**Course Number: XXXX**

**Course: Critical Infrastructure—Emergency Planning and Preparedness**

**University of XXXXXXXXXXXX**

**Fall/Spring Semester 20XX**

**name of school**:

**department**:

**professor**:

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

**course description/overview:**

This course provides an understanding of the issues associated with developing plans and policies to prepare for disasters, both natural and man-made. It includes an overview of the challenges posed by different kinds of disasters as well as discussions of regulatory requirements, sample plans, equipment requirements, collateral and mutual aid support agreements, and methods for testing and updating plans. The emphasis will be on building these preparedness plans and procedures to protect the Nation’s critical infrastructure from all hazards, for all stakeholders and all disciplines, based on the “Whole of Community” planning concept. The course will explore building more resilient communities and institutions and stronger strategic leadership through the use of standards, technology, training, and education.

The importance of disaster planning is highlighted from recent history: based on historic records from 1981-2010, an average year sees global economic losses of $75 billion. Global economic losses in 2010 jumped to $380 billion. The previous record year was 2005, with $220 billion in damages. Economic losses caused by the magnitude-9.0 Great East Japan Earthquake and the resulting tsunami came to $210 billion, making it the costliest natural catastrophe of all time. The Japanese disaster was also 2011’s deadliest catastrophe, with 15,840 fatalities reported. The earthquake and subsequent tsunami may cost insurers, alone, as much as $40 billion and another earthquake in New Zealand cost $13 billion. Floods in [Thailand](http://topics.bloomberg.com/thailand/) were the third- costliest event at about $10 billion. Other catastrophes included [Hurricane Irene](http://topics.bloomberg.com/hurricane-irene/), causing $7 billion in insured losses, and severe storms and tornadoes in the United States in April 2011, costing $7.3 billion.

**Some of the catastrophic events in 2011 were** **the type that could be expected only once every 1,000 years**. The damage to the nuclear power stations in Japan may take another 1,000 years for recovery. There are currently 3,500 employees still working daily at the Chernobyl plant to contain and to document the radiation. EMERCOM of Russia has an entire hospital in Saint Petersburg devoted to caring for disabled responders to the Chernobyl incident.

Though the number of geophysical disasters, such as earthquakes, does not appear to be increasing in recent years, the number of meteorological and climatological disasters is clearly rising, with global warming partly to blame. By continent, Asia (44% of the overall damage cost) and North America (37%) received most of the impacts from the disasters. Some surprises came from unexpected disasters, such as the hurricane hitting Vermont and an earthquake in Virginia. The wildfires in Texas were also very damaging.

The Great East Japan Earthquake presents many significant lessons for preparedness and planning for catastrophic events the status quo was interrupted, resulting in a new normal:

* The safety of nuclear power was discussed,
* New radiation limits were employed,
* Ongoing disposal and contamination of seawater became a concern,
* Future elections were impacted,
* Hundreds of thousands found themselves in shelters with no home to return to,
* Entire villages were swept away,
* Access to some land was permanently lost,
* The culture of local fishing was impacted long-term,
* Loss of faith and hope in traditional support systems,
* International assistance evacuated rather than take the risk of responding, and
* Slow response, while understandable, created an atmosphere of fear and distrust.

Terrorist attacks create many of the same fallouts and require some of the same responses, thus, this course takes the all hazards approach.

This graduate level course provides an introduction to emergency preparedness and planning as it relates to the critical infrastructure sectors, ensuring adequate protection and resilience from the all-hazards perspective. It therefore includes all sectors and all disciplines (emergency management, homeland security, fire service, emergency medical services, law enforcement, hazardous materials specialists, and public safety), with emphasis on standards, technology, and training/education, as methods of achieving critical infrastructure resilience going forward. This comprehensive emergency preparedness and planning process life cycle requires that every individual be a member of the team, thus, the “Whole of Community” planning and organizing concept is used. Federal, State, local, tribal, and territorial governments may lead, coordinate, and facilitate, but the private sector, nonprofit sector, colleges and universities, as well as individuals also have significant roles. The course covers all phases of emergency management — preparedness, mitigation, response, and recovery.

In addition to this holistic approach, the focus is global, as natural disasters and terrorist incidents do not honor borders.

**credits conferred**: 3

**prerequisite**: None

**learner outcomes/objectives**: (as mapped against the u.s. department of homeland security (dhs) and federal emergency management agency (fema) comprehensive preparedness guide (cpg) 101, version 2, november, 2010).

The course is designed to enable the learners to:

1. **Conduct community-based planning that engages the whole community by using a planning process that represents the actual population in the community and involves community leaders and the private sector in the planning process:**

* Risk Assessments
* History of Incidents and Disasters for Area

1. **Ensure plans are developed through an analysis of risk:**

* Analysis Templates
* Automated Excel Spreadsheets
* Prioritizing Risks

1. **Conduct practical risk assessments on which to build this analysis and to make it a part of outreach to stakeholders:**

* Hearings
* Interviews
* Surveys
* Town Hall Meetings
* Task Forces

1. **Identify operational assumptions and resource demands:**

* Culture
* Tradition
* Laws and Practices
* Resource Management: Priorities, Availability, and Tracking

1. **Prioritize plans and planning efforts to support seamless transition from development to execution for any threat or hazard:**

* Preparedness Plans
* Mitigation Plans
* Response Plans
* Recovery Plans: Short-Term and Long-Term
* Protection Plans
* Resilience Plans

