

EV 09 – Critical Incidents  
 Session 04 – LEPM/Targets  
 LD 43 – Emergency Management

**Date Revised:** 12/09/19

**Event Goal:** To teach recruit officers how to respond to a critical incident.

**Session Goal:** This module uses The National Strategy of Critical Infrastructure and Key Assets List to assist responders in identifying local potential targets of terrorism, and why terrorists may attack them. The law enforcement responder will be able to conduct vulnerability assessments of potential targets.

**Learning Objectives:**

- Identify the concepts of a threat and vulnerability assessment **[43.III.A]**
- Identify critical infrastructure sectors and key assets **[43.III.B]**
- Identify threat assessment rationale **[43.III.C]**
- Recognize why terrorists would target critical infrastructure and key assets
- Identify the preparation of vulnerability and risk analysis of potential Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) targets within local communities

**Session Time:** 1.5 Hours

<p><b>Resources:</b></p> <ul style="list-style-type: none"> <li>• Power Point</li> <li>• Audio/video device</li> <li>• Classroom with tables</li> <li>• White board</li> <li>• Dry-erase markers</li> </ul>	
<ul style="list-style-type: none"> <li>• <b>Session Summary:</b> The student will be able to list critical infrastructures and key assets to identify terrorist targets in the community and why terrorists would attack them.</li> </ul>	
Outline	Instructor Notes
<p>I. Targets</p> <p>A. Critical Infrastructure Sectors- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. While this document identifies targets in categories of critical infrastructure and key assets at a national level, each category can be related to the local jurisdictional level <b>[43.III.B]</b>  <b>[LD3,26,21] [1]</b></p> <ol style="list-style-type: none"> <li>1. Identifying and assuring protection of infrastructures and assets that we deem most critical.</li> <li>2. Providing timely warning and assuring protection of those infrastructures and assets facing a specific, imminent threat.</li> <li>3. Assuring protection of other infrastructures and assets that may become terrorist targets over</li> </ol>	<p>Facilitated discussion (1.5 hours)</p> <p><b>[1] ASK</b> – Tell me some possible targets in L.A.?</p> <ul style="list-style-type: none"> <li>• Answer-Looking for amusement parks, sporting event locations, monuments, LAX etc.</li> </ul> <p><b>[LD43]</b> – Identifying critical infrastructure sectors  <b>[LD26]</b> – Response to a U.O.  <b>[LD21]</b> – Adding critical infrastructures to your usual patrol route</p>

EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

<p>time by enabling a collaborative environment in which federal, state, and local governments, as well as the private sector can offer protection.</p> <ul style="list-style-type: none"><li>a. Agriculture and Food<ul style="list-style-type: none"><li>1) Supply chains for feed, animals, and animal products</li><li>2) Crop productions and supply chains of seed, fertilizer, and other necessary related materials.</li><li>3) The postharvest components of food supply chain from processing and packaging through storage and distribution to retail sales, institution food services and restaurant or home consumption.</li></ul></li><li>b. Water-This sector consists of two basic, yet vital, components-fresh water supply and waste water collection and treatment. The public water systems depend on reservoirs, dams, wells, and aquifers, as well as treatment facilities, pumping stations, aqueducts and transmission pipelines. Waste water utilities collect and treat sewage and process water from domestic, commercial, and industrial sources. It also includes storm water systems that collect and sometimes treat storm water runoff.<ul style="list-style-type: none"><li>1) Physical damage or destruction of critical assets, including intentional release of toxic chemicals.</li><li>2) Actual or threatened contamination of water supply.</li><li>3) Cyber attack on information management systems that control facilities, and determine routing of water supply and control storage facilities.</li><li>4) Interruption of services received from another infrastructure such as electrical power and transportation services.</li></ul></li><li>c. Public Health- This sector consists of state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceuticals stockpiles.</li><li>d. Emergency Services- This sector consists of</li></ul>	<p><b>[LD3]</b> –Critical Sites</p>
---	-------------------------------------

EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

highly mobile teams of specialized personnel and equipment including fire, fire rescue, Emergency Medical Services (EMS), law enforcement, and emergency management resources that react to save lives and property in the event of accidental and natural disasters or terrorist attack.

