2011-2012 CIKR Controversy Paper Proposal

Max Archer*
Brian Delong
Taylor Hahn
Jeff Kurr
Nick J. Sciullo
Aaron George Swanlek
Kelly Young, Ph.D.

*Authors in Alphabetical Order

Table of Contents

I. EXECUTIVE SUMMARY 3
II. INTRODUCTION TO THE CONTROVERSY 4
III. REASONS WHY THE DEBATE COMMUNITY SHOULD DEBATE CIKR 11
IV. REASONS WHY THE DEBATE COMMUNITY SHOULD NOT DEBATE CIKR (AND OUR RESPONSES) 13
V. TOPICALITY 17
VI. CIKR SECTORS 23
Agriculture and Food 24
Banking and Finance 30
Chemical 33
Commercial Facilities 48
Communication 51
Continuity of Government 57
Critical Manufacturing 64
Dams 73
Defense Industrial Base 79
Emergency Services 83
Energy 95
Government Facilities 99
Healthcare and Public Health 103
Information Technology 118
National Monuments and Icons 132
Nuclear Reactors, Materials and Waste 137
Postal and Shipping 145
Transportation Systems 147
Water 153
VII. GENERIC NEGATIVE GROUND 157

I. EXECUTIVE SUMMARY

As with any nation, the United States has been forced to acknowledge that certain assets have become critical to the continued functioning of its economy, political structure, and society. This topic paper seeks to inform the collegiate debate community as to how debating Critical Infrastructure and Key Resources will provide for an enjoyable and educational year of competition.

While the length of this document may be initially daunting, we advise the reader to remember that not all areas discussed in this paper need be included in the debate resolution. This paper is intended to lay out how each sector, if chosen, would function in the debate round. As such, much of this paper is devoted to evidentiary examples in an attempt to illustrate argumentative viability. Sectors are organized in a non-linear manner where the reader is able to read each area in whatever order they prefer without missing critical information pertinent to each sector.

For those community members intending to vote for other topic proposals; it is worth noting that nearly all of the proposed topics can be debated, in some form, through a Critical infrastructure resolution. Individuals considering the merits of opposing topic proposals are therefore asked to be particularly attentive to the Critical Infrastructure and Key Resources sectors that are capable of accommodating the plans that would be afforded through these other topic areas.

II. INTRODUCTION TO THE CONTROVERSY

A. The Definition of and Importance of U.S. Critical infrastructures and Key Resources (CIKR)

The protection and maintenance of the nation's infrastructures has been a major concern for the federal government for several decades. For many years, this attention was focused on the capabilities of the nation's public works. In this context, infrastructure is a fairly broad term that includes such things as roads, bridges, water and sewer systems, airports, ports, and public buildings. Beginning in the 1990s, infrastructure protection became a national security issue with the rising threat of international terrorism, accidents, natural disasters and other emergencies. With these threats in mind, numerous government reports, law and executive orders have identified infrastructures considered "critical" for the purposes of homeland security.[1] Most recent government documents use the term "critical infrastructure and key resources" (CIKR) to describe these assets. The Department of Homeland Security (DHS) broadly defines CIKR's as:

> **Critical Infrastructure** are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. **Key Resources** are publicly or privately controlled resources essential to the minimal operations of the economy and government.[2]

More specifically, CIKR's are listed by the DHS as the following 18 sectors[3]:

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

[1] John Moteff and Paul Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," CRS Report for Congress, Oct 1, 2004, http://fas.org/sgp/crs/RL32631.pdf.
[2] Department of Homeland Security, "Critical Infrastructure and Key Resources," Last Updated: Feb 19, 2010, http://www.dhs.gov/files/programs/gc_1189168948944.shtm.
[3] Ibid

As will be discussed later in the Topicality section, it is possible to narrow this list substantially by debating the protection and resiliency of just Critical Infrastructures, which generally includes just eight of these sectors.

In 1997, in the wake of the Oklahoma City bombing, Bill Clinton initiated the President's Commission on Critical Infrastructure Protection (PCCIP) to study the potential impacts of that bombing and future attacks might have on the nation's infrastructure system.[4] One of the early findings of this work was that CIKR's are vital to the nation because virtually every aspect of our daily's lives is impacted by the safety and reliability of our nation's CIKRs. As 1998 follow up report by the Clinton Administration contends, the entire foundation of our military and economic strength depends on the protection of our CIKRs:

> **The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.** Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. **As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks**. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security. **Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.**[5]

Additionally, every aspect of our nation's leadership and hegemony and society is impacted and interrelated with the strength of our critical infrastructure.[6] As a result, the nation and our society are weakened by infrastructure vulnerability:

> **Since the American Revolution**, **our greatest leaders have recognized that a key indicator of national strength is the development and maintenance of an advanced system of infrastructures**. **Our extensive built infrastructures**—postal, banking, roads, water, and pipelines, among others—**moved us from an agricultural society to a manufacturing powerhouse and marked us as the most advanced nation on earth in the industrial age. The recent emergence of complex and sophisticated information infrastructures** comprised of global computer networks and highly advanced control systems, have propelled us into the twenty-first century and have enabled pre-existing infrastructures to operate at enhanced levels with astounding results. Additionally, these enormous technological gains **have had an immense**

[4] Kathi Ann Brown, Critical Path: A Brief History of Critical Infrastructure Protection in the United States, 2006, http://cip.gmu.edu/archive/CIP_CriticalPath.pdf

[5] "The Clinton Administration's Policy on Critical Infrastructure Protection," Presidential Decision Directive 63, May 1998, http://clinton4.nara.gov/WH/EOP/NSC/html/documents/NSCDoc3.html.

[6] One of the many advantages of this topic is that the affirmative internal link to hegemony and US leadership is quite strong, as most critical infrastructure systems are necessary for the vitality of our economic, educational, military and trade systems.

> **impact on our culture in general. Like the threats to the infrastructures themselves, these simple facts have had an enormous cascading impact on the way we operate as a society and on our understanding of law, policy, economics, and business. However, in the process of advancing our national capacity and economic strength, a greater dependence on these technologies has created hidden interdependencies making us more vulnerable during both natural and man-made disaster**.[7]

The 2009 National Infrastructure Protection Plan, issued by the DHS, further explains what is at stake in increasing protection and maintenance of our nation's CIKRs:

> Protecting and ensuring the resiliency of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. **Attacks on CIKR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CIKR as weapons of mass destruction could have even more devastating physical and psychological consequences**.[8]

While many of the potential impacts to a CIKR attack or failure are catastrophic in nature, there are a host of common, everyday problems that typical CIKR decay has on our lives. As Andrew Hermann, American Society of Civil Engineers (ASCE) Treasurer explains,

> While it is easy to become caught up in large budget numbers and nationwide concerns, **the problems of America's infrastructure affect the everyday lives of Americans in a concrete way. For example, transportation systems across the U.S. are suffering the effects of age and overuse. Failure to invest in an already over-stressed transportation infrastructure is having a tangible impact on Americans' way of life, including longer commute times, greater wear on vehicles, and increased safety concerns. Decaying transportation systems also have a significant impact on U.S. businesses, by delaying freight delivery, creating unpredictability in supply chains, and increasing shipping costs, which increases consumer costs and diminishes competitiveness**.[9]

Due to the interconnected nature of many of our CIKR systems and sectors, failure or disruption of one system could harm the nation's security, public health, and economic activities.[10]

B. Nature of the Threats to CIKRs

There are numerous scenarios that threaten to substantially harm our vital CIKR sectors. While the threats posed by international and domestic terrorism attacks have received the most publicity, our CIKRs are also at considerable risk due to storms and other natural disasters and internal system failures and general wear and tear. We provide a glimpse into the general threats that exist at both an external and internal level to our CIKRs here, while our discussions later about specific CIKR sectors will highlight more specific sector vulnerabilities.

---

[7] Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*, 2006, http://cip.gmu.edu/archive/CIP_CriticalPath.pdf

[8] Department of Homeland Security, "National Infrastructure Protection Plan: Partnering to enhance protection and resiliency", 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[9] Andrew W. Herrmann, "America's Infrastructure," CIP Report, October 2009, http://cip.gmu.edu/archive/cip_report_8.3.pdf

[10] Marc Brooks, Nuclear Branch Chief of the Sector Specific Agency Executive Management Office, DHS, "Working Together for a More Secure and Resilient Nuclear Sector," CIP Report, March 2010, http://cip.gmu.edu/archive/cip_report_8.8.pdf

1. External Threats

a. Deliberate Attack

Perhaps the most widely discussed concern about our nation's CIKR protection is the risk of malicious attack from international terrorists or hostile regimes. These attacks could be cyber-terrorism attacks that disable or hijack our CIKRs or direct physical attacks against CIKR structures. Recent reports suggest that there is a rising threat posed by computer hackers and state-sponsored cyber-warfare. For example,

> **More than half of the operators of power plants and other "critical infrastructure" say** in a new study **that their computer networks have been infiltrated by sophisticated adversaries. In many cases, foreign governments are suspected**.**The findings come in a survey** being released Thursday **that offers a rare public look at the damage computer criminals can do to vital institutions such as power grids, water and sewage systems, and oil and gas companies. Manipulating the computer systems can cause power outages, floods, sewage spills and oil leaks.** The report was based on a survey completed by 600 executives and technology managers from infrastructure operators in 14 countries. The report was prepared by McAfee Inc., which makes security software, and the Center for Strategic and International Studies in Washington, which analyzed the data and conducted additional interviews. The respondents aren't named and specifics aren't given about what happened in the attacks. **The report comes as concerns are growing about state-sponsored hacking and threats to critical infrastructure.In November, CBS's "60 Minutes" reported that several Brazilian power outages were caused by hackers** -- a report that Brazilian officials have played down. **Last April, U.S. government officials said that spies hacked into the U.S. electric grid and left behind computer programs that would let them disrupt service. The intrusions were discovered after electric companies gave the government permission to audit their systems**.[11]

While no distributed denial of service attacks (DDos) have occurred on US infrastructure systems, it does not mean that there are severe vulnerabilities in our sectors. For instance, foreign nations such as China and Russia are suspected of spying on and mapping our infrastructure for future war planning or disruptive attacks:

> **Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system**, according to current and former national-security officials.**The spies came from China, Russia and other countries**, these officials said, **and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war**. "**The Chinese have attempted to map our infrastructure**, such as the electrical grid," said a senior intelligence official. "So have the Russians." **The espionage appeared pervasive across the U.S. and doesn't target a particular company or region,** said a former Department of Homeland Security official. "**There are intrusions, and they are growing,**" the former official said, referring to electrical systems. "**There were a lot last year**."[12]

According to the Cyber Division of the FBI, "cyber-terrorism may become a viable option to traditional physical acts of violence due to" its anonymity, diverse set of targets, low risk of detection, low risk of

[11] CBS News, "Hack Threats Aimed at Power Plants," Jan. 28, 2010, http://www.cbsnews.com/stories/2010/01/28/tech/main6150593.shtml?TB_iframe=true&height=650&width=850.
[12] Wall Street Journal, "Electricity Grid in U.S. Penetrated By Spies," April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html

personal injury, low investment, operate from nearly any location, few resources are needed.[13] A successful cyber-attack on U.S. CIKR could severally disrupt energy systems, emergency services, telecommunication systems, banking and finance networks, transportation and water systems, resulting in loss of life, public health and safety vulnerabilities and massive economic loss.

Another commonly discussed physical attack scenario includes nuclear, biological or chemical attacks on U.S. ports or other CIKRs. For instance, WMDs, dirty bombs, or chemicals and explosives in cargo vessels could be used to attack US ports, military vessels and bases, cruise ships and ferries, dams, power plants and other critical infrastructures.[14] As well, terrorist groups could use electromagnetic pulse (EMP) weapons against financial and national defense CIKRs to cripple a host of vital CIKRs. As Baker Spring of the Heritage Foundation explains,

> In 2004, **the** congressionally mandated **Commission to Assess the Threat to the United States from** Electromagnetic Pulse (**EMP) Attack released an unclassified executive report on its broader study of the U.S.'s vulnerability to EMP weapons strikes**.[1] **In 2008, the commission released a follow-up report that detailed the vulnerabilities of the critical infrastructures of the U.S. to EMP strikes**.[2] Taken together, these two reports make it clear that an EMP attack could inflict severe damage on the U.S. As the initial report stated, "**EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences**." Congress should not let the Obama Administration ignore the commission's findings. Instead, it should mandate an updated assessment of which countries may be pursuing EMP weapons and associated delivery systems and platforms. Further, Congress should demand that the Administration develop, test, and ultimately field defenses against EMP attacks, including improved ballistic missile defenses capable of countering short-range ballistic missiles that can carry EMP warheads. What Is EMP? **EMP is triggered by the detonation of a nuclear weapon at a high altitude over the earth. As a result of this detonation, an electromagnetic field radiates down to the earth, creating electrical currents. These fields cause widespread damage to electrical systems—the lifeblood of a modern society** like the U.S. **In turn, the damaged electronic systems can cause a cascade of failures throughout the broader infrastructure, including banking systems, energy systems, transportation systems, food production and delivery systems, water systems, emergency services, and—perhaps most damaging—cyberspace.**[15]

An additional physical attack scenario includes biological attack on the U.S. agricultural system. For instance, in 1984, a domestic cult group contaminated salad bars at several Oregon restaurants with *Salmonella* bacteria, making it the first bioterrorism attack on U.S. agriculture and food systems. While that attack was fairly small in scope, it highlights the vulnerability that a highly concentrated livestock and food processing industry poses.[16] More recent E. coli outbreak that spread throughout several states and caused millions of dollars of loss for food industries highlights how easily a biological attack on our

[13] US Army Training and Doctrine Command et al., "Critical Infrastructures: Threats and Terrorism," August 10, 2006, http://www.fas.org/irp/threat/terrorism/sup2.pdf
[14] Paul Parformak and John Frittelli, "Maritime Security: Potential Terrorist Attacks and Protection Priorities," CRS Report for Congress, January 9, 2007, http://italy.usembassy.gov/pdf/other/RL33787.pdf
[15] Baker Spring , "Electromagnetic Pulse Weapons: Congress Must Understand the Risk," Heritage Foundation, March 3, 2010, http://www.heritage.org/Research/Reports/2010/03/Electromagnetic-Pulse-Weapons-Congress-Must-Understand-the-Risk
[16] US Army Training and Doctrine Command et al., "Critical Infrastructures"

agricultural infrastructure can undermine consumer confidence and cause a host of public health problems.[17]

b. Storms/Natural Damage

The widespread damage to energy and chemical infrastructures caused by 2005's Hurricanes Katrina and Rita illustrate the threat posed by major meteorological events and natural disasters. Natural events such as hurricanes, tropical storms, floods, ice storms, earthquakes and tornadoes risk several damage to power, communication, public health and safety services sectors.[18] More concerning is the risk posed by meteorological events and natural disasters on nuclear power plants. In 1993, a severe flood of the Missouri River threatened the safety of the Cooper nuclear power station in Brownville, Nebraska. On June 24, 1998, the Davis-Besse nuclear power station near Toledo, Ohio was hit with tornados with wind speeds between 113 and 156 miles per hour. While the incident did not produce any long-term effects, several critical systems were knocked out, making a great deal of the station vulnerable to disaster. On April 27, 2002 the Calvert Cliffs nuclear power station near Chesapeake Bay nearly missed a 260 mile per hour tornado. Also in August 1992, Hurricane Andrew did considerable damage to the Turkey Point nuclear power station, located near Miami. The hurricane knocked out all offsite power and communication for several days and destroyed fire protection systems. The loss of power to these facilities due to natural disasters can quickly lead to core meltdown accidents:

> **Over 50% of all postulated accidents leading to a core melt accident begin with a station blackout according to NRC studies**. For example, **a natural disaster that disables the incoming power lines to a nuclear power station coupled with the failure of on-site emergency generators** (i.e. fouled diesel fuel in leaky storage tanks) **can result in the depletion of the emergency battery supply system after 4 hours. Without electricity** (AC and DC) t**he operator loses instrumentation and control power leading to an inability to cool the reactor core. According to one U.S. NRC report** "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," **in the event of station blackout at the Surry or Peach Bottom nuclear power stations "core damage was estimated to begin in approximately 1 hour if the auxiliary feedwater system and HPI** (high pressure injection) **flow had not been restored in time**."[19]

2. Internal Threats

a. Internal Failure

A number of threats to our nation's CIKR exist from poor upkeep and maintenance, wear-and-tear, and simple human error. For instance,

> **Simple wear-and-tear also poses a constant challenge to critical infrastructure. In the 1980s, a great deal of federal-level attention was devoted to discussing the deteriorating state of the nation's physical infrastructure**—the roads, bridges, dams, airports, and similar systems upon which the country depends. **The problem is not a small one: nearly four million miles of roadway alone crisscross the country**. **In its 1988 final report**, Fragile Foundations:

---

[17] Adam Stirrup, "COMMENT: HIDDEN CARGO: A CAUTIONARY TALE ABOUT AGROTERRORISM AND THE SAFETY OF IMPORTED PRODUCE," San Joaquin Agriculture Law Review, 2006/2007.
[18] Paul Parformak, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," CRS Report for Congress, December 21, 2005, http://cip.gmu.edu/archive/Concentrated_CritInfra.pdf
[19] Paul Gunter, "Natural Disasters and Safety Risks at Nuclear Power Stations," Nuclear Information and Resource Service, November 2004, http://www.nirs.org/factsheets/naturaldisaster&nuclearpower.pdf.

