Us homeland security related critical infrastructure matters

The statement: “ The Department of Homeland Security has complete responsibility for all U. S. homeland security related critical infrastructure (CI) matters” is not entirely accurate; originally, matters of national security were the sole “ responsibility of the federal government” (Homeland Security, 2003, p. 7). Today, national critical infrastructure protection is a joint effort among the federal government, public and private sectors. The Department of Homeland Security was established to protect and secure the homeland from both domestic and foreign threats. According to the Homeland Security Act of 2002, the development of a plan which will ensure the security of critical infrastructure is the responsibility of the DHS (Homeland Security, 2009). Likewise, the DHS is also responsible for “ recommending the measures necessary to protect the key resources and critical infrastructure of the United States” (Homeland Security, 2009, p. 2).

The mission of DHS is one that involves the protection of “ infrastructure and critical facilities and networks” (Homeland Security, 2010, p. 33). The DHS is responsible for the identification and assessment of all components which make up critical infrastructure. In addition to mitigating potential vulnerabilities; improving the resilience of critical infrastructure, is also a top priority of the DHS. This includes but is not limited to: “ stand-alone facilities and interdependent systems and networks within and across critical infrastructure sectors” (Homeland Security, 2010, p. 34).

The DHS serves as the leader and facilitator for those agencies who share responsibility for protecting the “ nation’s critical infrastructures” (Homeland Security, 2010, p. 31). Those agencies include territorial, tribal, local and state governments, as well as the private sector and other agencies not

associated with the government (Homeland Security, 2003). Conversely, when a disaster occurs these agencies are the first line of defense for national critical infrastructures.

Even though the DHS is responsible for leading critical infrastructure efforts, coordination of security measures within local and state governments and critical sector industry leaders are the responsibility of federal lead departments and agencies (Homeland Security, 2003). Similarly, it is the responsibility of state and local governments to provide protection to critical infrastructures that are located “ within their jurisdictions” (Homeland Security, 2003, p. 10). If and when a catastrophic event should occur which exhaust the capabilities of local and state governments, it is up to the federal government to coordinate a response (Homeland Security, 2003).

A majority of our nations critical infrastructures are privately owned or operated, which means that the private sector are initially responsible for providing protection against threats to their facilities (Homeland Security, 2003). When the threat becomes more than the private sector can handle then the government will step in to assist and ensure that our nations critical infrastructures and assets are protected (Homeland Security, 2003, p. 11). Likewise, the federal government will be there to provide support for “ an environment in which the private sector can better carry out its specific responsibilities” (Homeland Security, 2003, p. 11).

The chemical sector is one of the most vulnerable critical infrastructures to natural disaster and terrorist attacks, that being said the DHS is working with the EPA to enhance security at chemical facilities (Homeland Security, 2003).

In addition, special attention is being paid to those facilities which house “ large quantities of hazardous chemicals” (Homeland Security, 2003, p. 78). Studies conducted by the DHS and private sector are currently underway to identify and “ understand physical vulnerabilities within the telecommunications infrastructure and their associated risks” (Homeland Security, 2003, p. 61).

Even though the private sector must occasionally seek assistance from the DHS, there are times when the federal government must rely on the private sector to lend a hand in emergency response and recovery. An example of the federal government calling on the private sector for assistance was the anthrax scare of 2001. A large Washington D. C. construction corporation was contracted to oversee the abatement and restoration of the Brentwood Post office in Washington D. C. and the Trenton Post office facility in New Jersey.

One must also understand that quite a few of our nations critical infrastructures “ cross international borders” (Homeland Security, 2003, p. 35). Therefore the federal government has partnered with the neighboring countries to provide security for our “ interconnected infrastructures” (Homeland Security, 2003, p. 35). The United States partnership with Canada is is a vital asset to national critical infrastructure, efforts are being made to provide protection for international interconnected infrastructures. An example of this partnership is the Alaskan Canadian hightway. In order to transport goods and supplies to Alaska we must travel cross Canadian territory.

It is evident that matters of critical infrastrucutre involves not only the DHS but the public and private sectors as well. The DHS would not be able to carry out their responsibilites without the assistance of local and state agencies, the private sector and vice versa.