1. **Integrate and synchronize efforts across all levels of government:**

* Intergovernmental process: Federal, State, local, tribal, territorial, and regional
* Interdisciplinary: Emergency management, homeland security, fire service, law enforcement, emergency medical services, public works, schools and colleges, public safety, transportation, environmental protection, energy, and many others
* Interagency Cooperation and Coordination: All government agencies have a role to play and they know what it will be

1. **Identify applicable authorities, statutes, and standards:**

* These are the basis of the preparedness and planning authority and are crucial because many actions and costs stem from plans and requirement, and with different funding streams.
* Standards may currently be voluntary: With or without incentives to comply
* Meeting standards may enhance the reputation of a community, even serving an economic development purpose
* Meeting standards reflects a prudent approach to management of the risks of a community

1. **Gain insight into community risk perceptions:**

* Much of this will be gained through the initial risk assessment and analysis process
* Interviews with press are helpful, as well as researching the archives of the community

1. **Identify organizational arrangements used in the past:**

* Helpful in ascertaining and measuring public perceptions, as well as in predicting future human behavior
* Helpful also to manage change and expectations

1. **Identify mutual aid agreements (MAA) with other jurisdictions:**

* Usually found in Court House or City Records
* Blanket Agreements are common, from jurisdiction to jurisdiction

1. **Identify private sector planning that can complement and focus public sector planning:**

* Business Continuity Planning
* Private Sector Preparedness Standards (PS-PREP) set by the Secretary of Homeland Security

1. **Learn how historical planning issues were resolved:**

* Best Practices
* Lessons Learned

1. **Identify preparedness gaps:**

* Gap Analysis Studies
* Examples

1. **Deploy technology, develop interoperability of communications, and continue to build trust:**

* Phones
* Internet
* Texting
* Emergency Communications Among Responders
* Information Sharing
* Fusion Centers
* Emergency Operations Centers
* Social Media

1. **Integrate training and education, along with testing, drills, and exercises, to test plans and to assess training, as well as overall preparedness:**

* DHS/FEMA Courses
* State Courses
* Local Courses
* Core Competencies
* Colleges and Universities
* Foundation for Higher Education Accreditation in Emergency Management
* Fire and Emergency Services Higher Education Association
* Fire Service Accreditation Agencies
* Annual Exercises: Full scale, Table top, and “Thunderbolt” no-notice exercises
* Target
* Provide tools for management to test and evaluate plans and procedures; and assess if they are feasible and will work during an actual emergency
* Determine how well organization personnel understand their emergency response role
* Improve any coordination or communication among the response staff
* Decide which areas can be further developed
* Enhance the ability to respond to emergencies by management and staff

**delivery method:**

Course delivery will be through mini-lectures, structured collaboration projects, exercises, guest speakers, and interactive classroom discussion. The course readings include assigned and optional readings, including two textbooks, numerous government documents, and a series of relevant standards, policies, plans, and strategies. Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases, particularly the external reviews, and from multiple perspectives. The instructor will facilitate the discussion by asking different levels of questioning (factual, analytical, and application of the material) to evaluate the depth of the learner’s comprehension of the content.

Successful emergency preparedness planners are always building trust through partnerships and outreach, so each student should keep this in mind when perusing these materials, except for the textbooks: Were they developed in a collaborative process or are they more top down documents? Are they practical or theoretical? Are they currently widely accepted? Are they used? Additionally, 11 FEMA Independent Study Courses are cited here for reference that relate directly to this course.

**general course requirements:**

1. Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.
2. It is expected that assignments will be turned in on time (the beginning of the class in which they are due). However, it is recognized that learners occasionally have serious problems that prevent work completion. If such a dilemma arises, please speak to the instructor in a timely fashion.
3. The completion of all readings assigned for the course is assumed. Since class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class.
4. All beepers and cell phones should be turned off before class begins.

**grading:**

Class Participation 30%

Research Paper 30%

Research Paper Presentation 25%

Planning Process Exercise (Player Roles and Responsibilities Paper) 15%

**activities, exercise, and research projects:**

**1. Research Paper/Oral Presentation (55%)**

Each learner will prepare a 12-15 page research paper on an emergency preparedness and planning issue regarding critical infrastructure of their choice (national, regional, State, local, territorial, tribal, sector, or international focus). The paper should be completed using the following organizational format:

* Problem statement,
* Background (include key players, authorities, resources, etc.),
* Discussion (presentation of alternatives with the identification of pros and cons for each alternative), and
* Recommendations (including rationale behind their selection).

Footnotes and citations, if any, should be included on a separate sheet of paper in the proper format for review. The paper should focus on the benefits, drawbacks, and obstacles to the practical application of proposed policy alternatives. The recommendations section should clearly describe the rationale for the policy option of choice. Example research paper topics include the following:

* How to promote emergency preparedness planning strategies and practices.
* How to promote planning process information sharing among key partners.
* How to measure the performance of the planning process within and across sectors and jurisdictions.

As an alternative to a research paper, learners may submit a 12-15 page, section-by-section critique of an existing critical infrastructure sector or sub-sector level plan; critical infrastructure regional, State or municipal-level plan; or Federal-level critical infrastructure security and resilience (CISR) plan or policy. Learner critiques should include visioning and strategies for successful emergency preparedness planning, especially as it relates to CISR challenges within the sector, jurisdiction, or geographic region under study.