> A Report on America's Public Works, **a national council gave the nation's infrastructure a C-, "hardly something the world's largest industrial power can be proud of." Upkeep, much less expansion, presents an enormous and ongoing infrastructure chore. Other problems that can plague critical infrastructure include technological obsolescence, poor maintenance, accidents, or that perennial peril: human error. "There are more communications systems taken down per day by the backhoe than by anybody else,**" notes one infrastructure expert with a touch of humor.[20]

While these threats are not malicious in intent and are usually accidental or natural, they post a substantial threat to our nation's CIKRs nonetheless as failure of one system can lead to CI failure in other sectors.

b. Sabotage

Generally, most deliberate attack scenarios on U.S. CIKR assume external attack from international terrorists or hostile regimes. However, the Oklahoma City bombing and the recent arrest of the Hurattee Christian Militia group members remind us of the increasingly growing threat posed by domestic terrorism. Since Obama's election, there have been 25 terror plots by non-Muslim domestic extremists and 9 plots by Muslim and domestic and international groups. Since 9-11, there have been 51 total plots by domestic non-Muslim groups.[21] Given the ease of access to CIKR that these group have over international terrorists or other forces, domestic terrorism or sabotage poses a substantial risk. Additionally, terrorists or militias are not the only internal risk of sabotage to U.S. CIKR. As Michael Vatis explains,

> **In the past, threats to our infrastructures were physical in nature**, such as truck bombs or acts of sabotage, **and the likely perpetrators were terrorist groups and hostile foreign powers**. **Now the list of possible attackers includes disgruntled insiders seeking revenge, hackers testing their skills, criminals seeking financial gain, foreign intelligence operatives seeking sensitive government or industrial information, and terrorist groups or hostile nations conducting attacks on vital services such as electrical energy or telecommunications. The anonymity of the cyber world makes it difficult to identify those responsible for an intrusion, or their intentions**.[22]

[20] Kathi Ann Brown, Critical Path: A Brief History of Critical Infrastructure Protection in the United States, 2006, http://cip.gmu.edu/archive/CIP_CriticalPath.pdf
[21] Muslim Public Affairs Council, "MPAC Releases Policy Memo Analyzing Post-9/11 U.S. Terrorism Cases," MPAC, March 22, 2010, http://www.mpac.org/article.php?id=1075
[22] Michael A. Vatis, "National Infrastructure Protection Center," CALEA Online, 1999, http://www.calea.org/online/newsletter/No75/The%20National%20Infrastructure%20Protection%20Center.htm

III. REASONS WHY THE DEBATE COMMUNITY SHOULD DEBATE CIKR

The Critical Infrastructure literature base remains untapped

Pervious topics that have addressed issues relevant to CIKR, such as the 2004-05 energy topic, were constructed in fashion that separated the resolution from some of the most accurate and important literature base. The CIKR topic gets to the heart of how the U.S. maintains and operates its infrastructure, allowing debaters to focus on a holistic appreciation of CIKR or to hone in on one or two specific instances where the infrastructure is in desperate need of attention.

We have never really debated this subject. In 2001, we avoided debating 9-11 homeland security strategy when Ross Smith and others raised this possibility because it would have disrupted the season substantially and was perhaps too timely. However, we have never returned to debate this issue. Now after 10 years, perhaps we should finally examine how safe we are from a host of CIKR attacks and failures.

Despite some critic's[23] contention that this is a recycled topic, the only time we have debated any of these issues was on the 2001-2002 Indian Topic (Border Security Affs), the 1997-1998 Southeast Asia topic (Cyber-security Affs) and the 2004-5 Energy Topic (some advantages claimed to solve for infrastructure failure and Highway Safety Fund DAs). However, we have never debated an entire topic on these issues to any depth in recent years. It seems silly to eliminate this topic from considerable simply because we have had very minimal discussion of this topic on the margins of other topics. Under that logic, we would not be able to debate any topic in the future.

It's Timely

The most recent analysis of the United States infrastructure, conducted in 2009, gave the nation an average grade of a D[24]. While this grading system might appear arbitrary, it indicates systemic neglect throughout all infrastructure sectors within the United States. The American Society of Civil Engineers (ASCE) indicates that we would need over two trillion dollars to completely revamp our domestic infrastructure[25]. President Obama has acknowledged the need to revamp the domestic infrastructure, recently focusing on the creation of high-speed rail transportation[26]. Despite these moves, it is unlikely that the administration's efforts will moot core sections of the topic. Obama has recently proposed a six-

[23] http://cedadebate.org/forum/2010-2011-topic/need-for-a-discussion-of-standards-to-determine-a-yearly-topic/msg1395/#msg1395.
[24] American Society of Civil Engineers, 2010. http://www.infrastructurereportcard.org/
[25] Environment News Service, 2009. *Engineers Give U.S. Infrastructure a 'D', $2.2 Trillion Price Tag", http://www.ens-*newswire.com/ens/jan2009/2009-01-28-01.asp
[26] Smart Planet, 2010. *Obama's $50B infrastructure plan: what it means for rail*, 9/7/10, http://www.smartplanet.com/business/blog/intelligent-energy/obamas-infrastructure-plan-for-high-speed-rail/2616/

year infrastructure development plan totaling $50 billion[27], making the discussion of infrastructure increasingly prevalent in the news and academic spheres. However, even if the President's plan were passed in full, it would only provide 2.5% of the funding ASCE indicates would be necessary to solve our infrastructure.

2011 is an important year for infrastructure issues. First, the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU) expired Sept. 30, 2009 and has been extended several times without a proper reauthorization. Given the challenges posed in the upcoming budget debates, it is very likely that SAFETEA-LU reauthorization will be pushed after the election. Thus, while the issue will be timely and discussed in policy circles, it is very unlikely that any substantial federal action will occur next year.[28] Second, a host of other infrastructure debates will be occurring in policy circles that warrant our discussion in the near future. As Gerald L. Baliles, Director of the Miller Center of Public Affairs at the University of Virginia contends,

> The need for reform is thus well-established. Furthermore, SAFETEA-LU and Vision 100 Century of Aviation Reauthorization Act's expirations and the re-examination of the country's federal transportation laws and programs that will take place imminently make it a critical time for informed, forward-looking, credible discussion and study of future transportation policy.[29]

Increased argumentative diversity

While all of the topic choices will undoubtedly provide a far division of interesting ground, CIKR is unique in its potential to dramatically expand the core ground for both the affirmative and negative beyond the normal constraints of standard resolutions. The sheer diversity of topics ranging from energy to military defense to healthcare means that every debater, novice to varsity, can find something that they themselves find interesting. This is balanced by the narrow focus on how CIKRs are classified, providing diverse ground while simultaneously preventing a resolution that rewards small one-shot affirmatives. Additionally, the topic will require students to read from a different literature set other than the typical foreign policy and law journals, which provides great educational benefits to students. As West Georgia's Mike Hester argues,

> From the debate coach's perspective, I'd rather see a Critical Infrastructure topic than a Treaties topic. It's more timely in terms of what the US has ignored at its own peril, it's been wholly ignored by the college debate community, and it'd be nice to see debaters have to read some different literature rather than scouring backfiles for Congressional-Executive Agreement CPs.[30]

---

[27] CNN, 2011. *Obama: U.S. infrastructure has 'slipped'*,1/26/11 http://www.cnn.com/2011/US/01/26/obama.infrastructure/index.html
[28] See States News Service, "AED: It's Time to Jump Start Highway Reauthorization," March 16, 2011, http://www.forconstructionpros.com/online/article.jsp?siteSection=25&id=19739
[29] "Well Within Reach America's New Transportation Agenda," 2009, http://web1.millercenter.org/conferences/report/conf_2009_transportation.pdf
[30] http://cedadebate.org/forum/2010-2011-topic/soliciting-input-for-the-10-11-topic/msg407/#msg407

IV. REASONS WHY THE DEBATE COMMUNITY SHOULD NOT DEBATE CIKR (AND OUR RESPONSES)

Is the CIRK topic too big?

The biggest question that we've heard from the debate community is whether this topic would be too big to handle. While the size of the topic is perceptually daunting, this anxiety can be eased through an appreciation of the literature which illustrates that the topic is actually quite specific and strategically limited. This will be particularly true if the debate community choses to adopt our proposed resolution, including the terms 'protection' and 'resiliency' each of which deal with specific cores of literature that speak to real-world scenarios. As well, as our topicality section suggestions, the topic committee would have a number of options that could limit the topic even further.

Additionally, many infrastructure sectors, such as Postal and Shipping, could not function as stand-alone affirmatives. Rather, these sectors require significant overlap with other areas of the topic in order to function. This overlap is significant enough as to limit the number of affirmatives that could be created under the topic while still providing ample room for exploration of new arguments throughout the academic year.

Are CIKR sectors too intertwined to gain solvency for small affs?

It is true that certain small affs will be unable to find substantial ground due to alternative factors that prevent solvency. However, this weeding out of some affirmatives in no way indicates an inability for teams to run reasonably compact affirmatives that have large, focused impacts. While all CIKR sectors are critical, some are more critical than others and these lynchpin sectors will provide ample ground for small affirmatives to explore the topic area without having to do endorse a 'complete overhaul' affirmative.

Miswording of the resolution could explode the topic by incorporating foreign infrastructure key to the United States

Among the vast number of classified documents distributed by Wikileaks was one message in particular that identified hundreds of international resources deemed to be critical infrastructures and key resources[31]. Not owned or operated by the United States, these operations have been deemed critical to the continued functioning of the world economic system. Ranging from cobalt mines in Congo to electric power transformers in South Korea, it is easy to see why including these infrastructures in the topic would make the resolution unwieldy. This conundrum can be avoided through a careful wording of the resolution

[31] Buisness Insider, 2010. *Wikileaks Unveils Over 300 Foreign Sites That Are Critical To U.S. National Interests*, http://www.businessinsider.com/wikileaks-critical-foreign-dependencies-2010-12, 12/6/10

in which only operations owned and within the United States are topical. Once again, this is discussed in depth in the wording section of this paper.

There is no critical affirmative ground on this topic

First, it does not seem to be the case that offering clear and predictable affirmative critical ground will cause more critical teams to stay within the boundaries of the topic in a meaningful way. For instance, on the immigration topic – which offered a fairly broad range of critical options – many teams still operated metaphorically with the topic, refused to run plans, gave visas to Pokemon, etc. While some teams will operate within the boundaries of the topic, it's not clear in recent history that other critical teams will ever operate within the confines of any topic that uses "U.S. federal government" or "Resolved."

Second, while at first glance, that might appear to be the case, but after reading past the surface level of the topic, there are a number of critical argument affirmatives on the topic. A few of these options are outlined below:

One option would involve a host of Native American issues. A number of U.S. infrastructures lie on Native American tribal lands. This provides both critical affirmative ground to restore sovereignty and localized control for Native groups to best protect these CIKRs. Additionally, negatives could use arguments like these to contend that we should "give back the land," consult tribes and other similar arguments. Arguments from Jennifer Butts in 2003/2004 offer a glimpse of this kind of argument:

> The administration took these measures to guarantee the protection of border patrol and critical infrastructure. By doing this, the federal government was protecting the lives of United States citizens. But with the existing Homeland Security Act, not all critical infrastructure is adequately protected. n4 Borders are still open to illegal immigrants. This is because the Department of Homeland Security has failed to recognize the government-to-government relationship with tribal governments. The Tohono O'odham Nation shares a border with Arizona and Mexico. A similar situation occurs on our northern border with the Blackfeet Nation. Also important to consider is the amount of critical infrastructure present on tribal lands. This critical infrastructure includes the Grand Coulee Dam on the Colville reservation, which is the largest producer of hydroelectric power in the United States, and the third largest in the world. n5 Also present are nuclear [*375] power facilities, power grids, military supply manufacturers, and transportation routes. n6 These facts have gone overlooked for many years, but in a time of heightened awareness, they are more than a little unsettling. With miles and miles of open terrain bordering both Canada and Mexico, terrorists have an easy way to pass into the country undetected. The imagination runs wild with possible scenarios of illegal migrants entering the country to cause great tragedy and devastation, As Attorney General John Ashcroft said to a conference on border security, "our homeland security remains threatened so long as any portion of our international border remains unprotected." n7 A solution to this problem would be for Congress to amend the Homeland Security Act to recognize tribal sovereignty and to give tribes more localized control of detecting and preventing terrorism. Amendments have been presented in the Senate, but have yet to be passed. n8 The tribal amendments are necessary in order to carry out the function of the war on terror and protect the homeland from terrorism.[32]

[32] Jennifer Butts, "VICTIMS IN WAITING: HOW THE HOMELAND SECURITY ACT FALLS SHORT OF FULLY PROTECTING TRIBAL LANDS," 28 Am. Indian L. Rev. 373, 2003/2004

Also, Richard Coyne describes the ways in which the networked nature of infrastructures like transportation, information technology, communication networks, and financial systems intersect with Deleuze and Guattari's work:

> **The third lesson is to observe that the network notion has the capacity to move discourse towards the transcendent, avoiding the here and now, the existential moment, the phenomenon, in favour of something that does not exist, an ideal, a utopian appeal to the "not yet."** lxvi The appeal to the network notion masks our everyday experience of screens, keyboards, connecting and disconnecting, the sociality of communities of users, designers, entrepreneurs, breakdown, life outside the matrix of connections, outside the network, that which is disconnected and "other." **A further way to defuse this idealism is to regard networks in the same way we might consider diagrams. Networks can be thought of as projections, visualisations and images rather than windows into some deeper core of reality that otherwise defies representation**. To be sure, we now have dynamical, immersive, navigable, and complex visualisations, abetted by fast computer processing. The calculable and navigable properties of these networks are palpable. **Deleuze and Guattari have much to say about the diagram, and the map. In flattened terms a diagram has "neither substance nor form, neither content nor expression**" lxvii **Maps and diagrams provoke rather than describe, map**s 15 **are an "experimentation in contact with the real**." lxviii **Networks as maps are just such interventions and provocations, or more prosaically, assume status dependent on interpretation and evaluation**. We seem able to relate these diagrams to some state of affairs, such as the layout of Konigsberg, the urban condition, the configuration of the Internet, links within stock markets, transportation systems, stresses in a structure. **As with any diagram the process of establishing such relationships between a network and a state of affairs is interpretive, which is to say cultural, social, historical, situational, and hermeneutical.** One of the key characteristics of the network, the loop, can also be ascribed to the process of interpretation. It is commonly supposed that when interpreting a text, piece of music or a diagram we begin from a position of some partial expectation and understanding, which is then modified in light of an examination of the subject matter. **The process involves a backwards and forwards movement, a constant process of revision, a cycle of understanding, that converges on a practical understanding for the moment, but which is still subject to revision, a process sometimes characterised as the "hermeneutical circle**." lxix At one point Deleuze and Guattari briefly allude to this process in terms of shifting territories of impulses and circumstances. lxx As a life condition, this cycle of understanding can assume the "violent centrifugal movement" of Nietzsche's eternal return. The circular motion of this understanding can certainly be described benignly in network terms as a feedback loop. But **perhaps our attraction to the network notion is also driven by our inevitable participation in the cycle of interpretation, and our technologically-mediated desire to render this experience tangible, concrete and controllable, through the diagram. All of this can be resisted.**[33]

Work by Graham and Livesay also highlight the interrelationship between CIKR networks/structures and a critical understanding of the City:

> As we begin to consider the potential relationships between the expanded theory of the event provided above, with the contemporary city it is also useful to attempt to define the contemporary city in general terms. Cites emerged with the development of agriculture and the production of surplus food, which in turn led to settlements that supported both specialists (rulers, priests, soldiers, craftsmen, merchants/traders, etc.) and general labour, those not engaged in agriculture. **Essential to the structure of cities were the development of writing to keep records, a social structure, and technologies (particularly in transportation, tool making, and weaponry). Therefore, cities have been considered to be both material and immaterial, or social and formal, and they have been dependent on interconnectivity with the surrounding agricultural system, and extensive trading networks**. Cities draw people together into dense settlements. Since the emergence of the city in the Neolithic era, the fundamental aspects of the city have remained, however, the relative emphasis on the component elements has changed. **With the emergence of postmodernity the city has once again gone through dramatic changes in structure, social organization, and technology. The influential American urban historian and theorist**

[33] "The Net Effect Design, the rhizome, and complex philosophy, http://www.casa.ucl.ac.uk/cupumecid_site/download/Coyne.pdf

> **Lewis Mumford**, in his 1937 essay "What is a City?," provides one definition of the city when he **writes: The city is a related collection of primary groups and purposive associations….These varied groups support themselves through economic organizations…and they are all housed in permanent structures, within a relatively limited area….The city in its complete sense, then, is a geographic plexus, an economic organization, an institutional process, a theater of social action, and an aesthetic symbol of collective unity**. Mumford also provides a general definition of the city in the introduction to his 1938 book The Culture of Cities, he writes: **The city…is the point of maximum concentration for the power and culture of a community….The city is the form and symbol of an integrated social relationship: it is the seat of the temple, the market, the hall of justice, the academy of learning.** Here in the city the goods of civilization are multiplied and manifolded; here is where human experience is transformed into viable signs, symbols, patterns of conduct, systems of order. Here is where the issues of civilization are focused…. **Mumford's definitions provide a clear indication that the city represents for him a relatively stable condition, that it is the centre of religion, economy, law and education, and that it has a transformative impact on its citizenry**. For Mumford, a city occupies a distinctive location and 10 has material presence, but is also about social relationships, economic systems, laws, and symbolic structures; much of this accords with a brief description of the city provided by Whitehead in his book Adventures of Ideas.[34]

From this understanding of CIKRs and the City, affirmatives could argue that public transportation systems, communication, emergency and a host of "City" systems are crucial to interrogating privilege, power, and citizenship.

