the content to be learned.

Read and Review the Chapter

Once you have the scope and organization of the chapter in mind, turn to the corresponding chapter in the textbook and read the material carefully. Keep the learning objectives, key terms, and self-test questions in mind as you read.

Highlight important concepts and information in your study guide and write notes in the study guide as you read the textbook. These notes will help you study for the unit and final examinations.

Check Your Mastery of Each Chapter

When you feel that you have mastered the concepts presented in the chapter, complete the study guide self-test questions without referring to the textbook or your notes. Correct your responses using the answer key provided in the study guide. Your results will help you identify any areas you need to review.

Unit Examinations

Each course contains four unit examinations and a final examination. Unit examinations consist of 25 objective (multiple choice) test questions. The final examination consists of 100 objective (multiple choice) questions.

Unit examinations are open-book, do not require a proctor and are not timed. This will allow you to proceed at your own pace. As you go through the study guide, it will prompt you on when to complete a unit exam (approximately after every three to six chapters). The Table of Contents in this study guide will also give you an overview of which textbook chapters are covered in each of the four unit exams.

Writing Assignments

Each unit examination includes a written component. The writing assignments give students the opportunity to demonstrate a level of subject mastery beyond the objective unit examinations, which reflects his/her ability to analyze, synthesize, evaluate and apply his/her knowledge.

Writing assignments are judged on the quality of the response. Word count is NOT one of the criteria that is used in assigning points to writing assignments. However, students who are successful in earning the maximum number of points tend to submit writing assignments that are 350-500 words (1-2 pages) per question.

Plagiarism

All work must be free of any form of plagiarism. ***Put written answers into your own words.*** Do not simply cut and paste your answers from the Internet and do not copy your answers from the textbook.

Plagiarism consists of taking and using the ideas, writings or inventions of another, without giving credit to that person and presenting it as one's own. This is an offense that the university takes very seriously. An example of a correctly prepared written response may be found by visiting the Coast Connection student portal. You can find this in the portal by clicking on *Student Resources* and then *Writing Basics*.

Citation Styles

The ***majority*** of your response should be your own original writing based on what you have learned from the textbook. However, students may also use outside materials if applicable. Be sure to provide a citation and a reference for any materials used, including the required textbook. The following points are designed to help you understand how to provide proper citations and references for your work:

- Sources are listed in two places.
- The first, a citation, is briefly listed within your answer. This includes identifying information that directs the reader to your list of references at the end of your writing assignment.
- The second, a reference, is at the end of your work in the list of references section.
- All sources cited should follow APA style and provide enough identifying information so that the reader can access the original material.

More detailed information about citations and references can be located on the Coast Connection student portal. You can find this in the portal by clicking on *Student Resources* and then *Writing Lab*.

Submitting Your Unit Examinations and Writing Assignments via the Internet

Students may access the online testing features via the Coast Connection student portal. Unit examinations may be completed and submitted online.

Go to the California Coast University homepage at www.calcoast.edu and click on the *Student Login* icon at the upper right hand corner. After logging into your account, click on *My Academic Plan* and select the course you are working on to complete the unit examination. More detailed instructions on completing the examination online will be provided on that page. Remember to keep a copy of your answers for your own personal records.

Writing assignments may be submitted online as well. After logging into the student portal, click on *My Academic Plan* and select the course you are working on to complete the writing assignments. Here, you will find further information and instructions on how to submit writing assignments through the student portal. Remember to keep a copy of your writing assignments for your own personal records.

Alternatively, if you experience difficulty submitting your writing assignments through the student portal, then you may email your assignments as a Word document attachment to the following email address:

essays@calcoast.edu

When doing so, please adhere to the following guidelines:

- Always submit your **name, student number, course number, course title and writing assignment number (i.e. writing assignment 1, 2, 3, or 4)** with your writing assignment.
- Begin each writing assignment by identifying the question number you are answering followed by the actual question itself (in bold type).
- Use a standard essay format for responses to all questions (i.e., an introduction, middle paragraphs and conclusion).
- All responses must be typed double-spaced, using a standard font (i.e. Times New Roman) and 12 point type size for ease of reading and grading.

Submitting Your Unit Examinations by Mail or Fax

Send your completed unit examinations and/or any writing assignments to the following mailing address:

California Coast University
Testing Department
925 N. Spurgeon Street
Santa Ana, CA 92701

Unit examination answer sheets can also be faxed to the Grading Department at (714) 547-1451. Please do not resize your fax.

The Grading Department **WILL NOT** accept faxed writing assignments.

Challenging a Test Item

We make every effort to ensure that all examination items are fair and can be answered by reading and understanding the material in your textbooks. However, problems sometimes arise in the selection or interpretation of test items. For example, you might argue that two alternatives could be correct, based on the material you read, or that the correct answer is not among the choices. Occasionally, a typographical error might make a question difficult to answer.

If you encounter a problem with a test item while taking your exam, you may “challenge” it by providing a brief explanation along with the page number(s) from the textbook in which the correct answer can be found. Likewise, you may also submit a test item challenge after your exam has been graded if you feel a test item was scored incorrectly. Students may submit up to two test item challenges for each unit exam and up to four test item challenges for the final exam. Test item challenges are not permitted for the pre-test. You may submit test item challenges via the Coast Connection student portal or by U.S. mail.

Submitting Your Test Item Challenges via the Internet

Please log into the Coast Connection student portal for specific instructions on challenging a test item. You will submit your test item challenges directly through the student portal.

Submitting Your Test Item Challenges by Mail

- For each test question you wish to challenge, fill in option “F” on the answer sheet for that question.

- On a separate sheet of paper, indicate your name and student ID number, identify the examination you are working on (i.e., Unit Exam 1, 2, 3, etc.), and the specific question number you are challenging.
- Write out the question and its given choices and explain why you are “challenging” the test item.
- Provide a page reference from the textbook to support your answer. **If you do not provide a page reference, we may not be able to give you credit.**
- Mail your multiple choice answer sheet and test item challenge documents to the Testing Department.

The information you provide is important to us. It will help us further validate and correct any possible errors in the testing materials.

If you follow the Test Item Challenge procedure, your challenge will be reviewed and if correct, you will be given credit. You should allow an additional week for the review and scoring of your examination.

Repeating a Unit Exam

Requests to retake a unit examination will only be honored if the final exam has NOT been sent.

Students may retake one unit examination per course, free of charge. The cost for each additional, repeated exam will be \$90. Payment must be paid in full prior to repeating a unit exam and can be done via the student portal or by submitting a Repeat Unit Exam form.

Please contact the Testing Department for more information. When repeating a unit exam through the student portal, the original grade will be cleared out once you click *Re-take*.

Final Examination

Scheduling a Final Examination

Final examination requests can be submitted online through the Coast Connection student portal, via U.S. mail, or by calling the Testing Department at (714) 547-9625.

If you would like to request a final exam online, log into the Coast Connection student portal and click on *My Academic Plan*. Select the course you are working on and submit the Final Exam Request form located at the bottom of the page. **ALL INFORMATION MUST BE FILLED IN.**

A final exam scheduling form is also located on the last page of this study guide and can be mailed or faxed to the university. Please fill out **ALL** required fields if you choose to submit your final exam request using this form.

After we receive the Final Examination Request Form, CCU will send your final examination to your designated proctor via email or mail, along with further instructions.

Proctors

California Coast University requires that all undergraduate students complete all final examinations—with the exception of general elective courses—under the supervision of a proctor.

The proctor is selected by the student and approved by the university. A proctor can be any reputable person **EXCEPT** *a relative, someone who resides with the student, or a current/former California Coast University student*. Typical examples of approved proctors include friend, neighbor, job supervisor, co-worker, librarian, counselor, etc.

Proctors will have the following responsibilities:

- Ensure that all final examination materials are kept secure and confidential.
- Ensure that the student completes the examination without any outside assistance of any kind other than the course textbook, notes and other study materials.
- Verify the student's identification based on a government-issued photo ID. Proctors will need to verify the student's name and date of birth.
- Sign the final examination answer sheet (unsigned answer sheets will not be graded).
- Return the signed and completed answer sheet to California Coast University for grading and evaluation via the student portal, mail, or fax.

Submitting Your Final Examination

Submitting Final Examinations via the Internet

For online submissions, once you have logged into the student portal, click on *My Academic Plan*, select the course you are working on, and then click *Take Exam* to complete the final examination. Your proctor must input the unique password he/she was sent in order to unlock your final examination questions. Remember to keep a copy of your answers for your own personal records.

Submitting Final Examinations by Mail or Fax

Mail your completed and **signed** final examination answer sheet to:

California Coast University
Testing Department
925 N. Spurgeon Street
Santa Ana, CA 92701

Final examination answer sheets can also be faxed to the Grading Department at (714) 547-1451. Please do not resize your fax.

Your Overall Grade Point Average (G.P.A.)

In addition to receiving a passing grade for each course, all undergraduate students must maintain a required overall G.P.A. of 2.0 (C) on a 4.0 scale in order to graduate.

A = 4 grade points
B = 3 grade points
C = 2 grade points
D = 1 grade point
F = 0 grade points

Students who do not meet the overall G.P.A. requirement by the end of their program must pay the current cost of tuition to repeat courses until they improve their overall G.P.A.

Be sure to keep a copy of all work you submit to the university.

If you have any questions about how to proceed through the course or regarding any California Coast University policies and procedures, the easiest way to get help is to send us a message through the student portal, via email, or phone the university.

University office hours are Monday through Friday from 8:00 a.m. to 4:30 p.m., Pacific Standard Time.

California Coast University

925 N. Spurgeon Street, Santa Ana, California 92701

Phone: (714) 547-9625 Fax: (714) 547-5777

Test Answer Sheet Fax Line: (714) 547-1451

Email: testing@calcoast.edu

Don't forget: You are not alone! We are here to help you achieve your dream!



Learning Objectives

The learning objectives for this course are listed below:

Chapter 1: A History of Homeland Security

1. Examine the context of 9/11 from a historical perspective.
2. Analyze how domestic security has developed in the 20th century.
3. Assess the concepts of civil defense, emergency management, and homeland security, and how they are similar/different.

Chapter 2: Homeland Security Defined

1. Understand that there is no commonly accepted definition of homeland security and why that is the case.
2. Analyze common themes of homeland security as found through the homeland security bureaucracy, concepts, strategy, mission, goals, and areas of emphasis.
3. Consider the importance of having an acceptably shared definition of homeland security.

Chapter 3: Modern Terrorism and Natural Disasters

1. Understand the definitional issues surrounding the study of terrorism and why they are relevant.
2. Examine the components of terrorism and what differentiates it from regular crime.
3. Consider the relationship between terrorism and natural disasters as they relate to homeland security.

Chapter 4: The Development of Homeland Security

1. Understand that the Department of Homeland Security was initially conceived of as the Office of Homeland Security within the White House/Executive branch.
2. Examine the passage of the USA PATRIOT Act and the myriad laws it contained.
3. Comprehend that the Homeland Security Act established the Department of Homeland Security.
4. Analyze the role of Homeland Security Presidential Directives in the implementation of homeland security in America.

Chapter 5: The Department of Homeland Security

1. Understand the overview of the Department of Homeland Security.
2. Analyze the organizational structure of DHS.
3. Assess the missions and goals of DHS.

Chapter 6: Homeland Security Community

1. Examine the agencies responsible for homeland security in the U.S. including the intelligence, defense, and security communities.
2. Analyze the role of coordination in the intelligence community as it relates to homeland security.
3. Assess how the intelligence and security communities interact with the criminal justice system.

Chapter 7: Anti-terrorism and Counter-terrorism

1. Compare the differences between counter-terrorism and anti-terrorism and how those differences impact efforts towards achieving homeland security.
2. Identify the areas defined as “critical” in our nation’s infrastructure and describe why critical infrastructure protection is so important to homeland security.
3. Analyze the nine roles in the context of critical infrastructure and key resource protection and who is involved in those roles.
4. Assess the differences and similarities in the counterterrorism approaches from pre- and post-9/11, and between different presidential administrations.

Chapter 8: The National Strategy for Homeland Security

1. Examine the documents that define the government’s responses to emergencies that occur in the U.S.
2. Compare the National Strategy for Homeland Security and the National Response Plan.
3. Comprehend the evolution of the National Strategy for Homeland Security.
4. Analyze the roles of the federal, state, local, and tribal governments when an emergency occurs.

Chapter 9: Homeland Security Threats

1. Examine the different types of threats (chemical, biological, radiological, nuclear, and explosives) facing the U.S.
2. Analyze the effects of these types of weapons on humans.

Chapter 10: The Homeland Security Cycle

1. Examine the elements of the homeland security cycle and why they are important to homeland security.
2. Analyze the role of federal, state, local, and tribal governments in the homeland security cycle.

Chapter 11: National Incident Management System and Incident Command System

1. Examine the overall concept of the National Incident Management System (NIMS).
2. Analyze the five components of NIMS and their purpose.
3. Assess the overall concept of Incident Command System (ICS).
4. Recognize the 14 proven management characteristics of ICS.
5. Identify the members of the command and general staffs in ICS.

Chapter 12: Political Responses to Homeland Security

1. Examine the presidential responses to terrorism.
2. Assess the legislation passed by Congress to deter terrorism or help the country respond to an emergency event, such as terrorism or a natural disaster.

Chapter 13: Legal Responses to Homeland Security

1. Examine the balance between civil rights and the need to collect intelligence.
2. Analyze the objections civil rights advocates have about the USA PATRIOT Act.
3. Assess the Supreme Court's reactions to U.S. policies toward detainees.

Chapter 14: Homeland Security Communications and Technology Issues

1. Examine the role of communications and communications technology in homeland security and identify some of the major programs dealing with homeland security communications.
2. Identify different types of cyber threats and attacks, and understand the importance of cyber-terrorism in homeland security.
3. Analyze the role of technology in the context of homeland security, both as a benefit to homeland security professionals as well as a potential threat to homeland security.

Chapter 15: Domain Security and the Future of Homeland Security

1. Examine the importance of domain security, particularly airline security, port security, and border security.
2. Analyze the role TSA plays in airline security and its additional oversight responsibilities in reference to other elements of domain security.
3. Identify the roles of the U.S. Border Patrol and Immigration and Customs Enforcement in terms of border security.
4. Assess the challenges faced by homeland security in the future.

Resources and Learning Activities

Learning extends beyond the textbook, exams, and writing assignments. To help you find out more about the course you are completing, we have developed some learning activities and course resources that will accompany each course. Our intention is to encourage you to explore new ideas and concepts. You will find these located in your student portal.

We suggest you spend about 5 hours per Unit exploring and engaging in the learning activities and the course resources listed on the student portal. As we will be adding new material on a regular basis, we encourage you to check back frequently.

To give you an idea, here are some of the types of resources we've included in the student portal:

- Learning activities to help you explore the subject in some different ways.
- Suggested Readings.
- Websites related to your course.
- Professional organizations you might investigate.
- Videos to watch.

Lastly, education goes beyond just courses and degree programs. Hopefully, as a student, you are consistently learning and expanding your knowledge with education that transcends what you learn at the University.

To expand awareness and appreciation for the larger scope of education, we have included resources on the following:

- Critical Thinking
- Ethical Reasoning
- Social Responsibility
- Global Citizenship
- Civic Engagement
- Lifelong Learning

We wish you success on your educational journey!

Unit One

Chapter 1: A History of Homeland Security	1
Chapter 2: Homeland Security Defined	10
Chapter 3: Modern Terrorism and Natural Disasters	20
Unit 1 Examination Instructions	30
Unit 1 Examination	31
Unit 1 Writing Assignment	36

Unit Two

Chapter 4: The Development of Homeland Security	38
Chapter 5: The Department of Homeland Security	47
Chapter 6: Homeland Security Community	56
Chapter 7: Anti-terrorism and Counter-terrorism	65
Unit 2 Examination Instructions	74
Unit 2 Examination	75
Unit 2 Writing Assignment	80

Unit Three

Chapter 8: The National Strategy for Homeland Security	82
Chapter 9: Homeland Security Threats	91
Chapter 10: The Homeland Security Cycle	100
Chapter 11: National Incident Management System and Incident Command System	109
Unit 3 Examination Instructions	118
Unit 3 Examination	119
Unit 3 Writing Assignment	124

Unit Four

Chapter 12: Political Responses to Homeland Security	126
Chapter 13: Legal Responses to Homeland Security	135
Chapter 14: Homeland Security Communications and Technology Issues. .	145
Chapter 15: Domain Security and the Future of Homeland Security	154
Unit 4 Examination Instructions	163
Unit 4 Examination	164
Unit 4 Writing Assignment	169
Final Examination Instructions	171
Final Exam Scheduling Form	172

Chapter One

A History of Homeland Security

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the context of 9/11 from a historical perspective.
2. Analyze how domestic security has developed in the 20th century.
3. Assess the concepts of civil defense, emergency management and homeland security, and how they are similar and different.

