



01 Jan 2004

## A Methodology to Assess Critical Infrastructures and Their Relevance to Missouri

Tricia Mattson

Follow this and additional works at: <https://scholarsmine.mst.edu/oure>

---

### Recommended Citation

Mattson, Tricia, "A Methodology to Assess Critical Infrastructures and Their Relevance to Missouri" (2004). *Opportunities for Undergraduate Research Experience Program (OURE)*. 245.  
<https://scholarsmine.mst.edu/oure/245>

This Presentation is brought to you for free and open access by Scholars' Mine. It has been accepted for inclusion in Opportunities for Undergraduate Research Experience Program (OURE) by an authorized administrator of Scholars' Mine. This work is protected by U. S. Copyright Law. Unauthorized use including reproduction for redistribution requires the permission of the copyright holder. For more information, please contact [scholarsmine@mst.edu](mailto:scholarsmine@mst.edu).

**A Methodology to Assess Critical Infrastructures  
and Their Relevance to Missouri**

**OURE 2004-2005**

**Final OURE Report 2005**

**University of Missouri-Rolla**

**Nuclear Engineering**

**Research done by**

**Ms. Tricia Mattson**

**In collaboration with**

**Dr. Akira Tokuhiko**

**Submitted to Office of Undergraduate and Graduate Studies**

**On**

**April 1, 2005**

  
**Tricia Mattson**

# **A Methodology to Assess Critical Infrastructures and Their Relevance to Missouri**

**Tricia Mattson**  
**University of Missouri – Rolla**

## **ABSTRACT**

September 11, 2001, a day when thousands of lives were lost under unexpected and unprecedented circumstances, marked the beginning of a difficult national reality; that is, the vulnerability of our society and our infrastructures to terrorist attack. The events of that day have shaken the very foundations of national and the newly coined, “homeland security”. It is apparent that changes need to be made to the national/homeland security infrastructure at all levels. But how will change be brought about and what “roadmap” will we follow?

The research team of Dr. Tokuhiro has been studying complex social-technological issues. We are especially interested in how society will protect its sensitive materials and installations in the post-9/11 environment. One promising way appears to be an approach based on “eigenmetrics”; that is, largely on time and countable arguments (“numbers”) that apply to local, state and national security issues. Our approach provides a foundation, beyond endless discourse. The project presently consists of surveying the *9/11 Commission Report* and the *National Response Plan*. We will extract the overarching time- and number-scales from these reports and provide relevant examples for the State of Missouri.

## INTRODUCTION

After the terrorist attacks of 9/11, the government went into a frenzy seeking answers and trying to build a plan that would prevent events of the same magnitude from occurring again. The *National Strategy for Homeland Security*, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, the *National Incident Command System*, the *9/11 Commission Report*, and the *Initial National Response Plan* provided the fundamental ideas and drafts of the final *National Response Plan*. This comprehensive plan provides a template for any disaster that could occur on U.S. soil. However, the plan is based on the assumption that every state has an integrated organization, communication capabilities among all critical infrastructure, key asset, and emergency response entities, and an incident command system. There is also no clear way of enforcing the plan among states. Missouri is one of the states not yet ready to implement the *National Response Plan*. Missouri doesn't quite meet the assumptions of the plan, however, Missouri's homeland security program is about average compared to other states. On all levels—national, state, and local—the *National Response Plan* is going to take a lot longer than originally expected to fully implement.

## National Strategies

On October 8, 2001 President George W. Bush established the Office of Homeland Security along with its first responsibility of producing the *National Strategy for Homeland Security*. This strategy would be the first in a string of documents that analyze the state of homeland security and make recommendations for improvement.

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* focuses on one of the critical mission areas outlined in the *National Strategy for Homeland Security*: protecting critical infrastructures and key assets. Key assets include national monuments and icons, government facilities, and nuclear power plants. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* gives the Nuclear Regulatory Commission (NRC) the responsibility of developing a standard methodology for conducting vulnerability and risk assessments, improving the capabilities of nuclear power plant security forces, and enhancing public outreach and awareness programs and emergency preparedness programs. (NUCLEAR POWER PLANTS 74) This document serves as a connection between the *National Strategy for Homeland Security* and the *National Response Plan* (NRP).