Each learner will present his/her research topic or critical analysis (no more than 25-30 minutes in length) to the class during Lessons 13-14. The presentation format will mirror that of the research paper. **Research papers will be submitted prior to class on Lesson 15. Papers may be submitted electronically.**

Prior approval of the topic for the research paper is required. **Learners** **should submit a one-paragraph written description of their proposed topic in class or via email for approval no later than the beginning of class on Lesson 5.**

**2. Emergency Preparedness Planning Exercise (15%)**

Learners will participate in a role-based, interactive tabletop exercise simulating a planning session regarding a jurisdiction’s critical infrastructures and population centers within the United States. Each learner will be assigned a role as a key public or private sector official with attendant planning roles, concerns, and responsibilities. The exercise will include a risk assessment phase, a risk analysis phase, a prioritization phase, a preparedness and mitigation phase, an operational response phase, and post-incident recovery phase. In preparation for the exercise, each participant will develop a short 2-3 page paper in talking point format delineating his/her assigned role-based responsibilities during each phase of exercise play. **This paper will be submitted at the beginning of class on the day of the classroom exercise.**

**3. Expectations for Participation (30%):**

Participation includes coming to class prepared, participating in class discussion, and dynamic role playing during the whole emergency preparedness planning process, focusing on taking care of the critical infrastructure present in the exercise scenario jurisdiction.

**incorporation of feedback:**

The course instructor will offer multiple opportunities for learners to provide constructive feedback over the period of the course. These feedback channels may take the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to complete in-class evaluations at the end of Lesson 6, following the exercise, and at the end of the course. On-line feedback is also encouraged throughout the course. Finally, the instructor will provide written feedback to the students on the collaborative planning project, group oral presentation, and incident management point papers. Ongoing student dialogue with the instructor regarding project development, oral presentation preparation, and incident management exercise participation is highly encouraged.

**reading and resource materials**

**assigned readings**:

Radvanovsky, Robert and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010),

ISBN: 978-1-4200-9527-2.

Comfort, Louise K., Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010),

ISBN: 978-0-8229-6061-4.

National Fire Protection Association, NFPA 1600, 2010 Edition. Standard for Emergency Management and Business Continuity, available at [www.nfpa.org](http://www.nfpa.org) without charge.

Emergency Management Accreditation Program Standards, 2010 edition, very similar to NFPA 1600, available from Council of State Governments at [www.emap.org](http://www.emap.org).

DHS/FEMA Comprehensive Planning Guide (CPG) 101, version 2.0, *Developing and Maintaining Emergency Operations Plans*, (November, 2010 edition), <http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf>.

**recommended readings:**

Federal Continuity Directives 1, 2, and 3, <http://www.fema.gov/about/org/ncp/coop/planning.shtm>.

Continuity Template for Federal and Non-federal Entities (February 25, 2011), <http://www.fema.gov/pdf/about/org/ncp/coop/continuity_plan_federal_and_non_federal.pdf>.

ASIS, American National Standard, Organization Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use, ASIS SPC 1, (2009), <http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf>.

National Incident Management System Guidance, <http://www.fema.gov/emergency/nims/>.

National Response Framework, <http://www.fema.gov/pdf/emergency/nrf/about_nrf.pdf>.

National Disaster Recovery Framework, <http://www.fema.gov/recoveryframework/>.

DHS/FEMA accredited Independent Study Courses are available online, depending on student’s areas of interest, without charge, for reading and taking for CEU credit and for credit toward a CEM®, <http://training.fema.gov/is/crslist.asp?page=all>.

IS 235.b- Emergency Planning, deployed on 01/14/2012,

http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-235.b

IS-821 Critical Infrastructure and Key Resources Support Annex, deployed on 01/27/2009, <http://training.fema.gov/EMIWeb/IS/IS821.asp>.

IS-100.b Introduction to Incident Command System, ICS -100, deployed 10/12/2010, <http://training.fema.gov/EMIWeb/IS/IS100b.asp>.

IS-102.a Deployment Basics for FEMA Response Partners, deployed 12/28/2010, <http://training.fema.gov/EMIWeb/IS/is102a.asp>.

IS-130 Exercise Evaluation and Improvement Planning, deployed 01/23/2008, <http://training.fema.gov/EMIWeb/IS/IS130.asp>.

IS 805 Emergency Support Function (ESF) #5 – Emergency Management, deployed 12/17/2008, <http://training.fema.gov/EMIWeb/IS/IS805.asp>.

IS-806 Mass Care, Emergency Assistance, Housing, and Human Services, deployed 06/06/2009, <http://training.fema.gov/EMIWeb/IS/IS806.asp>.

IS-700.a National Incident Management System: An Introduction, deployed 12/28/2008, <http://training.fema.gov/EMIWeb/IS/is700a.asp>.

IS-703.a NIMS Resource Management, deployed 01/15/2010, <http://training.fema.gov/EMIWeb/IS/is703a.asp>.

IS-701.a NIMS Multiagency Coordination System Course, deployed 12/7/2009, <http://training.fema.gov/EMIWeb/IS/is701a.asp>.

IS-15.b Special Events Contingency Planning for Public Safety Agencies, deployed 07/22/2010, <http://training.fema.gov/EMIWeb/IS/IS15b.asp>.