Instructions to Students

- Read pages 1 - 18 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



On February 22, 1974, Samuel Byck hijacked a plane, on the ground, at Baltimore-Washington International. His intent was to fly the plane into the White House, killing President Richard Nixon. The incident resulted in a shootout and, ultimately, Byck's death before the plane could take off. The intent of the hijacking was kept from the public until 1987. However, the warning signs were there: an airplane could be hijacked and used as a missile. On September 11, 2001, several planes were used for just such a purpose. In the aftermath of 9/11, many, including high-ranking government officials, lamented that they never thought something like that could happen—that a group of civilians could commandeer a commercial aircraft and use it as a guided missile for terrorist purposes.

Homeland security has gone through many stages during the history of the United States. Early on, states were responsible for managing disasters with constraints placed on federal efforts. This viewpoint began to change with the onset of two World Wars when the federal government embraced a cooperative, albeit limited, response in the name of civil defense. By the time of FEMA, civil defense evolved into emergency management, and later a dual response policy for responding to natural and man-made disasters. Historically, ideas for U.S. policy towards homeland security have been discussed prior to the occurrence of disasters, but have generally only been made official policy post-disaster.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Homeland security:

Civil defense:

Emergency management:

Domestic security in the United States dates back well before 9/11, and long before the term, “Homeland Security” came into common use. Efforts included the protection of American settlers, response to natural disasters, civil defense during WWI and WWII, and threats from the Cold War. While the right of the federal government to defend the country from foreign threats was commonly accepted, how to handle domestic threats was in dispute. Shay’s rebellion exposed such a weakness, at a time when the U.S. was developing its constitution. Article 4 of the Constitution guaranteed states the federal government’s protection from invasion. This came into play successfully during the Whiskey Rebellion where the federal government’s role in national disasters was still unclear.

A few bills were passed in Congress during the 19th century providing funds for disaster victims, though these were exceptions. The extent of the military’s role in domestic peacekeeping was also in dispute until the passage of Ex Parte Milligan (1866) and the Posse Comitatus Act (1878). The federal government’s role in national disasters was further clarified after the American Red Cross response to the Johnstown Floods (1889) and the 1906 San Francisco Earthquake. Later chartered by the U.S., the Red Cross serves as the primary relief agency in such events, while the military is tasked with peacekeeping.

In the short time from the end of WWII to the beginning of the Cold War, civil defense was a low priority. Civil defense was considered a local issue. In response to Soviet threats in 1947, Congress passed the National Security Act, which created the Central Intelligence Agency (CIA); created the National Security Resources Board (NSRB); developed a plan for mobilizing civilian and military resources for response to war, specifically a nuclear attack; and restructured the Department of Defense to include the Office of Civil Defense Planning.

In 1950, Congress passed the Federal Civil Defense Act, which placed most civil defense efforts on states; created the Federal Civil Defense Administration (FCDA) to guide state efforts; and lead to shelter building, attack warning systems, and public education efforts. During the Eisenhower administration, funding of federal civil defense efforts and the FDCA was reduced, and more emphasis placed on local governments. The FDCA later became the Office of Civil Defense and Mobilization. In a renewed focus on federal civil defense, JFK divided the Office of Civil Defense and Mobilization into The Office of Emergency Planning (OEP) and the Office of Civil Defense (OCD) in 1961. The OEP advised the President on policy for nonmilitary emergency preparedness, while the OCD oversaw the nation’s civil defense program. Later, during the Johnson administration, civil defense funding and efforts dwindled due to “Great Society” programs and the Vietnam War. During the Nixon administration, several new agencies arose, and civil defense and emergency response tasks were spread across many existing government agencies which lead to a lack of centralized coordination and wasteful spending.

In 1979, President Carter created the Federal Emergency Management Agency (FEMA), to manage all federal civil defense spending and emergency response, focusing on non-man-made events. President Reagan expanded FEMA’s reach to include both natural disasters and homeland attacks. During the George H.W. Bush administration, in response to poor federal performance during several disasters, FEMA developed the Federal Response Plan (FRP), which coordinated the disaster response efforts of federal agencies and the Red Cross. President Bill Clinton appointed James Lee Witt as Director of FEMA, who created three internal directors corresponding to the major phases of emergency management: mitigation, preparedness, and response and recovery. Later in the Clinton administration, and early in the George W. Bush administration, ideas were floated to create centers to analyze all intelligence related to domestic threats. These ideas were never legislated until after the 9/11 attacks.

Multiple Choice Questions (Circle the correct answer)

1. Samuel Byck had intended to assassinate which President when he hijacked a Delta airplane?
 - a. Lyndon Johnson
 - b. Jimmy Carter
 - c. Richard Nixon
 - d. Ronald Reagan

2. What was the significance of Shays's Rebellion in regards to national security?
 - a. It showed the large expenses associated with national security.
 - b. It showed the need for a federal mechanism to handle disturbances.
 - c. It spurred the development of the Central Intelligence Agency.
 - d. It promoted states' rights.

3. Shays's Rebellion took place in which state?
 - a. Massachusetts
 - b. New York
 - c. Connecticut
 - d. Rhode Island

4. Which Article of the United States Constitution guarantees states' protection from invasion?
 - a. Article 1
 - b. Article 4
 - c. Article 5
 - d. Article 2

5. In what year was the Whiskey Rebellion put down by the U.S. Military?
 - a. 1787
 - b. 1798
 - c. 1802
 - d. 1794

6. Which of the following dealt with the suspension of habeas corpus during the Civil War?
 - a. Posse Comitatus Act
 - b. Presidio Act
 - c. Ex Parte Milligan
 - d. none of the above

7. The term “Homeland Security,” was first mentioned in the U.S. Constitution.
 - a. true
 - b. false

8. The U.S. Constitution contains a clause that guarantees federal resources for natural disaster recovery assistance to the states.
 - a. true
 - b. false

Key Term Definitions

Homeland security: A department within the Federal Government focused on prevention, mitigation, and responding to and recovering from both natural and man-made disasters.

Civil defense: An effort to protect the citizens of the United States from a military attack.

Emergency management: The preparation for and the carrying out of all emergency functions, other than functions for which military forces are primarily responsible.

Answers to Self Test

1. c
2. b
3. a
4. b
5. d
6. c
7. b
8. b

Chapter Two

Homeland Security Defined

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Understand that there is no commonly accepted definition of homeland security and why that is the case.
2. Analyze common themes of homeland security as found through the homeland security bureaucracy, concepts, strategy, mission, goals, and areas of emphasis.
3. Consider the importance of having an acceptably shared definition of homeland security.

Instructions to Students

- Read pages 19 - 39 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



The term “Homeland Security” entered the American lexicon after the events of September 11, 2001. After the creation of the Department of Homeland Security, those involved at all levels of government have attempted to define what the term encompasses. Definitions have greatly varied for many reasons and have evolved from the civil defense era early in the 20th century to the environment after 9/11. As of today, while there does not yet appear to be consensus on a homeland security definition, several common themes have surfaced. In this chapter we will analyze the common themes of homeland security as found through the homeland security bureaucracy, concepts, strategy, mission, goals, and areas of emphasis.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Homeland security goals:

Homeland security bureaucracy:

Homeland security enterprise:

Homeland security concepts:

Homeland security mission:

In 1993, Pakistani National Aimal Kasi used an AK-47 to shoot at cars stuck in a typical commute traffic jam trying to enter the CIA headquarters in Northern Virginia. He shot a total of five people, killing two. After the shooting, he fled the scene, hid in a park, and avoided law enforcement. Kasi was added to the FBI's Most Wanted Fugitives list. It was later discovered he had returned to Pakistan the day after the shooting, where a four-year search led to his capture and smuggling back into the United States. He was put on trial, found guilty of murder, and was executed in 2002.

The Kasi case was treated, in a sense, as a domestic local law enforcement issue for trial purposes. However, local law enforcement, the FBI, and the CIA had worked together to solve the case and apprehend Kasi. Kasi had appeared to act alone, and had no known associations with terror organizations, making it unclear whether the act could be considered terrorism, even though he hailed from a country where terrorist activity and anti-U.S. sentiment was prevalent. The 1993 World Trade Center bombing was carried out by terrorist organization, Al Qaeda, yet it was treated as more of a crime than terrorism. Two years later, the Oklahoma City bombing was considered terrorism, though an act of domestic terrorism rather than international. The attacks of 9/11, however, brought the concept of terrorism to the forefront of the minds of most Americans. This attack also introduced the concept of homeland security to most people, though the definition is multi-faceted—even to this day.

There is generally no accepted definition of the term, "Homeland Security." The concept of civil defense and homeland security has been ever-evolving. Civil defense arose out of fears during World War II. During the war, responsibility was still with the states, though they were guided by federal coordination. After 9/11, there was an emphasis on a wide-ranging government response in which emergency preparedness and response – FEMA's role – was only one part. The Department of Homeland Security was created for the purpose of civil defense, and FEMA's operations were brought under this umbrella. The true nature of civil defense and – today, homeland security – has by and large been a response to cataclysmic events in the United States, and an evolving bureaucratic organization in charge of this response.

The Hart-Rudman Task Force on Homeland Security recommended a new National Homeland Security Agency to consolidate and refine the missions of dozens of related agencies and departments. Such a recommendation was put into a bill that stalled in congressional committee in March, 2001. These efforts made by federal policy makers were meant to prevent, or plan a response to, future attacks, and were not a bureaucratic policy response to an actual, specific attack or natural disaster. The primary issue with acting on the Hart-Rudman Task Force's recommendations was public support—something that was not an issue after the events of September 11, 2001. Several post-9/11 strategic documents have attempted to define the term, "Homeland Security," including The 2003 National Strategy for Homeland Security (revised in 2007). These documents specifically addressed terrorism as part of homeland security. The "2008 Strategic Plan—One Team, One Mission, Securing Our Homeland" document referenced all-hazards (i.e. hurricanes), and border security, in addition to terrorism. These previous documents were superseded by several others, including the 2010 National Security Strategy.

Currently, at the national level, there does not appear to be a true attempt to align definitions and missions among the various federal entities. DHS is attempting to do so without prioritizing the missions. This can lead to gaps in funding for specific priorities. Still, a single homeland security definition currently does not exist. Congress may take up the task of assigning specific definitions and missions. The administration could also identify homeland security priorities and missions. Arguments continue as to whether homeland security is about simply the coordination of disparate stakeholders, or—also—about the strategic processes policymakers use in determining and prioritizing risks, stakeholders and their missions. Without a general consensus, many believe there will continue to be disjointed and disparate approaches to securing the nation. To achieve this end, efforts should be made to create a consensus definition of homeland security, followed by an accepted list of prioritized missions that are regularly evaluated.

Multiple Choice Questions (Circle the correct answer)

1. What agency was shooter Aimal Kasi's target in his 1993 attack?
 - a. FBI
 - b. CIA
 - c. NSA
 - d. FEMA

2. Which agencies partnered to capture and bring Aimal Kasi to justice?
 - a. CIA & FBI
 - b. CIA & NSA
 - c. FEMA & FBI
 - d. all of the above

3. How many terrorist organizations provided training and support for Aimal Kasi?
 - a. two
 - b. one
 - c. none
 - d. three

4. FEMA reports to what organization/agency?
 - a. CIA
 - b. FBI
 - c. Department of Emergency Services
 - d. Department of Homeland Security

5. What event caused the Department of Homeland Security to focus on natural disasters, as well as terrorism?
 - a. Hurricane Irene
 - b. Hurricane Sandy
 - c. Hurricane Katrina
 - d. Hurricane Beth

6. Which definition of "Homeland Security" is best described as an historical evolution that is created in the wake of the various cataclysmic events?
 - a. bureaucracy evolution
 - b. mission and goals
 - c. concept evolution
 - d. areas of emphasis

7. The 1993 attack on the World Trade Center was largely viewed as a terrorist attack, rather than a crime.
 - a. true
 - b. false

8. The term “homeland security” largely became popular in government circles shortly after the start of WWII.
 - a. true
 - b. false

Key Term Definitions

Homeland security goals: Those key tasks that must be accomplished in order for the homeland security mission to be accomplished.

Homeland security bureaucracy: The various federal, state, and local agencies that are directly or indirectly involved in the protection of America's homeland.

Homeland security enterprise: The collective efforts and shared responsibilities of federal, state, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities.

Homeland security concepts: Fundamental aspects of homeland security that are common to all responses whether they are natural disasters or terrorist attacks, such as preparedness.

Homeland security mission: Those key items that must be achieved in order for the homeland to be secure and the homeland security strategy implemented.

Answers to Self Test

1. b
2. a
3. c
4. d
5. c
6. a
7. b
8. b

Chapter Three

Modern Terrorism and Natural Disasters

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Understand the definitional issues surrounding the study of terrorism and why they are relevant.
2. Examine the components of terrorism and what differentiates it from regular crime.
3. Consider the relationship between terrorism and natural disasters as they relate to homeland security.

Instructions to Students

- Read pages 41 - 65 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



In this chapter, we will review the relationship between terrorism and natural disasters as they relate to homeland security. The 9/11 attacks, one of the seminal events of the early 21st century, brought about the modern change in United States homeland security. The attacks devastated the country through fear, as is typically the motivating force of terrorism. Despite the familiarity with terrorism, there is, essentially, no agreed-upon definition of the term, “terrorism.” There are, however, many consistent elements of terrorism that are commonly referenced.

Like terrorist attacks, natural disasters can be physically and emotionally devastating. Unlike terrorist attacks, natural disasters occur far more frequently each year. Both terrorist attacks and natural disasters require responses from every level of government. Homeland security’s migration to an “all-hazards” approach should promote closer ties across these types of events.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Domestic terrorism:

Hazard:

International terrorism:

Natural disaster:

Risk:

Strategy:

Terrorism:

Terrorism is not a new phenomenon, taking place as early as 32 A.D. Terrorism is not always perpetrated due to religious reasons, despite the emphasis today because of groups such as Al Qaeda. Due to wide-ranging motivations for terrorism, creating one, clear-cut definition has been difficult. Acts that could be classified as terrorism date back to the first century, with religious attacks by the Zealots. Religious terrorism is the oldest type of terrorism. State terrorism is fundamentally different from eras either before or after. It is typically carried out by nation-states, with a unified culture or belief system, or by those political entities in control of a country. The Reign of Terror during the French Revolution is an example of a nation-state carrying out acts of terror to control its population. WWII dictators such as Hitler, Mussolini, and Stalin are other examples. These acts show the political nature of terrorism.

Early political terrorism was accompanied by printed-word propaganda to specifically communicate goals and effect change. This type of terrorism was often unorganized. Some political terrorist attacks had major effects, even beyond the nation in which they were carried out. The assassination of Archduke Franz Ferdinand by Serbian nationalists was a leading factor that led to WWI. 1960s Soviet-supported terrorism, like the Red Army Faction and the Baader-Meinhoff Group, used violence for political ends. This began an era of cooperation between terrorist organizations, often trading arms for training.

A 1968 hijacking of Israeli airline El-Al by a PLO-related group is widely considered to be the first act of modern terrorism. The attack made use of wide media coverage, brought on by recently launched news satellites. The goal of the attack was also to force a negotiation with the terrorists, who had been previously ignored by Israel. Today, terrorists take credit for attacks through the media to maximize effect. The history of terrorism has progressed from a politically and religiously motivated activity, to a method of state control, to, once again, a politically and religiously motivated action.