## 9/11 Commission Report

In late 2002, President Bush formed the 9/11 Commission on Terrorist Attacks Upon the United States (9/11 Commission). The Commission's purpose was to complete a full report of findings, analysis, and recommendations surrounding the attacks of 9/11. On July 22, 2004 the Commission released the 9/11 Commission Report. The report outlined the events surrounding the World Trade Center (WTC) attack and made bold conclusions as to why the tragedy was allowed to occur. Two of the conclusions can be linked to nuclear security. These problematic areas are lack of an integrated communications system and lack of an incident commander (IC). If a nuclear disaster were to occur today, an effective communications system and an IC would be necessary to minimize the aftermath of the attack.

In terms of eigenmetrics, numbers can be extracted from the 9/11 Commission Report and applied to different situations on national, state, and local levels. The following numbers can be extracted for the WTC:

	total amount	initially responded
FDNY members	11,000	235
FDNY engine companies	205	21
FDNY ladder companies	133	4
NYPD members	40,000	922

elevators per tower	99
acres per floor	≈1
floors per tower	110
height of tower (ft)	1350

length of walls (ft)	208
number of central stairwells	3
number of windows	21,800
number of emergency exits	800
number of office workers	50,000

These numbers can possibly be applied to an incident on the state or local level and compared to highlight inefficiencies in pre-event, event, and post-event phases of an incident.

### **Incident Command System**

The 9/11 Commission Report states, "If New York and other major cities are to be prepared for future terrorist attacks, different first responder agencies within each city must be fully coordinated, just as different branches of the U.S. military are. Coordination entails a unified command that comprehensively deploys all dispatched... first responder resources." (HEROISM AND HORROR 321)

Recent military operations in Afghanistan and Iraq have been steady and successful, especially compared to the military's prosperity in the Vietnam War and the First Gulf War. The Goldwater-Nichols Department of Defense Reorganization Act of 1986 is responsible for this change in the military's efficiency. The Goldwater-Nichols Act passed because of previous problems of rivalry among different branches of the military in the Vietnam War and the Iranian hostage rescue mission of 1980<sup>1</sup>. The act unified military responsibilities under one Chairman of the Joint Chiefs, creating a unified command or an "incident commander" for the military.

A similar type of incident command was used on September 11<sup>th</sup> at the Pentagon and presided over all of the emergency responders and regions involved. Of all local, regional, state, and federal agencies responding to the Pentagon attack, one incident commander was quickly established to take control of rescue and relief efforts. While it is impossible to compare the attacks on the Pentagon and the WTC, it is obvious to see that the presence of an incident commander, organization, and communication improves emergency response by magnitudes.

The definition of Incident Command System (ICS) is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in domestic incident management activities. The ICS should have a command post somewhere near the location of the incident and communication capabilities with all of the emergency relief parties. For maximum efficiency of emergency response during an incident, it is necessary to establish an ICS. It is therefore necessary that planning for the execution of incident command systems should be implemented over the entire nation. Both the *9/11 Commission Report* and the *National Response Plan* recognize this need.

---

<sup>1</sup> Definition taken from Wikipedia's Goldwater-Nichols Act, 27 Mar 2005, at <[http://en.wikipedia.org/wiki/Goldwater-Nichols\\_Act](http://en.wikipedia.org/wiki/Goldwater-Nichols_Act)>

## **Homeland Security Presidential Directive - 5**

The *Homeland Security Presidential Directive* (HSPD-5) was published to establish a single, comprehensive approach to domestic incident management. HSPD-5 made the following demands of the Homeland Security Secretary, Tom Ridge: publish an *Initial National Response Plan* by April 1, 2003. This was accomplished as a draft for the final *National Response Plan*.

By request of the HSPD-5, the *National Incident Management System* document was issued by Secretary of Homeland Security, Tom Ridge, to provide a standardized national plan to help Federal, State, and local governments and private sector organizations to work together in the event of a domestic incident like a terrorist attack. State, local and tribal governments to work together effectively and efficiently to prepare for, prevent, respond to, and recover from terrorism.