[34] "Deleuze, Whitehead, the Event, and the Contemporary City," No Date, http://whiteheadresearch.org/occasions/conferences/event-and-decision/papers/Graham%20Livesey_Final%20Draft.pdf

V. TOPICALITY

THE RESOLUTION

A. Proposed Wording

We propose the following wording proposal to serve as a starting point of discussion:

> Resolved: the United States Federal Government should substantially increase the protection and resiliency of its Critical Infrastructures and Key Resources.

B. Discussion of Terms

Here are explanations and rationales for our preferred wording choice along with a discussion of alternatives.

1. "The United States Federal Government"

The agent of action should be the United States of America as expressed through the federal government located in Washington D.C., not one or more of the 50 state governments. The interaction between the federal government, state governments, and private actors is central to much of the literature on critical infrastructure protection. In our suggested wording, these issues could become negative arguments such as "State Counterplan," "Voluntary Private Action Counterplan," and other similar arguments.

2. "Substantially Increase"

Substantially and Increase are frequently used terms in many high school and college debate resolutions. Given that some levels of CIKR protection and failure prevention occurs in the status quo, some adverb is necessary to require the Affirmative to be greater than the SQ efforts. Unfortunately, this term and "significantly" really do not provide a clear guideline as to how much increase the affirmative should be.

3. The Verb/Mechanism—Several Options

Due to some changes in political verbiage and doctrinal changes, the central terminology used to describe CIKR protection has changed. This is in part because so much attention was given to responding to external attacks to the infrastructure after 9-11. With the Northeast Black Out of 2003 and the 2005 damage caused by Katrina, more emphasis was given to internal infrastructure failures or non-terrorist attack problems, which lead to the use of CIKR terms such as "resiliency", "mitigation."

a. "Protection"

Despite these changes in emphasis, the term "protection" is most frequently used as an umbrella term to describe a range of policies that ensure the resiliency, security, and preparedness of the U.S. CIKR sectors. According to the DHS' 2009 National Infrastructure Protection Plan, "protection" is defined as:

> **Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their inter-connecting links**. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident (see figure S-1). **Protection can include a wide range of activities, such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, install-ing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, business continuity planning, and restoration and recovery actions, among various others**.[35]

Additionally, "protection" is a term that means more than just defense from external attack. As the George Mason University Law School program on Critical Infrastructure Protection explains in 2009:

> Given the criticality of the systems, networks, and assets we rely on so greatly, the protection of such infrastructure is essential to not only our well-being, but also our way of life. Critical infrastructure protection, commonly referred to as CIP, is a priority for the Federal government, as well as the private sector and state, local, and tribal governments. With approximately 85 percent of the Nation's critical infrastructure owned by the private sector, and no single, overarching body managing this infrastructure, the task of protecting critical infrastructure is daunting. **Critical infrastructures must be protected from all hazards, both natural and man-made disasters and terrorism, whether a cyber-related threat or large-scale physical attack. Hurricanes, earthquakes, fires, and train crashes can impact infrastructure just as much as a premeditated act aimed at disrupting services or harming the populace. Considering this, we must better understand the Nation's infrastructure to ensure its protection**.[36]

However, Daniel Overbey[37], former NDT debater and coach who now works at the DHS in the Sector Specific Agency Executive Management Office that oversees 6 of the 18 CIKR sectors, raised an interesting problem that the use of the term "protection" might raise:

> One thing about "Protect" that will cause you a lot of grief - there are a handful of different "missions" within DHS. The overarching missions used to be Prevent, Protect, Respond, and Recover (PPRR), but that is losing favor lately because of "resiliency" and "mitigation." Also - "Preparedness" is one of the en vogue ways to describe the degree to which CIKR is ready for any disaster, internal or external.[38]

A 2010 GAO Report supports Overbey's observations, in arguing that "resiliency" is no longer used as a subset of "protection," but is used as an equally important area of risk security:

> **DHS increased its emphasis on resiliency in the 2009 NIPP by discussing it with the same level of importance as protection**. While the 2009 NIPP uses much of the same language as

[35] Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protecting and Resiliency, 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
[36] GMU Law School CIP website "What is CIP?", 2009 http://cip.gmu.edu/cip/.
[37] If this topic is selected, we strongly recommend that the committee consult with Dan over term of art issues and other issues on the topic. He was a great resource in the early shaping of this paper.
[38] Personal Email, March 31, 2010.

> the 2006 NIPP to describe resiliency, **the 2006 NIPP primarily treated resiliency as a subset of protection while the 2009 NIPP generally referred to resiliency alongside protection**. For example, while the Managing Risk chapter of the 2006 NIPP has a section entitled "Characteristics of Effective Protection Programs," the same chapter in the 2009 NIPP has a section entitled, "Characteristics of Effective Protection Programs and Resiliency Strategies." **DHS officials stated that these changes are not a major shift in policy; rather they are intended to raise awareness about resiliency as it applies within individual sectors. Furthermore, they stated that there is a greater emphasis on resilience in the 2009 NIPP to encourage more sector and cross-sector activities to address a broader spectrum of risks, such as cyber security**.[39]

b. "Resiliency"

"Resiliency" differs from "protection" activities in that it is more internally focused to ensure the functions and structures of CIKRs in the face of internal and external threats. As a March 2010 GAO Report explains,

> Part of the recent discussion over resiliency has focused on the definition of the concept. In February 2006, **the Report of the Critical Infrastructure Task Force of the Homeland Security Advisory Council defined resiliency as "the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must**." **Later in 2006, the Department of Homeland Security's National Infrastructure Protection Plan**—again focusing on critical infrastructure, not agencies—**defined resilience as "the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident.**" In May 2008, the House Committee on Homeland Security held a series of hearings focusing on resilience at which government and private sector representatives, while agreeing on the importance of the concept, presented a variety of definitions and interpretations of resilience. Also, **in April 2009, we reported that organizational resiliency is based on 21 attributes particularly associated with resilience and assigned them to five related categories. These categories are emergency planning, organizational flexibility, leadership, workforce commitment, and networked organizations**.1 **Likewise, government and academic organizations have discussed how resiliency can be achieved in different ways. Among these are an organization's robustness (based on protection, for example better security or the hardening of facilities); the redundancy of primary systems (backups and overlap offering alternatives if one system is damaged or destroyed); and the degree to which flexibility can be built into the organization's culture (to include continuous communications to assure awareness during a disruption, distributed decision-making power so multiple employees can take decisive action when needed, and being conditioned for disruptions to improve response when necessary**).[40]

c. Final opinion on the verbiage/mechanism issue:

The literature does not appear to make a significant distinction between "protection" and "resiliency." The terms seem to be used to emphasize certain DHS priorities rather than major substantive differences. Both definitions provided here provide a great deal of overlap in policies and actions. However, given that some distinction between the two is made in the literature, it would make sense to include both terms in

---

[39] GAO Report, CRITICAL INFRASTRUCTURE PROTECTION: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience," March 2010, http://www.gao.gov/new.items/d10296.pdf

[40] GAO Report, CRITICAL INFRASTRUCTURE PROTECTION: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience," March 2010, http://www.gao.gov/new.items/d10296.pdf

the resolution. While most topic areas are not affected by this distinction, including both verbs will ensure that potential affirmatives will not be excluded due to definitional issues.

The concern that this raises is that inclusion of both terms will explode the limits of the topic to make anything regarding CIKRs topical. We feel as though limiting the topic to be only about protection from external threats (e.g., terrorist attacks, storm damage) or resiliency issues (e.g., internal system failure, internal sabotage) would overly narrow the topic. As a result, it would probably make a great deal of sense to limit the scope of the topic with a list of CIKRs that could be debated. Given that there are 18-19 potential sectors, some limit on that part of the resolution seems necessary.

3. "Its"

Some infrastructure systems are highly interconnected and regional and global in scope. The size of the resolution would explode if the resolution does not limit the scope of policies to be directed at our infrastructures. However, if a sector such as Government Facilities, for instance, is included in the resolution, increasing protection and resiliency of embassies and other government facilities, perhaps even military bases, would become topical.

4. "Critical Infrastructure and Key Resources"

a. Inclusion of both terms

The term "critical infrastructure" was originally defined in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)). "Key resources" is defined in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)). As a 2006 GAO Report explains, CIKRs are:

> *Critical infrastructure* are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, and national public health or safety, or any combination of those matters. *Key resources* are publicly or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation's morale or confidence.[41]

As mentioned in the opening of this paper, CIKR's are listed by the DHS as the following 18 sectors[42]:

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base

[41] "GAO-07-39 Critical Infrastructure Protection Coordination Issues," October 16, 2006, http://www.gao.gov/new.items/d0739.pdf
[42] Ibid

- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

B. Eliminate Key Resources

We are sure that many people will be concerned by the rather long list of CIKRs. As a result, another wording option would be to include “Critical Infrastructures” without “Key Resources.” The only reasons to include “Key Resources” are: (1) current literature seems to recognize that key resources are important to protect as well; and (2) it provides a more diverse list of areas/sectors.

However, a good topic could be crafted using just the term “Critical Infrastructures.” This would reduce the current list of 18 to eight sectors.

The 1997 Report of the Technologies to The People's Commission on Critical Infrastructure Protection[43] provides a much narrower list of just Critical Infrastructures (CI) without Key Resources. This narrows the list to eight CI sectors:

- Information and Communications
- Continuity of Government Services
- Banking and Finance
- Water Supply
- Electrical Power, Oil and Gas Production and Storage
- Transportation
- Emergency Services
- Public Health Services

Executive Order 13010,2 signed by President Clinton on July 15, 1996, whichestablished the President’s Commission on Critical Infrastructure Protection[44], outlines a similar list of eight critical infrastructures:

- telecommunications
- electrical power systems;
- gas and oil storage and transportation;
- banking and finance;
- transportation;
- water supply systems;
- emergency services (including medical, police, fire, and rescue);
- continuity of government.

[43] http://www.irational.org/APD/IPC/criticalinf.htm
[44] http://www.fas.org/irp/crs/RL31556.pdf

5. Other Wording Concerns/Wording Options

A. Narrow by Eliminating "Key Resources"

The initial wording suggestion that we provide is admitted large in scope. We prefer to start with a broader wording as it is most likely that community discussion and topic wording papers will move to narrow the topic. Since this is an inherent tread in past years, we start rather broadly, but offer some wording suggestions to guide future consideration.

If there is a desire to have a much narrower topic that does not include a list, we would recommend eliminating "Key Resources" from the topic and just include "Critical Infrastructures," such as:

> Resolved: the United States Federal Government should substantially increase the protection and resiliency of its Critical Infrastructures.

B. Narrow by Including a List

Another way to narrow the scope of the resolution would be to create a list at the end of the resolution that lists the CIs or CIKRs that can be debated. For instance, an example of this kind of wording might be:

> Resolved: The USFG should increase the protection and resiliency of one or more of the following:…

We do not believe that list topics are inherently problematic, but we understand that some portions of the community dislike them. We believe that it would be much easier to narrow the scope of the resolution through a list option, but as mentioned above, there are other options to narrow the topic.

C. Narrow by Eliminating "Resiliency"

Another option to narrow the topic would be to eliminate "resiliency" from the resolution. While it would certainly eliminate some affirmative approaches, it would probably narrow the topic too much in ways that would make the topic become stale rather quickly. To just include "protection" might cause the topic to be focused only on external attacks (e.g., terrorists) or external damage (e.g., storms) without discuss of internal system failure, which is one of the largest concerns today. We contend that one of the other narrowing options listed above would be superior to eliminating "resiliency."

VI. CIKR SECTORS

The following section will provide a brief analysis of each CIKR sector and the ground it will provide for the affirmative and negative throughout the year. While these brief reviews provide a preview to how the resolution will function, we have chosen to view each sector in a vacuum rather than focusing on the interconnected nature and potential multi-sector plans afforded through the resolution. This tactic is employed due to the variety of topic words available, each of which will determine which, if not all, CIKR sectors will be included within the resolution.

It is important to note that all CIKR sectors have two important overseeing borders, the Government Coordinating Council (GCC) and the Sector Coordinating Council (GCC). These organizations work in tandem with the goal of informing governmental and private actors as to the needs and wishes of all parties involved in the relevant CIKR sector.

Agriculture and Food

Introduction

Before addressing the ground distribution of this sector it is important to note that this is *not* a rehashing of the recent agriculture topic. While the 2008-09 resolution dealt with agricultural subsidies, the CIKR topic area would address the security and resiliency of the nation's agriculture and food supplies. These topic areas differ substantially due to CIKR's focus on providing redundant fail-safes and increasing the security of our food resources; issues that were only addressed tangentially in previous years.

Choosing to debate critical infrastructure during the 2011-12 academic year will require students to greatly expand their knowledge of how threats are assessed and qualified in the agricultural sector. Presently, the government and private sector employ the "CARVER + Shock" approach of assessment.

> **CARVER is an acronym for** the following six attributes used to evaluate the appeal of a target for attack:
> - **Criticality**: Measure of **public health and** the **economic impacts** of an attack;
> - **Accessibility**: **Ability to physically access** and egress from **target**;
> - **Recuperability**: **Ability of system to recover** from an attack;
> - **Vulnerability**: **Ease of accomplishing attack**;
> - **Effect**: **Amount of direct loss** from an attack as measured by loss in production; and
> - **Recognizability**: **Ease of identifying target**.
>
> The seventh attribute, **Shock**, **represents** the combined **health, economic, and psychological impacts** of an attack.[45]

This breakdown is well-rooted in the literature of the topic area and provides not only a means of exploring potential affirmative ground, but also an excellent guide to determining the significance of harms and solvency. Concerning potential impacts in this sector, there are a great number of scenarios to consider. The vulnerabilities of our food supply are extensive, as disclosed in a 2004 Homeland Security Presidential Directive:

> The United States agriculture and food systems are vulnerable to disease, pest, or poisonous agents that occur naturally, are unintentionally introduced, or are intentionally delivered by acts of terrorism. America's agriculture and food system is an extensive, open, interconnected, diverse, and complex structure providing potential targets for terrorist attacks. We should provide the best protection possible against a successful attack on the United States agriculture and food system, which could have catastrophic health and economic effects.[46]

Taking these impacts into consider, it's easy to see why this sector is among those listed under CIKR protocols. Debaters will likely draw upon the experience of their coaches from the subsides topic, but will find that the particular scenarios outlined in the literature will require a fresh look into the agricultural sector and how its viability influences the American way of life.