Definitions of terrorism vary widely, depending on where the definition is generated. Some definitions are as simple as, "you know it when you see it," while others are complex explanations created by a department or committee. Even the various U.S. governmental departments have varied definitions, based along similar themes. The FBI defines it as "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives." The Department of State definition is given as "Premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents." The Department of Homeland Security has an even more wide-ranging definition, which includes both domestic and international terrorism. "Terrorism" can also spread beyond political targets to attacks on places such as animal testing labs, by animal-rights advocates. Terrorists themselves often reject being labeled as such, as they generally see themselves as "freedom fighters" or "insurgents," acting out against a larger enemy.

Despite differing definitions, there are typically five, generally agreed-upon themes that can be found to describe terrorist attacks: political (social or religious) motivation, violence or the credible threat of violence, sub-national actors, instrumental in nature, and victim/target separation. The political act/motivation is generally the key principle of terror attacks that differentiate them from general criminal acts. By and large, terrorism is a complex phenomenon with a wide variety of acts and actors.

There is a strong, ongoing disagreement among academics, and others, as to what specifically causes terrorism. There are generally two camps. One argues that certain psychological and/or sociological factors cause individuals to become terrorists. The other considers terrorism to be a choice made by those seeking to further a political or religious objective. Many theories have attempted to view terrorists through psychological or sociological lenses. Such theories look at relative deprivation of a group, poverty, type of government, or childhood trauma as reasons why people act out terror.

Attempts have been made to develop a psychological profile of a terrorist, but with little success. Most studies have shown that—psychologically, at least—known terrorists are very much like any other member of the general population. There has been successful research done on the psychology of terrorism itself, in addition to the psychology of not only the perpetrator, but also of the victims.

The U.S. is exposed to natural disaster threats on a regular basis. As in responses to terrorism, government agencies can help mitigate the threat of natural disasters, and aid significantly in recovery efforts. Natural hazards occur more frequently than terrorist attacks, and also cause more deaths and property damage. Varying types of disasters occur in various locations in the United States with varying frequencies. Floods are one of the most wide-ranging, and most-frequent types of disasters in the U.S. Others, such as tsunamis, are rare, but must still be accounted for when developing response plans. Compounding disasters should also be accounted for, as one – such as an earthquake – can lead to others, such as fires, floods, or even threats to nuclear power plants, as seen in Japan. While disaster preparation and emergency management has improved throughout the history of the U.S., natural disasters continue to affect both property and life.

Multiple Choice Questions (Circle the correct answer)

1. On what continent were two U.S. embassies attacked by terrorists in 1998?
 - a. North America
 - b. Europe
 - c. Africa
 - d. South America

2. What terrorist group was responsible for the Oklahoma City bombing?
 - a. Al Qaeda
 - b. domestic terrorists
 - c. international terrorists
 - d. Islamic Jihad

3. Terrorists are almost always motivated by what?
 - a. religion
 - b. socio-political objectives
 - c. single-issues
 - d. all of the above

4. Terrorism dates back to roughly what time period?
 - a. very early A.D.
 - b. medieval times
 - c. 1700s
 - d. 1900s

5. The assassination of Archduke Franz Ferdinand partially lead to what event?
 - a. WWII
 - b. WWI
 - c. Spanish-American War
 - d. none of the above

6. The Baader-Meinhoff Group and Palestinian Liberation Organization, together, were among the first terrorist groups to do what?
 - a. Use weapons of mass destruction.
 - b. Cooperate with each other for training, arms.
 - c. Hijack airplanes.
 - d. Use car bombs.

7. The U.S.'s strong response with cruise missiles to the 1998 terror bombing successfully deterred international terrorists for more than a decade.
 - a. true
 - b. false

8. Terrorist attacks occur about as often as natural disasters in the United States.
 - a. true
 - b. false

Key Term Definitions

Domestic terrorism: The use of violence and intimidation in the pursuit of political aims committed by those from within one's own state/country.

Hazard: A danger or risk.

International terrorism: The use of violence and intimidation in the pursuit of political aims committed by those from outside of one's own state/country.

Natural disaster: An event that occurs in nature, not caused by humans, that affects the environment and results in financial and/or human loss.

Risk: The possibility of loss or injury.

Strategy: A plan of action or policy designed to achieve a major overall goal.

Terrorism: The use of violence and intimidation in the pursuit of political aims.

Answers to Self Test

1. c
2. b
3. d
4. a
5. b
6. b
7. b
8. b

The Unit Examination

The unit examination contains 25 multiple choice questions, as well as a writing assignment.

Your grade on the examination will be determined by the percentage of correct answers. The university utilizes the following grading system:

A = 90% – 100% correct	4 grade points
B = 80% – 89% correct	3 grade points
C = 70% – 79% correct	2 grade points
D = 60% – 69% correct	1 grade point
F = 59% and below correct	0 grade points

Completing Unit One Examination

Before beginning your examination, we recommend that you thoroughly review the textbook chapters and other materials covered in each unit and follow the suggestions in the *Mastering the Course Content* section of the syllabus.

This unit examination consists of objective test questions as well as a comprehensive writing assignment selected to reflect the learning objectives identified in each chapter covered so far in your textbook.

Additional detailed information on completing the examination, writing standards and how to submit your completed examination may be found in the syllabus for this course.

Multiple Choice Questions (Enter your answers on the enclosed answer sheet)

1. In what year did Pancho Villa and his Villistas attack the United States in New Mexico?
 - a. 1916
 - b. 1902
 - c. 1914
 - d. 1924

2. In what year was the United States Border Patrol established?
 - a. 1914
 - b. 1924
 - c. 1917
 - d. 1912

3. Which of the following was established due to civil defense concerns during World War I?
 - a. Office of Emergency Planning
 - b. National Defense Council
 - c. Defense Advisory Committee
 - d. Office of Civil Defense

4. Former New York Mayor Fiorello La Guardia was named the director of which organization?
 - a. Office for Emergency Management
 - b. National Defense Council
 - c. New York Defense Authority
 - d. Office of Civilian Defense

5. Efforts for civil defense during WWII included which of the following?
 - a. creation of civil defense plans
 - b. air raid drills
 - c. sand bag stockpiling
 - d. all of the above

6. In addition to creating the CIA, which other organization was created by the National Security Act of 1947?
 - a. National Security Resources Board (NSRB)
 - b. Office of Civil Defense Planning
 - c. Department of Defense
 - d. all of the above

7. What was the primary recommendation of the 1950 plan known as the Blue Book?
 - a. massive funding for civil defense
 - b. creation of one agency to deal with coordinating America's civil defense
 - c. creation of a National Security Agency
 - d. creation of a Presidential commission on civil defense

8. Which 20th century President requested less funding for civil defense, and sought to stress the "civil" in "civil defense?"
 - a. John F. Kennedy
 - b. Harry Truman
 - c. Richard Nixon
 - d. Dwight Eisenhower

9. Which definition of "Homeland Security" is best described as being developed in the decade prior to 9/11?
 - a. mission and goals
 - b. concept evolution
 - c. bureaucracy evolution
 - d. areas of emphasis

10. According to several government documents published since 2003, what is the definition, or theme, of homeland security?
 - a. encompasses coordination of federal, state, and local authorities
 - b. involves securing against, responding to both hazard-specific and all-hazards threats
 - c. activities do not imply total protection or complete threat reduction
 - d. all of the above

11. Which definition of "Homeland Security" is best described as security stakeholders identifying and executing varied strategic efforts?
 - a. bureaucracy evolution
 - b. mission and goals
 - c. concept evolution
 - d. areas of emphasis

12. According to Naval Postgraduate School Instructor Christopher Bellavita, which of the following is not an area of homeland security focus?
- a. Security Über Alles
 - b. Meta Hazards
 - c. Military build-up
 - d. Jurisdictional Hazards
13. What is meant by “Security Über Alles”?
- a. protection of one’s allies
 - b. security above all
 - c. overall security
 - d. protection of civil liberties
14. Threats affecting the American way of life could be described as?
- a. meta hazards
 - b. national security
 - c. terrorism and catastrophes
 - d. jurisdictional hazards
15. Which document describes homeland security as a unified, national effort to prevent and deter terrorist attacks, protect and respond to hazards, and secure borders?
- a. 2007 National Strategy for Homeland Security
 - b. 2010 National Security Strategy
 - c. 2008 U.S. Department of Homeland Security Strategic Plan
 - d. 2010 Quadrennial Homeland Security Review
16. Which document describes homeland security as an effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards?
- a. 2012 Strategic Plan
 - b. 2007 National Strategy for Homeland Security
 - c. 2011 National Strategy for Counterterrorism
 - d. 2010 National Security Strategy

17. Which event is considered to be the first occurrence of modern international terrorism?
- a. the events of September 11, 2001
 - b. the 1993 World Trade Center attacks
 - c. the assassination of Archduke Franz Ferdinand
 - d. the hijacking of an Israeli El-Al airplane
18. Which of the following has made combating modern terrorism more difficult?
- a. communication technologies
 - b. financial networks
 - c. wide availability of information for creating weapons
 - d. all of the above
19. The creation of the Department of Homeland Security was a direct response to which event?
- a. bombings in Kenya and Tanzania
 - b. 1993 World Trade Center bombing
 - c. 9/11
 - d. the Oklahoma City bombing
20. What airline did a PLO-related group hijack in 1968?
- a. Delta
 - b. Air Pakistan
 - c. El-Al
 - d. British Airways
21. In what country was a U.S. Marine Corps barracks attacked by a truck bomb in 1982?
- a. Lebanon
 - b. Iraq
 - c. Iran
 - d. West Germany
22. In regards to the U.S., threats such as militia extremism, anarchist extremism, eco-terrorism, and animal rights terrorism are examples of what?
- a. small-scale threats
 - b. low-priority threats
 - c. domestic terrorism
 - d. international terrorism

23. Earthquakes, tornadoes, hurricanes, wildfires, floods, and lighting strikes fall into which of the following categories?
- a. risks
 - b. hazards
 - c. threats
 - d. all of the above
24. In 2011, a typical year for natural disasters, approximately how many declared disasters occurred?
- a. 9
 - b. 37
 - c. 80
 - d. 100
25. Psychologically speaking, according to studies, how do known terrorists compare with people from the general population?
- a. They are both similar.
 - b. Terrorists are more mentally unstable.
 - c. Terrorists often suffer from mental illness.
 - d. Terrorists become more susceptible to mental issues over time.

Writing Assignment for Unit One

- Include your **name, student number, course number, course title and unit number** with your writing assignment.
- Begin each writing assignment by identifying the question number you are answering followed by the actual question itself (in bold type).
- Use a standard essay format for responses to all questions (i.e., an introduction, middle paragraphs and conclusion).
- Responses must be typed double-spaced, using a standard font (i.e. Times New Roman) and 12 point type size.

Word count is NOT one of the criteria that is used in assigning points to writing assignments. However, students who are successful in earning the maximum number of points tend to submit writing assignments that fall in the following ranges:

Undergraduate courses: 350 - 500 words per question.

Graduate courses: 500 - 750 words per question.

Doctoral courses: 750 - 1000 words per question.

Plagiarism

All work must be free of any form of plagiarism. **Put written answers into your own words.** Do not simply cut and paste your answers from the Internet and do not copy your answers from the textbook. Be sure to refer to the course syllabus for more details on plagiarism and proper citation styles.

Please answer **ONE** of the following:

1. What is emergency management, how did it develop, and how is it different from civil defense?
2. Trace the origins of the term, "homeland security" and articulate how that has affected the bureaucratic perspective in defining this term. How are civil defense and emergency management related?
3. Compare and contrast the psychological explanations for terrorism to strategic explanations of terrorism. Which approach is more effective in explaining terrorism and why?

You have just completed Unit 1 of this course.

You are off to a great start!

Keep up the good work!



Chapter Four

The Development of Homeland Security

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Understand that the Department of Homeland Security was initially conceived of as the Office of Homeland Security within the White House/Executive branch.
2. Examine the passage of the USA PATRIOT Act and the myriad of laws it contained.
3. Comprehend that the Homeland Security Act established the Department of Homeland Security.
4. Analyze the role of Homeland Security Presidential Directives in the implementation of homeland security in America.

Instructions to Students

- Read pages 67 - 87 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



The terrorist attacks on September 11, 2001 called for an American response both overseas and domestically. Shortly after, the President created the Office of Homeland Security in the White House, and issued executive orders and Homeland Security Presidential Directives. The U.S. Congress passed the USA PATRIOT Act of 2001 and the Homeland Security Act of 2002, which created the Department of Homeland Security. Once the new Secretary of Homeland Security, Tom Ridge, was confirmed, the new department came into existence and began consolidating all of the agencies and agency components that made up the new department. This represented the largest organizational shift in federal bureaucracy since World War II.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Department of Homeland Security:

Homeland Security Presidential Directives:

Office of Homeland Security:

USA PATRIOT Act:

President George W. Bush was visiting a class of children at Emma Booker Elementary School in Sarasota, FL when the planes hit the Twin Towers during the attacks on September 11th, 2001. When he was told that a second plane had hit the second tower and that the country was under attack, he remained calm and stayed in the classroom for several minutes, rather than have the country see a panicked reaction in a moment of crisis. Soon after, the President spoke to several advisors, and, once they learned about the attack on the Pentagon, the Secret Service decided returning him to Washington would be unwise for the time being. When Air Force One took off at 9:54 a.m., it did not have any fixed destination. During this time, Vice President Cheney was moved to a shelter conference room within the White House. After some discussion, President Bush was taken to Barksdale Air Force Base in Louisiana, where he addressed the nation through a recorded message, for security reasons. The President next flew to Offutt Air Force Base in Nebraska, where he arrived in early afternoon. The idea was to take advantage of the base's elaborate command and control facilities, and large lodging arrangements. Later that afternoon, the President overruled his advisors and returned to Washington, where he addressed the nation at 8:30 p.m. that evening.

After visiting sites attacked on 9/11, including most memorably when he toured the remains of the World Trade Center site in New York City, President Bush returned to Washington to develop both proper military and domestic responses to the attacks. During a speech to Congress, the President announced the creation of the Office of Homeland Security, with former Pennsylvania Governor Tom Ridge named as the office's first director. An executive order on October 8, 2001 officially created the Office of Homeland Security, as well as the Homeland Security Council. This was the start of what became the largest major bureaucratic restructuring of the federal government since WWII.

Shortly after the attacks of 9/11, Congress became busy passing bills related to combating terrorism – some of which were held up from passing prior to the attacks. The depth and gravity of the attacks provided an environment of strong public support for anti-terrorism laws, and the wherewithal for Congress to follow through. Many of the bills discussed and passed walked a fine line in the debate of security vs. privacy. Several Democrats and the American Civil Liberties Union were concerned that these bills would infringe on the Constitutional rights of Americans, particularly the Fourth Amendment rights against unreasonable searches and seizures. Many Republicans and think-tanks were more focused on the anti-terrorism legislation, and were concerned that – without such laws – federal law enforcement would remain at a disadvantage in investigating terror threats. Many proposals that had been previously debated came together under one bill known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 – the USA PATRIOT Act. The Act was easily passed in the House of Representatives on Oct. 24, 2001, and passed just as easily in the Senate the next day. It became law on October 26, 2001 with the signature of President Bush. The Patriot Act was comprehensive and sweeping in scope. Much of the bill's provisions were set to expire on December 31, 2005.

Multiple Choice Questions (Circle the correct answer)

1. At what point was President George W. Bush informed about the attacks on 9/11?
 - a. when a plane hit the Pentagon
 - b. when the second plane hit the second World Trade Center tower
 - c. when the first plane hit the first World Trade Center tower
 - d. when an unresponsive plane was headed towards Washington, D.C.