### **National Response Plan**

In December 2005, after the establishment of the *National Strategy for Homeland Security*, *National Strategy for the Physical Protection of Key Assets and Critical Infrastructures*, *Presidential Directive for Homeland Security – 5*, *National Incident Management System*, and *9/11 Commission Report*, the United States Department of Homeland Security established a comprehensive template for all domestic emergency response efforts called the *National Response Plan*. This plan provides the framework for response to any possible domestic incident. It affirms the use of an incident command system, the establishment of an organization among all levels (national, state, and local), the establishment of a working communications system between all critical infrastructure, key asset, and emergency response entities.

The purpose of the NRP is to establish a comprehensive, national, all-hazards approach to domestic incident management across a spectrum of activities including prevention, preparedness, response, and recovery (NRP 2). The plan explicitly states the need for an integrated organization of all critical infrastructure, key asset, and emergency response entities, an incident command system, and an integrated communications system. Without this type of system, none of the Emergency Support Function Annexes, Support Annexes, or Incident Annexes established by the NRP to provide incident-specific support would prove to be useful. Together, the NRP and the NIMS integrate the capabilities and resources of various governmental jurisdictions, incident management and emergency response disciplines, nongovernmental organizations, and the private sector into a cohesive, coordinated, and seamless national framework for domestic incident management (NRP 1).

The NRP establishes the Nuclear/Radiological Incident Annex. This annex delegates the mitigation and consequences responsibility to the owner of the nuclear/radiological facility involved in the accident. They are responsible for notifying the state and local

government and containing any radiation. Any owner of a nuclear/radiological facility can request help directly from the United States Department of Homeland Security.

The greatest shortfall of the NRP is there is no entity to ensure states will implement the organization the NRP assumes. The Department of Homeland Security is responsible to make sure all annexes are fully functional and being used properly, but they have no role in making sure states have an organizational structure or means of communication throughout the structure.

### **Establishment of organization/integration among levels**

The national level includes all national governmental bodies, the president and Congress. The national level is responsible for helping to fund clean up efforts, analyzing the situation and dealing with the psychological effects the disaster would have on society. This level encompasses all critical infrastructure, key asset, and emergency response entities in all of the state levels.

The state level includes all state government bodies. The state is responsible for making sure local first responders are being timely and efficient, distributing federal funds to appropriate local and state entities, and relaying information and implementing security policies to the local entities.

The local level includes all first responders, fire fighters, police officers, and emergency management personnel. The local level responders are the first on the scene of the incident, and are the last to leave the scene. It is the quickness of efforts from the local level that will minimize the aftermath of the disaster.

There needs to exist an integration and coordination of all levels. This organization will reduce redundancy of actions, put all efforts in unison with one another, and increase the efficiency of the operation as a whole. In order to keep and maintain a functional organization below the state level of all critical infrastructure, key asset, and first responder entities, it is necessary to hold semiannual meetings, sustain a fusion center (usually the state highway patrol agency), and have entities report to the state homeland security office frequently. In order to maintain a working organization below the national level, it is important that the federal government establish clear and concise homeland security laws and orders. If the state is uncertain about certain documents or orders, nothing will get done. For example, the national government has implemented the National Response Plan as the core, comprehensive, operational plan for domestic incident management, but the requirements for state execution of the plan are unclear.

### **Evaluating an Event in terms of Phases**

In addition to evaluating security on the national, state, and local levels, it is valuable to evaluate an attack in terms of time phases. An attack can be broken into pre-event, event, and post-event phases.



The pre-event stage includes planning, funding distribution, training, integration and information sharing among common entities, use of an integrated organization of critical infrastructure, key asset, and emergency response entities, and the establishment security policies. The pre-event time phase deserves greater attention considering the actions taken during this phase can alter the other two phases significantly. For example, a skydiver is in greater danger if he were to jump out of a plane without a parachute and having ambulances on site, than if he were to jump out with a parachute and a Band-Aid. Having the parachute will most likely eliminate the need for first aid. In comparison, having more funds and time spent with the pre-event time phase will provide a wall of protection. Only if a terrorist attack cannot be prevented in the pre-event time phase, will the incident leak through to event and post event.

The event stage includes use of funding, detection, first responders, and establishment of an ICS. This is the phase that determines whether the terrorist attack will be success or a failure. The use of funding, planning, and training is tested during this phase. The event phase is usually the shortest phase in terms of a timescale.