**course outline**

**lesson 1 topic: risk assessment**

**1. Learning Goals/Objectives:**

* Recognize with the various approaches to conducting risk assessments.
* Recognize and explain the importance of not using assumptions without real research findings and documentation.
* Recognize the significance of the risk assessment process and findings.
* Explain the extensive research necessary to find out the frequency and intensity of actual past disasters.
* Explain how to conduct interviews, as well as where to go to find the necessary information.
* Recognize the various risk assessment templates.

**2. Discussion Topics**

* Why do a risk assessment?
* What is the definition of risk?
* Don’t emergency services personnel/officials know which disasters they may face?
* Emergency services staff are so busy, why should they take the time and make the effort to do a risk assessment when they have so many disasters to handle, day to day?
* How can you assure that a community uses its risk assessment results wisely?
* What happens if a risk assessment is not done?
* What all should be included in a risk assessment?
* How do you know you have included all threats, all hazards, all vulnerabilities, and therefore all risks?

**3. Required Reading:**

Robert Radvanovsky and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010), Chapters 1 and 7.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 143 – 157.

NFPA 1600, section on Risk Assessment and Hazard Analysis, Section 5.4, pages 7 – 8, <http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf>.

DHS Risk Lexicon, <http://www.dhs.gov/files/publications/gc_1232717001850.shtm>.

**lesson 2 topic: risk analysis**

**1. Lesson Goals/Objectives:**

* Develop a sense of the tools available for the analytical process following the assessment.
* Explore best practices and lessons learned regarding risk analysis.
* Identify the uses of analysis.
* Recognize the uses of risk analysis for prioritizing the risks for which a community must plan, train, and exercise.
* Recognize that risk analysis is the foundation for mitigation planning, preparedness planning, response planning, and recovery planning.

**2. Discussion Topics:**

* Which is the most important — conducting an asset identification and valuation to identify critical activities, functions, services, products, partnerships supply chains, and stakeholder relationships or developing a practical plan as fast as possible?
* If everybody already knows what the risks are for an area, because they have lived there for a long time or been the emergency manager for a jurisdiction for many years, is it necessary to do a risk assessment and hazard analysis?
* When considering which hazards to research for a jurisdiction, how would you go about compiling such a list?
* After a risk analysis is completed, with whom should you share your results?
* Who would be interested in seeing the results of this analysis?
* Does this risk analysis have anything to contribute to your training program or your exercise program?

**3. Required Reading:**

NFPA 1600, sections on “Common Plan Requirements,” Section 5.2, page 7, “Panning and Design,” Section 5.4, page 7, and “Business Impact Analysis,” Section 5.5, page 8, <http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf>.

EMAP Standard on Risk Assessment and Analysis, if available.

David Alexander, “Rapid Adaptation to Threat: The London Bombings of July 7, 2005,” in Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 143 – 157.

**lesson 3 topic**: **program standards**

**1. Lesson Goals/Objectives:**

* Identify the differences among the standards.
* Learning the substance of the various standards.
* Recognizing and summarizing the history and role of each of the sets of standards.
* Learning the difference between mandatory and voluntary standards.
* Recognizing the incentives available for compliance with voluntary standards.
* Describing the process of developing and applying standards, including accreditation processes, as well as credentialing and certification.

**2. Discussion Topics:**

* Why would the National Fire Protection Association launch a standards setting process for emergency management and business continuity?
* What is the connection between the Emergency Management Accreditation Program, sponsored by the National Emergency Management Association, the Council of State Governments, and the International Association of Emergency Managers, and the DHS/FEMA?
* Is FEMA guidance on any subject a standard?
* Is there a difference between guidance and standards?
* Once an entity meets a standard, what happens?
* Do meeting standards improve community resilience, CISR, or emergency management?

**3. Required Reading:**

Visit <http://www.fema.gov/ps-preptm-voluntary-private-sector-preparedness> for standards for private sector preparedness and CISR preparedness.

Robert Radvanovsky and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010), Chapters 1, 4, and 8.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 1 -12.

**lesson 4 topic**: **training and education standards**

**1. Lesson Goals/Objectives:**

* Recognize all of the training available through the public, private, and nonprofit sectors that may be helpful in CISR, homeland security, and emergency management.
* Understand the history and substance of the Core Competencies Section of the DHS/FEMA Higher Education Program website.
* Recognize the various accreditations achieved by the courses offered at DHS/FEMA Emergency Management Institute and the Center for Domestic Preparedness.
* Learn the various ways in which training can be and often is tested.
* Recognize the various courses and training opportunities available in your area or community.
* Enroll in such a course online.

**2. Discussion Topics:**

* Look up the website for the Foundation for Higher Education Accreditation in Emergency Management and determine how much influence NFPA, EMAP, and FEMA Guidance have on their standards?
* Should an agency require its contractors to have had or take requisite training for the area of the project they are supporting?
* Should private sector participants be included in training, even if they are not contractors? What would be the advantage and the disadvantage?
* What are the various ways of determining professional competence?
* Is it possible to teach leadership? What would some approaches be?
* How does training and education contribute to CISR?

**3. Required Reading:**

Look up the course catalog for the Center for Domestic Preparedness on its website and pick five courses that would enhance CISR.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 129 – 142, 158 – 179, and 272 – 284.

**lesson 5 topic**: **templates**

**1. Lesson Goals/Objectives:**

* Recognize some of the templates in the area of planning, CISR, as well as emergency preparedness and business continuity.
* Describe the role of templates in planning.
* Identify the weaknesses and strengths of templates.
* Learn how to use a planning template.