2. The creation of the Office of Homeland Security, passage of the USA PATRIOT Act, and the creation of the Department of Homeland Security happened within roughly what period of time?
 - a. six years
 - b. two years
 - c. fourteen months
 - d. three years

3. Where was President George W. Bush flown shortly after he learned of the 9/11 attacks?
 - a. Barksdale Air Force Base
 - b. Andrews Air Force Base
 - c. Offutt Air Force Base
 - d. JFK Airport

4. Who was the first director of the Office of Homeland Security?
 - a. Tom Ridge
 - b. Colin Powell
 - c. Condoleezza Rice
 - d. Norman Minetta

5. What position did Dr. Condoleezza Rice hold at the time of the attacks of 9/11?
 - a. FBI Director
 - b. CIA Director
 - c. National Security Advisor
 - d. Chief of Staff

6. The Homeland Security Act was signed into law during what year?
 - a. 2000
 - b. 2003
 - c. 2001
 - d. 2002

7. President George W. Bush created the Department of Homeland Security through executive order.
 - a. true
 - b. false

8. The USA PATRIOT Act was passed by Congress and signed into law by President George W. Bush.
 - a. true
 - b. false

Key Term Definitions

Department of Homeland Security: A federal cabinet-level agency created in 2002 by taking various pre-existing agencies and placing them under one federal bureaucracy charged with protecting America's homeland.

Homeland Security Presidential Directives: Presidential Executive Orders that are focused on Homeland Security and advise the federal bureaucracy on administrative requirements the President wants implemented.

Office of Homeland Security: The office inside of the White House (Executive Branch) led by former Governor Tom Ridge, charged with securing the homeland, and which served as the nucleus for the Department of Homeland Security.

USA PATRIOT Act: An Act of Congress passed in 2001, six weeks after the 9/11 Terrorist Attacks that gave new tools to investigate potential terroristic threats in the United States. Commonly referred to as The Patriot Act.

Answers to Self Test

1. b
2. c
3. a
4. a
5. c
6. d
7. b
8. a

Chapter Five

The Department of Homeland Security

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Understand the overview of the Department of Homeland Security.
2. Analyze the organizational structure of DHS.
3. Assess the missions and goals of DHS.

Instructions to Students

- Read pages 89 - 106 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



The Department of Homeland Security (DHS), formed by President Bush and Congress in the days after 9/11, was developed to help protect the country from future terrorist attacks. The department reorganized and consolidated many other federal agencies, or portions of agencies, that had some previous role in homeland security. The DHS has continued to collect and analyze intelligence about terrorism to understand terrorist groups and break up any potential plots against the U.S. The DHS has also helped state and local governments prepare for any future attacks.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Federal Emergency Management Agency (FEMA):

National Terrorism Advisory System:

President George W. Bush used his executive power to establish the Office of Homeland Security about a month after the attacks of 9/11. The office was given five basic responsibilities: work with federal, state, and local agencies to prepare for a possible terrorist event; mitigate the consequences of threats and attacks; coordinate efforts between federal agents as well as other agencies to prevent terror attacks in the U.S.; protect critical infrastructure from terror attacks; and provide incident management, continuity of government, and education to people about preventing terrorism. Former Pennsylvania Governor Tom Ridge was chosen to run the new organization. Seeking a more permanent agency, Congress later created the Department of Homeland Security.

The intent of the Homeland Security Act was to organize government operations and communications devoted to national security into one organization. The law consolidated all or portions of 22 existing federal agencies and departments into the DHS. It represented the largest reorganization of the federal government since the beginning of the Cold War. The Department of Homeland Security has five major mission areas: counter-terrorism; security of U.S. borders, be they land, sea, or air; enforcement of our nation's immigration laws; protection of cyberspace; and preparation in advance for, and quick response to, any type of emergency that might occur.

Multiple Choice Questions (Circle the correct answer)

1. How long after 9/11 did it take for President George W. Bush to create the Office of Homeland Security?
 - a. one week
 - b. three months
 - c. one month
 - d. one year

2. Which of the following leaders was not part of the Homeland Security Council when originally established?
 - a. the Director of CIA
 - b. the Attorney General
 - c. the Secretary of Defense
 - d. the Secretary of Treasury

3. Once the Department of Homeland Security was established, who was its first Secretary?
 - a. Bernard Kerick
 - b. Tom Ridge
 - c. Michael Chertoff
 - d. Janet Napolitano

4. How many federal agencies, or departments, were consolidated into DHS when it was created?
 - a. 27
 - b. 22
 - c. 32
 - d. 19

5. Which of the following federal agencies was not folded into the DHS?
 - a. Federal Protective Service
 - b. Office of Domestic Preparedness
 - c. Nuclear Incident Response Team
 - d. Internal Revenue Service

6. How many divisions was the Department of Homeland organized into upon its creation?
 - a. four
 - b. six
 - c. five
 - d. two

7. Upon becoming President, Barack Obama quickly reduced the overall budget allocated to the DHS by half in an effort to save money.
 - a. true
 - b. false

8. Admiral James Milton Loy served as Secretary of DHS for two weeks.
 - a. true
 - b. false

Key Term Definitions

Federal Emergency Management Agency (FEMA): An agency within the Department of Homeland Security charged with providing federal assistance to citizens and first responders in all-hazard events declared as necessitating a federal response.

National Terrorism Advisory System: A new general threat level system that replaced the old color-coded system much derided by the public and the media.

Answers to Self Test

1. c
2. a
3. b
4. b
5. d
6. a
7. b
8. a

Chapter Six

Homeland Security Community

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the agencies responsible for homeland security in the U.S. including the intelligence, defense, and security communities.
2. Analyze the role of coordination in the intelligence community as it relates to homeland security.
3. Assess how the intelligence and security communities interact with the criminal justice system.

Instructions to Students

- Read pages 107 - 130 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



The homeland security community is a complex one, with multiple levels of government crossing over various areas of expertise. The homeland security community has the difficult task of identifying and responding to threats, while also coordinating activities among themselves to ensure safety. While coordination at the federal level is more effective with the advent of the ODNI, state-and-local-level coordination is mixed. While communication is not perfect, there is little doubt it has improved since 9/11. With the span of time between major attacks increasing, whether it remains a priority has yet to be seen. In this chapter, we will examine the agencies responsible for homeland security in the U.S., including the intelligence, defense, and security communities.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Fusion centers:

Homeland security policing:

Intelligence community:

Intelligence cycle:

Office of the Director of National Intelligence:

The National Commission on Terrorist Attacks upon the United States (also known as the 9/11 Commission Report) criticized the U.S. intelligence community. Specific criticism cited the bureaucratic cultures that separated the various agencies, preventing them from maximizing their missions. The report led to serious reevaluation of the structure and mission of the national intelligence apparatus, including how the federal government interacts with state and local authorities on intelligence.

While each agency in the intelligence community has a specific mission, inter-agency cooperation and interactions with local and state authorities are essential for understanding homeland security operations in the U.S. The Director of National Intelligence (DNI) is responsible for coordinating activities of the nation's other 16 intelligence agencies. The Office of the Director of National Intelligence (ODNI) supports the DNI's mission. The ODNI was created as a direct response to reforms suggested by the 9/11 Commission Report. The National Counterterrorism Center (NCTC) exists within the ODNI, and is the primary government organization responsible for integrating and analyzing intelligence related to terrorism. The ODNI also develops intelligence products for policymakers related to homeland security threats.

The CIA is the only cabinet-level agency which has a primary responsibility of intelligence. Operating since the end of WWII, it is the most important intelligence-gathering tool possessed by the U.S. government. In addition to intelligence, the CIA produces a wide variety of intelligence products to support government missions. Despite its huge presence, the CIA plays a relatively small role in homeland security because of its limitations regarding American persons, playing a part only when foreign intelligence relates to domestic intelligence problems.

The Department of Defense (DOD) plays an important role in protecting the homeland. DOD has two major components aside from intelligence: homeland defense and civil support. Homeland defense is the primary mission of DOD, and provides military security for the nation's borders, as well as applying force at a threat's origin. In some cases, the force serves to promote deterrence. The DOD also protects "forward" regions—territories and bases, oceans, and airspace surrounding the country.

Multiple Choice Questions (Circle the correct answer)

1. The National Commission on Terrorist Attacks upon the United States is also known as what?
 - a. NATCOM-TAUS
 - b. The 9/11 Commission Report
 - c. The National Terrorism Battery
 - d. The Threat Report

2. Which is not a member agency of the U.S. Intelligence Community?
 - a. Department of Energy
 - b. Drug Enforcement Agency
 - c. National Intelligence Bureau
 - d. National Geospatial-Intelligence Agency

3. Which member of the U.S. Intelligence community would be used to analyze foreign languages?
 - a. Central Intelligence Agency
 - b. Federal Bureau of Investigation
 - c. National Security Agency
 - d. National Reconnaissance Office

4. Which agency's director coordinates the activities of the 17 different intelligence agencies?
 - a. Federal Bureau of Investigation
 - b. Office of the Director of National Intelligence
 - c. Central Intelligence Agency
 - d. National Security Agency

5. Which department/agency can track financial transactions in an effort to track terrorist movements?
 - a. Central Intelligence Agency
 - b. U.S. Customs Service
 - c. Federal Bureau of Investigation
 - d. Department of Treasury

6. The Central Intelligence Agency (CIA) was created during which era?
 - a. shortly after the Vietnam War
 - b. after 9/11
 - c. shortly after WWI
 - d. shortly after WWII

7. The steps of the Intelligence Cycle are always followed in a specific order.
 - a. true
 - b. false

8. The 9/11 Commission Report was considered incomplete, and was later replaced by a more thorough report.
 - a. true
 - b. false

Key Term Definitions

Fusion centers: An information sharing center created by the U.S. Department of Homeland Security and the Department of Justice to assist state and local law enforcement.

Homeland security policing: The local police role in protecting the homeland.

Intelligence community: A group of government agencies and organizations that carry out intelligence activities for the United States government; headed by the Director of Central Intelligence.

Intelligence cycle: A five-step process for intelligence that consists of planning and direction, collecting, processing, analysis and production, and dissemination.

Office of the Director of National Intelligence: The Director of National Intelligence serves as the head of the intelligence community, overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security.

Answers to Self Test

1. b
2. c
3. c
4. b
5. d
6. d
7. b
8. b

Chapter Seven

Anti-terrorism and Counter-terrorism

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Compare the differences between counter-terrorism and anti-terrorism and how those differences impact efforts towards achieving homeland security.
2. Identify the areas defined as “critical” in our nation’s infrastructure and describe why critical infrastructure protection is so important to homeland security.
3. Analyze the nine roles in the context of critical infrastructure and key resource protection and who is involved in those roles.
4. Assess the differences and similarities in the counterterrorism approaches from pre- and post-9/11, and between different presidential administrations.

Instructions to Students

- Read pages 131 - 151 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



In this chapter we will compare the differences between counter-terrorism and anti-terrorism and how those differences impact efforts towards achieving homeland security. Anti-terrorism and counter-terrorism are the two primary elements of the U.S. homeland security mission. Both are often thought of as the same, but they have distinct differences. Anti-terrorism attempts to keep Americans safe and to promote resiliency. Counter-terrorism seeks not only to identify and apprehend terrorists, but to counter the threat before it occurs. President Bush made both the centerpiece of homeland security during his administration. While scaled back a bit during President Obama's administration, they still play an important role in government policy.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Anti-terrorism:

Counter-terrorism:

Critical infrastructure key resources:

Joint Terrorism Task Force:

National Infrastructure Protection Plan:

National Strategy for Counterterrorism:

Two of the primary requirements of homeland security in the U.S. are counter-terrorism and anti-terrorism. Counter-terrorism includes all offensive activities dedicated to tracking and eradicating terrorists both domestically and internationally. Anti-terrorism includes defensive aspects of protection from terrorism, ranging from academic study to “target hardening.” Anti-terrorism is an underutilized term in the American lexicon. The U.S. Department of Defense defines anti-terrorism as, “Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces.”

Counter-terrorism is one of the most visible aspects of homeland security efforts due largely to media coverage and entertainment (movies). Still, there are several areas the U.S. government grapples with in terms of counter-terrorism, such as the legality of drone strikes and enhanced interrogation. Counter-terrorism has undergone a sea change since 9/11. In general, before 9/11, terrorism was not seen as a big threat to the U.S. homeland and there was no clear direction in counter-terrorism prior to the 9/11 attacks. Though on the security agenda, few resources were made available for counter-terrorism other than those dedicated to stopping WMD's. Counter-terrorism post 9/11 was unique in that the U.S. consistently operates outside of its boundaries, but still requires a domestic presence and is not focused on a single adversary.

Multiple Choice Questions (Circle the correct answer)

1. Which U.S. military entity was responsible for killing Osama bin Laden?
 - a. Army
 - b. Green Berets
 - c. Navy Seals
 - d. Marines

2. Which act best describes anti-terrorism?
 - a. hardening of targets
 - b. killing of suspected terrorists
 - c. tracking suspected terrorists
 - d. international coordination in seeking terrorists

3. Most terror-related legislation shortly after 9/11 took on what kind of tone?
 - a. prosecutorial
 - b. stay the course
 - c. multi-national
 - d. preventative

4. Prior to post-9/11 legislation, that allowed for the sharing of terrorist-related information, which government entity was in charge of the terrorist screening process?
 - a. Federal Bureau of Investigation
 - b. Department of Justice
 - c. Department of State
 - d. National Security Agency

5. Which President created the National Counterterrorism Center (NCTC) through executive order?
 - a. John F. Kennedy
 - b. Ronald Reagan
 - c. George W. Bush
 - d. Bill Clinton

6. What is the primary role of the federal government in anti-terrorism?
 - a. manpower
 - b. supply of troops
 - c. appointment of directors
 - d. coordination and legislation

7. President Barack Obama has taken on a completely new strategy in regards to counter-terrorism, that in hardly any way resembles the strategy of President George W. Bush.
 - a. true
 - b. false

8. Seal Team Six was the team responsible for killing Osama Bin Laden.
 - a. true
 - b. false

Key Term Definitions

Anti-terrorism: Represents all offensive activities dedicated to tracking and eradicating terrorists both domestically and internationally.

Counter-terrorism: The defensive aspects of protection from terrorism and can range from academic study to “target-hardening.”

Critical infrastructure key resources: Critical infrastructure protection is comprised of the activities meant to prevent, deter, neutralize, or mitigate the effects of a terrorist attack on the nation’s critical infrastructure.

Joint Terrorism Task Force: A partnership between various American law enforcement agencies that is charged with taking action against terrorism.

National Infrastructure Protection Plan: Provides a unifying framework that integrates a range of efforts designed to enhance the safety of our nation’s critical infrastructure.

National Strategy for Counterterrorism: The Federal government’s approach to dealing with the terrorist threat and identifies the range of tools that are critical to the strategy’s success.

Answers to Self Test

1. c
2. a
3. d
4. c
5. c
6. d
7. b
8. a

The Unit Examination

The unit examination contains 25 multiple choice questions, as well as a writing assignment.

Your grade on the examination will be determined by the percentage of correct answers. The university utilizes the following grading system:

A = 90% – 100% correct	4 grade points
B = 80% – 89% correct	3 grade points
C = 70% – 79% correct	2 grade points
D = 60% – 69% correct	1 grade point
F = 59% and below correct	0 grade points

Completing Unit Two Examination

Before beginning your examination, we recommend that you thoroughly review the textbook chapters and other materials covered in each unit and follow the suggestions in the *Mastering the Course Content* section of the syllabus.

This unit examination consists of objective test questions as well as a comprehensive writing assignment selected to reflect the learning objectives identified in each chapter covered so far in your textbook.

Additional detailed information on completing the examination, writing standards and how to submit your completed examination may be found in the syllabus for this course.