---

[45] Department of Homeland Security, Food (Meat, Poultry, and Egg Products) and Agriculture Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/nipp-ssp-ag-food.pdf, 2007

[46] FAS, Homeland Security Presidential Directive / HSPD-9: Defense of United States Agriculture and Food, http://www.fas.org/irp/offdocs/nspd/hspd-9.html, 1/30/04

Mainly controlled by the Food and Drug Administration (FDA) and the Department of Homeland Security (DHS), this sector is responsible for maintaining the critical infrastructures required for maintaining a steady food supply within the United States. Like many other sectors, agriculture and food depends upon the continued functioning of other CIKRs including "the Water Sector for clean irrigation and processed water; the Transportation Systems Sector for movement of commodities, products, and livestock; the Energy Sector to power the equipment needed for agriculture production and food processing"[47]. Despite its importance, the agriculture and food sector remains in a state of disarray with multiple agencies failing to coordinate, creating a patchwork regulatory environment.[48]

Agriculture has several characteristics that pose unique vulnerabilities. Farms are geographically disbursed in unsecured environments. Livestock are frequently concentrated in confined locations, and transported or commingled with other herds. Many agricultural diseases can be obtained, handled, and distributed easily. International trade in food products often is tied to disease-free status, which could be jeopardized by an attack. Many veterinarians lack experience with foreign animal diseases that are eradicated domestically but remain endemic in foreign countries. More troubling than the patchwork nature of food safety system, "neither the FDA nor the USDA have the authority to order recalls of contaminated foods and must ask companies to recall contaminated foods voluntarily".[49]

While all aspects of agriculture depend upon the continuing functionality of external resources, only part of the food sector has been classified as a critical infrastructure. Still on the books, the 2003 national strategy for the protection of CIKRs stipulates that only "the supply chains for feed, animals, and animal products; crop production and the supply chains of seed, fertilizer, and other necessary related materials; and the post-harvesting components of the food supply chain, from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and restaurant or home consumption" qualify as being critical[50].

Affirmative

According to the Department of Homeland Security and the FDA, "the mission of the Food and Agriculture Sector is twofold: (1) to protect against any attack on the food supply, including production agriculture, that would pose a serious threat to public health, safety, welfare, or the national economy; and (2) to provide this steadily evolving sector with a central focus, emphasizing protection and strengthening of the Nation's capacity to supply safe, nutritious, and affordable food"[51]. Affirmatives

---

[47] Department of Homeland Security, *National Infrastructure Protection Plan Agriculture and Food Sector*, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_agriculture.pdf, 2009.
[48] Adam Stirrup, "Comment: Hidden Cargo: A Cautionary Tale About Agroterrorism And The Safety Of Imported Produce," San Joaquin Agriculture Law Review, 2006/2007.
[49] Adam Stirrup, "Comment: Hidden Cargo: A Cautionary Tale About Agroterrorism And The Safety Of Imported Produce," San Joaquin Agriculture Law Review, 2006/2007.
[50] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, 2003.
[51] Department of Homeland Security, Food (Meat, Poultry, and Egg Products) and Agriculture Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/nipp-ssp-ag-food.pdf, 2007.

seeking to address this topic area should consider the role of purposeful sabotage of the food supply as well as shortfalls thorough natural disasters or human error.

Affirmatives will be able to include plan mechanisms that deal with food production, processing, and delivery systems in addition to ensuring a generalized capacity to feed people both within and outside of the United States. The ability to feed people outside of the United States in included due to the importance of U.S. food supply on a global scale, supplying around 20% of the total market in 2005[52].

Despite being a robust sector with different commodities, farm sizes, and production styles, governmental interaction with private industry is surprisingly standardized. The vast majority of federal funds towards this sector are currently oriented towards R&D at an industry-wide level, leaving private industry responsible for research and development that is not covered by this holistic approach[53]. Correcting this one-size-fits-all system is one possible affirmative which would also yield a modeling advantage:

> **Department of Homeland Security,07**
> (Food (Meat, Poultry, and Egg Products) and Agriculture Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/nipp-ssp-ag-food.pdf, 2007)
> The **complexity of** the Food and Agriculture **subsectors makes designing a critical infrastructure protection plan applicable across its entirety a challenge**. The plan will divide the sector into discrete portions that are individually examined and then tied back to the overall sector goals. First, the plan will address infrastructure protection within the production agriculture subsector, which encompasses livestock and crop production at the farm level. Next, the plan will examine infrastructure protection within the food processing (meat, poultry, and egg products) subsector. All other food product infrastructure protection considerations will be addressed in the FDA SSP. USDA and FDA have collaborated to design the two plans so that together they would provide a complete picture of food-related infrastructure protection activities for the sector. Lastly, the plan will focus on infrastructure protection for food distribution activities. **Separating** the plan **into distinct subsectors will allow sector security partners to more easily follow** the plan **and** thus **implement it** more effectively. **A significant portion of** SSP **users** w**ill be Federal, State, local, or tribal** government **officials** that have regulatory responsibility for the sector. **They will look to the plan for guidance when developing their own infrastructure** protection activities. These individuals may represent agriculture, food, public health, or law enforcement entities.

Focusing on increased specificity in current policy will provide debaters with a focused and real-world analysis of how these resources are protected in the status quo. This specificity will need to be balanced with broader goals seeking to protect an entire nation's food supply. Plans seeking to increase the protection and resiliency of agriculture and food will need to institute solvency mechanisms capable of supplementing the policies already responsible for over a million farms and 87,000 food processing plants in the United States[54].

---

[52] "Farm Attack–The Forgotten Terrorism," The Age, October 1, 2005.
[53] Department of Homeland Security, Food (Meat, Poultry, and Egg Products) and Agriculture Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/nipp-ssp-ag-food.pdf, 2007.
[54] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, 2003.

Recent reports illustrate the current vulnerabilities of the agriculture and food sector. Tests conducted in March of 2011 found that increased computerization of food processing made multiple levels of the agricultural sector open to sabotage[55]. This study was prompted by the fear that viruses similar to Stuxnet, the worm responsible for crippling Iran's nuclear program, could cause a breakdown or allow unauthorized access to food processing areas. One option available to affirmatives is to increase our national capacity for contamination testing. Much of the literature base for this sector speaks to the need to dramatically improve the government's capacity to conduct wide range tests for potential containments including biological, chemical, and radiological . Beyond providing ample advantage ground for agro-terrorism impacts, this observation also pertains to accidental contamination that can occur through neglect or ignorance. The timeliness of these scenarios is of particular importance considering recent reports that the U.S. is on the brink of a food crisis .

Plans focusing on this sector would be able to propose methods of closing these security gaps, ensuring that unauthorized access remains unlikely. Literature offering specific solvency mechanisms for these affirmatives is not difficult to find, much of it advocating the merger of relevant regulators in an effort to increase the efficiency of federal policy:

Stirrup, 07
(Adam Stirrup, "Comment: Hidden Cargo: A Cautionary Tale About Agroterrorism And The Safety Of Imported Produce," San Joaquin Agriculture Law Review, 2006/2007.)
In 2004, Representative Rosa **DeLauro**, co-chair of the Congressional Food Safety Caucus, **introduced legislation in the House of Representatives to consolidate our food safety agencies into a single agency called the Food Safety Administration** ("FSA"). n134 **Senator** Richard **Durbin has also introduced similar bills for Senate approval.** n135 **The FSA would have the responsibility of enforcing the food safety laws, inspecting food to ensure its safety and establishing the relevant food safety standards.** n136 The new agency would integrate the food safety inspection and regulation aspects of the USDA and the FDA and other food safety programs currently handled by other federal departments. n137 An Administrator appointed by the President and confirmed by the Congress would be placed in charge of the FSA. n138 **In addition to the creation of a single food safety agency, the food safety legislation currently in effect must be replaced by a modernized and consistent food safety-statute.** n139 The new laws would be implemented by the FSA with a clear definition of the [*188] role and responsibilities of the new unified agency. n140 **The FSA must also be granted enhanced authority to inspect imported foods through increased inspections at our country's ports of entry and the ability to initiate mandatory recalls of contaminated food.** n141 **Numerous other countries have already created a unified food safety system that cover the entire food supply and now exist in the U.K., Netherlands, Germany, and New Zealand**. n142 The European Union has even established the European Food Safety Authority, an independent agency designed to monitor food safety throughout the European Union nations through a unified network of laws. n143 In five years, the consolidated agency in the U.K. has successfully increased public confidence in food safety and has reduced the number of food safety outbreaks. n144 **In the U.S**., on the other hand, **Congress has failed to follow the recommendations to create a single food safety agency and modernize the nation's food safety system.** n145 **The current governmental agencies have only attempted to protect their own funding and resources and have not worked to consolidate our outdated national food safety system**. n146 **It is time for the federal government to**

[55] Knapp, Alex. Increased Computerization Means Increased Vulnerability, http://blogs.forbes.com/alexknapp/2011/03/28/increased-computerization-means-increased-vulnerability/, 3/28/11.

> **take "politics out of food safety**," n147 **consolidate our food safety system and stop simply reacting to crises after they occur when it is too late to prevent them**. n148

As of March of this year, DeLauro still advocates the consolidation of food safety agencies into a single agency: “DeLauro said she favors a single independent food-safety agency because, currently, there are 15 agencies that deal with food safety, so the ability of the government to deal with foodborne illnesses is hindered by bureaucracy’.[56]

Negative Ground

Much of the negative ground available under this sector will be based upon the mechanisms the government would need to employ in order to solve. Any plan that attempts to employ a blanket cure-all will run the risk of not providing specific solvency for individual harms. Additionally, regulation of the agricultural sector has proven extremely controversial in recent years, providing ample ground for political and perception-based link scenarios.[57]

Controversy over the enactment of new regulation in the agriculture sector goes beyond the typical political capital link scenario. Owners of agricultural and food-based businesses are likely to backlash against plans that do not consult their needs prior to enactment. While the private sector does have a forum in which to air their grievances, it does not appear that consultation of this organization falls under the normal means of policy implementation:

> **Department of Homeland Security, 07**
> (Department of Homeland Security, Food (Meat, Poultry, and Egg Products) and Agriculture Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/nipp-ssp-ag-food.pdf, 2007)
> Significant **progress in the Food and Agriculture Sector** on homeland security goals **can only be accomplished through a partnership effort between all levels of government and those who own the critical infrastructure.** The Food and Agriculture Sector’s main coordination mechanisms for security partners are the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC). The GCC, with representation from Federal, State, local, and tribal governments, is the public sector portion of the public/ private partnership framework. The objective of the GCC is to provide effective coordination of Food and Agriculture Sector defense strategies and activities, policy, and communication across government and between the government and the sector to support the Nation’s homeland security mission. The GCC plays a coordination role to address the public health and clinical issues that would result from a terrorist act involving the food supply. It acts as the counterpart and partner to the private industry-led SCC to plan, implement, and execute sufficient and necessary sector-wide security programs for the Nation’s Food and Agriculture Sector critical assets, systems, networks, and functions. The GCC works to accomplish this objective through the following activities: • Identifying Items That Need Public/Private Coordination and Communication of Issues. The GCC will bring together diverse Federal, State, local, and tribal interests to identify and develop collaborative strategies that advance the protection of critical assets, systems, networks, and functions. While the focus is on CI/KR

[56] Pediatric SuperSite, “Foodborne illnesses may cost U.S. more than $150 billion annually,” March 2, 2010, http://www.pediatricsupersite.com/view.aspx?rid=61506
[57] Department of Homeland Security, Food (Meat, Poultry, and Egg Products) and Agriculture Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/nipp-ssp-ag-food.pdf, 2007.

> protection, the GCC will also function during events of national emergency or significance to coordinate and share information to augment existing emergency operation channels within Federal, State, local, and tribal government and with industry. • Identifying Needs/Gaps in Plans, Programs, Policies, Procedures, and Strategies. • Acknowledging and Recognizing Successful Programs and Practices. The GCC shall facilitate the sharing of experiences, ideas, best practices, and innovative approaches related to the protection of critical assets, systems, networks, and functions. The GCC shall acknowledge and recognize accomplishments that further the objective. • Leveraging Complementary Resources Within Government and Between Government and Industry. **The SCC is a self-governing body representing the food and agriculture industry that provides a forum for the private sector to discuss infrastructure protection issues among their members or to communicate with the government** through the GCC. The purpose of the SCC is to represent and communicate the interests of its subcouncils to the SCC leadership and to the GCC. SCC objectives include keeping subcouncil members apprised of key sector, inter-sector, and sector/government activities and bringing to bear their best judgment upon SCC decisions based on their understanding and experience within their subcouncil business area.

Failing to work cooperatively with the Sector Coordinating Council (SCC) would likely derail or at least delay plan enactment. The incredible specificity of this scenario might warrant negative teams running specific consult counterplans focusing on the SCC and similar organizations.

In addition to implementation issues, the policies required to increase security and reliability in the agriculture sector are potentially troubling. Much of the solvency evidence for terrorism advantages will likely stem from the introduction of biometric technologies to authenticate personnel:

> **Department of Homeland Security, 03**
> (The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, 2003)
> **We must provide better means of identifying people in order to increase the security of our critical facilities**, systems, and functions. We must create a uniform means of identifying law enforcement and security personnel and individuals with access to critical facilities and systems. **Technologies** to be examined for this authentication scheme **include biometric identifiers**, magnetic strips, microprocessor-enabled "SMART" cards, **and other systems. Such tools would enable quick authentication of identities in the protection and emergency response domains**. The **enhanced "scene control" entailed would facilitate investigations at the sites of terrorism incidents, and** create an investigative baseline for comparing different analytical data.

These proposals give negative teams the chance to introduce kritiks of technology and governmental control. Regardless of how each team choses to refute an agriculture-based affirmative, there appears to be considerable ground for negative teams to explore and develop arguments that will sustain this CIKR sector as an area of heated debate throughout the year.

Banking and Finance

Introduction

Given the recent economic crises occurring all over the world, it is easy to see why banking and finance would qualify as a critical infrastructure, Furthermore, the instability of this sector should be readily apparent, taking into account the recent U.S. bailouts and the near-collapse of many foreign economies, such as Greece.

According to the Department of Homeland Security, this sector includes "depository financial institutions (banks, thrifts, credit unions), insurers, securities brokers/ dealers, investment companies, and certain financial utilities".[58] The sheer diversity of these services makes it initially difficult to ascertain what parts of the financial sector fall under the definition of CIKR. Luckily, a great deal of attention has been paid to this issue. Recent literature stipulates that securing this sector does not require the continued reliability of physical assets, but rather of entire intangible assets.[59] Taking into account, the Department of Homeland Security offers the following:

> **Department of Homeland Security, 07**
> (Banking and Finance Sector-Specific Plan,
> http://replay.web.archive.org/20100205205722/http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf)
> The Banking and Finance Sector is a service-based industry providing a wide variety of financial services in the United States, and many such services throughout the world. These se**rvices range from the simple cashing of a check to highly complex arrangements that facilitate the transferring of financial risks.** Financial institutions are organized and regulated based on the services the institutions provide. Therefore**, the sector profile is best described by defining the services offered. These categories include: (1) deposit and payment systems and products; (2) credit and liquidity products; (3) investment products; and (4) risk-transfer products.**

Affirmative Ground

Affirmatives interested in addressing this sector should focus their efforts on the four categories mentioned by the DHS. It is worth nothing that none of these areas require the continued operation of a specific bank or institution in order to succeed. Therefore, if an affirmative were to focus on securing one particularly susceptible bank from attack than their plan would likely not solve the harms identified in the literature base. Rather, teams will have to address meta-issues pertaining to the reliability and resiliency of the banking and finance industry.

Given how many things affect this industry, the potential harms relating to this sector are legion. While particularly advantages will be extremely diverse, there are two core areas that they are likely to stem from.

> **Weiss, 09**

[58] Department of Homeland Security, 2007, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_banking.pdf
[59] Department of Homeland Security, 2007, Banking and Finance Sector-Specific Plan, http://replay.web.archive.org/20100205205722/http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf

> (N. Eric, Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges, May 4, http://www.fas.org/sgp/crs/misc/RL31873.pdf)
> **Financial institutions face two categories of emergencies** that could impair their functioning. **The first is directly financial: a sudden drop in the value of financial assets,** whether originating domestically or elsewhere in the world, that could cause a national or even global financial crisis. **The second is operational: the failure of the support structures that underlie the financial system.** Either could disrupt the nation's ability to supply goods and services. They could reduce the pace of economic activity, or at an extreme, cause an actual contraction of economic activity.

The first type of impact, a sudden drop in assets, could arise from the lack of redundant systems and balances ensuring economic resilience. These impacts could also stem from perception-based issues such as consumer confidence.

The second type of impact, those pertaining to the operational capacity of the sector, focus on the capacity for the financial world to continue operating. These impacts will mostly stem from scenarios, such as terrorist attacks or natural disasters, which have the capacity to prevent financial transactions. While impact s stemming from issues such as terrorism are relatively obvious, there exists other scenarios that might surprise affirmative teams, including an extensive disease-based literature base:

> **Weiss, 09**
> (N. Eric, Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges, May 4, http://www.fas.org/sgp/crs/misc/RL31873.pdf)
> **A flu pandemic** is not just a concern of the United States. The International Monetary Fund published a report in 2006 that, in part, addresses the problems that **could confront financial institutions**. 9 **These include continuity of operations, increased delinquency and default on loans due to illness at borrowers' business, and business disruption. The IMF recommended that financial businesses plan for a contagious outbreak, including provisions in case key staff become ill and for working from multiple locations**. Other suggestions included finding ways for staff to commute without using mass transit.