**2. Discussion Topics:**

* Pull up a copy of the “Continuity Plan Template for Federal and Non-Federal Entities” published on February 25, 2011, and available on the DHS/FEMA website, and describe its content.
* How does this template relate to CISR?
* How does a line of succession contribute to protection and resilience?
* Would this template be of any use to the nonprofit sector?
* What are the pros and cons of using a template?
* How does this template relate to DHSS/FEMA Federal Continuity Directives 1, 2, and 3?

**3. Required Reading:**

Federal Continuity Directives 1, 2, and 3 at

http://www.fema.gov/guidance-directives#6.

Comprehensive Planning Guide (CPG) 101, Version 2, pages 3-1 to 3-18 at http://www.fema.gov/pdf/about/divisions/npd/CPG\_101\_V2.pdf.

**lesson 6 topic**: **target capabilities**

**1. Lesson Goals/Objectives:**

* Recognize the overall skill, training, technology, capability, and resources sought in order to enhance and support CISR, as well as emergency preparedness and planning.
* Identify the diversity of challenges facing officials and citizens around general emergency preparedness and planning, as well as CISR.
* Recognize the overlaps from one area of activity to another.
* Explain how to use this list as a standard guide or a to-do checklist.
* Ascertain the comprehensiveness of this list.
* Identify and describe the difference among standards, templates, and target capabilities lists.

**2. Discussion Topics:**

* Is this Target Capabilities List up to date?
* How would one go about composing such a list?
* What is the value of such a list?
* What are the strong points and the weak points of such a list?
* How does the list relate to the standards?
* How would such a list be enforced?
* How would you use this list?

**3. Required Reading:**

* CPG 101, sections 4-11 through 4-25.
* Target Capabilities List, http://www.fema.gov/pdf/government/training/tcl.pdf, which can serve as a checklist for a program of emergency preparedness planning around critical infrastructure and all hazards, **putting it all in context**:

1. **Phase I Capabilities**

* Common Capabilities
* Planning
* Communications
* Community Preparedness and Participation
* Risk Management
* Intelligence and Information Sharing and Dissemination

1. **Prevention/Mitigation Mission Capabilities**

* Information Gathering and Recognition of Indicators and Warning
* Intelligence Analysis and Production
* Counter-Terror Investigation and Law Enforcement
* Chemical, Biological, Radiological, Nuclear, and Explosives Detection

1. **Protection Mission Capabilities**

* Critical Infrastructure Security and Resilience
* Food and Agriculture Safety and Defense
* Epidemiological Surveillance and
* Investigation
* Laboratory Testing

1. **Response Mission Capabilities**

* On-Site Incident Management
* Emergency Operations Center Management
* Critical Resource Logistics and Distribution

1. **Using the Target Capabilities List**

* Volunteer Management and Donations
* Responder Safety and Health
* Emergency Public Safety and Security
* Animal Disease Emergency Support
* Environmental Health
* Explosive Device Response Operations
* Fire Incident Response Support
* WMD and Hazardous Materials
* Response and Decontamination
* Citizen Evacuation and Shelter-in-Place
* Isolation and Quarantine
* Search and Rescue (Land-Based)
* Emergency Public Information and Warning
* Emergency Triage and Pre-Hospital Treatment
* Medical Surge
* Medical Supplies Management and Distribution
* Mass Prophylaxis
* Mass Care (Sheltering, Feeding and Related Services)
* Fatality Management

1. **Recovery Mission Capabilities**

* Structural Damage Assessment
* Restoration of Lifelines
* Economic and Community Recovery

The Target Capabilities List (TCL) is a reference document that describes the capabilities for achieving national preparedness and resilience. It also serves as a planning, assessment, and training tool. Various implementation tools are being developed from the TCL to help decision-makers and managers at all levels define their preparedness requirements and assess levels of preparedness. Some uses are briefly described below:

**Risk Assessment**: The determination of risk includes identification and characterization of threats, their consequences and vulnerabilities. While each is important for capabilities-based planning and national preparedness, determinations of vulnerability are important since they include not only exposure and sensitivity, but resilience. Resilience is key, since it refers to our coping capacity to absorb events, adapt, respond to, and recover from its effects.

**Planning:** The TCL includes a Planning Capability designed to establish and maintain the ability to develop, update, and test plans. In addition, each capability contains both preparedness and performance tasks and measures that support the capability outcome and serve as a guide for preparedness planning. The preparedness tasks and measures describe major elements or issues that should be addressed in plans, procedures, and systems, as well as authorities, relationships, and agreements that need to be in place to prepare to use the capability. The performance tasks and measures also inform the planning process.

**Strategy Development and Investment Justifications**: The common framework provided by the Guidelines, priorities, and capabilities serve as a guide to enhance homeland security strategies and investment justifications at all levels.

**Assessment of Preparedness**: The TCL provides a basis for assessing preparedness to help jurisdictions and agencies to plan strategically, design appropriate programs that meet proven needs, and evaluate the effectiveness of investments over time.

**Focus Training on Task Performance**: Training programs should be modified as appropriate to ensure that they provide participants with the knowledge, skills, and abilities to perform the critical tasks defined by the TCL to a proficiency level sufficient to achieve the capability outcomes.

**Test Capabilities through Exercises**: Exercises provide a means to test and validate preparedness. The Homeland Security Exercise and Evaluation Program (HSEEP) is designed to encourage a common exercise design, conduct, and evaluate methodology across all levels of government and the private sector. HSEEP exercises are designed and evaluated to demonstrate capability levels through the assessment of performance of critical tasks and achievement of outcomes, as defined by the TCL.

