Lesson 12 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 12 TOPIC: CISR INCIDENT MANAGEMENT EXERCISE (STUDENT ACTIVITY)

Today's class involves an interactive, discussion-based table top exercise (TTX) driven by a terrorism- or major hurricane-based scenario, per the discretion of the instructor. The TTX scenario will consist of four modules (Pre-incident, Warning, Activation, and Extended Response) in chronological order. The TTX will focus on the roles and responsibilities of, and the interaction between FSLTT governments; the private sector; and the general public in the context of an emergent threat as well as an incident in progress. Learners will be pre-assigned specific roles to play during the TTX and will develop a point paper addressing their specific responsibilities and anticipated actions during the various phases of the emergent threat/incident response *(See specific instructions provided in Course Introduction above)*. Participant discussion will focus on communication and information sharing, coordination, integration of capabilities, and problem identification and resolution. A complete outline of each exercise scenario and corresponding discussion modules is located at **Attachment 1 (Terrorism Scenario) and Attachment 2 (Hurricane Scenario)**.

Suggested Learner TTX Roles (Terrorism Scenario):

- DHS Senior Leaders (HQ Leadership, NPPD, TSA)
- FBI Senior Leaders
- State Governors
- State and Large Urban Area Emergency Managers
- Major Urban Area Chiefs of Police
- Fusion Center Directors
- ISAC Directors
- NICC Director
- DHS Protective Security Advisors
- Critical Infrastructure Security Directors (Transportation—all modes, commercial facilities, government facilities)

Suggested Learner TTX Roles (Hurricane Scenario):

- DHS Senior Leaders (HQ Leadership, FEMA)
- State Governors
- State and Large Urban Area Emergency Managers

- FEMA NRCC Director
- ISAC Directors
- NICC Director
- DHS Protective Security Advisors
- Critical Infrastructure Emergency Preparedness Directors (Transportation—all modes, commercial facilities, government facilities, energy, communications, water/wastewater)

1. Lesson Goals/Objectives:

- Understand the various roles and responsibilities of government, the private sector, and the general public in the context of an emergent manmade or naturally occurring threat as well as an incident in progress.
- Become familiar with the critical infrastructure key incident management nodes and the processes through which they interact as discussed in the NPF and the NRF and its Critical Infrastructure Support Annex.
- Understand the short and long term impacts on the sectors resulting from a major emergent threat or incident.
- Become familiar with and assess public-private sector information and intelligence sharing in the context of incident management.
- Become familiar with the processes and mechanisms used to build situational awareness and facilitate public-private critical infrastructure-related prevention, protection, response, and recovery activities during incidents.

2. Discussion Topics:

- What are the roles and responsibilities of the various NIPP partners vis-à-vis national incident management?
- What are the key government and private sector incident management nodes according to the NIPP 2013 and the NRF?
- How are information and intelligence shared between the various public and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? Does the process work? How could it be improved?
- What actions do the various critical infrastructure sectors take in response to an emergent threat or national level NTAS elevation? How does that process work? What are the near and long term ramifications across the sectors?
- How is situational awareness maintained among the various NIPP partners during incident response?
- How are private sector requests for information and assistance assessed and addressed during incident response operations according to the NRF Critical Infrastructure Support Annex?

3. Required Reading:

U.S. Department of Homeland Security, *National Prevention Framework*, May 2013, http://www.fema.gov/media-library-data/20130726-1913-25045-6071/final_national_prevention_framework_20130501.pdf

U.S. Department of Homeland Security, *National Response Framework*, 2013, http://www.fema.gov/media-library/assets/documents/32230?id=7371http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.