Multiple Choice Questions (Enter your answers on the enclosed answer sheet)

1. Prior to joining the Office of Homeland Security, Tom Ridge had served as governor of what state?
 - a. New York
 - b. Pennsylvania
 - c. Maryland
 - d. Vermont

2. What state was President George W. Bush in when he first heard of the attacks of 9/11?
 - a. Nebraska
 - b. Florida
 - c. Louisiana
 - d. New York

3. Which scholar created the five stages of the “issue attention cycle”?
 - a. John W. Kingdon
 - b. Andrew Card
 - c. Anthony Downs
 - d. Tom Daschle

4. When was the USA PATRIOT Act signed into law?
 - a. 2001
 - b. 2005
 - c. 2002
 - d. 2003

5. Which Senator was the lone dissenter during the vote to pass the USA PATRIOT Act?
 - a. John Kerry
 - b. John McCain
 - c. Russ Feingold
 - d. Patrick Leahy

6. Which administrative function created The Office of Homeland Security?
 - a. act of Congress
 - b. Judicial Order
 - c. Executive Order
 - d. committee

7. USNORTHCOM is specifically charged with the protection of what region?
 - a. Europe
 - b. Canada
 - c. United States homeland
 - d. North and Central America

8. Which Agency manages SIGINT?
 - a. National Security Agency
 - b. Central Intelligence Agency
 - c. Navy Intelligence
 - d. Department of State

9. Which of the following seeks to standardize the interactions between local, state, and federal first-responding organizations?
 - a. HSPD
 - b. NIMS
 - c. JTTF
 - d. OIA

10. Which is not a step in the intelligence cycle?
 - a. planning
 - b. formatting
 - c. processing
 - d. disseminating

11. Of the following agencies/departments, which has the smallest relative role to play in homeland security?
 - a. Federal Bureau of Investigation
 - b. Central Intelligence Agency
 - c. National Security Agency
 - d. National Counterterrorism Center

12. Information is interpreted during which step in the intelligence cycle?
 - a. processing
 - b. conclusion
 - c. analysis and production
 - d. planning

13. About how much of the U.S.'s critical infrastructure is owned by the private sector?
- a. 80 percent
 - b. 50 percent
 - c. 65 percent
 - d. 75 percent
14. Which task would not typically be handled by the National Counterterrorism Center (NCTC)?
- a. planning of anti-terrorism efforts
 - b. sending in national guard troops to a mall
 - c. distributing a report showing depth of a threat
 - d. analyzing a terror threat made online
15. Which group performs regulatory, advisory, policy, or business oversight related to critical infrastructure protection?
- a. state, local, tribal, and territorial governments
 - b. sector-specific agencies
 - c. boards, commissions, authorities, councils
 - d. department of Homeland Security
16. Which entity is in charge of developing the National Infrastructure Protection Plan (NIPP)?
- a. Department of Homeland Security
 - b. sector-specific agencies
 - c. private-sector
 - d. state and local governments
17. The post-harvest food industry accounts for what percentage of the country's overall workforce?
- a. 25 percent
 - b. 40 percent
 - c. 15 percent
 - d. 10 percent
18. The food industry makes up what percentage of the U.S. economy?
- a. 25 percent
 - b. 20 percent
 - c. 30 percent
 - d. 10 percent

19. Which agency/department generally handles domestic Human Intelligence (HUMINT) ?
- a. Federal Bureau of Investigation
 - b. National Security Agency
 - c. Department of Defense
 - d. Immigration and Customs Enforcement (ICE)
20. The Office of the Attorney General is housed within which department?
- a. Federal Bureau of Investigation
 - b. Department of Justice
 - c. Joint Terrorism Task Force
 - d. Department of Treasury
21. SIGINT involves all of the following except?
- a. code-breaking
 - b. cryptanalysis
 - c. satellite imagery analysis
 - d. foreign language analysis
22. For homeland security purposes, which department/agency bridges the intelligence world and the law enforcement community?
- a. Joint Terrorism Task Force
 - b. Federal Bureau of Investigation
 - c. Central Intelligence Agency
 - d. Department of Justice
23. Which agency/department is in charge of developing map-based intelligence solutions?
- a. National Geospatial-Intelligence Agency
 - b. National Security Agency
 - c. National Reconnaissance Office
 - d. Defense Intelligence Agency
24. USNORTHCOM will mobilize at what point during a disaster?
- a. once local, state, and federal agency capabilities are exhausted
 - b. in coordination with FEMA efforts
 - c. immediately when a disaster strikes
 - d. once local and state agency capabilities are exhausted

25. Which agency/department coordinates with state and local law enforcement agencies through their participation in Joint Terrorism Task Forces?
- a. Central Intelligence Agency
 - b. Department of Justice
 - c. Federal Bureau of Investigation
 - d. all of the above

Writing Assignment for Unit Two

- Include your **name, student number, course number, course title and unit number** with your writing assignment.
- Begin each writing assignment by identifying the question number you are answering followed by the actual question itself (in bold type).
- Use a standard essay format for responses to all questions (i.e., an introduction, middle paragraphs and conclusion).
- Responses must be typed double-spaced, using a standard font (i.e. Times New Roman) and 12 point type size.

Word count is NOT one of the criteria that is used in assigning points to writing assignments. However, students who are successful in earning the maximum number of points tend to submit writing assignments that fall in the following ranges:

Undergraduate courses: 350 - 500 words per question.

Graduate courses: 500 - 750 words per question.

Doctoral courses: 750 - 1000 words per question.

Plagiarism

All work must be free of any form of plagiarism. **Put written answers into your own words.** Do not simply cut and paste your answers from the Internet and do not copy your answers from the textbook. Be sure to refer to the course syllabus for more details on plagiarism and proper citation styles.

Please answer **ONE** of the following:

1. How and why was the Department of Homeland Security established? What is the organizational structure of DHS?
2. What role does collaboration play in the intelligence community, and what organization is responsible for collaboration among intelligence agencies? What makes the process difficult?
3. What are the major elements of the National Strategy for Counter-Terrorism and how do they match up with the Obama Administration's counter-terrorism actions? How do they compare with previous administration's actions?

**With Unit 2 complete, you are half way through the course.
Take a break and reward yourself
for a job well done!**



Chapter Eight

The National Strategy for Homeland Security

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the documents that define the government's responses to emergencies that occur in the U.S.
2. Compare the National Strategy for Homeland Security and the National Response Plan.
3. Comprehend the evolution of the National Strategy for Homeland Security.
4. Analyze the roles of the federal, state, local, and tribal governments when an emergency occurs.

Instructions to Students

- Read pages 153 - 170 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



Since 9/11 four plans have been developed by the federal government to coordinate the country's preparedness for, and responses to, future terrorist threats and natural disasters. Each recognizes the important role local first-responders play during incidents. Coordination of activities and sharing of information is key to preventing and mitigating future events. These four plans address these issues in different ways and will be the focus of this chapter.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

9/11 Commission:

National Response Framework:

National Response Plan:

National Strategy for Homeland Security:

The 9/11 Commission's task was to examine the circumstances surrounding the attacks, provide an assessment of the government's response to the attacks, and make recommendations for establishing improved future security policies. The Commission completed the report in 2004, concluding that intelligence agencies were not prepared for such a large-scale attack and that there were serious gaps between the different intelligence groups in terms of information sharing. The report included 41 recommendations, split into three broad categories: homeland security and emergency response, intelligence and congressional reform, and foreign policy and nonproliferation.

The 9/11 Commission Report was the basis for government action to increase homeland security. As a result, President Bush charged his administration with creating new policies that would guide the national effort to ensure a more coordinated response should another terrorist attack occur. These policies can be categorized as follows:

- Science and technology – New processes and technologies to expand the analysis of information to detect and counter potential attacks.
- Information sharing and systems – Reducing gaps in databases of federal law enforcement, and ensuring first responders has compatible communications equipment.
- International cooperation – Creation of “smart borders,” identifying fraudulent travel documents, increasing security of international shipping containers, intensifying international law enforcement cooperation, and helping foreign nations fight terrorism.

Most recommendations in the National Strategy were based on the findings of the 9/11 Commission. Recommendations covered five broad areas:

- The Secretary of Homeland Security is responsible for coordinating federal operations through the Homeland Security Operations Center.
- Secretary of Defense can authorize Defense Support of Civil Authorities (DSCA) as directed by the President.
- Other agencies can play roles including the Department of State, Secretary of Agriculture, Administrator of the Small Business Administration, Secretary of Commerce, Secretary of Health and Human Services, and the U.S. Army Corps of Engineers.
- FBI's Strategic Information and Operations Center (SIOC) is the control center for federal intelligence and law enforcement activities concerning terrorist incidents/threats.
- Serves as a clearing-house to collect, process, and disseminate relevant information.

Events such as hurricanes, earthquakes, tornadoes, chemical spills, etc. pose threats to the nation's infrastructure, and require the same kinds of government responses to protect victims, provide services, and rebuild affected communities quickly and efficiently.

Multiple Choice Questions (Circle the correct answer)

1. The National Commission on Terrorist Attacks Upon the United States was later known as what?
 - a. National Strategic Plan
 - b. The 9/11 Commission Report
 - c. National Response Framework
 - d. The National Terror Commission Report

2. Which homeland security document was published first?
 - a. National Response Plan
 - b. National Strategy for Homeland Security
 - c. National Strategic Plan
 - d. National Response Framework

3. Which of the following was not one of the three broad categories of recommendations listed in The 9/11 Commission Report?
 - a. homeland security and emergency response
 - b. intelligence and congressional reform
 - c. funding Appropriations
 - d. foreign policy and nonproliferation

4. Which principle below was not outlined in the National Strategy for Homeland Security?
 - a. responsibility and accountability
 - b. measured preparedness
 - c. expansion of government spending
 - d. risk management and resource allocation

5. The National Strategy separated homeland security functions into six mission areas. Which of the mission areas below is intended to minimize damage and recover quickly from attacks?
 - a. Defending Against Catastrophic Threats
 - b. Emergency Preparedness and Response
 - c. Domestic Counter-terrorism
 - d. Border and Transportation Security

6. The USA PATRIOT Act was the result of which foundation of the National Strategy?
 - a. international cooperation
 - b. law
 - c. information sharing
 - d. domestic cooperation

7. The 9/11 Commission report included 41 recommendations.
 - a. true
 - b. false

8. When implemented, every component of the National Response Plan must be followed.
 - a. true
 - b. false

Key Term Definitions

9/11 Commission: Formally named the National Commission on Terrorist Attacks Upon the United States, it was formed after the terrorist attacks on September 11, 2001 to investigate the attacks and to make recommendations for future preparations.

National Response Framework: Part of the National Strategy for Homeland Security which provides the guiding principles enabling all levels of domestic response partners to prepare for and provide a unified national response to disasters and emergencies.

National Response Plan: The National Response Plan (NRP) is an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. It provides the structure and mechanisms for the coordination of federal support to state, local, and tribal incident managers and for exercising direct federal authorities and responsibilities. It was replaced by the broader National Response Framework.

National Strategy for Homeland Security: A strategic document which guides, organizes, and unifies our Nation's homeland security efforts.

Answers to Self Test

1. b
2. b
3. c
4. c
5. b
6. b
7. a
8. b

Chapter Nine

Homeland Security Threats

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the different types of threats (chemical, biological, radiological, nuclear, and explosives) facing the U.S.
2. Analyze the effects of these types of weapons on humans.

Instructions to Students

- Read pages 171- 185 of your textbook
- Reference: *Introduction to Homeland Security: Policy, Organization, and Administration* by Oliver, Marion, and Hill, 1st edition, 2015



Threats to homeland security can come from both manmade sources, chemical, biological, radiological, nuclear, and explosive weapons referred to as CBRNE, and natural events. CBRNE attacks are fairly unlikely due to the difficulty in obtaining them. Still, many people are fearful that terrorists both desire and will attempt to use them against U.S. citizens. In this chapter we will examine the different types of threats (chemical, biological, radiological, nuclear, and explosives) facing the U.S.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Biological weapon:

Category A biological weapon:

Category B biological weapon:

Category C biological weapon:

CBRNE:

Chemical weapon:

Dirty bomb:

Explosive weapon:

Nuclear weapon:

The ability of terrorists to use CBRNEs – in large quantities – is limited. A chemical attack is one that uses a device that disperses poisonous liquids, solids, gasses, and vapor agents to cause death or injury to humans, animals, and plants. It can cause a wide range of ailments, from simple discomfort to permanent injuries and death. Large-scale lethal attacks are difficult to accomplish, as they would need to take place in large, open areas. A major chemical attack would require large volumes of the chemical, making such attacks unlikely. First responders require proper training and equipment so they may be able to respond to possible chemical attacks safely and efficiently.

Biological weapons are easier to use than nuclear material, and more dangerous than chemical weapons, as they are relatively easy to produce or obtain. Such weapons are most lethal in aerosol form, from a sprayer. Use of such weapons can be difficult to recognize quickly as their consequences can take hours, days or weeks to emerge. First responders should be trained about the potential use of biological weapons, in an effort to detect them more quickly and reduce the spread of infection. Victims can be treated during an attack with vaccines, but such treatments can be costly, or take time to develop.

Terrorists could introduce radioactive material into food and water supplies, but such attacks would not cause much contamination. A more effective method would be for the terrorists to use explosives (such as dynamite) to scatter radioactive material over a large area in a weapon known as a “dirty bomb”. These are sometimes called radiological dispersion devices (RDDs). An attack on a nuclear facility could result in the same effects produced by a dirty bomb, but could potentially be far more widespread due to the size of the facility. Radiological weapons are the most difficult for terrorists groups to develop, or obtain, and are thus considered the lowest threat when compared to other types of weapons. In an attempt to reduce the chance of terrorists collecting nuclear material, the Domestic Nuclear Detection Office within DHS attempts to monitor the movement and smuggling of nuclear material within the US and around the world. A substantial amount of radiological material remains unaccounted for in the U.S. and around the world in places such as the former Soviet Union.

Natural events, such as natural disasters, can also be a threat to homeland security. Natural disasters, like earthquakes, can strike at any moment, without warning. While there is virtually no way to prevent these events from occurring, there are steps that can be taken to minimize damage and loss of life, such as early warning systems, better construction, and mandatory evacuations. Responses to natural disasters can be similar to the response for terrorist attacks.

Multiple Choice Questions (Circle the correct answer)

1. Which of the following is considered an irritant?
 - a. BZ
 - b. ricin
 - c. botulinum
 - d. pepper spray

2. Which item is not part of CBRNE?
 - a. energy
 - b. chemicals
 - c. radiological
 - d. nuclear

3. Chlorine is what type of chemical agent?
 - a. choking/pulmonary
 - b. blister
 - c. blood
 - d. nerve

4. Mustard gas is a popular form of what type of agent?
 - a. nerve
 - b. choking/pulmonary
 - c. incapacitating
 - d. blister

5. Incapacitating agents are what part of CBRNE?
 - a. radiological
 - b. explosive
 - c. biological
 - d. chemical

6. Hydrogen cyanide is what type of agent?
 - a. nerve
 - b. irritant
 - c. blood
 - d. incapacitating

7. CBRNE attacks can result in both long- and short-term effects.
 - a. true
 - b. false

8. One problem confronting homeland security is the fact that CBRNEs are very easy for terrorists to procure in large quantities.
 - a. true
 - b. false

Key Term Definitions

Biological weapon: Weapons that use a biologically derived or living microorganism, bacteria, virus, rickettsia, or fungi to deliberately harm people, animals, or crops through infections that can incapacitate or kill.

Category A biological weapon: Agents that can easily be disseminated over a large area and infect many people to potentially cause a public health catastrophe.

Category B biological weapon: Agents that are easily disseminated over a large area but have a lower mortality rate.

Category C biological weapon: Common pathogens that could potentially be used as terrorist weapons.

CBRNE: Chemical, biological, radiological, nuclear, and explosives.

Chemical weapon: A device that uses poisonous liquids, solids, gasses, and vapor agents to cause death or injury to humans, animals, and plants.

Dirty bomb: A device that involves the use of conventional explosive material that also contains radioactive material.

Explosive weapon: Conventional weapons that have explosive properties.

Nuclear weapon: An explosive device that derives its destructive force from nuclear reactions, either fission or a combination of fission and fusion.

Answers to Self Test

1. d
2. a
3. a
4. d
5. d
6. c
7. a
8. b

Chapter Ten

The Homeland Security Cycle

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the elements of the homeland security cycle and why they are important to homeland security.
2. Analyze the role of federal, state, local, and tribal governments in the homeland security cycle.

Instructions to Students

- Read pages 187 - 199 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



In this chapter we will examine the elements of the homeland security cycle and why they are important to homeland security. There are four stages to the homeland security cycle: mitigation, preparedness, response, and recovery. The first two stages involve activities taken to lessen the chance of an event. The second two stages involve activities taken after an event has occurred. All levels of government may be involved in each stage of the cycle.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Emergency declaration:

Incident Command System:

Joint field office:

Mitigation:

National Incident Management System:

Preparedness:

Recovery:

Response:

The homeland security cycle refers to the four stages necessary to prepare for an event, and to respond to it. Two stages occur before an event happens: mitigation and preparedness. Two stages occur after an event happens: response and recovery.