**lesson 7 topic**: **technology**

**1. Lesson Goals/Objectives:**

* Recognize the various technologies available to support CISR and emergency preparedness planning.
* Learn the process of conducting a technology gap analysis.
* Recognize and explain the evolving role of social media in the emergency management/homeland security areas.
* Recognize the technology gap analysis work being done by the DHS Science and Technology Directorate.
* Identify gap analysis methodologies.
* Recognize the importance and uses of situational awareness.

**2. Discussion Topics:**

* What are some of the most often used technologies in emergency situations and planning?
* How should legacy systems be treated, used, or discarded?
* Do all technologies address all hazards, all phases, and all sectors?
* What is your experience with emergency technologies?
* What is the state of cybersecurity at this point in time?
* Should we have standards for technology used in CISR and emergency preparedness planning?

**3. Required Reading:**

Look up DHS/FEMA’s HAZUS risk assessment/analysis system and check out how it works at <http://www.fema.gov/plan/prevent/hazus/>.

Robert Radvanovsky and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010), Chapter 2.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 33-62.

**lesson 8 topic**: **universal interoperability**

**1. Lesson Goals/Objectives:**

* Explain the impact of the lack of interoperability during the September 11, 2001 attacks.
* Recognize the work over the years since an achieving universal interoperability.
* Identify the barriers to interoperability.
* Describe the costs of interoperability.
* Recognize the government programs supporting interoperability.

**2. Discussion Topics:**

* What does it mean to have a scalable, adaptable, and interoperable information system?
* How far have we come since September 11, 2001 in achieving universal interoperability?
* How much further do we have to go to achieve viable interoperability?

**3. Required Reading:**

Robert Radvanovsky and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010), Chapters 9 and 11.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 173-174 and 244-271.

Research the SAFECOM Program at DHS, <http://www.safecomprogram.gov/default.aspx>.

Look up the 9/11 Commission Report Card on the 10th Anniversary of the attacks on the need for more interoperability and better coordination. The report was issued by the Bipartisan Policy Center’s National Security Preparedness Group (NSPG), a follow on to the 9/11 Commission, which said dramatic improvements are needed in interoperability for emergency responder communications radio spectrum and gear (<http://www.bipartisanpolicy.org/library/report/tenth-anniversary-report-card-status-911-commission-recommendations>).

**lesson 9 topic**: **preparedness planning**

Perhaps the most challenging natural disaster in American history was Hurricane Katrina hitting the Gulf Coast, especially hitting the City of New Orleans hard by causing the breach of its elaborate and delicate levy system, causing a second surge of even heavier and deadly flooding. The U.S. Congress responded by passing several pieces of legislation ordering FEMA to upgrade its own capability and the general capacity building, specified in the new laws, the largest of which was the Post Katrina Emergency Management Reform Act of 2006, which, in short, provided the following:

FEMA's mission is:

(1) Leading the nation's efforts to prepare for, respond to, recover from, and mitigate the risks of, any natural and man-made disaster, including catastrophic incidents;

(2) Implementing a risk-based, all hazards plus strategy for preparedness; and (

(3) Promoting and planning for the protection, security, resiliency, and post-disaster restoration of critical infrastructure and key resources, including cyber and communications assets.

Sets forth provisions regarding the role, qualifications, authority, and responsibilities of the Administrator of FEMA, who shall:

(1) Have not less than five years of executive leadership and management experience, significant experience in crisis management or another relevant field, and a demonstrated ability to manage a substantial staff and budget;

(2) Report to the Secretary of Homeland Security (the Secretary) without being required to report through any other DHS official;

(3) Be the principal emergency preparedness and response advisor to the President, the Homeland Security Council, and the Secretary;

(4) Provide federal leadership necessary to mitigate, prepare for, respond to, and recover from a disaster;

(5) Develop a national emergency management system capable of responding to catastrophic incidents; and

(6) Develop and submit to Congress annually an estimate of the resources needed for developing the capabilities of federal, state, and local governments necessary to respond to a catastrophic incident.

Requires FEMA to be maintained as a distinct entity within DHS.

Establishes within FEMA a Director for Preparedness and a Director for Response and Recovery.

Requires: (1) The Administrator to establish 10 regional offices and area offices for the Pacific, for the Caribbean, and in Alaska;

(2) Each Regional Administrator to establish multi-agency strike teams to respond to disasters, including catastrophic incidents; and

(3) The Secretary to establish a National Advisory Council on Preparedness and Response.

Establishes within FEMA a National Incident Management System Integration Center, a Chief Medical Officer, a National Search and Rescue Response System, and an Office of Emergency Communications.

Continues the Metropolitan Medical Response System and the National Infrastructure Simulation and Analysis Center.

Establishes within DHS a National Operations Center, a System Assessment and Validation for Emergency Responders Program, an Office for the Prevention of Terrorism, and an Assistant Secretary for Cybersecurity and Telecommunications.

Authorizes grants for administering and improving the Emergency Management Assistance Compact.

Provides for the credentialing of DHS personnel and assets likely to be used to respond to major disasters.

Directs the Administrator to:

(1) Provide technical assistance to states and local governments that experience severe weather events, including the preparation of hurricane evacuation studies and plans assessing storm surge estimates, evacuation zones, evacuation clearance times, transportation capacity, and shelter capacity; and

(2) Ensure state, regional, and local emergency preparedness by establishing minimum performance requirements for public and community preparedness.