The post-event stage includes clean-up, containment, analysis of event, public communications, and restoring public confidence. This phase is hard to predict because it depends completely upon the success of the pre-event and event phases.

This method is especially useful when analyzing risk. The risk that something will occur in the event stage is totally dependent upon what happens in the pre-event stage. The actions that take place in the post-event stage are dependent upon the event stage, and therefore the risk is dependent upon the pre-event stage.

**Nuclear Risk Analysis in Time Phases**

<b>Time Phase</b>	<b>Pre-event</b>	<b>Event</b>	<b>Post-event</b>
<b>Risk Analysis</b>	<b>Probability of specific accident scenarios</b>	<b>Potential radiation release from the plant</b>	<b>Potential public health consequences</b>

Using a chart like this can help in analyzing the probability of an event occurring and determine how big a risk the situation carries.

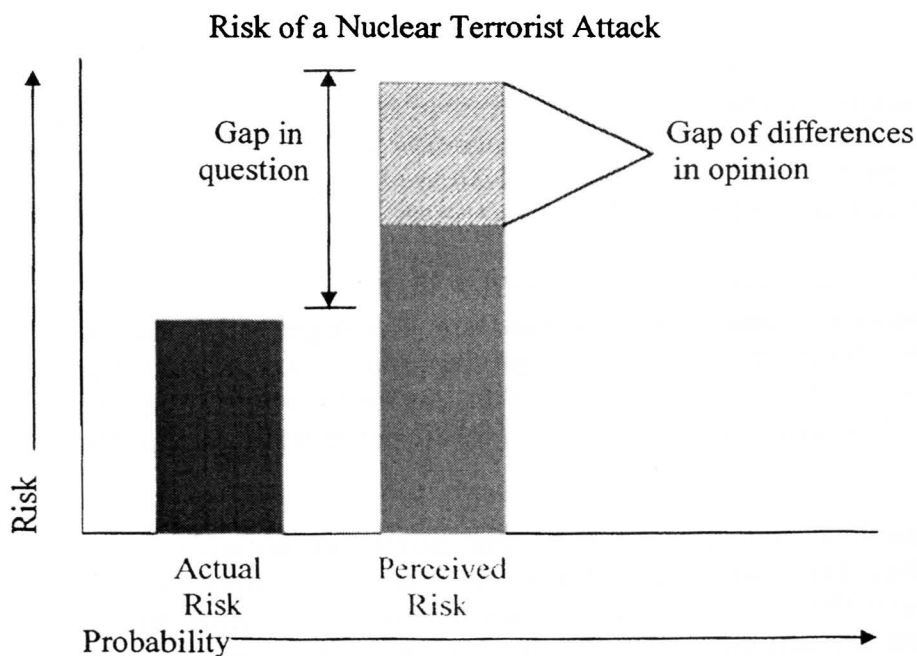
### **Importance of Public Relations**

Aside from the recommendations made in the 9/11 Commission Report and the strategies established in the National Response Plan, there are other, less direct methods for fighting against nuclear terrorism. Nuclear terrorism is the use or threatened use of a nuclear mechanism against civilians with the purpose of instilling fear in societies for political or religious reasons. This definition encompasses the use (or threatened use) of nuclear weapons, radiological dispersion devices, or nuclear reactors as weapons. Using this definition to isolate the root of nuclear terrorism, the authors have evaluated a different approach to preventing a terrorist attack on a reactor.

A more overlooked option for fighting nuclear terrorism is decreasing the desirability of nuclear reactors for terrorists. We have to ask ourselves, if society gains a better understanding of nuclear safety, could that itself decrease the desirability of nuclear reactors to terrorists? It is the opinion of the authors that gaining public acceptance would significantly decrease the risk of nuclear reactors as terrorist targets.

A better understanding of nuclear safety by the public would increase reactor credibility. Improving the credibility would take definition out of nuclear terrorism. This is because once the public understands the risk of a terrorist using a nuclear plant against society, there will be less of a psychological scare factor for the terrorist to use. This would make nuclear reactors less desirable for a terrorist attack.