- e. Defense Industrial Base- This sector consists of the private sector defense industry and supporting military facilities that manufacture and provide the equipment, materials, services, and weaponry used by our armed forces.
- f. Telecommunications- This sector provides telecommunications through voice and data services to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet and private enterprise networks. The PSTN provides switched circuits for telephone, data, and leased point-to-point services. Enterprise networks are dedicated networks supporting the voice and data needs and operations of large companies and industries.
- g. Energy- This sector is commonly divided into two segments- electricity and oil and natural gas. The electric industry services almost 130 million households and institutions. Almost every form of productive activity-whether in businesses, manufacturing plants, schools, hospitals, homes, or agriculture- requires electricity. Production of other forms of energy, such as oil or nuclear materials, require the use of large amounts of electricity.
- h. Transportation- This sector consists of several key modes of transportation: aviation, rail, highways, trucking and busing, pipelines, maritime traffic, and public mass transit.
  - 1) Aviation- The aviation system is vast and contains thousands of entry points. The aviation system consists of two main parts:
    - a) The airports and associated assets needed to support their operations,

EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

<p>and the aircraft served by those airports</p> <p>b) Aviation command, control communications, and information systems needed to support and maintain the safe use of our national airspace</p> <p>2) Railroads- The nation’s railway system is vast and complex with multiple points of entry. Railroads are different in design, structure and purpose. Trains are confined to specific routes and are controllable. Railroads have bridges and tunnels that are subject to destruction; however, such destruction would usually resort in a localized problem. A vulnerability of the entire system is that thousands of miles of track exist in an unguarded condition and are subject to destruction.</p> <p>3) Highways, Trucking, Busing- Without resources of highways trucking, and busing, the movement of people, goods, and services would be greatly impeded and almost every other infrastructure would be affected adversely. Components of the infrastructure include highways, roads, interchanges, bridges, tunnels, trucks, buses, maintenance facilities, and roadway crossings. Choke points exist in each component and present unique security challenges. Choke points are those areas or points along the highways or railway routes that, if damaged or destroyed, would impede the flow of traffic.</p> <p>4) Pipelines- The United States has thousands of miles of pipelines- many of which are underground- that carry oil, refine petroleum products, and natural gas. Most elements of pipelines can be repaired or by-passed quickly to restore services in the event of an attack. Loss of a pipeline for a long period could seriously impact the industries and facilities dependant on the product.</p> <p>5) Maritime- The maritime infrastructure</p>	
--	--

EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

includes ports and their associated structures, ships and passenger transportation systems, coastal inland waterways, locks, dams, and canals. It also includes the system of railroads and pipelines that connect the water borne system to the inland system. There are 361 seaports in the United States, and through these ports pass tons of cargo each year. The volume of traffic and diversity of cargo makes a complete inspection of every vessel and cargo an extremely difficult undertaking.

- 6) Mass Transit Systems- Each year, passengers take approximately 9.5 billion trips on public transportation in the U.S. Mass transit carries more passengers daily than does air or rail transportation. Cities rely on their mass transit systems to move the workforce, and they rely on mass transit as a means of evacuation in an emergency. Mass transit systems were designed for ease of access, which makes it difficult to monitor all points of entry. An explosive material can be carried aboard mass transit systems with ease.
  - i. Banking and Finance- This sector consists of a variety of physical structures such as buildings and financial utilities, as well as highly skilled human capital. Physical structures to be protected house retail or wholesale banking operations, financial markets, regulatory institutions, and physical repositories for documents and financial assets. There are approximately 26, 500 Federal Deposit Insurance Corporations (FDIC) insured financial institutions within the U.S. The financial utilities infrastructures include electronic devices such as computers, storage devices, and telecommunication networks.
  - j. Chemical Industry and Hazardous Materials- This sector provides products essential to the U.S. economy and standard of living. The chemical industry manufactures products that are fundamental elements of other

EV 09 – Critical Incidents  
 Session 04 – LEPM/Targets  
 LD 43 – Emergency Management