U.S. Department of Homeland Security, National Response Framework, CIKR Support Annex, May 2013, http://www.fema.gov/media-library-data/20130726-1914-25045-5422/nrf_support_annex_cikr_20130505.pdf

IS 800, *National Response Framework: An Introduction*,. http://emilms.fema.gov/IS800b/index.htm

IS 821, *Critical Infrastructure Key Resource Support Annex.* http://training.fema.gov/is/courseoverview.aspx?code=IS-821.a

4. Additional Recommended Reading:

https://www.fema.gov/national-incident-management-system

ATTACHMENT 1
CISR INCIDENT MANAGEMENT EXERCISE
TERRORISM SCENARIO

MODULE 1: PRE-INCIDENT

1. Scenario Build

- A new video is released by a well-known terrorist organization on several internet sites. The video describes "striking the infidels where they are most vulnerable," using advanced weapons and tactics. The spokesperson references the possibility of attacks targeting European and American interests worldwide, with particular emphasis on transportation, commercial facilities and sports venues, religious worship sites, iconic symbols, financial centers, and government buildings.
- Daily news reports include brief mention of the video. Government sources acknowledge the video, but take no further public action.
- Officials in Europe apprehend a person described as being an "Operational Chief to multiple terrorist cells worldwide." The man's name is withheld, but he provides information describing future attacks within Europe (timing unspecified) and admits to planning a failed attack in Istanbul late last year.
- Violent extremist group Internet "chatter" and known-terrorist-organization's website activities are on the increase, with focused pronouncements of violent intent with near-term implications. The number of websites featuring homemade bomb-making instructions and chemical agent applications has proliferated greatly in recent months.

2. One Month Later

- The main multi-modal train station and several popular tourist sites are attacked in a major European capital city. A man carrying a backpack is apprehended by local authorities after his suicide vest failed to completely detonate inside the station while awaiting the arrival of a fully loaded passenger train. The bomb injured six commuters and severely burned the suspect. The suspect is quickly taken to a local detention facility for questioning after being treated for second-degree burns at a local hospital. A second bomb explodes in a crowded plaza outside the main train station, serving as an immediate rally point for those fleeing the station. Twenty people are killed and three dozen more are wounded. Traces of the bomber's clothing and personal effects have been found on scene, but he is believed to have been killed during the attack. It is believed that the two separate bombing incidents are linked based upon preliminary analysis of video surveillance footage taken in and around the station.
- The transit bombing suspect is identified as a militant associated with a European affiliate of the terrorist organization. He states that his planned attack was to serve as a warning to all countries with "Criminals assaulting his god." He is quoted as saying "When the criminal governments fall, we will be triumphant." The suspect

has also provided information that leads to the conclusion that there are additional active cells elsewhere in Europe that may be in the final stages of operational planning and mission rehearsal.

- The affected Government has elevated security around governmental facilities, major transportation hubs and other potential "mass gathering" targets across the country. The city's metro system remains open, but is operating under heightened security conditions.

3. Discussion Questions

- What types of information would European authorities likely be sharing with U.S. government counterparts at this time? What information would the U.S like to be shared?
- What types of intelligence likely would be circulating domestically within the Federal government, between Federal and local authorities, and between government and the private sector?
- Would there be any likely changes recommended to protective measures across the critical infrastructure sectors based on an event occurring abroad with no corresponding credible threat in the United States?
- What types of prevention/protection activities would your jurisdiction/agency/sector likely be engaged in at this time?
- What would the various key nodes of the National Prevention and Response Frameworks be doing at this time?

MODULE 2: WARNING

1. Scenario Build

- During the week after the terrorist attack on the mass transit system in the major European capital, the FBI and DHS have received increased reporting of planning for possible near term attacks on commercial facilities, government facilities, national monuments, financial centers, and the transportation sector (highways, rail, mass transit, ferries, and ports) across the United States.

- Exact methods and timing of these potential attacks are unknown, but the various sources from which the reporting has originated have been deemed credible.

- A tape is released on the Internet and on television by an affiliate with known terrorist operations in Europe and Southwest Asia which trumpets forthcoming attacks in the United States and makes additional claims regarding the possession of an unspecified "WMD" capability.

- Several major news agencies receive phone calls from unidentified sources warning of an impending "reign of terror" in the United States.

- In response to this threat reporting, the FBI and DHS issue a joint intelligence

bulletin warning of possible attacks against commercial facilities, government facilities, and surface transportation and conduct national conference calls and provide briefings on the threat to critical infrastructure sector partners.