Requires the Administrator, acting through the Director for Emergency Communications, to:

(1) Develop a National Emergency Communications Strategy to achieve national emergency communications capabilities and interoperable emergency communications;

(2) Conduct a baseline operability and interoperability assessment;

(3) Evaluate the feasibility and desirability of DHS developing a mobile communications capability to support emergency communications at the site of a disaster; and

(4) Review federal emergency communications grants and standards programs.

Directs:

(1) The Secretary to establish a comprehensive research and development program to promote communications capabilities and interoperability among emergency response providers;

(2) The Administrator to establish at least two pilot projects to develop and evaluate strategies and technologies for such capabilities in a disaster in which there is significant damage to critical infrastructure; and

(3) The Administrator, through the Office of Grants and Training, to make grants to states and eligible regions for initiatives to improve emergency communications and interoperability.

Establishes an International Border Community Interoperable Communications Demonstration Project.

**1. Lesson Goals/Objectives:**

* Recognize the basics of planning, as well as best practices.
* Identify the standards and guidance related to preparedness planning.
* Learn the relationship among preparedness planning, mitigation planning, response planning, and recovery planning.
* Become familiar with the preparedness plan for your individual community.
* Become familiar with the provisions and visions of preparedness planning examined in depth in the Comprehensive Planning Guide (CPG) 101, version 2.0.
* Examine the Presidential Policy Directive 8 (PPD-8), which sets a strategic vision for national preparedness using a comprehensive approach to preparedness, on the FEMA website, [www.fema.gov](http://www.fema.gov). The implementation of PPD8 includes the following relevant and instructive documents:
* [National Preparedness Goal](http://www.fema.gov/prepared/ppd8.shtm#3)
* [National Preparedness System](http://www.fema.gov/prepared/ppd8.shtm#3)
* [Campaign to Build and Sustain Preparedness](http://www.fema.gov/prepared/ppd8.shtm#4)
* [National Preparedness Report](http://www.fema.gov/prepared/ppd8.shtm#1)

Other similar guidance documents are being developed and will be available broadly in the coming months.

**2. Discussion Topics:**

* What is the relationship between preparedness planning and technology planning?
* How does a sound preparedness plan help or hurt a response?
* Does a community need to have a preparedness plan, as well as a mitigation plan, a response plan, and a recovery plan?
* How does a preparedness plan protect — or not — the critical infrastructure sectors of critical infrastructure?
* Former President Eisenhower is quoted as having said something similar to, "The plan is not important; it is the planning process that is important." How could the planning process be more important than the plan?
* How do communities test their plans most effectively — during real disasters or during exercises?

**3. Required Reading:**

Robert Radvanovsky and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010), Chapters 3 and 6.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 84-105 and 180-243.

Use Comprehensive Planning Guide (CPG) 101, Version 2.0, as a reference.

**lesson 10 topic**: **mitigation planning**

**1. Lesson Goals/Objectives:**

* Describe the different roles of pre-disaster and post-disaster mitigation.
* Become familiar with the relationship between preparedness and mitigation, as well as between mitigation and recovery.
* Describe the role of mitigation in the overarching, holistic goal of resilience.
* Recognize the cost-benefit value of mitigation.
* Describe the roles of various professions involved in mitigation, such as planners, emergency managers, emergency medical technicians, firefighters, law enforcement and other usual emergency personnel and officials, but also architects, engineers, cartographers, geographic information systems, urban and rural planners.
* Recognize the mitigation planning for the critical infrastructure sectors .

**2. Discussion Topics:**

* What is the relationship between risk assessment, risk analysis and mitigation planning?
* Does mitigation come before or after disasters?
* What is the role of insurance in mitigation and resilience?
* Is there a coordinated mitigation plan for U.S. critical infrastructure?
* If you were going to become a mitigation planner, which courses should you take? And why, for each course?
* What is the effectiveness of "See Something, Say Something?"

**3. Required Reading:**

DHS/FEMA Disaster Resistant Universities Guidance, mitigation planning for institutions of higher education.

Read NFPA 1600, section on Mitigation, <http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf>.

Go to DHS/FEMA/USFA website and subscribe to the critical infrastructure EMR-ISAC, which covers nationwide mitigation planning for critical infrastructure, as well as read the Power Point presentation on the homepage.

Robert Radvanovsky and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010), Chapter 10.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 129-142.

**lesson 11 topic**: **response planning**

**1. Lesson Goals/Objectives:**

* Recognize that emergency management and homeland security includes much more than response alone.
* Identify and describe the many aspects of response, such as search and rescue, fire service, resource management, command and control, and military support to the civil authorities.
* Recognize the National Incident Management System (NIMS) and the National Response Framework (NRF), including the work and coordination of the 15 Emergency Support Functions (ESFs).
* Explain the voluntary standards that relate to response planning and the actual response operations.
* Describe the difference in roles of fire service and emergency management during a disaster.
* Summarize the history of the Incident Command System (ICS), as well as the NIMS.
* Become familiar with response planning around critical infrastructure sites.

**2. Discussion Topics:**

* What was it about the wildland fires in California that created the situation where all stakeholders realized they must come together and develop a special ICS?
* Do all fire departments use the ICS approach? Why or Why not?
* How does fire service response planning differ from emergency management response planning?
* Describe the history of the ICS. For which critical infrastructure disaster was it originally designed to protect?
* Compare and contrast the original ICS system with the one contained in the DHS/FEMA NIMS system.
* What are the differences between civilian and military command and control during disasters?