To date, these initiatives have not been initiated. While some banks have taken measures to ensure their continued operation during a disease event, the sector on a whole remains unprepared.

In order to protect this sector against events that could cripple the industry, affirmatives will have to consider how best to facilitate redundant systems in an effort to decentralize the operations of the American economic system.

> **Jackson**, Specialist in Financial Institutions Government and Finance Division, **05**
> William D., "Homeland Security: Banking and Financial Infrastructure Continuity," http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL3187303282005.pdf
> This paper suggests that **practices for recovery and continuity include "robust" backup facilities for clearance and settlement activities, resumption of normal business within two hours, regular testing of backup facilities, and backup personnel**. Issuing agencies stressed that it will take several years to carry out recommended sound practices fully. They did not recommend moving primary offices of financial and securities firms, contrary to some expectations.

Negative Ground

Much of the negative ground for this sector will focus on the ramifications of the plan as they apply to specific economic entities. While negatives could merely discuss the solvency of creating

redundant systems, there is also ground to PIC out of certain sub-sectors or even kritik particular companies. For instance, negatives could address the ethical implications of propping up institutions such as the World Bank or the International Monetary Fund.

> **Abugre**, Ghanaian development economist, **2000** [Charles, June" Still Sapping the Poor: A Critique of IMF Poverty Reduction Strategies", http://www.globalexchange.org/campaigns/wbimf/imf0600.html, Google Scholar]
> To the surprise of many, **the International Monetary Fund (IMF) announced its new commitment towards poverty reduction** at its Annual Meetings in September 1999. The **key element** of this announcement was a new initiative **to tackle poverty**, **the Poverty Reduction Strategy Paper (PRSP)** initiative. It appeared that developing country governments would now be asked to produce these PRSPs, in consultation with their citizens, **and that these would form the framework for all IMF and World Bank operations** in those countries. This represented a potentially major change, particularly for the IMF. **PRSPs threaten to deliver little in benefits to poor countries and poor people by way of debt relief and democratisation but more in cost, both in time, and more significantly the further erosion of the sovereignty of poor countries**. The early days of the PRSP initiative coincided with two massive mobilizations against globalisation. In December 1999, throngs of protesters shut down the World Trade Organisation's (WTO) trade negotiations in Seattle. In April 2000, police action prevented thousands of protesters from shutting down the spring meetings of the IMF and the World Bank in Washington, D.C. Mobilisations in the North -- especially in the notoriously insular U.S. -- are a new phenomena. This is not the case **in the Global South**, where **twenty years of structural adjustment programmes (SAPs) has created more losers than winners.** Estimates show that there have been of 146 public demonstrations against structural adjustment policies in 39 countries between 1976 and 1992.1 Still, neither the shareholding governments of the IMF or the World Bank, nor the institutions themselves, have taken stops to predict or address the impacts of adjustment programmes on people or ecosystems. **There is a wide gulf between the rhetoric and the reality of globalisation and between the rhetoric and reality of IMF and World Bank operations. The rhetoric promises progress toward broad-based prosperity and environmental stewardship. Many citizens see a different reality: pockets of obscene wealth in the midst of growing human misery, social dislocation, and environmental devastation. Perhaps most troubling is another disconnect -- that of citizens from their governments. "**

Additionally, much of the ground available through other sectors, such as Commercial Facilities, is equally applicable to this sector since both address issues of private industry maintaining their economic prosperity.

Chemical

Introduction

In 2003, the Department of Homeland Security (DHS) was named the lead agency for protecting and ensuring the resilience of the chemical sector of the nation's network of critical infrastructure. This authority is, however, limited; DHS has never had the power to impose security requirements on the chemical sector and its staff cannot enter a chemical plant for inspection without an invitation. Because of this, DHS has had to coax voluntary participation by the chemical sector. This has led the American Chemistry Council (ACC) to create its own Responsible Care program to help the industry avoid regulation by imposing its own safety and environmental regulations, and to improve its image in the wake of the 1984 Bhopal, India disaster. "While this is laudable, participation in these initiatives is voluntary and the extent to which individual companies across the industry are addressing security issues is unclear. Furthermore, voluntary efforts cannot ensure widespread participation and, unless chemical facilities' vulnerabilities are identified and addressed on a widespread basis across the sector, the security of the chemical industry as a critical national infrastructure remains at risk." ACC is in "complete agreement with the need for federal legislation…Our view is you need federal standards, national standards, so you have one standard".[60]

In Section 550 of the Homeland Security Appropriation Act, 2007 (P.L. 109-295), Congress established statutory authority for the Department of Homeland Security to regulate security at select chemical facilities. While a step in the right direction, this statutory authority expired three years after enactment.[61] In 2009, it appeared as though more stringent regulations were on the way. However, political posturing has prevented such measures from being enacted:

> **New York Times, 09**
> (New York Times (Editorial). (2009, August 3). Chemical Plants Could Be More Safe. Retrieved from http://www.nytimes.com/2009/08/04/opinion/04tue2.html?_r=2.)
> **This should**, by all rights, **be the year that Congress passes a tough chemical plant safety bill**, protecting the public from one of the most serious terrorism vulnerabilities. **There are already signs**, however, **that the chemical industry and its Republican allies may succeed yet again in blocking effective safety rules**. The White House, which has remained in the background, needs to speak out, and Democratic leaders in Congress should work to make sure a strong bill is enacted without further delay. Since Sept. 11, 2001, **experts have warned that an attack on a chemical plant could produce hundreds of thousands of deaths and injuries**. Public safety and environmental advocates have fought for strong safety rules, but **the chemical industry used its clout in Congress in 2006 to ensure that only a weak law was enacted**. That law sunsets this fall, and **the moment is right to move forward**. For the first time in years, there is a real advocate for chemical plant security in the White House. As a

[60] Suburban Emergency Management Project. (2006, March 14). Pervasive Civilian Vulnerability to Toxic-Inhalation-Hazard Industrial Chemical Terrorist Attack. Biot Report #341. http://www.semp.us/publications/biot_reader.php?BiotID=341
[61] Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. CRS Report for Congress. http://www.fas.org/sgp/crs/homesec/RL33847.pdf.

> senator, President Obama co-sponsored a strong bill, and he raised the issue repeatedly in last year's campaign. Both chambers of Congress are controlled by Democrats who have been far more supportive than Republicans of tough safety rules. **A** good **bill** is **moving through the House**. It **would require the highest-risk chemical plants to switch to less dangerous chemicals** only in limited circumstances, **but** Republicans have still been fighting it. In the House Homeland Security Committee, **the Republicans** recently **succeeded in adding several weakening amendments**, including one that could block implementation of safer-chemical rules if they cost jobs. **Saving jobs is important**, **but not if it means putting large numbers of Americans at risk** of a deadly attack. **The Obama administration needs to come out forcefully for a clean bill that contains strong safety rules** without the Republican loopholes. Janet Napolitano, the secretary of homeland security, said last week that she considers chemical plants a major vulnerability and promised that the administration will be speaking out on the subject in the days ahead. It is looking increasingly likely that Congress will extend the current inadequate law for another year to take more time to come up with an alternative. That would be regrettable. **There is no excuse for continuing to expose the nation to attacks that could lead to mass casualties**.

Even within the established statutory authority, "the federal chemical facility security regulation thus does not require the application or use of any particular security measure".[62] The consequences of this lack of regulation are significant:

> **National Academy of Sciences. 06**
> (Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities. (2006, June). http://dels-old.nas.edu/dels/rpt_briefs/chem_vulnerabilities_final.pdf.)
> History proves that **chemical incidents can be catastrophic in terms of human casualties**. **In December 1984**, **a leak of methyl isocyanate gas from the Union Carbide India Limited Bhopal claimed 4,000 lives**, resulted in **an estimated 200,000 to 500,000 injuries**, **and contributed to** an accumulation of **15,000 to 20,000 disaster-related deaths in subsequent years**. **America's worst chemical catastrophe occurred** on a loading dock **in Texas City**, TX on April 16, 1947 **when an explosion of** 2,300 tons of **ammonium nitrate** in a Liberty ship **cascaded into widespread destruction of** nearby **petroleum refineries**, **chemical production facilities**, **and another fertilizer liberty ship**, **ultimately claiming nearly 600 lives and causing approximately 3,500 injuries**.

And so, as a nation, we find ourselves facing the possibility of chemical facilities acting as a target for deliberate or accidental incident that puts the nation at risk. This paper advocates for the inclusion of the chemical sector within the Critical Infrastructure and Key Resources debate resolution. The paper begins by identifying the critical issues at work in this area of the topic, then will outline possible affirmative and negative strategies for engaging the chemical sector in policy debate.

As a debate topic, terrorism will obviously serve as a prominent fixture in chemical sector debates:

> **Shea, 06**
> (D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.)
> **Federal officials**, **policy analysts**, **and homeland security experts express concern about the current state of chemical facility security**. **Referring to them as** "**the**

[62] Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. CRS Report for Congress. http://www.fas.org/sgp/crs/homesec/RL33847.pdf.

single greatest danger of a potential terrorist attack in our country today," **some experts fear these facilities are at risk of a potentially catastrophic terrorist attack**. 1The Department of Homeland Security (**DHS**) **identifies chemical facilities as being one of the highest priority critical infrastructure sectors**. 2

Though not originally included in critical infrastructure definitions, the potential for chemical facilities to act as a target for terrorist attacks and/or as a site to obtain material for such incidents provides a strong justification for including this sector in the resolution's broader focus on Critical Infrastructure and Key Resources:

Moteff and Paromak, 04
Moteff, J. & Parfomak, P. (2004, October 1). Critical Infrastructure and Key Assets: Definition and Identification. *CRS Report for Congress*. Retrieved from http://www.fas.org/sgp/crs/RL32631.pdf.
This list of critical infrastructures encompasses those of E.O. 13228, but adds chemicals, and postal and shipping services due to their economic importance. **While there may be some debate, in particular, about why the chemical industry was not on earlier lists that considered military and economic security, it seems to have been added also because individual chemical plants could be sources of materials that could be used for a weapon of mass destruction, or whose operations could be disrupted in a way that would significantly threaten the safety of surrounding communities**. While not identifying it as such in this list, the National Strategy also discusses "cyber infrastructure" as closely connected to, but distinct from, physical infrastructure. The Strategy states that DHS "will place an especially high priority on protecting our cyber infrastructure." 21

The high probability of these types of incidents significantly magnifies the potential impacts referenced in historical accounts of Bhopal and Texas City:

Stephenson, 03
John. (2003, March). Voluntary Initatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown. GAO Report to Congressional Requesters. Retrieved from http://www.gao.gov/new.items/d03439.pdf.
Experts agree that chemical facilities present an attractive target for terrorists intent on causing massive damage because many facilities house toxic chemicals that could become airborne and drift to surrounding areas if released. **Alternatively**, **terrorists could steal chemicals**, which could be used **to create a weapon** capable of causing harm. **Justice** has been warning of the terrorist threat to chemical facilities for a number of years and **has concluded that the risk of an attempt** in the foreseeable future to cause an industrial chemical release **is both real and credible**. In fact, according to Justice, **domestic terrorists plotted to use a destructive device against a U.S. facility that housed millions of gallons of propane in the late 1990s**. **In** testimony on February 6, **2002**, **the Director of the Central Intelligence Agency warned of the potential for an attack by al Qaeda on chemical facilities**. Some chemical facilities may be at higher risk of a terrorist attack than others when they contain large amounts of toxic chemicals and are located near population centers assuming that the objective is a catastrophic release. **Attacks on such facilities could harm a large number of people**, **with health effects ranging from mild irritation to death**, **cause large-scale evacuations**, **and disrupt the local or regional economy**. No specific data are available on what the actual effects of successful terrorist attacks on chemical facilities would be. However, facilities subject to the RMP provisions submit to EPA estimates of the potential consequences to surrounding communities of hypothetical accidental "worst-case" chemical releases from their plants. These estimates include the residential population located within the range of a toxic gas cloud produced by a "worst-case" chemical release, called the "vulnerable zone." According to EPA, **123 chemical**

facilities located throughout the nation have toxic "**worst-case**" **scenarios where more than one million people would be in the** "**vulnerable zone**" **and could be at risk of exposure to a cloud of toxic gas**. 5 **About 600 facilities could each potentially threaten between 100,000 and a million people**, and **about 2,300 facilities could each potentially threaten between 10,000 and 100,000 people** within these facilities' "vulnerable zones." Figure 1 shows the residential population within the "vulnerable zone" that could potentially be threatened by an accidental toxic chemical release from a U.S. facility under a "worst-case" scenario. According to EPA, "worst-case" scenarios do not consider the potential causes of a release or how different causes or other circumstances, such as safety features, could lessen the consequences of a release. Hence, the "worst-case" scenario calculations would be overstating the potential consequences. However, the RMP regulation requires facilities to estimate the effects of a toxic chemical release involving the greatest amount of the toxic chemical held in a single vessel or pipe—not the entire quantity on site. Therefore, for some facilities it is conceivable that **an attack**, **where multiple chemical vessels were breached simultaneously**, **could result in an even larger release**, **involving more severe potential consequences**, **than those estimated in the** RMP "**worst-case**" **scenarios**. Other factors could also make a facility a more attractive target. For example, a facility that is widely recognizable, located near a historic or iconic symbol, or critical to supporting other infrastructures could be at higher risk. The Army has also estimated high potential damage to the population from a toxic chemical release. During a 2001 informal meeting with a number of agencies, the Army Office of The Surgeon General proposed, based on generic estimates, that **it was conceivable that as many as 2.4 million people could request medical treatment if a terrorist caused a release of a toxic chemical**. 6 According to officials from that office, these estimates include anyone who seeks medical attention as a result of the release—including people with minor irritations or concerns. Finally, **a 2002 Brookings Institution report ranks an attack on toxic chemical plants behind only biological and atomic attacks in terms of possible fatalities**. 7 **Currently**, **no one has comprehensively assessed security across the nation at facilities that house chemicals**. According to a 1999 study by **the Agency for Toxic Substances and Disease Registry** (ATSDR), security at chemical plants in two communities was fair to very poor. ATSDR **observed security vulnerabilities such as freely accessible chemical barge terminals and chemical rail cars parked near residential areas** in communities where plants are located. Furthermore, during a limited review of chemical industry vulnerabilities conducted primarily before September 11, 2001, Justice found that security at 11 chemical facilities was comparable to security found at other industrial facilities. **According to Justice**, **some facilities may need to implement more effective security systems and develop alternative means to reduce the potential consequences of a successful attack**. The effectiveness of security at some facilities may also be in doubt as evidenced by several media accounts of reporters and environmental activists gaining access to chemical tanks and computer centers that control manufacturing processes at these facilities.

The economic contribution made by the chemical sector provides another strong justification for inclusion within the Critical Infrastructure and Key Resources debate. As of 2006, the chemical industry was a $460 billion sector of the U.S. economy, contributing nearly 3 percent to the nation's GDP, 6.2 million jobs (or 5% of the total American workforce), and is the largest exporting industry with a strong presence in all 50 states.[63]

[63] Kelliher, Marybeth. (2006, November 1). Risk Management Division: Critical Infrastructure Protection Efforts. DEA Chemical Industry Conference, Louisville KY. Retrieved from http://www.deadiversion.usdoj.gov/mtgs/chem_industry/conf_2006/terrorism_kelliher.pdf

This economic contribution also allows debaters to investigate questions revolving around the production, distribution and use of many of the products that are central to the American good life, including direct products such as plastics, fibers and drugs along with secondary products such as paper, fibers, cosmetics and electronics (National Academy of Science, 2006). In fact,

> **Stephenson, 03**
> (John. (2003, March). Voluntary Initatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown. GAO Report to Congressional Requesters. Retrieved from http://www.gao.gov/new.items/d03439.pdf.)
> **Chemical facilities manufacture a host of products—including** basic **organic chemicals**, **plastic materials and resins**, **petrochemicals**, **and industrial gases**, to name a few. **Other facilities**, **such as fertilizer and pesticide** facilities, **pulp and paper manufacturers**, **water facilities**, **and refineries**, **also house large quantities of chemicals**.