One way to increase reactor credibility is to reduce public perceived risk. Nuclear safety is numerically represented by the term “risk” which is very subjective; each person perceives it differently. Perceived risk is larger than actual. There needs to be a reduced gap between perceived and actual risk. This would enhance public acceptance. Increasing actual risk to close the gap would obviously be counterproductive, so there needs to be a decline in perceived risk. The following graph depicts the situation described:



The question is how can public perceived risk be decreased? To answer this question risk measurements must be analyzed. Nuclear risk assessment involves likelihood and probability. For example, if the likelihood that an accident will occur is great, so is the risk. There is a probability that a smoker will develop some sort of lung-related disease at some point in their life. The bigger the probability for the disease, the bigger the risk the smoker is taking for contracting the disease. If the general public can recognize there is a

small likelihood or probability of a nuclear attack occurring, the corresponding risk would also be small. Helping society recognize this idea can be accomplished by several means:

- Increasing political support
- Handing out public educational tools (informational pamphlets, videos, etc.) to areas surrounding reactors
- Holding press conferences
- Conducting lectures and forums open to the public
- Taking a grassroots initiative
- Gaining media cooperation

### **Homeland Security in Missouri**

Even though the Missouri Homeland Security Office was the first state office established after 9/11, Missouri still has a long road ahead in improving homeland security. Missouri is in the very preliminary stages of implementing the National Response Plan. There are no enforcing entities to guarantee full implementation for Missouri, and there needs to be a better communication of the plan between national, state, and regional levels. The basic roots of Missouri's homeland security needs will come from full implementation of the NRP.

In Missouri, more focus needs to be placed on the pre-event phase. Missouri is lacking in efforts made in the areas of: distribution of funding, integration and information sharing among common entities, and use of an integrated organization of critical infrastructure, key asset, and emergency response entities.

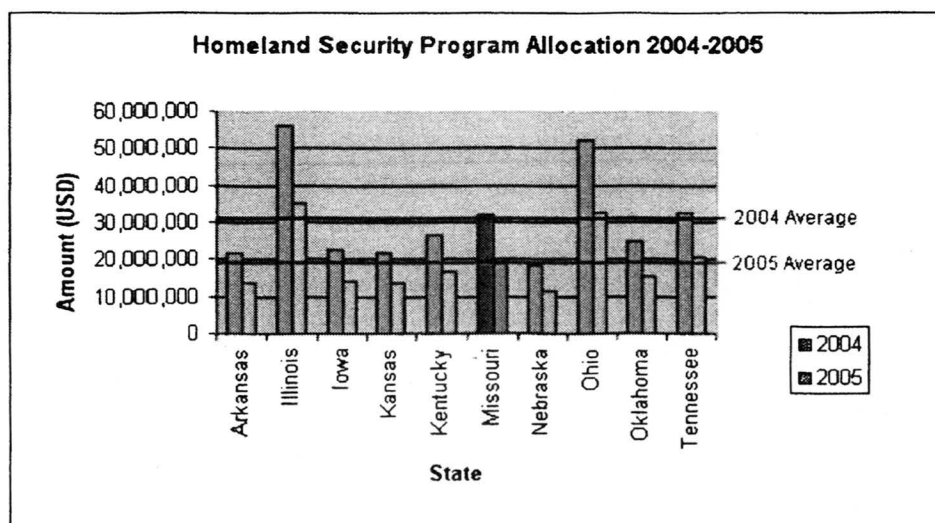
First, there needs to exist an organization among all entities in Missouri involving a state key asset, critical infrastructure, or emergency response team. This organization must be arranged so actions can be streamlined to appropriate groups or people in the event of an emergency. The establishment of this organization would allow for Missouri to improve integration and standardization among common entities, funding distribution, and public relations.

Once the organization is established, there needs to be semi-annual collaborative meetings of common entities. For example, one of these collaborative meetings would include all groups that deal with nuclear materials. Representatives from UMRR, MURR, Callaway, Cooper, and Fort Leonard Wood would attend the meeting to share information and discuss pertinent security issues. These information-sharing sessions would help the entities standardize their safety and emergency plans.