On the federal level, the Federal Emergency Management Agency (FEMA) is primarily responsible for the cycle, while state and local agencies are also involved. Emergencies can be terror attacks, natural disasters, or human-made disasters. Mitigation is the actions taken with the intent of avoiding an incident, or intervening in an effort to limit the effects if an incident occurs. Mitigation also allows for risk management, allowing more resources to be assigned to protecting things such as critical infrastructure. Policies and actions that can be implemented include activities such as restrictive building codes, improved surveillance of critical sites, immunizations against diseases, and increased security.

FEMA created a Mitigation Directorate to aid in protecting lives and preventing loss of property. While it is impossible to prevent natural disasters, it is possible to reduce their impact through mitigation measures, such as stricter building codes, evacuation plans, and levee construction and other structures. Many of the nation's actions to prepare for emergencies can be found in the National Response Framework document. The federal government created the National Incident Management System (NIMS) to help oversee and coordinate the efforts described in the National Response Plan. FEMA also assists states and local governments through the Homeland Security Grant Program, suggesting ways to prepare for the various events that could happen. Other federal agencies also help with planning and preparedness, such as the Centers for Disease Control (CDC).

Response actions are primarily delivered by first responders (police, fire, emergency medical personnel) in an effort to secure the scene, maintain order, assist victims, and contain the specific disaster. A critical step in response is to ensure all responses are carried out, with little overlap. Volunteer groups can also play a critical role in providing specific emergency response services in support of first responders. The National Response Plan outlines the federal government's plan for emergency response, along with NIMS. On the local level, each jurisdiction has the responsibility to provide qualified first responders who can handle a variety of emergencies, as they will more than likely be the first responders to an emergency. When the emergency grows too complex or costly, a local mayor or governor can request assistance from the federal government. State governors can also formally request that the president declare a major disaster, or provide an emergency declaration.

Multiple Choice Questions (Circle the correct answer)

1. In 2012, the FBI, using a paid informant, disrupted a domestic plot to blow up a bridge in what city?
 - a. New York City
 - b. Cleveland, OH
 - c. Atlanta, GA
 - d. San Francisco, CA

2. The FBI or other law enforcement agency using a paid informant to gather intelligence on a terrorist group would be considered part of which stage of the homeland security cycle?
 - a. response
 - b. mitigation
 - c. preparedness
 - d. recovery

3. How many of the stages in the Homeland Security Cycle are devoted to actions before an event occurs?
 - a. one
 - b. two
 - c. three
 - d. four

4. Which Federal department or agency has the primary responsibility for helping the United States with the stages of the homeland security cycle?
 - a. DOD
 - b. Red Cross
 - c. FEMA
 - d. FBI

5. Which government agency manages the National Flood Insurance Program?
 - a. FEMA
 - b. NIMS
 - c. CDC
 - d. FBI

6. Roughly how many state and local intelligence fusion centers are currently operating in the United States?
 - a. 70
 - b. 40
 - c. 125
 - d. 55

7. The CDC provides information on its website on how to prepare for a zombie attack.
 - a. true
 - b. false

8. Mitigation and Response are considered to be stages in the homeland security cycle that occur before an event.
 - a. true
 - b. false

Key Term Definitions

Emergency declaration: Emergency declarations trigger aid that protects property, public health, and safety, and lessens or averts the threat of an incident becoming a catastrophic event.

Incident Command System: The Incident Command System (ICS) is a standardized, on-scene, all-hazards incident management approach.

Joint field office: When an incident is of such severity, magnitude, and/or complexity that it requires coordinated federal assistance, the Secretary of Homeland Security, in coordination with other federal departments and agencies, initiates actions to respond to and recover from the incident, including the establishment of the Joint Field Office to provide the Incident Commander Federal Resources.

Mitigation: The effort to reduce loss of life and property by lessening the impact of disasters.

National Incident Management System: Identifies concepts and principles that answer how to manage emergencies from preparedness to recovery, regardless of their cause, size, location, or complexity.

Preparedness: A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response.

Recovery: The efforts taken to restore the infrastructure and the social and economic underpinnings of a community to a state of normalcy.

Response: Any measures taken at the onset of an emergency to save lives and protect property.

Answers to Self Test

1. b
2. b
3. b
4. c
5. a
6. a
7. a
8. b

Chapter Eleven

National Incident Management System and Incident Command System

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the overall concept of the National Incident Management System (NIMS).
2. Analyze the five components of NIMS and their purpose.
3. Assess the overall concept of Incident Command System (ICS).
4. Recognize the 14 proven management characteristics of ICS.
5. Identify the members of the command and general staffs in ICS.

Instructions to Students

- Read pages 201 - 221 of your textbook
- Reference: ***Introduction to Homeland Security: Policy, Organization, and Administration*** by Oliver, Marion, and Hill, 1st edition, 2015



In the wake of the 9/11 attacks, the federal government created the National Response Plan (NRP). Hurricane Katrina tested the NRP and found it to be highly deficient due to lack of widespread implementation. Since Katrina, the National Incident Management System (NIMS) has become the method by which the nation, at all levels, coordinates the preparations and response throughout the homeland security cycle, and ICS. The events of 9/11, and the hurricane seasons of 2004 and 2005 highlighted the need to focus on improving emergency management, incident response capabilities, and coordination processes across the country, at all jurisdictional levels.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Command staff:

Emergency Operations Center (EOC):

General staff:

Incident Command Post (ICP):

Multiagency Coordination System(s) (MACS):

Nongovernmental Organizations (NGOs):

Unified command (UC):

In 2005, Hurricane Katrina caused massive devastation across the Gulf Coast of Florida, Mississippi, Alabama, and Louisiana, including the flooding of New Orleans. More than 1,300 people died as a result of the storm. Seemingly, it appeared that local, state, and federal officials were unable to respond effectively to the crisis. Emergency plans at all levels of government, including the National Response Plan, were put to the test, and, ultimately, came up short. In Katrina's aftermath, President Bush commissioned a group to study the federal response to Katrina, and what went wrong. A 2006 report noted that the National Incident Management System (NIMS), and the use of Incident Command Systems were not yet developed enough, and with a subsequent lack of training, the federal response was inadequate for such a disaster. Recommendations included intensified efforts to educate responders at all levels in NIMS and the Incident Command System (ICS)

NIMS framework outlines this nationwide approach. Incidents predominantly begin and end locally, with upper levels of government and functional agencies assisting as needed. NIMS uses a systematic approach to integrate the best existing processes and methods into a unified, national framework for incident management. This framework forms the steps for interoperability and compatibility that will enable the many diverse public and private organizations to conduct well-integrated and streamlined emergency management and incident response operations. It improves capabilities to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other man-made disasters. The framework utilizes a common incident management framework, providing a flexible, but standardized system. This system constructs a set of standardized, organizational structures, integrating existing best practices into a consistent, nationwide, systematic approach that is applicable across all levels of government, nongovernmental organizations (NGOs), and private-sector interests.

Specific measures and capabilities are described that emergency management/response personnel and their affiliated organizations can develop and incorporate into their own overall preparedness programs. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are the primary goals of this NIMS component. This allows for a predictable dissemination and sharing of information within all responding organizations and agencies. Incident communications are facilitated through development and use of a common communications plan and interoperable communications equipment, processes, standards, and architectures. During an emergency, resources such as personnel, teams, facilities, equipment, and supplies need to be carefully managed. Standardized resource management concepts will help facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident. Resource management should be flexible and scalable in order to adapt to the sometimes changing conditions of any incident. Resources may support on-scene and command operations through the Incident Command Post (ICP) or function within the Multiagency Coordination Systems (MACS) serving at an Emergency Operations Center (EOC) or similar site. In situations where there is competition for critical resources, MACS may be used to prioritize and coordinate resource allocation and distribution.

Multiple Choice Questions (Circle the correct answer)

1. In what year did Hurricane Katrina strike?
 - a. 2012
 - b. 2004
 - c. 2005
 - d. 2010

2. The National Incident Management System (NIMS) is considered to be many things, except which of the following?
 - a. scalable
 - b. a response plan
 - c. a systematic approach
 - d. a dynamic system

3. Which of the following is not an ICS management characteristic?
 - a. information and intelligence management
 - b. incident facilities and locations
 - c. management by objectives
 - d. management by dispatch

4. Which event led to a redoubled emphasis to educate first responders on the National Incident Management System (NIMS)?
 - a. Hurricane Andrew
 - b. Hurricane Katrina
 - c. the events of 9/11
 - d. Hurricane Sandy

5. In its beginning, ICS was based on how many management characteristics?
 - a. 22
 - b. 14
 - c. 18
 - d. 7

6. The NIMS systematic approach to incident management is comprised of five major components. Which of the following is not one of them?
 - a. resource management
 - b. preparedness
 - c. communications and information management
 - d. martial law coordination

7. NIMS is a dynamic system that promotes ongoing management and maintenance.
 - a. true
 - b. false

8. Ongoing development in the area of science and technology is integral to the continual improvement of NIMS.
 - a. true
 - b. false

Key Term Definitions

Command staff: Incident Command's staff that provides information, liaison, and safety services for the entire Incident Command and reports directly to the Incident Commander.

Emergency Operations Center (EOC): A central command and control facility for carrying out emergency management.

General staff: This staff focuses the key functions of incident command, operations, planning, logistics, and finance/administration and reports directly to the Incident Commander.

Incident Command Post (ICP): The physical location of the Incident Commander and his or her staff.

Multiagency Coordination System(s) (MACS): A process that allows all levels of government and all disciplines to work together more efficiently and effectively. Multiagency coordination occurs across the different disciplines involved in incident management, across jurisdictional lines, or across levels of government.

Nongovernmental Organizations (NGOs): Legally constituted corporations by people that operate independently from any form of government, such as the American Red Cross.

Unified command (UC): A structure that brings together the "Incident Commanders" of all major organizations involved in the incident in order to coordinate an effective response while at the same time carrying out their own jurisdictional responsibilities.

Answers to Self Test

1. c
2. b
3. d
4. b
5. b
6. d
7. a
8. a

The Unit Examination

The unit examination contains 25 multiple choice questions, as well as a writing assignment.

Your grade on the examination will be determined by the percentage of correct answers. The university utilizes the following grading system:

A = 90% – 100% correct	4 grade points
B = 80% – 89% correct	3 grade points
C = 70% – 79% correct	2 grade points
D = 60% – 69% correct	1 grade point
F = 59% and below correct	0 grade points

Completing Unit Three Examination

Before beginning your examination, we recommend that you thoroughly review the textbook chapters and other materials covered in each unit and follow the suggestions in the *Mastering the Course Content* section of the syllabus.

This unit examination consists of objective test questions as well as a comprehensive writing assignment selected to reflect the learning objectives identified in each chapter covered so far in your textbook.

Additional detailed information on completing the examination, writing standards and how to submit your completed examination may be found in the syllabus for this course.

Multiple Choice Questions (Enter your answers on the enclosed answer sheet)

1. The utilization of local emergency management officials during an emergency would fall under which broad area covered in the National Strategy?
 - a. information
 - b. border and transportation security
 - c. response
 - d. cooperation

2. The National Response Plan was published in what year?
 - a. 2004
 - b. 2002
 - c. 2012
 - d. 2007

3. The National Response Plan was created by what?
 - a. Homeland Security Presidential Directive
 - b. Congressional act
 - c. Executive Order
 - d. none of the above

4. At what point would federal resources be used to respond to an incident, according to the National Response Plan?
 - a. immediately
 - b. upon state or local request
 - c. after a minimum of seven days
 - d. after a minimum of ten days

5. In regards to the National Response Framework, a local police department providing security during an emergency would be an example of what?
 - a. engaged partnership
 - b. unity of effort through unified command
 - c. tiered response
 - d. scalability and flexibility

6. Following the National Response Plan, which is a temporary entity, only created and called upon when necessary?
 - a. JFO
 - b. IIMG
 - c. SIOC
 - d. RRCC

7. Category A, B, and C agents are what part of CBRNE?
 - a. chemical
 - b. nuclear
 - c. biological
 - d. energy

8. There are typically how many types of biological weapons?
 - a. Two
 - b. Four
 - c. Three
 - d. Five

9. An attack on a nuclear power plant, or nuclear research facility can produce effects similar to what other type of weapon?
 - a. Explosive
 - b. Dirty bomb
 - c. Chemical
 - d. None of the above

10. Which of the following is a Category A agent?
 - a. Ricin
 - b. Tuberculosis
 - c. Small pox
 - d. Glanders

11. VX is an example of which of the following agents?
 - a. Blister
 - b. Nerve
 - c. Blood
 - d. Choking/pulmonary

12. Which of the following is a Category C agent?
- a. Botulism
 - b. Hantavirus
 - c. Q fever
 - d. Tularmeria
13. Which of the following is a pathogen?
- a. Anthrax
 - b. Ricin
 - c. Botulinum
 - d. All of the above.
14. What biological agent was used in an attack against the United States in the days shortly after 9-11?
- a. Anthrax
 - b. Small pox
 - c. Ricin
 - d. Mustard Gas
15. Which agent can be considered a chemical weapon?
- a. Choking/pulmonary
 - b. Irritants
 - c. Incapacitating agents
 - d. All of the above.
16. What type of weapon is a “dirty bomb?”
- a. Explosive
 - b. Biological
 - c. Chemical
 - d. Radiological
17. Which federal resource has the ability to warn the entire nation of a national threat or emergency on very short notice?
- a. National Incident Management System
 - b. Emergency Response System
 - c. National Response Plan
 - d. Emergency Alert System

18. The National Strategy for Homeland Security suggests several categories for intelligence analysis. Which of the following is not one of them?
- a. strategic analysis of the enemy
 - b. tactical threat analysis
 - c. threat-vulnerability integration
 - d. none of the above
19. The American Red Cross is an example of what type of group that may assist in responding to an emergency?
- a. federal
 - b. volunteer
 - c. state
 - d. command and control
20. In NIMS, incidents by and large begin and end at what level?
- a. federal
 - b. local
 - c. state
 - d. regional
21. Which NIMS component establishes and maintains a common operating picture, and ensures accessibility and interoperability?
- a. communications and information management
 - b. martial law coordination
 - c. preparedness
 - d. ongoing management and maintenance
22. Which major component of NIMS involves an Incident Command Post?
- a. resource management
 - b. communications and information management
 - c. preparedness
 - d. command and management
23. Which system or entity can assist during a response when competition exists for critical resources?
- a. National Incident Management System (NIMS)
 - b. Multiagency Coordination System (MACS)
 - c. Incident Command Post
 - d. Emergency Operations Center

24. The management of the majority of incident responses typically rises to what level of government?
- a. federal
 - b. state
 - c. local
 - d. regional
25. What provides strategic direction for NIMS oversight, and supports routine maintenance and system refinement?
- a. National Integration Center (NIC)
 - b. Multiagency Coordination System (MACS)
 - c. Emergency Operations Center
 - d. Incident Command System (ICS)

Writing Assignment for Unit Three

- Include your **name, student number, course number, course title and unit number** with your writing assignment.
- Begin each writing assignment by identifying the question number you are answering followed by the actual question itself (in bold type).
- Use a standard essay format for responses to all questions (i.e., an introduction, middle paragraphs and conclusion).
- Responses must be typed double-spaced, using a standard font (i.e. Times New Roman) and 12 point type size.

Word count is NOT one of the criteria that is used in assigning points to writing assignments. However, students who are successful in earning the maximum number of points tend to submit writing assignments that fall in the following ranges:

Undergraduate courses: 350 - 500 words per question.

Graduate courses: 500 - 750 words per question.

Doctoral courses: 750 - 1000 words per question.

Plagiarism

All work must be free of any form of plagiarism. **Put written answers into your own words.** Do not simply cut and paste your answers from the Internet and do not copy your answers from the textbook. Be sure to refer to the course syllabus for more details on plagiarism and proper citation styles.