The range of facilities within the chemical infrastructure will provide space for creativity and experimentation for both the affirmative and the negative, as different facilities manufacture large quantities of chemicals while others produce small batches for specific use.[64] Even beyond this quantifiable classification, one could consider costs and benefits for chemical regulations within refineries, startup specialty companies, and the ways chemicals are transported, including truck, rail, pipeline and marine vessel.[65] The types of products produced combined with the means of storage and transport offer potential to tap into these product specific debates, including changing regulations to include the protection of liquefied natural gas storage facilities, hazardous liquids pipeline pumping stations, and hazardous materials shippers.[66]

Indeed, the extent to which protection and resilience policies should apply to the vast network of chemical facilities offers an intriguing solvency debate since "determining which chemical facilities to protect is a challenge" for policymakers.[67] Some are led to believe that it is the chemicals manufactured and distributed that should be the classifactory scheme, while others wish to expand the list to include any site containing chemicals, based upon the potential consequences and/or industrial standards as the more effective approach.[68] What we consider chemical facilities is an important determination in policymaking:

> **Shea, 06**
> D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
> **One challenge** in using this approach **may be determining which chemicals to include** when considering chemical facility security. **Existing federal chemical lists are generally** developed for other reasons, and therefore may **not** be **appropriate for security purposes**. For example, the Department of Transportation list for regulation of

[64] National Academy of Sciences. (2006, June). Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities. http://delsold.nas.edu/dels/rpt_briefs/chem_vulnerabilities_final.pdf
[65] National Academy of Sciences. (2006, June). Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities. http://delsold.nas.edu/dels/rpt_briefs/chem_vulnerabilities_final.pdf
[66] Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. CRS Report for Congress. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
[67] Stephenson, John. (2003, March). Voluntary Initatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown. GAO Report to Congressional Requesters. Retrieved from http://www.gao.gov/new.items/d03439.pdf.
[68] Stephenson, John. (2003, March). Voluntary Initatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown. GAO Report to Congressional Requesters. Retrieved from http://www.gao.gov/new.items/d03439.pdf.

> transport of hazardous materials contains several thousand chemicals, not all of which are a security risk. 29 The OSHA process safety standard applies to a group of highly hazardous chemicals selected because of their potential hazard to workers. 30 The EPCRA lists several hundred chemicals in order to ensure the safety of first responders in the event of a chemical accident. 31 The Clean Air Act, Section 112(r), requires a risk management plan (RMP) for facilities possessing more than threshold quantities of any of 140 chemicals. 32 These chemicals are included because of their potential for acute, offsite consequences to human health or the environment in the event of a sudden, large, accidental release. The risk management program requires these facilities to estimate the population that might be affected under a worst-case scenario release, calculating the population that resides within a circle surrounding the facility, with the radius of the circle determined by the distance the worst-case scenario release might travel. 33 While these estimates are not intended to model a potential terrorist release, the potentially affected population in a worst-case scenario is often cited in discussing chemical facility security risks. Such hazardous chemical lists generally identify chemicals based on an inherent hazard, such as toxicity or flammability. **One potential drawback to defining facilities by referring to these lists is that they exclude potentially hazardous chemicals for reasons other than risk**. For example, **the RMP list**, **often referred to in discussions of chemical facility security**, **does not include explosives**. 34 **It also exempts** material already regulated under 49 CFR 192, 193, and 195, such as **liquified natural gas**, **which is covered by other safety regulations**. 35 **The list** of RMP facilities **was further reduced by statute to exclude facilities where flammables are stored on site as fuel or for retail distribution as fuel**. 36 **Congress may or may not want to include such exempted materials** when considering chemicals in a terrorism context. Of course, any of the above lists, or any other chemical list, might be edited to meet the security need. **To better focus federal resources**, **a much shorter list of chemicals might be desirable**. **Alternatively**, **an appropriate federal agency might develop a new chemical list specifically for security purposes**, **avoiding a focus on previous lists**.

Thus, a central focus of this sector of the Critical Infrastructure and Key Resources resolution would be considering the costs and benefits of applying protection and resilience policies to different products and facilities. The vast array of chemical facilities will offer much by way of intriguing debate since inspections and enforcement of the plan's application to a specific product or facility could "tax DHS resources".[69]

Affirmative Ground

There is a wide range of affirmative options for enhancing protection and resilience of chemical facilities, policies ranging from providing grants to increase security at high risk facilities, mandating site vulnerability assessments, compelling vulnerability remediation, establishing federal security standards, and providing first responders with federal funding to secure critical infrastructure. The incomplete status of various pieces of legislation such as the Chemical Facility Security Act of 2005, the Chemical Facility Anti-Terrorism Act of 2005 and the Chemical Security and Facility Security Act of 2005 certainly points toward a variety of legislative proposals and policy considerations.[70]

A. Vulnerability Assessment & Remediation Compliance Affirmatives

[69] Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. CRS Report for Congress. http://www.fas.org/sgp/crs/homesec/RL33847.pdf.

[70] Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. CRS Report for Congress. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.

Expanding existing enforcement procedures will offer much by way of affirmative ground. Currently, the DHS only visits 272 select chemical facilities for inspection, leading some to advocate on behalf of the expansion of auditing regimes. Furthermore, an affirmative could advocate extension of the Buffer Zone Protection Program as a means of enhancing the security of areas surrounding critical infrastructure facilities.[71] The following offers an overview of the potential extension of existing programs, with a built-in consideration of negative ground in this area:

> **Shea, 06**
> D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
> Auditing of Vulnerability Assessments and Security Plans. **Existing federal laws governing some chemical facilities have taken diverse approaches to vulnerability assessments for chemical facilities**. The Maritime Transportation Security Act (MTSA) requires both the development of site vulnerability assessments and the remediation of those vulnerabilities identified. The Safe Drinking Water Act (SDWA), as amended, requires drinking water facilities to develop site vulnerability assessments and emergency response plans, but not to remediate vulnerabilities. Under both laws, the appropriate federal regulatory agency receives the site vulnerability assessments. Under the MTSA, **the DHS has the authority to inspect port facilities**, **assess their security plans and actions**, **and determine whether the facilities meet DHS security standards**. **The EPA was not granted similar authorities** under SDWA. **Policymakers might decide to require that site vulnerability assessments be performed for all chemical facilities and supplied to the federal government or others**. **Verification and validation of voluntary security plans is a topic of continuing concern by advocacy groups**, **so policymakers might provide the federal oversight agency the authority to inspect and assess compliance with vulnerability assessments and any remediation requirements**. However, **in contrast to the 238 chemical facilities covered by MTSA**, **a broad legislative definition of chemical facilities could include thousands of facilities**. **The logistical burden of inspecting these facilities on a recurring basis could be quite high for a federal agency**. **Current agency staffing may be insufficient to meet this requirement**. **Consequently**, **requiring federal auditing and validation of chemical facility security may be difficult to implement in a timely manner**. **Auditing responsibilities could be delegated to state or local officials to reduce the burden placed on federal agencies**. **Alternatively**, **Congress could authorize agencies to license third-party auditors and accept compliance reports they might submit on behalf of chemical facilities**. DHS Secretary Chertoff has expressed support for congressional consideration of such third-party validation. 50 Fees from such a program could offset auditing costs. **If such auditing were done by third parties or was enforced by a different mechanism**, **such as holding facility owners or operators liable for security measures at the chemical facilities**, **costs might be somewhat reduced**. **Critics of outside auditing question the impartiality and rigor of such reviews**, **citing breakdowns in analogous financial auditing approaches**.

Yet another, straightforward affirmative would shore up the enforcement capabilities of the DHS:

> **Suburban Emergency Management Project, 06**
> (Pervasive Civilian Vulnerability to Toxic-Inhalation-Hazard Industrial Chemical Terrorist Attack. (2006, March 14). *Biot Report* #341. Retrieved from http://www.semp.us/publications/biot_reader.php?BiotID=341)

[71] Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. CRS Report for Congress. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.

Congress should consider enhancing DHS' ability to collect comprehensive information on industry preparedness and better ensure the security of the chemical sector by performing two actions: **1. Granting DHS the authority to require high-risk chemical facilities to assess their vulnerability** to terrorist attacks **and**, where necessary, **to take corrective action and 2. Providing DHS with the enforcement capability to ensure that facilities are following these practices. Regulating the security apparatus of the nation's chemical-sector facilities is long overdue**. **The Congress needs to give DHS the same regulatory authorities to improve chemical sector readiness as it has given to other sectors**, such as nuclear and food. **We know that this legislative advance will occur after the first gassing of a population within the US**, **but it sure shouldn't wait until then**.

B. Inherently Safer Technology Affirmatives

Another main area for the affirmative team centers around the use of Inherently Safer Technologies. The National Academy of Sciences states that the "most desirable solution to preventing explosive and harmful chemical releases is to reduce or eliminate the hazard where possible." NAS (2006) has found that the "economic incentives for industrial funding are frequently absent," causing companies to ignore options such as "process intensification, 'just in time' chemical manufacturing, and the use of smaller scale processes" as well as "improving storage security" by stor[ing] chemicals in adsorbents, use of low pressure storage or underground storage technologies.[72] These policies are certainly amendable to switch-side debate:

Shea and Tatelman, 08
(Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. *CRS Report for Congress*. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33847.pdf.)
Considerable congressional debate on chemical facility security revolved around the issue of inherently safer technology. During this debate, **the application of inherently safer technology as a risk-reducing security measure was generally supported by environmental groups and opposed by industry groups**. **Environmental groups proposed that reducing the inherent consequences from a release at a chemical facility would increase its security**, **as the incentive to attack such a lower-consequence facility would be reduced**. **Industry groups argued that chemical substance and technology changes were business and process safety concerns**, not related to security issues, **and best left to the discretion of the chemical facility**, rather than the federal government.

Options in this area are also plentiful:

Shea, 06
(Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.)
The application of inherently safer technology to increase chemical facility security is also a subject of debate. **The concept of inherently safer technology involves altering a chemical process by substituting less hazardous materials**, **minimizing the amount of hazardous material on hand**, **altering the process conditions**, **or designing operation so that it is more tolerant of error**. 59 Advocates of inherently safer technology state that **its application would directly reduce security risks**, **because the hazard posing the security risk would be replaced or reduced**. 60 While acknowledging that not all chemical processes have inherently safer alternatives,

[72] National Academy of Sciences. (2006, June). Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities. http://dels-old.nas.edu/dels/rpt_briefs/chem_vulnerabilities_final.pdf

advocates cite cases where inherently safer alternatives are known and could be employed. 61 They claim that **federal security legislation should require at least the consideration of these technologies when addressing chemical facility vulnerabilities**.

Given these numerous options, it should come as no surprise that there are effective negative attacks to be made on the solvency of such affirmatives:

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Industry trade associations are generally resistant to legislation mandating the use of, or incorporating a requirement to consider, **inherently safer technology**. They state that decisions regarding the use of inherently safer technology are weighed on a process and facility basis and are regularly considered by process engineers when optimizing and assessing process change. 62 Additionally, **they cite the potential to impact process safety negatively should inherently safer technology approaches be incorrectly implemented**. For example, **if stockpiles of a hazardous chemical are reduced**, **more**, **smaller shipments may be required**. **More connections would be required to transfer the same amount of material** from smaller shipments. **This might lead to greater risk for workers making these transfers**. Lastly, industry trade associations express concern that if inherently safer technology implementation decisions are not made by process safety experts, future difficulties and potential impracticalities may arise. 63 **Another consideration** discussed in the context of inherently safer technologies **is the potential to transfer risk from one chemical facility to another chemical facility**. **Process changes**, such as the conversion of wastewater treatment from chlorine as a disinfectant to sodium hypochlorite as a disinfectant, **may lower the potential consequences at that facility**, **reducing the risk to the surrounding area**. **Those process changes may**, **however**, **increase the risk at a different point in the supply chain**. For example, the facility converting chlorine into sodium hypochlorite may increase its chlorine stocks to address a greater demand for the sodium hypochlorite end product, increasing the potential consequences surrounding that manufacturing facility. **Depending on the relative population at each facility**, **fewer or more individuals may be put at risk by the facility process change**.

C. Emergency Response Affirmatives

A final area for the affirmative to consider is an examination of the short term response measures to chemical emergencies. NAS includes recommendations for "explor[ing] ways to enable rapid analysis and communication of data for decision-making and communication to the public during and after an emergency." Indeed, "early warning" strategies such as reliable detection techniques, research and development on chemical sensors, and use of inventory controls may provide ways to enhance emergency response effectiveness, thereby increasing the resilience of the chemical industry to security breaches and/or emergency situations.[73]

In conclusion, the legislative options for chemical security regulations are numerous and provide ample opportunities to consider a variety of policy approaches:

Shea and Tatelman, 08

[73] National Academy of Sciences. (2006, June). Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities. http://dels-old.nas.edu/dels/rpt_briefs/chem_vulnerabilities_final.pdf

Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. *CRS Report for Congress*. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33847.pdf.
Policymakers may ultimately decide that the regulatory structure established by DHS does not satisfy homeland security needs or will prove too onerous to industry and opt to enact new chemical facility legislation. **Such legislation might expand the reach of the regulatory structure**, for example, **by mandating the inclusion of particular chemical substances as potentially dangerous**; **restrict the scope of regulation**, for example, **by lowering regulatory burdens or requirements on small businesses**; **or direct the agency to include or exclude particular components from its regulations**.

Negative Ground

A. Resolution-Based Generics

1. Voluntary Compliance Counterplans

The Voluntary Compliance counterplan will provide a core negative option for those that wish to discuss the economic and industry considerations of chemical sector regulations:

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Supporters of voluntary efforts cite the large investment made in site security since 2001 and other efforts to reduce risk **as signs of their effectiveness**. **The ACC**, for example, **notes that its member companies invested over $2 billion in security enhancements** since 2001. 11 Additionally, **some facilities voluntarily switched chemicals**, **changed manufacturing processes**, **or reduced the amount of chemicals onsite**. 12 **As one industry trade association representative testified**, "**Our efforts show that industry does not need to be prodded by government mandates to take aggressive and effective steps to secure its facilities**." 13

Cooperation with these voluntary regimes might be induced by allowing the negative to fiat incentives-based measures:

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Some chemical facilities engage in security activities absent regulation. **Policymakers may decide whether these actions should be rewarded**. **Potential mechanisms for recognizing these activities include economic offsets for security costs**, **granting exemptions from the regulatory framework for facilities undertaking voluntary efforts**, **and recognizing voluntary efforts with full or partial equivalency with regulatory requirements**. Some analysts assert that voluntary efforts should not be rewarded, since a business incentive — reduced liability — already exists for chemical facilities to improve security. Furthermore, even with this incentive, current voluntary security activities may not rise to an acceptable level.

These Voluntary Compliance counterplans offer significant solvency debates as the most discussed trade association security requirements created by the American Chemical Council affect "only a small fraction of the total number of chemical manufacturers," leaving approximately 20% high risk chemical facilities

outside of the participatory regime. These measures have also been criticized as "vague, inappropriately focused…and difficult to verify".[74]

2. Business Confidence Disadvantages

The Business Confidence disadvantage will serve as an effective stand-alone option and/or as a net-benefit to the Voluntary Compliance counterplan:

> **Shea and Tatelman, 08**
> Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. *CRS Report for Congress*. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33847.pdf.
> **Developing new legislation**, **or changing existing legislation**, to alter the DHS interim final rule **may bring additional costs**, especially **to facilities that have already come into compliance**. **If new regulations**, established under new or amended authority, **present new requirements for chemical facilities**, **security efforts enacted under the original interim final rule may not be entirely applicable**. **Chemical facilities may be required to invest in additional security measures to meet these new requirements**, **potentially incurring further cost**. When considering whether to enact new legislation or amend existing law, policymakers may opt to consider methods to mitigate additional costs to chemical facilities that have already complied with the interim final rule. As the initial statute had a three-year sunset provision, Congress may have intended that future legislation build upon P.L. 109-295, Section 550, so that future regulations would be harmonized with the interim final rule initially promulgated.

Indeed, the affirmative's decision about which chemical facilities to include offers significant link ground for these economy-based disadvantages:

> **Shea and Tatelman, 08**
> Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. *CRS Report for Congress*. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33847.pdf.
> **Defining chemical facilities** according to industry classification **might lead to the** "**one size fits all**" **approach to chemical facility security criticized by various industry groups**. 45 Such an approach may require facilities that are not a security risk to increase their security solely because of their industry classification, rather than their actual risk. **Such security efforts might not reduce the national risk and might be viewed as counterproductive**, **potentially impairing economic efficiency without increasing security**. Moreover, **due to fiscal constraints**, **smaller facilities might be unable to meet requirements designed for larger facilities**, **potentially damaging a company's ability to operate**. 46 47

3. Politics Disadvantages

The discussion of Congressional legislation included in the introduction of this section of the proposal paper indicates that chemical industry regulations are controversial and require the use of political capital because of their impact on jobs and business practices. As lead agency for securing the chemical sector, DHS has had to navigate a variety of entrenched business interests just to ensure continued support for status quo voluntary measures:

> **Suburban Emergency Management Project, 06**

[74] Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. CRS Report for Congress. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.