<p>economic sectors. For example, it produces fertilizer for agriculture and chlorine for water purification. Additionally, more than \$97 billion of the sector’s products go to healthcare. Currently, the chemical sector is the nation’s top exporter accounting for 10 cents out of every export dollar <b>[LD41]</b></p> <p>k. Postal and Shipping- Americans depend heavily on the postal and shipping sector. Each day, we place more than two-thirds of a billion pieces of mail into the U.S. postal system, and each day more than 300,000 city and rural postal carriers deliver that mail to more than 137 million delivery addresses nationwide. In all, the vast network operated by the United States Postal Service (USPS) consists of a headquarters in Washington D.C., tens of thousands of postal facilities nationwide, and hundreds of thousands of official drop-box locations.</p> <p>B. Key Assets-Key Assets are comprised of facilities, sites, and structures whose destruction or disruption could have serious consequences. The category includes sites and structures that are not critical to our national defense and alone may not be vital to the continuity of critical services, but whose destruction might produce significant loss of life and could have serious impact on public health and safety, public confidence, and the economy. <b>[LD3,21]</b></p> <p><b>[2]</b></p> <ol style="list-style-type: none"> <li>1. National Monuments Icons- This category consists of U.S. national monuments and icons (e.g., Mt. Rushmore, the Statue of Liberty, the Lincoln Memorial, national parks, etc). The protection of national monuments and icons typically combines the authorities, responsibilities and resources of federal, state, and local jurisdictions, and in some cases, private foundations. The Department of the Interior (DOI) is the lead federal department with primary jurisdiction over national icons and monuments.</li> <li>2. Nuclear Power Plants- This category is comprised of nuclear power plants, representing about 20% of our nation’s electrical generation capacity. The U.S. has 104 commercial nuclear reactors in 31 states. Nuclear power plants are among the most strongly constructed structures in the country,</li> </ol>	<p><b>[LD41]</b> – Hazardous materials incident risk as far as response</p> <p><b>[2] ASK</b> – What do you think would be the benefit to attacking monuments?</p> <ul style="list-style-type: none"> <li>• Answer – The possibilities for mass casualties and symbolism.</li> </ul> <p><b>[LD3]</b> –Critical Sites</p> <p><b>[LD21]</b> – Adding critical infrastructures to your daily patrol</p>
---	--

EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

<p>and a terrorist attack would be considered a significant security and psychological event.</p> <ol style="list-style-type: none"><li>3. Dams- Some of the larger and more symbolic dams are major components of other critical infrastructure systems, providing water and electricity to large populations, cities, and agriculture complexes. There are approximately 80,000 dam facilities identified in the national inventory. The federal government is responsible for roughly 10% of the dams, whose failure could cause significant loss of life, property damage, or public health and safety consequences. The remaining dams belong to state or local governments, utilities, and corporate or private owners.</li><li>4. Government Facilities- This category is composed of buildings the federal government owns, and others leased from the private sector. Government organizations also occupy buildings used by a variety of nongovernmental tenants, such as shops and restaurants. The General Services Administration (GSA) is the principle federal agency responsible for the management of federal government facilities.</li><li>5. Commercial Key Assets- This category consists of prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational past times. Daily protection of such facilities is the responsibility of their commercial owners and operators in close cooperation with local law enforcement. The federal government's responsibility to this key asset is providing timely threat indicators and warnings.</li></ol> <p>C. Target Selection- Developing an effective strategy for critical infrastructure and key asset protection requires a clear understanding of the threats we face and the potential consequences they entail. Targets are selected to generate fear, social impact, political change, and financial chaos.</p> <p>D. Benefits to Terrorists Attacking Critical Infrastructure- Critical infrastructure sectors are independent. Given the extent to which our daily lives rely on them, a successful attack to disrupt or destroy them could have tremendous impact beyond the immediate</p>	
--	--

EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

target, and could continue to resurface thru other correlated or independent infrastructures long after the immediate damage is done. Terrorists are inventive and resourceful in terms of target selection, as well as in their selection and use of specific instruments of violence and intimidation to achieve their objectives; terrorists may choose to target critical infrastructures and key assets as a low-risk means to generate mass casualties, shock, and panic.

