



COUNTY JUDGE ED EMMETT
DIRECTOR

Harris County Office of Homeland Security and Emergency Management
Harris County, TX

Sharing Information
Enhancing Preparedness
Strengthening Homeland Security

Lessons Learned
Information Sharing
LLIS.gov

LESSON LEARNED

Infrastructure Systems: Developing a Critical Infrastructure and Key Resources (CIKR) Plan

SUMMARY

Identifying CIKR is intended to support collaborative planning efforts and provide necessary information for steady-state risk management and to support incident management during response/recovery efforts. Critical infrastructure is defined as the physical or virtual assets, systems, networks, and functions so vital that their



CIKR SECTORS

disruption would have a debilitating impact on security, the economy, public health and safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to operation of the economy and the government. Previous disasters have proven that not having a structured CIKR plan can have a negative impact on response and recovery time. The creation of a CIKR plan ensures local emergency management has an understanding of the critical infrastructure and key resources, in order to make multi-disciplinary, multi-resource, and multi-tiered informed decisions regarding preparedness, incident response and recovery.

DESCRIPTION

After such incidents as Tropical Storm Allison, 9/11, Hurricanes Katrina, Rita, Ike and numerous other natural disasters, the Harris County Office of Homeland Security and Emergency Management recognized the need to have a local CIKR plan in place. Having a CIKR plan ensures that local partners understand the infrastructure dependencies, interdependencies, and associated cascading effects within the community and the local, state and national cross-sector impact to CIKR. It also assures emergency management can rapidly identify, assess and efficiently allocate resources that will sustain the community and enhance response and recovery efforts.

There are essential steps to identifying and protecting critical infrastructure, which may include; conducting risk assessments and prioritizing assets, understanding the interdependencies of key infrastructure, analyzing cross-sector cascading effects, and coordinating with private and public sectors to improve protection and resiliency. To implement this plan, Harris County categorized infrastructure into five levels. A Level 5 asset is identified as something that is critical to the local county/city. A Level 4 asset is

LLIS.gov defines a Lesson Learned as a positive or negative experience derived from an actual incident, operation, training, or exercise obtained from a personal experience, validated After Action Report or interview.

identified as critical to the region. A Level 3 asset is identified as critical to the state. Lastly, Level 1 and Level 2 include assets critical on the national scale. The National Critical Infrastructure Prioritization Program (NCIPP) defined criteria to determine Level 1 and Level 2.

In order to determine the Level an asset is categorized as, emergency managers need to understand the 16 sectors identified by Presidential Policy Directive 21, 2014 National Protection Framework and the 2013 National Infrastructure Protection Plan. These categories are listed in the picture (CIKR SECTORS) above. Identifying local resources and coordinating with the private and public sectors is crucial to a well-developed plan. Identifying these assets will assist emergency management in assigning it the appropriate level of criticality.

Level 5 –Local Impact

Emergency management must first target the entities that are vital to the local community. Examples include the local law enforcement, fire stations, and EMS response units. Other local assets critical to the community's well-being include the water supply, sewer system, power supply, hospitals, chain of food suppliers, communications, banking, stadiums, schools and many other type of first response resources in the community.

Criteria to determine level five are as follows:

1. Between 0-100 prompt fatalities
2. Between \$0-\$99,999 first-year economic consequences
3. Mass evacuations (100's to 1000's) with a prolonged absence of more than one week

These CIKR can directly impact the local economy and capabilities.

Level 4 – Regional Impact

At this level, several steps should be taken to ensure the region is well positioned to respond to events that typically accompany disasters, such as regional electrical outages, fuel shortages, cyber-attacks, transportation problems, regional water supply issues, and other crises. For example, knowing the location of bulk fuel supply would assist during a fuel shortage.

Criteria to determine level 4 are as follows:

1. Greater than 100 prompt fatalities
2. Greater than \$100 million in first-year economic consequences
3. Mass evacuations with a prolonged absence of more than 2 weeks

Level 3 – State Impact

At the state-wide level, resources become even more focused on the 16 sectors. It is important to identify cross-sector dependencies and the cascading effects and why/how each sector is important to the state, based on cascading impact. A strong foundation for CIKR preparedness, especially at the state level, is based on 16 specific sectors. By targeting what is most important by sector will help make a thorough CIKR plan. Criteria to determine level 3 are as follows:

1. Greater than 1,000 prompt fatalities
2. Greater than \$1 billion in first-year economic consequences
3. Mass evacuations with a prolonged absence of greater than 3 weeks

If the economy is impacted nationally it is moved to Level 1 or Level 2.