**3. Required Reading:**

Read NFPA 1600 sections on operations planning and response command and control, <http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf>.

Review the Coast Guard Command, Control, and Communications Engineering Course (C3CEN), available at [http://www.uscg.mil/hq/c2cen/default.asp](http://www.uscg.mil/hq/c2cen/default.aspp).

Review DHS/FEMA presentation, "Introduction to the Incident Management Assistance Teams," available at <http://www.slideserve.com/albany/introduction-to-the-incident-management-assistance-teams>.

Robert Radvanovsky and Allan McDlugall, *Critical Infrastructure: Homeland Security and Emergency* *Preparedness*, 2nd Edition, (Boca Raton, FL: CRC Press, 2010), Chapter 5.

Louise K. Comfort, Arjen Boin, and Chris C. Demchak (eds.), *Designing Resilience: Preparing for* *Extreme Events*, 2010 Edition, (Pittsburgh, PA: University of Pittsburgh Press, 2010), 62-83 and 106.

**lesson 12 topic**: **recovery planning**

**1. Lesson Goals/Objectives:**

* Recognize and explain the relatively new National Disaster Recovery Framework (NDRF).
* Become familiar with the ESF for Long-Term Community Recovery.
* Describe the difference between the role for Individual Assistance and Public Assistance during the recovery process following a disaster.
* Describe which sector of critical infrastructure plays the initial and first role in the recovery process, under the DHS/FEMA Emergency Support Function.
* Identify the difference in time involved in response vs. recovery.
* Describe the role of contingency planning in the recovery process.

**2. Discussion Topics:**

* What is the difference between a Federal response and a national response?
* What are some of the limits to government response?
* Refer to the NRF to describe how each of the 15 ESFs support critical infrastructure.
* Discuss the many variables and significance of international partnerships in critical infrastructure recovery.
* What is the difference between response planning and recovery planning in terms of the actors involved?
* What is the role of nonprofit sector in the recovery process?

**3. Required Reading:**

DHS/FEMA National Disaster Recovery Framework, as a reference.

DHS/FEMA Emergency Support Function 14 (ESF 14), from the NRF, the bridge between the NRF and the NDRF.

**lesson 13 topic**: **training and education**

**1. Lesson Goals/Objectives:**

* Recognize all of the sources of training in emergency preparedness and planning.
* Describe the role of Instructional Design Specialists in preparing courses in emergency management and homeland security.
* Discover all of the training centers under the DHS.
* Identify those training centers that have courses in CISR.
* Summarize the history of the DHS/FEMA Higher Education Program and its almost 260 institutions of higher education partners, as well as the role of the Fire and Emergency Services Higher Education Program, National Post-Graduate School, the DHS Centers of Excellence, and the Homeland Security Consortium Universities.
* Identify the availability of emergency preparedness and planning training opportunities in your area.
* Identify the special training centered around CISR.

**2. Discussion Topics:**

* Who can enroll in the DHS/FEMA EMI?
* What is the relationship between training for general continuity of operations planning and the continuity of government planning (COOP and COG)?
* How would the all hazards approach influence the training curriculum needed?
* Find out and assess the Integrated Emergency Management Course format and philosophy.
* Which university departments are known to house emergency management or homeland security degree programs? Search the http://www.training.fema.gov/emiweb/edu/collegelist/ under the "college programs" section.
* Which parts of the critical infrastructure does the Center for Domestic Preparedness cover?
* Are most of these classes classified or open to the public?
* Is there an accreditation process in place for such degree programs?
* What is the status of the DHS/FEMA credentialing program?

**3. Required Reading:**

Emergency Management Institute Course Catalog.

Center for Domestic Preparedness Course Catalog.

Naval Post-Graduate School Course Catalog.

Texas A&M University, Louisiana State University, New Mexico Tech University Continuing Studies Course Catalog.

**lesson 14 topic**: **testing and exercises**

**1. Lesson Goals/Objectives:**

* Explain the DHS/FEMA National Exercise (NLE) Program.
* Describe the evolving role of the National Leaders Exercise Program.

Identify the difference between full field exercises, table top exercises, notice and no notice exercises, and "Thunderbolt" exercises.

* Explain how exercises test an area's planning and training, as well as overall readiness.
* Recognize the exercises designed around CISR.
* Identify and describe the challenges of conducting exercises, composing scenarios, and building trust.

**2. Discussion Topics:**

* Why does the NLE often evoke considerable controversy?
* How are exercises funded at the Federal, State, local, tribal, and territorial level?
* Should exercises contain multiple disasters occurring at once or focus on one?
* What is the controller role in an exercise?
* Refer to the DHS/FEMA guidance for exercises — the Homeland Security Exercise and Evaluation Program (HSEEP) — what is the role of evaluation?
* Look up one example of an After Action Report (AAR).
* Notice the difference between AARs and Corrective Action Recommendations.

**3. Required Reading:**

DHS/FEMA Homeland Security Exercise and Evaluation Program Guidance, <https://hseep.dhs.gov/pages/1001_HSEEP7.aspx>.

National Leader Exercise 2011, New Madrid Earthquake, After Action Report, <http://www.fema.gov/pdf/media/factsheets/2011/nle11_quick_look_report.pdf>.