Please answer **ONE** of the following:

1. What are the key missions and goals identified in the 2012 Department of Homeland Security Strategic Plan?
2. Examine the roles of the federal, state, local, and tribal governments in each of the stages of the homeland security cycle.
3. Explain how the National Incident Management System fits into the homeland security apparatus.

Unit 3 is done!

**You're close to the finish line
and we're cheering you on to victory!**



Chapter Twelve

Political Responses to Homeland Security

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the presidential responses to terrorism.
2. Assess the legislation passed by Congress to deter terrorism or help the country response to an emergency event such as terrorism or a natural disaster.

Instructions to Students

- Read pages 223 - 242 of your textbook
- Reference: *Introduction to Homeland Security: Policy, Organization, and Administration* by Oliver, Marion, and Hill, 1st edition, 2015



There was a great public outcry after the attacks of 9/11 for the president and Congress to pass new laws allowing law enforcement to better investigate terrorists and deter future attacks. President George W. Bush responded with 24 Homeland Security Presidential Directives (HSPDs), and announced National Security Presidential Directives (NSPDs) on homeland security. Since 9/11, the president and Congress have taken action to keep Americans safe from terrorist attacks. Both Presidents Bush and Obama have issued multiple executive orders and presidential directives that have impacted U.S. homeland security policy. Congress has also passed numerous pieces of legislation aimed at limiting terrorist acts, and helping communities respond quickly to emergencies.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Executive order:

National Security Presidential Directives:

Shortly after the 9/11 attacks, President Bush issued numerous executive orders, HSPDs on homeland security. Presidential executive orders are given with the consent of an executive level agency or department, and checked by Congress through their budget authority. The most recognizable law passed by Congress related to terrorism since 9/11 is the USA PATRIOT Act. Immediately after 9/11, President Bush and Attorney General John Ashcroft asked Congress for new laws that would enhance law enforcement's ability to gather intelligence related to terrorism. This included the ability to use roving wire-taps, nation-wide search warrants, wider electronic access, Internet disclosure, immigrant detention, and consolidated appeals. At first, many in Congress from both parties were hesitant to support these changes due to civil liberty issues; however, law enforcement groups were well in favor, arguing they needed these proposed new powers to ensure the country's safety. The bill was eventually passed easily and signed into law on October 26, 2001. Many of the more controversial provisions of the original Patriot Act were to be phased out in December 2005. After some debate, Congress compromised by giving the FBI power to seek roving wiretaps and gain access to business records, granting a four-year extension of the provision. This allowed law enforcement to seek warrants against "lone-wolf" terrorists (not associated with any foreign power), making 14 provisions of the original act permanent, such as allowing law enforcement to use wiretaps and other surveillance techniques to investigate such terrorist acts as computer fraud and adding additional safeguards to protect privacy and civil liberties. The Patriot Act was up for reauthorization again in 2009, and Congress extended the three expiring sections.

Since 9/11, every state has reviewed their existing emergency response plans, and either developed new agencies and polices, or modified existing agencies. Cities have also updated their own preparation capabilities, realizing they are the most at risk to be targeted by a terrorist attack, and they will likely be the first entities to respond. Changes since then have improved intergovernmental relations surrounding homeland security activities. Two grant programs were established—the State Homeland Security Grant Program (SHSGP) and the Urban Area Security Initiative (UASI). With the new funds, states continue to develop new ways to respond to emergencies, developing response plans customized to the characteristics of each state.

Multiple Choice Questions (Circle the correct answer)

1. In the four months following 9/11, how many counter-terrorism resolutions did Congress pass?
 - a. 45
 - b. 65
 - c. 74
 - d. 32

2. What U.S. City was Najibullah Zazi planning to attack?
 - a. Denver
 - b. Boston
 - c. New York City
 - d. Chicago

3. Which Homeland Security Presidential Directive covered the continuity of the federal government in the event of catastrophic emergency?
 - a. HSPD-3
 - b. HSPD-20
 - c. HSPD-16
 - d. HSPD-8

4. About what percentage of Congressional actions were related to counter-terrorism resolutions in the 16 months after 9/11?
 - a. 55 percent
 - b. 97 percent
 - c. 38 percent
 - d. 86 percent

5. Which Homeland Security Presidential Directive effectively created the National Incident Management System (NIMS)?
 - a. HSPD-5
 - b. HSPD-7
 - c. HSPD-20
 - d. HSPD16

6. Which Homeland Security Presidential Directive created the color-coded warning alert system for terrorist activity?
 - a. HSPD-3
 - b. HSPD-5
 - c. HSPD-2
 - d. HSPD-7

7. Presidential executive orders are checked by Congress through their budget authority.
 - a. true
 - b. false

8. President Obama created the color-coded warning system to indicate the nation's alert level through executive order.
 - a. true
 - b. false

Key Term Definitions

Executive order: A presidential order that directs the executive branch or a specific agency within the executive branch to take some form of action.

National Security Presidential Directives: Similar to an executive order, these directives center on directing the various agencies in the executive branch with a focus on matters concerning national security.

Answers to Self Test

1. a
2. c
3. b
4. b
5. a
6. d
7. a
8. b

Chapter Thirteen

Legal Responses to Homeland Security

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the balance between civil rights and the need to collect intelligence.
2. Analyze the objections civil rights advocates have about the USA PATRIOT Act.
3. Assess the Supreme Court's reactions to U.S. policies toward detainees.

Instructions to Students

- Read pages 243 - 257 of your textbook
- Reference: *Introduction to Homeland Security: Policy, Organization, and Administration* by Oliver, Marion, and Hill, 1st edition, 2015



Post-9/11, the government had to balance the need to obtain information and intelligence, with the need to protect law-abiding citizens from being treated unfairly. They had to find a balance in policies that preserved long-treasured civil liberties while protecting citizens from terrorists. The Patriot Act was passed immediately after 9/11 as a way to provide law enforcement with added powers to track down and punish those responsible for attacks against the U.S., as well as preventing future attacks. The new powers were controversial, with opponents arguing that the law violates the First, Fourth, Fifth, Sixth, and Eighth Amendments. Critics also argue that U.S. citizens are given the right to be free from government infringement on their Constitutional rights.

Key Terms

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Enemy combatant:

Guantanamo Bay:

The Patriot Act was passed immediately after 9/11 as a way to provide law enforcement with added powers to track down and punish those responsible for attacks against the U.S., as well as preventing future attacks. A simple objection centered on the new definition of “domestic terrorism,” which was expanded to include nonviolent crimes such as computer fraud and intelligence leaks. This resulted in expanded surveillance against a greater number of citizens. Law enforcement surveillance activities against citizens were made easier through the Patriot Act, with restrictions on wiretaps reduced and expanded powers to track other types of communications, such as email. The law also expanded domestic surveillance through changes to the Foreign Intelligence Surveillance Act (FISA), allowing surveillance for only “significant” purposes, rather than national security. Roving wiretaps were also introduced, so wiretaps could expand beyond a single computer or telephone, “roving” wherever the target goes. Opponents argue this violates the Fourth Amendment’s requirement that a warrant specify the place to be searched, and evidence to be seized. Under the law, if law enforcement believes national security is jeopardized, they are allowed “sneak and peek” searches, in which they conduct a search of a facility, review documents, and remove possessions without informing the person targeted in the search that the search took place. Opponents argue that the law violates the First Amendment by requiring phone and Internet service providers to turn over customer records to law enforcement, while being forbidden to notify their customers. The law also allows the government to more easily oversee bank records, making opponents uncomfortable from the potential intrusion. The government argues they need this ability in order to curtail terrorism financing.

Concerns have arisen over the use of the “No-Fly Watch List” and “Automatic Selectee” list. Anyone on the No-Fly list is not permitted to board an airplane at all. Those on the “Automatic Selectee” list are identified for closer scrutiny when passing through airport security. While the reasons behind the creation of such lists are understandable, they can create an issue when data supplied by U.S. intelligence agencies is incomplete and/or inaccurate, causing some innocent people to have trouble, or be unable to board a plane. The American Civil Liberties Union (ACLU) has challenged the “No-Fly Watch List” in courts, alleging that the government refused to explain why some names are on the list and arguing the collection and sharing of information on citizens who are not under investigation for a specific crime is forbidden by the Bill of Rights. The proposed national DNA database has also raised concerns. The Department of Justice is considering a plan to add a DNA database to the FBI’s existing crime-related database, which would collect DNA from those arrested as a suspect in a terrorist plan or act. Opponents argue the DNA is of little use in deterring crime, as the crime has already been committed, and it would also be ineffective due to the large number of people to analyze. A proposed National Identity System has also raised concerns, in that it would be a way for the government to collect information on all citizens, even if they haven’t been accused of a crime.

After the 9/11 attacks, both President Bush and Vice President Cheney felt the president and the executive branch had the power to designate certain terrorists, “enemy combatants.” This would allow for their trial in special military courts, bypassing the U.S. Court system. Similarly, they argued the president has the authority to ask federal law enforcement and intelligence agencies to monitor phone calls originated in the U.S. to suspected terrorists in foreign countries. These and similar acts were expanded using executive power, without congressional oversight. Critics argued this approach was an abuse of executive power. During times of emergency, police are allowed more intrusions into people’s behavior, but did 9/11 represent a time of emergency?

In June 2006, the U.S. Supreme Court ruled against President Bush, ruling that detainees at Guantanamo Bay could not be tried in military courts. In response, Bush persuaded Congress to pass the Military Commissions Act of 2006, allowing detainees to be tried by a special military commission called military tribunals. Many Americans favor detention without arrest and military tribunals for suspected terrorists, even if it means the denying of their civil rights. Conversely, civil libertarians tend to support providing constitutional protections to suspected terrorists, including trials in civilian courts and the dismantling of facilities like Guantanamo Bay. Upon his election, President Obama tried to reverse some of the Bush administration policies, vowing to close the Guantanamo Bay facility and trying five suspects in the 9/11 attacks in New York City for a civilian trial. Opposition immediately rose against the decision to try them in New York City, and the decision was reversed. In addition, President Obama has continued many of the security measures originally started in the Bush administration.

Multiple Choice Questions (Circle the correct answer)

1. After his arrest, how long was Jose Padilla kept from contact with an attorney, his family, or any nonmilitary personnel?
 - a. eight months
 - b. two years
 - c. eighteen months
 - d. six months

2. Which Constitutional Amendment guarantees U.S. Citizens the right to a speedy, public trial?
 - a. sixth
 - b. fourteenth
 - c. first
 - d. fifth

3. United States citizens are granted their civil rights through what?
 - a. The Constitution
 - b. The Bill of Rights
 - c. The first 10 Amendments of the Constitution
 - d. all of the above

4. In what year did the U.S. Supreme Court rule that Jose Padilla was entitled to due process because he was a U.S. citizen?
 - a. 2002
 - b. 2007
 - c. 2005
 - d. 2009

5. The Department of Justice is considering the creation of what kind of database in an effort to track terrorists?
 - a. fingerprint
 - b. DNA
 - c. photo recognition
 - d. iris scan

6. Which Constitutional Amendment is generally not one that Patriot Act opponents cite as being infringed upon by the act?
 - a. sixth
 - b. second
 - c. eighth
 - d. first

7. Yaser Hamdi was captured upon his return to the United States and charged with planning to set off a dirty bomb in New York City.
 - a. true
 - b. false

8. Human rights include the basic rights that people should have if they are citizens of the United States.
 - a. true
 - b. false

Key Term Definitions

Enemy combatant: Historically it meant someone fighting against the United States military, but the Bush Administration used the term to mean someone who is fighting the United States unlawfully and therefore did not have the protections the Geneva Convention affords a soldier fighting for a country.

Guantanamo Bay: A bay located in Cuba that the U.S. acquired in the 1960s, converted into a U.S. military prison in 2002.

Answers to Self Test

1. c
2. a
3. d
4. c
5. b
6. b
7. b
8. b

Chapter Fourteen

Homeland Security Communications and Technology Issues

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the role of communications and communications technology in homeland security and identify some of the major programs dealing with homeland security communications.
2. Identify different types of cyber threats and attacks, and understand the importance of cyber-terrorism in homeland security.
3. Analyze the role of technology in the context of homeland security, both as a benefit to homeland security professionals as well as a potential threat to homeland security.

Instructions to Students

- Read pages 259 - 276 of your textbook
- Reference: *Introduction to Homeland Security: Policy, Organization, and Administration* by Oliver, Marion, and Hill, 1st edition, 2015



Issues in communications and cyber defense are becoming a high priority in terms of homeland security. With the overall increase of technology in our lives, the risk of a cyber attack has increased. While communication issues were identified after the attacks of 9/11, not all of the issues have been resolved. The Homeland Security Advanced Research Projects Agency (HSARPA) was created for homeland security purposes. The HSARPA is working on new technologies and have assisted first responders at all levels. New surveillance options, as well as communications equipment and explosive detection technology, have assisted in securing the homeland. Technology is likely to remain both a focal point for future threats, as well as a method by which such threats can be neutralized.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Cyber crime:

Cyber-attack:

Cyber-terrorism:

Cybersecurity:

GETS:

HSARPA:

NUSTL:

USCYBERCOM:

Technology is one of the most identifiable elements of nearly all aspects of modern society. While providing convenience, technology also provides targets for terrorists, especially technology linked to infrastructure. Different agencies have developed different communications platforms that are not always interoperable, causing potential issues during emergencies. Technology is providing homeland security professionals with additional tools to protect the homeland in both the physical and cyber world.

One of the largest issues facing homeland security post-9/11 was operational communications between agencies. Compatible and adequate communications among public safety organizations at all levels was the primary issue. Progress has been made over the last decade, though there is still no comprehensive solution within a homeland security context, as political will for a solution has been somewhat lacking. In response, the Department of Homeland Security, in 2007, created the Office of Emergency Communications (OEC), which is responsible for partnering with communications stakeholders at all levels to improve emergency capabilities. By executive order in 2010, President Obama abolished the National Communications System, and established a National Security/Emergency Preparedness Executive Committee (CEC), responsible for program management through the Communications Portfolio Branch. Programs specifically designed to assist the government in times of national security were created, such as the Government Emergency Telecommunications Service (GETS) program. This program keeps national security call completion rates high on land lines during times of emergency. Another program allows priority access for government communications, even on private networks during emergencies. In addition to federal efforts, the OEC has also mandated that states and territories develop and submit Statewide Communication Interoperability Plans (SCIPs), which examine current issues, as well as plan for future development of communications across jurisdictions.

Cyber attacks, and cyber-terrorism, are some of the most technologically-dependent threats, and potentially some of the most damaging to the United States and beyond if carried out on a large scale. Cyber security was mentioned as far back as a 1991 National Academy of Sciences report. Generally, all cyber attacks are uses of malicious computer code meant to disrupt the normal processing or logic of the target system, or to steal information. Considering all the variable factors involved, defining cyber-terrorism has been contentious among academics and practitioners. The federal government, in fact, does not officially define cyber-terrorism. One academic definition sees cyber-terrorism as “politically motivated hacking operations intended to cause grave harm such as loss of life, or severe economic damage.”

The National Cyber Response Coordination Group is comprised of 13 federal agencies and is the principle entity responsible for coordination and recovery during an attack. The Computer Emergency Response Team (US-CERT) is the operational arm for the NCSD, and is tasked with the security of government cyber operations, and collaboration among state, local, and private-sector partners.

While increasing technology has increased threats, it also provides opportunities to better safeguard the homeland. Technological solutions to problems have been part of DHS’s mission since its inception. Similar to the Defense Department’s Advanced Research Projects Agency (DARPA), the Homeland Security Advanced Research Projects Agency (HSARPA) was created for homeland security purposes.