1. Direct infrastructure affects- disruption or arrest of the functions of critical infrastructure of key assets thru direct attacks on a critical node, system, or function. Disruption or destruction of the asset itself brings about damage to the sector that is desired
  2. Indirect infrastructure affects- Cascading disruption and financial consequences for government, society, and economy thru public and private sector reactions to an attack. An example would be the use of hijacked airplanes to destroy the World Trade Center (WTC). Because of the large involvement of financial interests in the WTC, world financial markets were deeply affected.
  3. Exploitation of infrastructure- Exploitation of elements of infrastructure to disrupt or destroy another target. While the WTC was the target, the effects crippled the airlines because people were afraid to fly; tourism and other industries suffered catastrophic results.
- E. Vulnerability Analysis-Vulnerability is defined as the characteristics of an asset's design, location, or operation/use that render it susceptible to damage, destruction, or incapacitation by terrorists or other intentional acts, mechanical failures, and natural hazards **[43.III.A]**
- F. Protection of Targets - Local governments are the front lines of protection against terrorist attacks. They play a key role in preparing for emergencies and in developing plans for the protection of residents and facilities within their jurisdictions. Initially every incident is local and, therefore, involves the local law enforcement responder **[43.III.C]**
1. Conduct an inventory of assets- It is probably a mistake to view a critical infrastructure component or key asset as being a probable terrorist target or not. In almost every instance it



EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

<p>is not known what specific assets are being viewed as targets by the terrorists</p> <ol style="list-style-type: none"><li>2. Identify and assess vulnerabilities- Each asset identified through the inventory process should be thoroughly examined to determine whether characteristics of the asset’s design, location, or operation make it vulnerable to destruction, damage, or incapacitation by acts of terrorism, mechanical failure, or acts of nature. The vulnerability assessment should include identification of both strength and weaknesses.</li><li>3. Conduct analysis and prioritize assets- It is impossible to afford complete protection to every critical infrastructure component and key asset across the U.S. There are simply not enough resources. The process of assessing vulnerabilities should identify those components that have weaknesses that would make them higher risk targets. The analysis and prioritization process looks at each potential target in terms of reducing vulnerability verses the overall costs of such in terms of actual costs, use of man power, and other resources.</li><li>4. Develop and Implement Protective Programs- Once the assets are inventoried, and have their vulnerabilities assessed and have their priorities established, plans should be made to prevent, deter, or mitigate attacks on the assets per their priorities. Such plans might include entering mutual protection programs with our jurisdictions, or coordinating plans with state agencies to ensure plans are complete and workable.</li></ol> <p>G. Intelligence and Information Analysis as Key Components- There are four distinct categories of intelligence and information analysis listed in the National Strategy for Homeland Security that can be used to assist in the planning for the protection of vulnerable targets.</p> <ol style="list-style-type: none"><li>1. Vulnerability assessments- Vulnerability assessments must be an integral part of the intelligence cycle. They allow planners to view the consequences of an attack against specific targets, and which assets require protection against threats. The vulnerable assets are subject to constant change and plans must be kept current to reflect those changes.</li></ol>	<p><b>[LD43]</b> – Identifying the concepts of a threat and vulnerability assessment.</p> <p><b>[LD43]</b> – Identify threat assessment rationale</p>
---	---

EV 09 – Critical Incidents  
Session 04 – LEPM/Targets  
LD 43 – Emergency Management

2. Threat vulnerability integration- Mapping terrorist threats and capabilities- both current and future- against specific facility and sector vulnerabilities will allow authorities to determine which organizations pose the greatest threats, and which facilities and assets are most at risk. Facilities facing specific, identified threats must be re-evaluated frequently to determine whether their vulnerabilities have changed and plans must be updated accordingly.
3. Tactical threat analysis- Tactical threat analysis provides useful warning to specific targets, security, public safety professionals, and general population.
4. Strategic analysis of the enemy-U.S. intelligence agencies must have a keen understanding of the organizations with a global reach that may conduct terrorist attacks against U.S. targets. Knowing the identities financial and political sources of support, motivation, goals, current and future capabilities, and vulnerabilities of these organizations will assist the U.S. and preventing and pre-empting future attacks on specific targets chosen by terrorists.