- DHS and the FBI issue a Joint Intelligence Bulletin with specific emphasis on commercial facilities, national monuments, government facilities, and the transportation sector, as well as for the geographical areas of the National Capital Region and New York State Region.

2. Discussion Questions

- What are your major personal and organizational concerns at this point?
- Would types of information updates should be provided to the private sector or State and local government officials at this time? If so, how would this process work?
- What are the essential elements of intelligence and related information required by your jurisdiction, agency, community, industry?
- What preventive/protective measures would government and the private sector likely put in place at this point? How would they be communicated to one another?
- What recommendations would these entities make regarding the NTAS threat level? How does this process work?
- In the absence of government guidance or action, would the private sector be likely to initiate any changes in protective measures and emergency response posture?
- If so, would these changes be individually considered or would industry within a sector come together and collaborate?
- What types of activities would the various key nodes of the NIPP partnership framework be engaged in at this point?
- How would the NIPP partnership act to better understand the nature of and take action to mitigate the unspecified "WMD" threat? Are critical infrastructure owners/operators and mass public venue security officials prepared to deal with chemical and other potential WMD threats?

MODULE 3: ACTIVATION

1. Scenario Build

- **Today 8:32 a.m. EDT**
    - Two large rental trucks drive into the Ft. Pitt and Squirrel Hill tunnels in Pittsburgh, Pennsylvania, and explode. As a result, there are numerous unconfirmed casualty reports, and the major interstate network servicing the greater Pittsburgh area is closed except to emergency vehicles. It is later determined that 55 commuters are killed and over one hundred are injured.

- **8:35 a.m. EDT**
    - An IED is detonated in Washington, D.C.'s Capitol South Metro Station; six people are killed and 30 people are injured. Two metro lines have been closed to the public inside the Beltway pending further investigation.

- **8:40 a.m. EDT**
    - An IED is found outside the main entrance of a crowded public shopping mall near the Pentagon in Arlington, Virginia. The IED is cordoned off and disarmed without incident. The mall and surrounding commercial businesses are temporarily closed to the public while further bomb sweeps are conducted.

- **9:00 a.m. EDT**
    - In Chicago, a minivan is detained in front of Chicago's O'Hare Airport for loitering in the Passenger Drop-off Zone. Upon investigation, the minivan is found to be carrying ten unidentified "chemical" canisters packed with homemade explosive. The driver is taken into custody and held at a local FBI detainment facility. O'Hare Airport remains open to the public, although under heightened security conditions.

- **9:18 a.m. EDT**
    - In Indianapolis, two bombs explode in the vicinity of the Soldiers' and Sailors' monument. Six people are injured in the blast. There are no fatalities. Local law enforcement authorities and the FBI are investigating surveillance camera video of the area. The immediate area around the monument has been closed to the public and traffic has been rerouted pending further investigation.

- **10:00 a.m. EDT**
    - An imminent alert is issued under NTAS for airports, tunnels and bridges, mass transit, commercial facilities, government facilities and national monuments and icons. All other sectors are under an NTAS elevated alert .

- **12:00 a.m. EDT**
    - Internet video is released from a terrorist affiliate claiming responsibility for the attacks on the United States. The video is several minutes long and includes the following statement: "A first blow has been struck, the suffering of the oppressors has begun and their nightmare will continue. Every city of evil will be touched; the child of every criminal will know fear and death as our children have known it."

2. Discussion Questions

- What are your principal concerns and priorities at this time?
- How does the "WMD Factor" complicate emergency protection and response activities?
- What types of intelligence information would likely be provided at this time, to whom, and by whom?
- What protection and emergency response actions are Federal, State and local government and private sector authorities taking following these events?
- How is situational awareness being maintained across government and between the government and the private sector at this point?
- Do you have sufficient authorities, capacities, and resources to deal with the events above as they impact your area of responsibility? If not, where do you go for help?
- What key nodes of the NRF are operational at this point?
- What actions are being undertaken by the sector operations centers, ISACs or other information sharing entities?
- How would you handle internal and external messaging of the events as they pertain to you and your organization, community, jurisdiction, or sector? How is this messaging coordinated with external partners to include various levels of government and industry?