Level 2 – National Impact

The federal government developed the NCIPP to identify Level 1 and Level 2 CIKR. These include CIKR that, if disrupted, could cause nationally or multi-state significant loss of life, public health, economic, and/or national security impacts. CIKR are identified as Level 2 if disruption could result in at least two of the following consequences:

1. Greater than 2,500 prompt fatalities
2. Greater than \$25 billion in first-year economic consequences
3. Mass evacuations with a prolonged absence of greater than 1 month
4. Severe degradation of the country's national security capabilities to include intelligence and defense functions, but excluding military facilities

Level 1-National Impact

CIKR is identified as Level 1 if disruption could result in at least two of the following consequences:

1. Greater than 5,000 prompt fatalities
2. Greater than \$75 billion in first-year economic consequences
3. Mass evacuations with prolonged absence of greater than 3 months
4. Severe degradation of the country's national security capabilities to include intelligence and defense functions, but excluding military facilities

There are key elements to be considered when overcoming challenges associated with identifying and protecting critical infrastructure. These elements include, developing partnerships and coordinating with the private sector directly related to CIKR, conducting vulnerability and risk assessments, identifying and understanding the interdependencies, recognizing and understanding the government's role in protecting critical infrastructure.

Threats to critical infrastructure should be assessed in the context of natural, man-made, and technological events. CIKR are physical and cyber-based systems that are essential to the operations of the economy and government. Evolving threats to critical infrastructure are mainly pandemics, extreme weather, accidents or technical failures, acts of terrorism, and cyber threats. Risks should be determined based on those threats, including the likelihood of occurrence and the impact these threats would have on the immediate infrastructure and on interdependent systems and facilities. Critical infrastructure is not a distinct collection of physical entities. Instead, it is an interconnected system of systems, each part relying on and affecting the operations of other parts of the system, also known as a cascading impact. Failure of one part of the system will affect the system and create cascading effects throughout. For example, petroleum refineries rely on transportation systems, such as trains, ocean-going vessels, trucks, and pipelines, to move products. These transportation systems rely on refining capacity to provide the fuels needed to operate. Additionally, the computer-based systems that control much of the infrastructure rely on the electrical grid to operate the process controls and industrial control systems necessary to operate complex processes. Disruption in any part of the cross-sector supply chain may have a direct impact on the local, regional or state economic stability and the inability to provide vital life-line services. Developing a local CIKR plan is essential to mitigation.

RECOMMENDATIONS

In developing the Harris County CIKR plan we utilized numerous partners to help in identifying, evaluating, and securing the CIKR assets. These partners include local law enforcement, the U.S. Coast Guard, Port Authority, the Private Sector, Fire Services, Health Authorities, Chemical Sector, IT Cyber, Utility Districts, Tax Assessor, GIS data, and our local DHS-Protective Security Advisor.

REFERENCES

Critical Infrastructure Sectors

<http://www.dhs.gov/critical-infrastructure-sectors>

Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies

http://lyle.smu.edu/emis/cmml5/Ibarra/DeskTop/2004_PhD_041406/Dissertation/Papers/Paper_Misc/CIP_Interdependencies_IEEE_Control_Systems.pdf

National Infrastructure Protection Plan

http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

What is Critical Infrastructure?

<http://www.dhs.gov/what-critical-infrastructure>

DISCLAIMER

The views expressed in this document are those of the author and do not necessarily reflect those of Lessons Learned Information Sharing. Lessons Learned Information Sharing (LLIS.gov) is the Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the emergency management and homeland security communities. The Web site and its contents are provided for informational purposes only, without warranty or guarantee of any kind, and do not represent the official positions of the Department of Homeland Security. For more information on LLIS.gov, please email feedback@llis.dhs.gov or visit www.llis.gov