The U. S. government has made great strides in developing techniques and strategies to harden U. S. critical infrastructures which will make them more resistant to terrorist attack and natural disasters. One of the U. S. government’s goals is to establish a strong partnership that spans across all levels of government, in addition to the private sector and the American people (Homeland Security, 2009). The Protected Critical Infrastructure Information Program is just one of many steps taken by the U. S. government to harden critical infrastructure. This program provides protection to “ security-related” critical infrastructure information (Homeland Security, 2009, p. 5).

By breaking down each critical infrastructure sector it is easier to understand how the U. S. government has been successful in hardening each critical infrastructure. The agriculture and food sector is one of the most vulnerable critical infrastructures, that being said, efforts to harden this sector are an ongoing challenge (Mark Sauter & James Carafano, 2005). The U. S. government has revised its measures by providing more protection through the hiring of more health inspectors, and adding “ more reporting requirements” (Sauter & Carafano, 2005, p. 291). Contamination of our nation’s water supply is often a topic of concern; efforts are being made by the Environmental Protection Agency as well as the Department of Homeland Security to conduct a vulnerability and threat assessment (Sauter &

Carafano, 2005). These assessments will improve not only “ site security at high threat locations” it will also “ enhance monitoring and sharing of information” (Sauter & Carafano, 2005, p. 292).

With regards to the critical infrastructure of public health the U. S. government has implemented measures to harden biomedical surveillance (Sauter & Carafano, 2005). This is extremely important because of the risks of a biological attack. There have also been improvements in hardening security of “ emergency stockpiles of medical supplies” (Sauter & Carafano, 2005, p. 294). In order to improve the physical security of medical structures the U. S. government has provided “ incentives to the private sector” (Sauter & Carafano, 2005, p. 294).

In response to hardening the critical infrastructure of emergency services the U. S. government has established measures to harden “ interoperable and redundant communication networks” (Sauter & Carafano, 2005, p. 295). The U. S. government has instituted a tougher national emergency preparedness exercise program which teaches better security and “ promotes consistent protection planning and response protocols” (Sauter & Carafano, 2005, p. 295). Since the defense industrial base critical infrastructure sector is owned by a majority of the private sector the U. S. government has implemented new measures to include “ critical infrastructure protection requirements in contract processes” (Sauter & Carafano, 2005, p. 296). Likewise, security is being strengthened in the “ defense related commercial production and distribution processes” (Sauter & Carafano, 2005, p. 296).

The telecommunications critical infrastructure has been assessed by the U. S. government, and in return a program has been designed to identify where the most vulnerable areas are in the communication architecture and then address the security issue (Sauter & Carafano, 2005). Conversely, there have also been efforts made in the energy critical infrastructure sector to " enhance resilience" of the energy facilities (Sauter & Carafano, 2005, p. 298). Facility equipment is being repaired and replaced and there have also been improvements in " restoration and recovery of services" (Sauter & Carafano, 2005, p. 298).

Significant improvements have been made to harden the transportation critical infrastructure sector; for example, security initiatives have been established to provide commercial airliners with protection " from shoulder fired missiles" (Sauter & Carafano, 2005, p. 299). There have also been new developments in screening technology which help identify potential threats to transportation as well as aiding the postal service sector in identifying " suspicious mail" (Sauter & Carafano, 2005, pp. 301-302).

Despite the many efforts being made to harden critical infrastructure, there are still several weaknesses in the U. S. government's strategy. Let's face it, the only other thing that is more costly than hardening critical infrastructure is the disruption or potential loss of operations in those critical infrastructures. It is clear that trying to harden all critical infrastructures is too daunting of a task and is not cost effective. The U. S. government needs to focus on those areas of the United States where our critical infrastructures are most vulnerable (e. g. New York City, Los Angeles, Washington D. C. etc.).

The federal government also needs to look at the protection of our nation’s water ways. Information security systems need to be deployed to “ guard the locks on the Mississippi and St. Lawrence seaways” (Bruce Don & David Mussington). By employing an information security system it will enable “ the monitoring of vessels and ships while in locks or approaching locks” (Don & Mussington). To provide another level of security, “ river marshals could be deployed to accompany dangerous shipments through the locks” (Don & Mussington). Many people don’t realize that a large majority of our nation’s goods are transported through inland waterways, which is why it is important that more attention be paid to the transportation sector.