MODULE 4: EXTENDED RESPONSE

1. Scenario Build

- **Two weeks from the Attacks in the United States**
    - DHS releases a statement from the Secretary revising the NTAS alert with guidance for government facilities, commercial facilities, national monuments, and the transportation sector (highways, rail, ferries, mass transit, ports and airports).
    - The FBI announces that they have arrested three men associated with the attacks and that their investigation will continue. At least one of the men is believed to be connected to the Berlin mass transit bombings as well.
    - The national and international impacts of the terrorist attacks in the United States have been extraordinarily high, cascading across the sectors domestically and internationally. The stock market has fallen to recession levels, with downward trends globally.
    - State and local officials have severely taxed their local first responder communities over the course of the period of heightened alert following the attacks. Private sector security and emergency response forces have been similarly stressed. The costs of a "new threshold for security" are being felt to varying degrees across the sectors.

- Public messaging across levels of government has been fairly consistent in the two weeks following the attacks. Public confidence remains low and apprehension regarding follow-on attack remains high.

- **Three weeks from the attacks in the United States**

  - DHS releases a statement from the Secretary cancelling the NTAS alert.

  - Pipe bombs are found at a high school in Chicago, Illinois. Two students are arrested.

  - There are numerous media reports of other threats involving the use of IEDs being reported to local authorities ranging from attacks against transit, schools, commercial facilities, and national monuments and icons. Public apprehension remains high.

2. Discussion Questions

- What are your principal concerns in this phase of incident management?
- What types of enhanced prevention and protection activities would you be continuing at this point? Do you have sufficient resources? If not, where do you go for help?
- What impacts have the various NTAS alerts had on your organization/ constituency?
- What is the "new normal" for your agency, jurisdiction, corporation, sector at this point? How do you resume your operations?
- What are the long term economic and psychological implications of the attacks from your perspective?
- How do we regain public confidence in the aftermath of the attacks?
- What are the major lessons that you have learned from this exercise?

ATTACHMENT 2
CISR INCIDENT MANAGEMENT EXERCISE #2
HURRICANE SCENARIO

MODULE 1: PRE-SEASON

1. Scenario Build

- The Atlantic hurricane season extends from June 1st through November 30th each year, with the peak hurricane threat extending from mid-August to late October. Annually, an average of 11 tropical storms develops in the Atlantic Ocean, Caribbean Sea, or Gulf of Mexico, six of which typically become hurricanes. This year's hurricane season is expected to be particularly active. The National Hurricane Center (NHC) is predicting 12-18 named storms, 6-8 hurricanes, and 2-3 major hurricanes. In comparison, the NHC's historical averages from 1966-2009 are 11.3 named storms, 6.2 hurricanes, and 2.3 major hurricanes.

- While hurricanes and their accompanying storm surges pose the greatest threat to life and property, tropical depressions and tropical storms can also be devastating. In addition, storm surge can account for a large number of casualties and personal property damage. Flooding resulting from storm surge or heavy rains and severe weather, such as tornadoes, can also cause loss of life and extensive damage.

- Preparation for, response to, recovery from, and mitigation against hurricanes require a coordinated response involving Federal, State, local, and tribal governments, the private sector, and nongovernmental organizations. This in-classroom exercise will be focused on the coordinated actions of the critical infrastructure community in preparation for and response to a generalized hurricane threat as well as a specific catastrophic storm.

2. Discussion Questions

How do the various critical infrastructure protection and resilience public and private sector partners prepare jointly and coordinate with each other prior to the onset of hurricane season each year? What form does this coordination take? How does the agency/organization that you represent fit into this scheme?

- Is your organization/entity a participant in locally-based NIMS structures?
- What types of analytical products, storm forecasts, best practices information, etc., are available to help guide critical infrastructure protection and resilience partner hurricane preparedness and planning activities? How is this information communicated within the NIPP framework?
- What types of assistance can the National Infrastructure Simulation and Analysis Center provide State and local agencies and the private sector prior to the onset of hurricane season?
- What are the most significant concerns of the agency/organization that you represent at this stage of hurricane season?

