ATTACHMENT
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?