Multiple Choice Questions (Circle the correct answer)

1. Following 9/11, what was discovered as one of the primary obstacles to adequate emergency communications?
 - a. lack of compatible technology
 - b. too many people communicating at once
 - c. lack of development in technology
 - d. political influences

2. The Office of Emergency Communications (OEC) was created in what year?
 - a. 2002
 - b. 2007
 - c. 2006
 - d. 2005

3. Which OEC branch is responsible for its coordination of strategy?
 - a. Policy and Planning
 - b. Public Safety and National Security and Emergency Preparedness Partnership
 - c. Technical Assistance
 - d. Communications Portfolio Management

4. Which OEC branch is responsible for technical analyses and assessments of new technology?
 - a. Communication Portfolio Management
 - b. Regional Coordination
 - c. Architecture and Advanced Technology
 - d. Technical Assistance

5. What communication system/process did President Obama abolish and replace with a 2010 executive order?
 - a. Government Emergency Telecommunications Service (GETS)
 - b. Emergency Preparedness Committee
 - c. Communications Portfolio Branch
 - d. National Communications System

6. Which strategy or system provides government communications with priority during times of emergency or crisis?
 - a. Government Emergency Telecommunications Service
 - b. National Security Strategy
 - c. Office of Emergency Communications
 - d. National Communications System

7. The use of specific, standardized communication technology for emergency responders was mandated through a Department of Homeland Security regulation in 2007.
 - a. true
 - b. false

8. The federal government officially defines cyber-terrorism as “politically motivated hacking operations intended to cause grave harm, such as loss of life or severe economic damage.”
 - a. true
 - b. false

Key Term Definitions

Cyber crime: Criminal activity carried out through computing.

Cyber-attack: Any type of attack on America carried out through computing.

Cyber-terrorism: An attack that is conducted for terroristic purposes against the United States and is carried out through computing.

Cybersecurity: Measures taken to protect computers against criminal or unauthorized use of electronic data.

GETS: Government Emergency Telecommunications Service designed to ensure calls get through when a national emergency creates a congested phone line system.

HSARPA: The Homeland Security Advanced Research Projects Agency (HSARPA), which is focused on providing security for critical infrastructure in the U.S.

NUSTL: National Urban Security Technology Laboratory, focused on providing security for large cities and metropolitan areas.

USCYBERCOM: U.S. Cyber command is specifically tasked with managing risk within DOD networks and making sure those networks are resilient in case of an attack.

Answers to Self Test

1. a
2. b
3. a
4. c
5. d
6. a
7. b
8. b

Chapter Fifteen

Domain Security and the Future of Homeland Security

Learning Objectives

Upon successful completion of this chapter, you should be able to:

1. Examine the importance of domain security, particularly airline security, port security, and border security.
2. Analyze the role TSA plays in airline security and its additional oversight responsibilities in reference to other elements of domain security.
3. Identify the roles of the U.S. Border Patrol and Immigration and Customs Enforcement in terms of border security.
4. Assess the challenges faced by homeland security in the future.

Instructions to Students

- Read pages 277 - 297 of your textbook
- Reference: *Introduction to Homeland Security: Policy, Organization, and Administration* by Oliver, Marion, and Hill, 1st edition, 2015



In this chapter we will examine the importance of domain security, particularly airline security, port security, and border security. Domain security—securing air, land, and sea—remains one of the most important elements of homeland security. While 9/11 focused attention on air passenger safety, other elements of domain security are also essential for overall security of the country. Addressing these issues is the mission of several elements of the DHS. Security efforts are made more complicated due to the changing nature of homeland security threats—international, domestic, and political. Homeland security will remain an essential part of the United States security apparatus for the foreseeable future.

The key terms listed below are terms with which you should be familiar.
Write your definition below each item. Check your answers at the end of this chapter.

Border security:

Domain security:

Maritime security:

Transportation Security Administration:

Homeland security is challenging due in large part to the variety of environments the United States has to protect. Air security is – by and large – the most familiar to Americans, due to the changes since 9/11. The Transportation Security Administration (TSA) was created by virtue of the Aviation and Transportation Security Act of 2001, passed two months after 9/11. As of 2010, TSA had approximately 52,000 employees and a budget of almost \$8 billion.

While focused on aviation, 9/11 suggested vulnerabilities of all modes of transportation. Port security has been highlighted for its importance in deterring and dealing with terrorist threats. The U.S. Coast Guard (USCG) is the principle agency in charge of maritime homeland security, operating under the direction of the DHS. Customs and Border Protection (CBP) inspects cargo and containers of incoming commercial ships. TSA tracks containers through ports and manages a Worker Identification Credential system. The risks to ships that are not actually in port are also significant.

Rail systems are also vulnerable to attack. Subway systems in major cities carry roughly five times as many passengers as airlines do per day. This volume makes it an attractive terrorist target and makes individual-level screening virtually impossible. As such, risk-mitigation and consequence management have been the focus of transit security. While there has been some efforts made to help secure bus systems through increased surveillance at stations, and on buses, the 19 million people per day that use the system are still vulnerable to attack.

Border security has been an issue for the United States long before 9/11. Today, there is an increasing set of threats emerging at the border. The Immigration and Nationality Act (INA) prohibits the movements of certain people into the country. The threat of terrorists crossing illegally is far greater than the threat of illegal immigration, though the latter remains a significant homeland security issue.

The environment for homeland security is always changing, providing a difficult challenge for those involved with keeping the population safe. Three items, in particular, can affect the homeland security threat environment: international threats, domestic threats, and political climate. Many improvements were made to homeland security efforts in the wake of events such as 9/11 and Hurricane Katrina, when public support was high. The lack of such events since then may remove the impetus for further improvements in the short term as the public may lose interest over time. Domestic issues unrelated to security, such as a poor economic climate, can also impact homeland security, as budgets for security programs are cut. The future of homeland security is difficult to predict, as there are many moving parts, and much of the risk that homeland security seeks to mitigate is difficult to assess even in the best of circumstances.

Multiple Choice Questions (Circle the correct answer)

1. What did Al Qaeda terrorist Richard Reid try to light in an effort to explode a hidden bomb on an international flight headed for Miami?
 - a. suitcase
 - b. back pack
 - c. shoe
 - d. iPod

2. The Transportation Security Administration was created in what year?
 - a. 2001
 - b. 2007
 - c. 2002
 - d. 2005

3. Approximately how many people are employed by TSA?
 - a. 435,000
 - b. 52,000
 - c. 136,000
 - d. 96,000

4. What is considered to be the fourth and final layer of TSA's "layered approach" to aviation security?
 - a. passenger name screening
 - b. stopping attacks in-progress
 - c. physical screening of passengers
 - d. intelligence

5. Which is not an aviation-related responsibility of TSA?
 - a. screening of passengers and baggage
 - b. screening of air-freight and cargo security
 - c. general aviation aircraft certification
 - d. review of passenger names

6. Commercial shipping and general aviation make up what percentage of the commercial value of the aviation industry?
 - a. 50 percent
 - b. 35 percent
 - c. 14 percent
 - d. 25 percent

7. After Al Qaeda operative Richard Reid attempted to detonate a bomb aboard an airplane, TSA mandated that passengers remove all jackets while going through physical passenger screening.
 - a. true
 - b. false

8. U.S. Air Marshalls are part of TSA's layered approach to aviation security.
 - a. true
 - b. false

Key Term Definitions

Border security: Protecting the land borders of the United States from illegal movement.

Domain security: Securing the environments of air, land, and sea.

Maritime security: Protecting the coastal waters of the United States from illegal movement.

Transportation Security Administration: The federal department under Homeland Security responsible for transportation security in the U.S.

Answers to Self Test

1. c
2. a
3. b
4. b
5. c
6. d
7. b
8. a

The Unit Examination

The unit examination contains 25 multiple choice questions, as well as a writing assignment.

Your grade on the examination will be determined by the percentage of correct answers. The university utilizes the following grading system:

A = 90% – 100% correct	4 grade points
B = 80% – 89% correct	3 grade points
C = 70% – 79% correct	2 grade points
D = 60% – 69% correct	1 grade point
F = 59% and below correct	0 grade points

Completing Unit Four Examination

Before beginning your examination, we recommend that you thoroughly review the textbook chapters and other materials covered in each unit and follow the suggestions in the *Mastering the Course Content* section of the syllabus.

This unit examination consists of objective test questions as well as a comprehensive writing assignment selected to reflect the learning objectives identified in each chapter covered so far in your textbook.

Additional detailed information on completing the examination, writing standards and how to submit your completed examination may be found in the syllabus for this course.

Multiple Choice Questions (Enter your answers on the enclosed answer sheet)

1. Which President Obama Executive Order effectively retracted a previous President Bush Executive Order dealing with prohibitions against abuse and torture for certain prisoners?
 - a. Executive Order 13491
 - b. Executive Order 13456
 - c. Executive Order 13493
 - d. Executive Order 13492

2. Which Presidential Executive Order called for the removal of prohibitions against abuse and torture for certain prisoners, deemed “unlawful enemy combatants”?
 - a. Executive Order 13491
 - b. Executive Order 13340
 - c. Executive Order 13493
 - d. Executive Order 13539

3. Between the time of the September 2001 attacks and January 11, 2002, over _____ counter-terrorist resolutions were passed.
 - a. 200
 - b. 300
 - c. 450
 - d. 550

4. In its 2011 reauthorization, the USA PATRIOT ACT was extended until what year?
 - a. 2014
 - b. 2017
 - c. 2015
 - d. 2020

5. Which power did the USA PATRIOT Act grant to U.S. law enforcement agencies in an effort to fight terrorism?
 - a. roving wire-taps
 - b. immigrant detention
 - c. consolidated appeals
 - d. all of the above

6. Which Congress enacted the Identity Theft Penalty Enhancement Act?
 - a. 105th
 - b. 111th
 - c. 107th
 - d. 108th
7. What type of authority was President Bush attempting to use when he designated certain terrorists “enemy combatants”?
 - a. congressional power
 - b. war power
 - c. designation power
 - d. executive power
8. The Patriot Act’s allowance of roving wiretaps can be seen as violating which Constitutional Amendment?
 - a. first
 - b. fourth
 - c. sixth
 - d. second
9. In what year did President Bush persuade Congress to pass the Military Commissions Act?
 - a. 2006
 - b. 2002
 - c. 2008
 - d. 2005
10. The requirement that phone companies and Internet service providers turn over customer records to law enforcement, without customer notice, has been seen by Patriot Act opponents as violating which Constitutional Amendment?
 - a. sixth
 - b. fourteenth
 - c. fifth
 - d. first

11. Supporters of the Patriot Act claim the law is necessary for which purpose?
 - a. finding evidence that a person is engaged in terrorist activity
 - b. tracking terrorists who use modern technology
 - c. increasing federal law enforcement's ability to respond to terrorism
 - d. All of the above.

12. Roughly how many names are currently listed on the "No-Fly Watch List?"
 - a. 45,000
 - b. 157,000
 - c. 20,000
 - d. 85,000

13. Upon his election, in which city did President Obama propose trying five suspects accused of roles in the 9/11 attacks?
 - a. Chicago, IL
 - b. Guantanamo Bay
 - c. New York City
 - d. Miami, FL

14. Terrorists have increasingly been using the Internet to accomplish which task?
 - a. communication
 - b. training
 - c. proselytizing
 - d. All of the above.

15. A cyber-attack would rise to the level of cyber warfare if committed by which entity?
 - a. Al Qaeda
 - b. white supremacy group
 - c. Taliban
 - d. China

16. According to homeland security experts, how likely is a large-scale cyber-attack on the information systems of a facility, such as an energy plant?
 - a. very likely
 - b. likely to occur several times per year
 - c. likely to occur on an almost daily basis
 - d. highly unlikely

17. In what year did the National Academy of Sciences first report on computer threats to national security?
- a. 1961
 - b. 2001
 - c. 1991
 - d. 1979
18. Of the agencies involved with cyber defense, which agency's activities are largely classified?
- a. FBI
 - b. DHS
 - c. DOD
 - d. CIA
19. Which agency or department considers cyberspace to be a domain?
- a. DOD
 - b. NSA
 - c. DHS
 - d. CIA
20. Roughly how many cargo and passenger terminals are there in the United States?
- a. 1,000
 - b. 2,400
 - c. 300
 - d. 3,700
21. United States' economic activity is responsible for what percentage of worldwide shipping volume?
- a. 20 percent
 - b. 43 percent
 - c. 28 percent
 - d. 50 percent
22. Which government agency is not involved with port security?
- a. Bureau of Customs and Border Protection
 - b. FBI
 - c. TSA
 - d. U.S. Coast Guard

23. Which entity is primarily responsible for maintaining maritime homeland security?
- a. TSA
 - b. U.S. Navy
 - c. U.S. Coast Guard
 - d. Bureau of Customs and Border Protection
24. Compared to the number of passengers who fly American commercial aviation each day, how many people travel on subways in American cities?
- a. five times as many
 - b. half as many
 - c. three times as many
 - d. double as many
25. The U.S. Coast Guard became part of the Department of Homeland Security in what year?
- a. 2001
 - b. 2003
 - c. 2005
 - d. 1996

Writing Assignment for Unit Four

- Include your **name, student number, course number, course title and unit number** with your writing assignment.
- Begin each writing assignment by identifying the question number you are answering followed by the actual question itself (in bold type).
- Use a standard essay format for responses to all questions (i.e., an introduction, middle paragraphs and conclusion).
- Responses must be typed double-spaced, using a standard font (i.e. Times New Roman) and 12 point type size.

Word count is NOT one of the criteria that is used in assigning points to writing assignments. However, students who are successful in earning the maximum number of points tend to submit writing assignments that fall in the following ranges:

Undergraduate courses: 350 - 500 words per question.

Graduate courses: 500 - 750 words per question.

Doctoral courses: 750 - 1000 words per question.

Plagiarism

All work must be free of any form of plagiarism. **Put written answers into your own words.** Do not simply cut and paste your answers from the Internet and do not copy your answers from the textbook. Be sure to refer to the course syllabus for more details on plagiarism and proper citation styles.

Please answer **ONE** of the following:

1. Examine some objections held by civil rights advocates against the Patriot Act.
2. Analyze the role communications technology plays in homeland security and the problems identified by the 9/11 Commission as issues.
3. Border security has been an issue in the U.S. for a long time. What elements of border security are most important and why?

Congratulations!

You have completed Unit 4.

Now let's sharpen our pencils for the Final Exam.

We are confident you will do well.



About the Final Examination

After you have successfully completed all of the unit examinations and writing assignments, it will be time for you to take the final examination.

The final examination will be provided by student services only after you have completed all four unit examinations and submitted all four writing assignments.

Scheduling a Final Examination

Final examination requests can be submitted via U.S. mail, online through the Coast Connection student portal, or by calling the Testing Department at (714) 547-9625.

A final exam scheduling form is located on the last page of this study guide. Please fill out ALL required fields and mail it to the university.

If you would like to request a final exam online, log into the Coast Connection student portal and click on My Academic Plan. Select the course you are working on and submit the Final Exam Request form located at the bottom of the page. ALL INFORMATION MUST BE FILLED IN.

Final exams will only be sent if you have completed all four unit examinations and submitted all four writing assignments.

Submitting Your Final Examination

Final Examinations can be submitted by mail, fax or online through the Coast Connection student portal.

After you have completed your exam, you or your proctor can fax it to the Grading Department at (714) 547-1451 or mail it to the university. When faxing exams, please do not resize your fax.

For online submissions, once you have logged into the student portal, click on My Academic Plan and select the course you are working on to complete the final examination. You must input the unique password that was sent to your proctor in order to unlock your final examination questions. Remember to keep a copy of your answers for your own personal records.

The university requires all final examinations to be completed under the supervision of a proctor. A proctor can be any reputable person other than a relative, someone who resides with you or a current/former CCU student.

It is your responsibility, as the student, to inform your proctor of the following duties:

- The proctor must assure that all final examination material is kept secure and confidential.
- Verify the student's government issued identification.
- Assure that the student completes the examination without any outside assistance of any kind other than the course textbook, notes and other study materials.
- Follow all online instructions for submitting the final examination, **or**
- Return the signed and completed answer sheet to CCU for grading and evaluation via mail or fax.

Today's Date: _____ Student I.D.: _____

Student's Name: _____

Student's Email: _____

Daytime Telephone: _____ Evening Telephone: _____

Course Number: _____ Course Title: _____

Please send the Final Examination to:

Proctor's Name: _____

Relationship to the Student: _____

Street Address: _____

City: _____ State: _____ Zip Code: _____

Proctor's Email: _____

Proctor's Telephone Number: _____

Student's Signature _____

All information must be filled in, otherwise, your request will not be processed.