MODULE 2: PRE-LANDFALL (H-HOUR)

1. Scenario Build

- At the end of August, a tropical disturbance formed off the coast of Africa. On September 1st, the tropical disturbance was designated as Tropical Storm Heidi, located west of the Cape Verde Islands. During the next few days, Heidi continued to strengthen and was officially designated a hurricane on September 2nd. By the early morning hours of September 4th, Heidi was upgraded to a major hurricane with sustained winds of 115mph based on aircraft reports and satellite imagery. Heidi passed near the Turks and Caicos Islands as a Category 3 hurricane on September 7th, with sustained winds of more than 120mph and entered the Gulf of Mexico on September 9th with little change in strength. The governors of Texas and Louisiana and big city mayors across the region plan to announce mandatory evacuations of citizens. Both State governors declare major emergencies and request Federal assistance. Initial Federal emergency equipment and supply caches are moved to forward staging areas outside the projected hurricane impact zone.

2. Discussion Questions

- What actions does the organization/entity that you represent take at the 48 hours prior to landfall decision point? At 24 hours? At 12 hours?
- What are the principal concerns of the agency/organization that you represent at this stage? What are your information sharing priorities?
- How do the various critical infrastructure protection and resilience public and private sector partners coordinate with each other and maintain a common situational awareness prior to hurricane landfall? What form does this coordination take? How does the agency/organization that you represent fit into this scheme?
- What types of analytical products, storm forecasts, best practices information, etc., are available to help guide critical infrastructure protection and resilience partner actions at this stage? How is this information communicated within the NIPP framework?
- What types of assistance can the National Infrastructure Simulation and Analysis Center provide State and local agencies and the private sector prior during this stage? (storm surge, wind damage, population displacement, specific sector-level impacts)
- What is the role of DHS at this stage? FEMA? State and local officials with critical infrastructure protection and resilience responsibilities?
- What key nodes of the NRF Critical Infrastructure Support Annex are activated at this point, and how do they interact with one another?
- What government policies and public messaging processes come into effect during this stage that may impact critical infrastructure owner/operators? (Evacuation decisions, continuity of operations site activations, contra-flow transportation plans, MOUs with private sector entities, senior official public proclamations, etc.)
- What are the priorities of private sector entities within the projected path of the

hurricane at this stage?

MODULE 3: LANDFALL (H-HOUR)

1. Scenario Build

- From September 9th through the 12th, Hurricane Heidi moved along a Northwest path in the Gulf of Mexico, threatening Southwest Louisiana and the Northern Texas Coast. There was much uncertainty as Heidi turned slowly north and then northeast over the next two days before finally making landfall in Southeastern Louisiana west of Grand Isle, LA, as a Category 4 storm during the early morning hours of September 14th.

- Widespread storm surge flooding occurred in Southeast Louisiana, with Federal protection levees overtopping in the metro New Orleans area, producing pockets of significant flooding in low lying areas along the Mississippi River. In addition, Heidi produced 8-10 inches of rainfall which aggravated the storm surge flooding and brought many of the major rivers north of Lake Pontchartrain into flood stage. Although Heidi weakened upon moving inland, strong winds and torrential rains make movement impossible even in areas that were not inundated by flood waters.

- Presidential disaster declarations are made for the impacted counties in TX and LA. Federal incident coordination structures and field offices are activated.

- Over 2.5 million people are displaced from the region running from Northeast Texas to New Orleans. Additionally, the following major infrastructure damages/disruptions are noted:

    - Over 4M customers are without power in the region, to include numerous major hospitals and special needs facilities
    - Numerous major transformer towers are down in SW Louisiana
    - Major rail and highway networks are shut down and/or damaged
    - The I-10 bridge across Lake Pontchartrain has been dismembered in several places; other secondary and tertiary bridges are down throughout the region
    - Two major nuclear power plants in the region have suffered minor damages, but have been placed in shut down mode
    - Over a dozen major oil and natural gas pipelines are inoperative, with extent of damages unknown
    - More than one hundred Gulf oil platforms have been evacuated; several are now “free-floating”
    - Six major oil refineries in the region have been extensively damaged and will require long repair times
    - Cellular communications have been significantly degraded throughout the region; cell towers are down across the area
    - Dozens of major chemical plants and hazmat facilities are under 4-8 feet of water; numerous chlorine rail tankers are overturned on site throughout the

area
  - The Mississippi River channel is blocked by floating debris and sunken vessels in numerous locations south of New Orleans and is temporarily closed to commercial traffic; major petroleum and agricultural import/export operations have been suspended
  - Gasoline is in short supply across the region; first responder operations have priority
  - Minor civil disorder and looting activities are reported in several cities and towns in the impacted area