Missouri receives \$125 million in federal funds for homeland security. Approximately 20% of federal funds are supposed to support homeland security on the state level. The remaining 80% of funds are supposed to support homeland security on the local level. Missouri has spent less than 25% of this federal grant money. The reason for the inefficiencies in grant spending is largely due to the lethargic distribution of funds across

both the national to state levels and the state to local levels. If Missouri had an organization, funds received from the government can be allocated and streamlined to appropriate groups faster and more efficiently. An example of an area of funding distribution that needs improvement is Missouri's development of the Joint Information System established in NIMS. The Missouri Homeland Security Annual Report for 2003 states that one of the additional needs toward ...for the department is "The State should consider taking the first steps toward establishment of a Statewide Communications system." Nothing has been done since the publication of the report in terms of establishing a statewide communications system because no organization exists among the levels of state key asset and critical infrastructure entities. There are no defined groups to distribute communication services and equipment.

Missouri does receive enough funding from the government to ensure a safe place for residents. \$20 million of the total comes from the Homeland Security Grant Program



## **NOMENCLATURE**

***Initial National Response Plan (INRP)*** – document published by the Department of Homeland Security as the first step in aligning incident management response and actions between all Federal, state, tribal, local, and private communities. Later to be superseded by the final National Response Plan

**Nuclear Regulatory Commission (NRC)** - The U.S. Nuclear Regulatory Commission (NRC) is an independent agency established by the Energy Reorganization Act of 1974 to regulate civilian use of nuclear materials.

**Missouri Security Panel** – A governor appointed (Executive Order 02-15 and Executive Order 02-16) panel organized to examine Missouri security and propose recommendations for improvement in communication, security of critical infrastructures and public safety

## **ACKNOWLEDGEMENTS**

Dr. Tracia (West) Love  
Sandia National Laboratories  
University of Missouri-Rolla

Michael Chapman  
Missouri Homeland Security Director  
Missouri Homeland Security Office

Dr. Akira Tokuhiro  
Assistant Professor Nuclear Engineering Department  
University of Missouri-Rolla

## REFERENCES

- The Nuclear Energy Institute, *Safety Benefits of Risk Assessment at U.S. Nuclear Power Plants*, March 2002, <<http://www.nei.org/doc.asp?docid=805>>.
- The White House, February 2003, *National Strategy for Homeland Security*, <<http://www.whitehouse.gov/pcipb/physical.html>>.
- The White House, *National Strategy for the Protection of Key Assets and Critical Infrastructures*, February 2003, <[http://www.whitehouse.gov/pcipb/physical\\_strategy.pdf](http://www.whitehouse.gov/pcipb/physical_strategy.pdf)>.
- Federal Emergency Management Agency, *National Incident Management System*, March 1, 2004, <[http://www.fema.gov/nims/nims\\_compliance.shtm#nimsdocument](http://www.fema.gov/nims/nims_compliance.shtm#nimsdocument)>.
- Missouri Homeland Security Office, *Missouri Strategy for Homeland Security*, November 17, 2004, <<http://www.homelandsecurity.mo.gov/StateStrategy111704.pdf>>.
- United States Government Printing Office, *9/11 Commission Report*. July 2004, <<http://a257.g.akamaitech.net/7/257/2422/05aug20041050/www.gpoaccess.gov/911/pdf/fullreport.pdf>>.
- U.S. Department of Homeland Security Office for Domestic Preparedness, *Fiscal Year 2005 Homeland Security Grant Program*, <<http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf>>.
- U.S. Department of Homeland Security Office for Domestic Preparedness, *Fiscal Year 2004 Homeland Security Grant Program*, <[http://www.ojp.usdoj.gov/odp/docs/fy04hsgp\\_appkit.pdf](http://www.ojp.usdoj.gov/odp/docs/fy04hsgp_appkit.pdf)>.
- U.S. Department of Homeland Security Office for Domestic Preparedness, *Fiscal Year 2003 State Homeland Security Grant Program – II*, <<http://www.ojp.usdoj.gov/odp/docs/fy03shsgp2.pdf>>.
- U.S. Department of Homeland Security Office for Domestic Preparedness, *Fiscal Year 2003 State Homeland Security Grant Program*, <<http://www.ojp.usdoj.gov/odp/docs/ODPApplication.pdf>>.
- U.S. Department of Homeland Security Office for Domestic Preparedness, *Fiscal Year 2002 Domestic Preparedness Grant Program Application Kit*, <<http://www.ojp.usdoj.gov/odp/docs/02odpkit.pdf>>.