(2006, March 14). Pervasive Civilian Vulnerability to Toxic-Inhalation-Hazard Industrial Chemical Terrorist Attack. *Biot Report* #341. Retrieved from http://www.semp.us/publications/biot_reader.php?BiotID=341
Fifth, **the DHS shares threat information with the industry and coordinates sector activities with the Chemical Sector Coordinating Council**, an industry-led working group that acts as a liaison for the chemical sector. As of November 2005, **major players in this council included the Adhesive and Sealant Council**; **the American Chemistry Council**; **the American Forest & Paper Association**; **the Chemical Producers and Distributors Association**; **the Chlorine Chemistry Council**; **the Chlorine Institutes**; **the Compressed Gas Association**; **CropLife** America; **the Fertilizer Institute**; **the Institute of Makers of Explosives**; **the International Institute of Ammonia Refrigeration**; **the National Association of Chemical Distributors**; **the National Paint and Coatings Association**; t**he National Petrochemical and Refiners Association**; **the Society of the Plastics Industry**, Inc., **and the Synthetic Organic Chemical Manufacturers Association**. (11) **Many of these organizations extensively lobby the US Congress**.

4. States Counterplans

One of the main benefits to including the chemical sector in critical infrastructure debates from the negative's perspective is clearly delineated distinctions between federal and state actions. As Shea puts it,

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Many in the public and private sector call for federal legislation to address chemical facility security. 3 **Still**, **disagreement exists over whether federal legislation is the best approach to securing chemical facilities**, **and**, if legislation is deemed necessary, **what approaches best meet the security need**. **Since the population potentially affected by a chemical release generally resides near specific facilities**, **some experts may argue that chemical facility security concerns should be dealt with by state or local authorities**. **Other experts claim the potentially catastrophic nature of a terrorist attack and the widespread distribution of chemical facilities make chemical facility security an issue of national concern**. Policymakers may decide that chemical facility security is a matter of national homeland security and is best addressed at the federal, rather than state level.

Indeed, states such as New Jersey, Maryland, and New York have already taken the initiative to establish their own chemical facility security regulations, leading Shea to believe that the states can capture many of the benefits to federal action by acting independently:

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Several states have safety or environmental laws applying to chemical facilities, **but three**, New Jersey, Maryland, and New York, **have enacted security laws that specifically target chemical facilities**. **Under New Jersey's Domestic Security Preparedness Act** of 2001, **the New Jersey Domestic Security Preparedness Task Force is authorized to adopt and enforce security standards on the public and private sector**, following review and approval by the Governor. 14 **In** November, **2005**, **the Task Force mandated chemical facilities to comply with previously voluntary best practices**, **including reviewing existing processes for inherently safer**

alternatives at specific facilities. Facilities must report to the New Jersey Department of Environmental Protection. 15

While this independent action may provide the debate community with the impression of the unbeatable States counterplan, there are still adequate defenses of federal action:

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Policymakers who believe that states are better suited to assess local threats and vulnerabilities may prefer chemical facility security measures to be developed locally. **A potential concern of industry about such state laws is that a patchwork of regulations could develop**, **with different standards applying to facilities located in different states**. **Consequently**, **facilities in some states might be more secure than in others**, **or a facility's out-of-state competitors might face very different security costs**. Policymakers who believe such an approach does not provide sufficient security to the population at large, or places an uneven burden on industry may prefer a national standard. Also, **some chemical facilities located near state borders may pose risks across state lines**, **supporting efforts for a national standard**.

These solvency distinctions, combined with a well-crafted State Budgets or State Politics disadvantage, should provide the affirmative with effective options versus the formidable States counterplan.

5. Federalism Disadvantages

The Federalism disadvantage may serve as an effective net-benefit to these States counterplans:

Shea and Tatelman, 08
Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. *CRS Report for Congress*. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33847.pdf.
Another area of congressional debate was whether federal chemical facility security legislation should preempt such activities on the state level. 27 **Several states have begun to enact security regulations for chemical facilities**. 28 **Supporters of explicit federal preemption assert that a patchwork of state regulation provides a competitive disadvantage to companies** on a state-by-state basis **and may lead to uneven security efforts**. **Opponents of explicit federal preemption claim that federal security regulation should set a floor**, **rather than a ceiling**, **for security efforts**; individual states should, in their opinion, be allowed to require additional security measures, so long as the federal standard is surpassed.

6. Delegation / Agency Action Counterplans

The agent of action selected by the affirmative and/or defined as normal means can make a difference in terms of counterplan and disadvantage ground for the negative, including the use of Regulatory Negotiations:

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Which federal agency should possess chemical facility security oversight responsibilities is a topic of debate. **Some analysts assert that the EPA possesses a historic relationship with both the chemical industry and specific chemical facilities**. **They claim that the EPA is knowledgeable about chemical facility operation and security**, **that the EPA would be well positioned to understand the**

potential impacts of security regulation, **and that the EPA would be likely to create effective regulation**. This coupling of safety and security was supported by the U.S. Coast Guard, which testified that security auditing under MTSA often occurred while the U.S. Coast Guard was present at the chemical facility for safety reasons. 49 **Other analysts claim that the EPA is unlikely to be the correct oversight body for chemical facility security**. **They cite the potentially contentious relationship that the EPA**, **which already oversees safety and facility emissions**, **might develop with the chemical industry**. **They assert that regulation of security may need to be met through a collaborative process between the oversight agency and the facilities**, **so it should be divorced from environmental regulation**. **The DHS is the other federal agency most often cited as appropriate for overseeing chemical facility security**. **Advocates claim that a good working relationship already exists between DHS and industry and that DHS's expertise in security is a dominant factor**. **Opponents of this view argue that security measures**, **absent environmental protection and safety considerations**, **may generate adverse side effects**. For example, while burying storage tanks underground might increase the security of these tanks, such an approach might pose an environmental risk from potential tank leakage. Consequently, some analysts suggest an approach combining the skills of both DHS and EPA in overseeing chemical facility security.

B. Chemical Sector Specific Negative Options

The old "Net-Widening" DA and Coercion arguments may return within a chemical facilities debate. This is because the Secretary of DHS "must audit and inspect chemical facilities and determine regulatory compliance".[75] These types of Coercion arguments might be augmented by the use of the aforementioned Voluntary Compliance counterplan:

Shea, 06
Shea, D. A. (2006, April 12). Legislative Approaches to Chemical Facility Security. *CRS Report for Congress*. Retrieved from http://www.cnie.org/NLE/CRSreports/06May/RL33043.pdf.
Some analysts and industry representatives submit that the current mix of voluntary and mandatory activities provide adequate security enhancements and that market forces are good drivers of chemical facility security needs. 68 While acknowledging that mandates are needed, DHS Secretary Chertoff recognized the power of market forces, stating, "... we want to acknowledge and recognize that **ultimately**, **the marketplace itself creates a very strong incentive through business self-interest in enhancing security**." 69 **Supporters of the status quo do not advocate for new chemical facility security legislation**, **but instead** suggest that current security activities focusing on a public/private partnership with the DHS, coupled with federal support of local first responders and law enforcement, continue to provide chemical facilities with security. They **assert that the voluntary chemical facility security measures are likely to be implemented at an appropriate and sustainable level based on the risk perceived by the facility owners and operators**.

Yet another potential negative strategy would focus on the effects of inspection and auditing regimes on the protection of intellectual property and ensuring informational security. Stephenson elaborates that:

Stephenson, 03
John. (2003, March). Voluntary Initatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown. GAO Report to Congressional Requesters. Retrieved from http://www.gao.gov/new.items/d03439.pdf.

[75] Shea, D. A., & Tatelman, T. B. (2008, January 10). Chemical Facility Security: Regulation and Issues for Congress. CRS Report for Congress. http://www.fas.org/sgp/crs/homesec/RL33847.pdf.

> Fourth, **industry officials voiced concern about government agencies' ability to protect sensitive information relating to facility vulnerabilities and security**. **They stated that companies may be hesitant to share information about site-specific vulnerabilities and security unless government agencies implement specific safeguards to protect this information**. We have also reported that public-private information sharing practices are central to critical infrastructure protection. Specifically, practices such as taking steps to ensure that sensitive information is not inappropriately disseminated and developing standards and agreements on how shared information will be used and protected are critical to successful information sharing. 23

Conclusion

The chemical industry's vulnerability to terrorism, contribution to the nation's economic base and its criticality to everyday products we often take for granted provides a strong justification for inclusion of this sector within a Critical Infrastructure and Key Resources resolution. This area of the topic fits well within the resolution's broader focus on critical infrastructure while allowing optimal diversification of debates to capture the important features of this sector. Inclusion of the chemical sector within the resolution will allow the community to learn about high probability events that can disrupt their daily lives and will prepare them to contribute to discussions that inform the processing, manufacture, transport and purchase of many products taken for granted by everyday Americans.

.

Commercial Facilities

Introduction

Primarily owned and operated by the private sector, the commercial facilities sector includes private businesses that have been deemed critical to the sustained operations of the United States. In regard to, this area can be considered the private sector of critical infrastructure and key resources. The Department of Homeland Security breaks up the industries in this sector as follows:

> The Commercial Facilities Sector consists of the following eight subsectors:
> 1. Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers);
> 2. Sports Leagues (e.g., professional sports leagues and federations);
> 3. Resorts (e.g., casinos);
> 4. Lodging (e.g., hotels, motels, conference centers);
> 5. Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades);
> 6. Entertainment and Media (e.g., motion picture studios, broadcast media);
> 7. Real Estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage); and
> 8. Retail (e.g., retail centers and districts, shopping malls).[76]

This sector can be the catch-all for private industries that are critical to the economy but do not constitute their own CIKR sector (as the banking industry does). While the government does not have direct oversight over the methods of securing these industries, there is a strong precedent for various forms of government regulation in each subsector. Casinos are governed by the gaming commission, sports leagues (increasingly) by Congress, and retail locations by the Department of Commerce. The goal of teams engaging this sector will be to solve vulnerabilities that would prevent these subsectors from being able to sustain themselves following a major incident.

Affirmative Ground

The importance of commercial facilities is readily apparent for teams interested in debating the economy. The retail subsector alone is listed as having generated over 4.4 trillion dollars in sales in 2008, illustrating not only the importance of maintaining physical assets in the sector but also of ensuring consumer confidence and spending.[77] Affirmatives focused on this area will need to ensure the continued functionality of these facilities and simultaneously reassure consumers of the market's stability in time of a crisis. Threats against this sector are very real and well documented:

> **Department of Homeland Security. 07**
> (Strategic Sector Assessment (U//FOUO) Commercial Facilities Sector , http://info.publicintelligence.net/HITRAC_CommFacilities.pdf)
> **Al-Qa'ida continues to pose the greatest terrorist threat to the Commercial Facilities Sector** (CFS). **DHS has specific and credible reporting from multiple**

[76] Department of Homeland Security, National Infrastructure Protection Plan: Commercial Facilities Sector, 2008, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_commercialfacilities.pdf
[77] Humantech, "Understanding the Commercial Facilities Sector,2008, http://www.humtech.com/fema/cikr_rc/comFac1.htm

sources indicating al-Qa'ida's historical interest in attacking specific elements of the CFS. DHS is not aware of any specific imminent threat to critical infrastructure in the sector, but **an attack against a sector asset likely would meet al-Qa'ida's strategic targeting criteria, which are to inflict American casualties, cause psychological damage to the U.S. population by attacking symbols of U.S. culture or symbolic value, and damage the national economy.**

Taking these threats into account, affirmatives will need to find policy initiatives that create defenses against unknown threats with only a vague idea of their agenda. Similar threats emanate from domestic terrorists, who are increasingly hostile given economic hardships.[78]

Specific affirmatives should consider a number of plans that could potentially solve the harms addressed in this sector. These include:

Department of Homeland Security. 07
(Strategic Sector Assessment (U//FOUO) Commercial Facilities Sector , http://info.publicintelligence.net/HITRAC_CommFacilities.pdf)
The 11 September 2001 attacks demonstrated that **mitigating the most significant risks to commercial facilities probably lies outside the scope of what most owners** and operators can do. Owners and operators of CFS assets, however, do have the capability to protect against the prevailing threats against the sector—suicide bombers and VBIEDs. **Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Implementation of protective measures involves the commitment of resources in the form of people, equipment, materials, time, and money. Protective measures are designed to meet the following objectives**: (U//FOUO) **Devalue: Lowering the value of a facility to terrorists makes it a less attractive targe**t. Some common protective measures that would make a commercial asset a less useful target are: – (U) Providing adequate perimeter fencing or walls around facility grounds. – (U) Developing and maintaining a plan for communicating information to the public, including quelling rumors. Relationships should be cultivated with the media ahead of time with an identified public information officer. – (U) Using temporary barriers to expand the zone around the buildings/facility and populated areas. – (U) Providing inspection areas that are not visible to the public. – (U) Evacuating personnel from any facility where a confirmed threat exists and considering closing the facility until the threat level is reduced. (U//FOUO) **Detect: Spotting the presence of adversaries or dangerous materials provides information needed to mount an effective response.** Some protective measures that can be put in place for detection are: – (U) Training security staff regularly to include counter-surveillance techniques. – (U) Incorporation of a screening process that denies access to patrons with hand-carried items until the items have been physically inspected. – (U) Monitoring of all access points and restricted areas 24 hours, 7 days a week to include the use of CCTV. – (U) Increasing the number of police patrols and providing additional weapons and equipment to the security force at any facility where a confirmed threat exists. – (U) Prohibiting the presence of nonessential vehicles at the venue or facility grounds and thoroughly searching all vehicles entering the area, to include the undercarriage. – (U) Providing daily security and awareness briefings to administrative and other essential personnel. – (U) Employing advanced security surveillance technologies. (U//FOUO) **Deter: Make the facility more difficult to attack successfully**. Common protective measures to deter an attack include: – (U) Randomly screening guests, employees, event participants, and delivery,

[78] Department of Homeland Security. Strategic Sector Assessment (U//FOUO) Commercial Facilities Sector , 2007, http://info.publicintelligence.net/HITRAC_CommFacilities.pdf

service, and emergency services personnel before they are allowed to enter the venue or facility. – (U) Physically inspecting all vehicles and identifying the driver before he or she is allowed to approach the venue or facility. – (U) Strategically placing barriers to guide the flow of vehicles for access to drop-off and pick-up points, parking areas, and delivery points. – (U) Ensuring grounds are covered by plain view CCTV and are monitored 24 hours, 7 days a week. – (U) Ensuring lighting illuminates the venue facility and is integrated with backup power in the event of an emergency. – (U) Arranging for law enforcement vehicles to park randomly near entrances and exits before and during all high-profile events. – (U) Coordinating with local authorities regarding closing of public roads and facilities. – (U) Increasing stand-off by limiting parking in the vicinity of the structures. – (U) Pre-positioning and mobilizing specially trained teams or resources. – (U) Providing continuous guard visibility. (U//FOUO**) Defend: Defense involves responding to an attack to defeat adversaries, protecting the facility, and mitigating any effects of an attack.** Some common protective measures that would be effective in the defense of an attack on a commercial asset include: – (U) Ensuring that all appropriate personnel protection measures have been taken. – (U) Ensuring that all security force and emergency responders have the appropriate tools, equipment, and personal protective equipment – (U) Notifying appropriate staff and employees of any change in the threat condition. – (U) Implementing emergency and contingency plans, including plans to help carry out evacuation measures or to respond to emergency management requests. – (U) Activating command and support centers and assigning staff members to local government emergency operations centers. – (U) Ensuring that Unified Incident Command Teams work closely with law enforcement, fire departments, and other agencies to prepare for emergencies through planning and drills.

Negative Ground

Much of the negative ground in this topic area will focus on economy-related scenarios, many of which are addressed in the Banking sector of this topic paper. Negative teams will also be able to employ a considerable a considerable number of kritiks since this sector unapologetically endorses a very capitalist method of impact assessment, often calculating physical assets are equal if not more important than individuals.

Communication

Introduction

The use, maintenance, and regulation of communication technology continue to be an uncertain issue for the Federal Government. Diverse forms of technology including cable, satellite, wireless, and wireline modes of communication make it difficult to organize a holistic approach to maintaining the sector. Faced with rapid innovation, Congress often finds itself scrambling to find the proper methods of regulating new forms of communication that they oftentimes do not fully understand. As such, much of the communication sector remains in the hands of private businesses, receiving oversight from regulators such as the Federal Communication Commission. Responsible for the allowed forms of communication, this commission stops short of ensuring the protection and resiliency of communication assets.

One of the first attempts to account for digital technology and ensure the protection of this sector came from President Clinton, who in 1998 initiated Presidential Decision Directive 63 (PDD-63), calling for a commitment to the protection and reliability of all telecommunications by May of 2003.[79] Since then, the goals of the communication sector have expanded. The most recent analyses indicate that the primary goal of this sector is to "ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster."[80] Cyber and physical security are the primary concerns of the communication sector, with increasing attention being paid to digital assets and cyber terrorism.