2. Discussion Questions

- What are the principal concerns of the agency/organization that you represent at this stage? What are your information sharing requirements at this stage? How are you getting the information you need?
- How do the various critical infrastructure protection and resilience public and private sector partners coordinate with each other and maintain a common situational awareness following hurricane landfall? What form does this coordination take? How does the agency/organization that you represent fit into this scheme?
- What types of analytical products, imagery, damage assessment products/services are available to help guide critical infrastructure protection and resilience partner actions at this stage? How is this information communicated within the NIPP framework?
- What is the role of DHS at this stage? FEMA? State and local officials with critical infrastructure protection and resilience responsibilities? Other Federal agencies?
- What key nodes of the NRF Critical Infrastructure Support Annex are activated at this point, and how do they interact with one another?
- What government policies and public messaging processes come into effect during this stage that may impact critical infrastructure owner/operators? (Evacuation decisions, continuity of operations site activations, contra-flow transportation plans, MOUs with private sector entities, senior official public proclamations, etc.)
- What are the priorities of private sector entities within the damage footprint of the hurricane at this stage?
- How are private sector requests for assistance communicated to and considered for action by State and Federal governments post-landfall?
- How are private sector facility security concerns addressed post-landfall? Damage assessments? Civil disorder and looting?
- How are critical infrastructure restoration priorities determined by government and industry at this point?
- How do State and local officials deal with the issue of private sector restoration reentry and access? How does the Federal government weigh in on this issue?

MODULE 4: POST-LANDFALL TO RECOVERY (2 DAYS TO 2 MONTHS FROM LANDFALL)

1. Scenario Build

- By September 15th, Heidi had weakened to a tropical storm and was located in eastern Mississippi, moving generally N-NE. Extensive rainfall and winds of 10-20 mph are noted along the path of the storm. By the 17th, Heidi has been downgraded to a tropical depression moving northward into the Ohio Valley and into Canada.

- Federal, State and local officials are dealing with more than a million shelter inhabitants and otherwise displaced individuals. Property damage to residences and businesses across the hurricane impact zone has been extensive.

- Dozens of important critical infrastructure facilities are under 4-8 feet of standing water. Suspected hazmat leaks are prevalent throughout the area.

- Long-term impacts to the regional transportation network and power grid are extensive. Over 2.5M customers remain without power for weeks into the event.

- Loss of pipeline capacity is causing major gas price hikes all along the Gulf Coast and Eastern Seaboard. Oil production in the Gulf area will take several months to be restored; regaining full production capacity remains doubtful.

- Most communications in the area have been restored within the first week of the event.

- Local water and waste water treatment facilities are inoperative across the region, exacerbating infrastructure restoration/recovery operations.

2. Discussion Questions

- What are the principal concerns of the agency/organization that you represent at this stage? What are your information sharing requirements at this stage? How are you getting the information you need?
- How do the government and private sector organize to support long term restoration and recovery operations? How do things "get turned back on" and in what sequence?
- What the major concerns at the sector level during this stage?
- How are key decisions made and priorities established between government and industry during this stage (i.e. to rebuild vice relocate, etc.)? How are these communicated?
- What is the role of DHS at this stage? FEMA? State and local officials with critical infrastructure protection and resilience responsibilities? Other Federal agencies?
- What government policies and public messaging processes come into effect during this stage that may impact critical infrastructure owner/operators?
- How are private sector requests for assistance communicated to and considered for action by State and Federal governments in this stage?
- How are major lessons from this event applied to the next cycle of preparedness?
- Does the NIPP framework adequately address long term recovery issues?
- What are the major takeaways that you have from this exercise?