While the loss of a single form of communication (the disabling of a cell phone tower for instance) is relatively inconsequential, the interconnected nature of the communication sector means that loss of certain facilities could have a cascading effect as other resources become overwhelmed with offset demand.[81,82] Lack of telecommunication resources is likely to have major repercussions on all sectors and it would not take long for this to translate into the loss of life.[83] This threat is exasperated by the risk of inaccurate rumors remaining uncontested due to inadequate communication during a disaster. Inaccuracies of this nature not only confuse the general public, but severely hamper governmental response to continuing crisis.[84] In seeking to reinforce the communication sector, there are two security areas that must be considered: cyber and physical.

Cyber security

[79] Presidential Decision Directive/NCS-63, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
[80] Department of Homeland Security, National Infrastructure Protection Plan: Communications Sector, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf, 2008.
[81] Department of Homeland Security, National Infrastructure Protection Plan: Communications Sector, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf, 2008.
[82] Department of Homeland Security, 2008 Sector CIKR Protection Annual Report for the Communication Sector, http://info.publicintelligence.net/commsector2008.pdf
[83] Doorn, Matthias H. van, Product Manager for Ethernet & Licensed Spectrum Radio Systems at Freeway Technologies, Resilient Wireless Data Communication for Critical Infrastructure: Securing wireless data communication for mission critical applications, http://www.freewave.com/files/whitepapers/Resilient%20Wireless%20White%20Paper.pdf
[84] Congressional Report S. Rpt. 109-322, "Hurricane Katrina: A Nation Still Unprepared." Chapter 20: Protecting Infrastructure; Public Communication; Role of the Media, 2006, http://www.gpoaccess.gov/serialset/creports/pdf/sr109-322/ch20.pdf

The communication sector prioritizes two types of cyber security threats: Denial of Service attacks (DoS) and Intrusion attempts.[85] DoS attacks attempt to make a specific communication system unavailable for its intended user, usually by overwhelming the network with useless data or requests whereas intrusion is an attempt to obtain private or classified information from a communications network. These attacks are used prolifically, impacting public networks, private databases, and governmental facilities.

Digital networks are uniquely susceptible to attack since malicious actions are easily and rapidly distributed throughout a wide network. The impact of these attacks ranges from individuals having their identities stolen to the United States government losing control or oversight of its assets. This is particularly frightening considering recent study of the US-CERT team, tasked with protecting non-military agencies against cyber-attacks, indicating that the agency is incapable of responding to threats in real-time.[86] Military networks are not doing much better, recently receiving a grade of 'C' due to their inability to protect Pentagon networks from the millions of attacks occurring every day, some of which originate from foreign governments such as China.[87]

Physical Security

Though underappreciated in contemporary discussion, the threats posed by a weakened communication sector due to the compromising of physical systems are very real. Given our collective dependence on digital media, we often forget that physical assets are critical to the sustainability of virtually every communication system. This was made obvious following Hurricane Katrina, identified as the worse collapse of our critical infrastructure since World War II.[88] Immediately following the devastation of Katrina, some scholars thought that greater attention would be paid to the reliability of critical infrastructure; unfortunately this has not been the case:

> **Miller**, Senior Research Professor at the National Defense University, **06**
> Dr. Roberts, Hurricane Katrina: Communications & Infrastructure Impacts,
> http://www.carlisle.army.mil/DIME/documents/Hurricane%20Katrina%20Communications%20&%20Infrastructure%20Impacts.pdf
> **Virtually all of the critical infrastructure sectors in the region were put out of commission at the same time**. **Failures in one sector had cascading effects** on others. **These simultaneous failures far exceeded the experience base and available resources** of public officials, and led to a partial or complete breakdown in command and

[85] Doorn, Matthias H. van, Product Manager for Ethernet & Licensed Spectrum Radio Systems at Freeway Technologies, Resilient Wireless Data Communication for Critical Infrastructure: Securing wireless data communication for mission critical applications, 2010, http://www.freewave.com/files/whitepapers/Resilient%20Wireless%20White%20Paper.pdf
[86] TG Daily, "U.S. Government unprepared for cyberattacks, says report", June 17th, 2010, http://www.tgdaily.com/security-features/50245-us-government-unprepared-for-cyberattacks-says-report
[87] Associated Press, "U.S. Cyberattack Defenses Are Weak, Ineffective," March 18, 2011, http://www.crm-daily.com/news//story.xhtml?story_id=0320013QDNI8
[88] Dr. Miller, Roberts. Senior Research Professor at the National Defense University, Hurricane Katrina: Communications & Infrastructure Impacts, http://www.carlisle.army.mil/DIME/documents/Hurricane%20Katrina%20Communications%20&%20Infrastructure%20Impacts.pdf, 2006.

> control and in public order. Widespread critical infrastructure collapse is one of the marker elements that helps differentiate "catastrophes" from "disasters." **The concept of critical infrastructures is one of those classic inside-the-beltway obsessions that often seem to have little resonance in saner parts of the country.** That's unfortunate, because I suspect that **as the 21st century goes along we will all find ourselves paying more attention to the implications of vulnerabilities in our critical infrastructures. There's reason for this concern, given the ways in which today's globalized, just-in-time, interconnected world magnifies the consequences of regional catastrophes**. Globalization and interconnections mean that events which once could have been handled locally will have widespread ripple effects, and that these effects can be unexpectedly disruptive.

In order to maintain critical communication networks in a time of national crisis, updated and reinforced assets are desperately needed.

Affirmative Ground

The need for affirmative action in the communication sector is well documented. With recent cuts in research & development initiatives towards sector security, the entire industry finds itself uncertain of the years to come.[89] While the communication sector is expected start deteriorating in the coming years, there are already a number of risks that exist including the lack of local and regional cyber security, which creates a backdoor for cyber threats to infiltrate the national system.[90]

Digital Security

Focusing on internet-based communication, there are a number of options available to affirmatives. Maintaining a stable and safe network free of spyware or exploitation is difficult given the ad hoc nature of cyber security. One possibility for affirmatives would be to revamp the internet, creating a more structured security system:

> **Paris, 08**
> (Paul Parisi, CTO of DNSstuff.com, Q&A: Threats to the US critical communications infrastructure, http://www.net-security.org/article.php?id=1182&p=2)
> Internet – **the Internet by its very nature and design is a network of trust, largely only regulated by each participant's common sense**. In some ways it is similar to a large road and highway infrastructure, but with no police or legal authority to enforce common sense. Typically problems are only "noticed" when it is too late and the impact of the problem is felt by multiple people. **The current protocols in use on the Internet do not offer explicit nor implicit security. If we begin to layer on new protocols and allow the old protocols to persist, we leave ourselves open to nearly all of the problems of the older protocols.** In response to the problems**, a significant step would be to disallow the old protocols.** However, this would be very painful. Potentially **a new Internet could be deployed which addresses these inherent issues and only allow peering with compliant participants.**

Typically problems are only "noticed" when it is too late and the impact of the problem is felt by multiple people. The current protocols in use on the Internet do not offer explicit nor implicit security. If we

[89] Department of Homeland Security, 2008 Sector CIKR Protection Annual Report for the Communication Sector, http://info.publicintelligence.net/commsector2008.pdf
[90] Department of Homeland Security, 2008 Sector CIKR Protection Annual Report for the Communication Sector, http://info.publicintelligence.net/commsector2008.pdf

begin to layer on new protocols and allow the old protocols to persist, we leave ourselves open to nearly all of the problems of the older protocols. In response to the problems, a significant step would be to disallow the old protocols. However, this would be very painful. Potentially a new Internet could be deployed which addresses these inherent issues and only allow peering with compliant participants.

Beyond the public sector, affirmatives could focus on the cyber security of governmental assets, including those responsible for maintaining classified data. One option avaialbe would be to install new security into the governmental network, such as the Einstein 3 program:

> **Customer Relations Management News, 3/18/11**
> (http://www.crm-daily.com/news//story.xhtml?story_id=0320013QDNI8)
> **Homeland Security Department Undersecretary** Phil **Reitinger told** the House of Representatives Homeland Security Committee **that the ongoing budget deadlock will trigger funding cuts and hurt the agency's effort to install the Einstein 3 program across the federal networks**. **Einstein 3** is a sophisticated system that **will detect and automatically block intrusions.** Alexander and James Miller, the principal defense undersecretary for policy, said the Pentagon is working steadily to better harden its networks and work with the administration to figure out what authorities the military needs in order to respond to cyberattacks against the government and critical infrastructure which is generally owned and operated by private companies.

Physical Security

Many towers now have backup generators, but are incapable of handling the increased amount of data requested during natural or manmade disasters (cell service is typically overwhelmed during large disasters or holidays, such as New Year's Eve). This threat is coupled with the potential for a major event that completely devastates an entire region, crippling communication networks beyond repair. The harms of these scenarios is well documented, indicating a social dependence on the communication sector that translates into the loss of countless lives:

> **FCC, 06**
> (Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, http://www.fcc.gov/eb/Orders/2006/FCC-06-83A1.html)
> **The destruction to communications companies' facilities in the region**, and therefore to the services upon which citizens rely, **was extraordinary. Hurricane Katrina knocked out more than three million customer phone lines** in Alabama, Louisiana, and Mississippi. The wire line communications network sustained enormous damage—**dozens of central offices and countless miles** of outside plant **were damaged or destroyed** as a result of the hurricane or the subsequent flooding**. Local wireless networks also sustained considerable damage**—more than a thousand cell sites were knocked out of service by the hurricane. **At the hurricane's height, more than thirty-five Public Service Answering Points** (PSAPs) **were out of service, and some parishes in Louisiana remained without 911** or enhanced 911 (E911) **service for weeks.**

Following a major catastrophe, either human-caused or natural, it takes little imagination to consider the implications of weeks without emergency service or reliable forms of communication. Affirmatives could alleviate these harms by responding to the urgency of the situation, something that is agreed upon but

has yet to be acted upon.[91] One option is to increase the reliability and readiness of second-responders; individuals tasked with repairing infrastructure assets following a disabling event:

> **Miller**, Senior Research Professor at the National Defense University, **06**
> Dr. Roberts, Hurricane Katrina: Communications & Infrastructure Impacts, http://www.carlisle.army.mil/DIME/documents/Hurricane%20Katrina%20Communications%20&%20Infrastructure%20Impacts.pdf
> Some of the **policy options that may improve the speed and effectiveness of both first- and second-responder actions in the communications sector include: 1.Taking further steps to make it easier for military assets in areas such as wireless communications to backstop local response and law enforcement resources**. Military communications networks often encrypted and with a heavy emphasis on security, have not been designed to carry out homeland defense missions that require interoperability with emergency responders and civilian agencies. Although this lack of interoperability may have made operational sense in the 20th century, it is worth re-examining in light of current realities**. 2. Embarking on a broader re-examination of the military's proper role in responding to catastrophic incidents.** Under the National Response Plan, the general rule is that the military backs up but does not supplant other responders. However, it is increasingly obvious that only the active duty military has the resources, mobility and deployability needed to respond to catastrophic events that affect large areas and cross state lines. **3. Building more redundancy into the current telecommunications networks at critical nodes. 4. Requiring public communications carriers to maintain adequate and tested back-up facilities. 5. Devoting resources to improving our ability to collect and disseminate accurate, prompt public information in order to reduce the kinds of false rumors that were so widely disseminated by the media in the immediate aftermath of the hurricane. 6. Taking steps to reduce the time and effort needed to restore critical services and infrastructures when things do go wrong,** including intensified efforts to create more rapid-deployment resources within DHS and creating more rapid-deployment federal/state/local joint operations centers.

In their own right, each of these proposals would serve to improve the communication sector. Taking this into account, it will be necessary for debaters to consider the significance of each proposal, possibly choosing to incorporate multiple actions into a single plan text.

Negative Ground

Specific negative ground in this sector will greatly depend upon the type of affirmative being read. For example, affirmatives dealing with cyber security are likely to employ technology, such as Einstein 3, that dramatically reduces the privacy rights of the average citizen.

> **L.A. Times, 09**
> (NSA's cyber overkill, July 14th, 2009, http://articles.latimes.com/2009/jul/14/opinion/oe-radack14)
> Cyber security is a real issue, as evidenced by the virus behind July 4 cyber attacks that hobbled government and business websites in the United States and South Korea. It originated from Internet provider addresses in 16 countries and targeted, among others, the White House and the New York Stock Exchange. Unfortunately, the Obama administration has chosen to combat it in a move that runs counter to its pledge to be transparent. The administration reportedly is proceeding with a Bush-era plan to use the

[91] Dr. Miller, Roberts. Senior Research Professor at the National Defense University, Hurricane Katrina: Communications & Infrastructure Impacts, http://www.carlisle.army.mil/DIME/documents/Hurricane%20Katrina%20Communications%20&%20Infrastructure%20Impacts.pdf, 2006.

> National Security Agency to screen government computer traffic on private-sector networks. AT&T is slated to be the likely test site. This classified pilot program, dubbed **"Einstein 3," is developed but not yet rolled out. It takes two offenders from President Bush's contentious secret surveillance program and puts them in charge of scrutinizing all Internet traffic going to or from federal government agencies**. Despite its name, **the Einstein 3 program** is more genie than genius -- an omnipotent force (run by the NSA via AT&T's "secret rooms") that **does the government's bidding -- spying**. The last time around, this sort of scheme was known as the "special access" program -- "special" being code for "unconstitutional." Einstein 3 purportedly is meant to protect government networks from hackers. **But cyber-security experts -- such as Babak Pasdar,** who blew the whistle on a mysterious "Quantico Circuit" while working for a major service provider -- **agree that Einstein 3 offers no intrinsic security value. The program is implemented where servers exchange traffic between one another -- in the heart of a network system rather than at the perimeter, which interfaces with the outside world. This is similar to a home security system that only monitors the central interior of a house, rather than keeping an eye on the actual doors** (and the purpose of hackers may simply be to enter.)

Given the specificity of the proposals found in the literature base, it is likely that much of the negative ground in this sector will stem from case turns and specific counterplans. The negative for this area heavily overlaps with the Information Technology (IT) Sector paper, which lists a number of disadvantage, counterplan and critical argument options.

Generally speaking, Negative teams can also benefit from the surprising implications of increasing the resiliency of communication networks. Unfortunately, it is incredibly difficult to isolate benign forms of communication from those used to inflict harm to others. Creating a strong network ensures the ability for violent individuals, such as terrorists, to continue attacking Americans and their assets even after the first attacks have occurred.[92]

[92] Doorn, Matthias H. van, Product Manager for Ethernet & Licensed Spectrum Radio Systems at Freeway Technologies, Resilient Wireless Data Communication for Critical Infrastructure: Securing wireless data communication for mission critical applications, 2010, http://www.freewave.com/files/whitepapers/Resilient%20Wireless%20White%20Paper.pdf

Continuity of Government

Introduction

While the Department of Homeland Security (DHS) does not include Continuity of Government (CoG) in their current assessment of critical infrastructures, the debate community should strongly consider including this area in next years' resolution. Much of the literature emanating from the DHS identifies critical infrastructures as "the personnel, physical assets, and communication/cyber systems that must be intact and operational 24x7 in order to ensure survivability, continuity of operations, and mission success. In other words, they are the essential people, equipment, and systems to prevent or mitigate the catastrophic results of all man-made and natural disasters".[93] Based on the available ground for the aff and neg surrounding CoG, topic wordings including this subsection of critical infrastructures should be considered. Even if CoG is not explicitly listed as a topic area, it is possible that Continuity of Government protocols could be classified under the current DHS critical infrastructure list as an 'emergency service' or as a subsection to 'government facilities'.[94] This option is less favorable since it makes any potential CoG ground questionably topical.

The DHS's reluctance to continually include CoG protocols in their list of critical infrastructures is a curious situation since CoG is included in some reports, but entirely absent from others (FAS 04). The inconstant appearance of CoG operations should not discourse the debate community. The creation of the Continuity of Government Commission in 2009 proves that this topic area is a major concern to current policy makers. This commission, in conjunction with other literature available on the topic, makes the inclusion of CoG a feasible option. Furthermore, the occasional absence of CoG protocols likely points to the convoluted nature of classified data and the uncertain disclosure policies of the DHS. Rather than hurting our ability to debate the CoG, the periodic absence of CoG likely indicates a rapidly changing and dynamic field of study. The following analysis will focus on the available ground concerning CoG protocols in relation to Critical Infrastructure development.

The term 'Continuity of Government' (CoG) refers to an emergency government protocol that is designed to prevent a 'decapitation' event against the United States government in which a majority of critical personnel is either killed or incapacitated. Ronald Reagan established the first CoG at the height of the Cold War, fearing a nuclear attack by the Soviet Union[95]. Regan's plan organized three autonomous groups of cabinet members and military officers that would each flee to a separate undisclosed location in the event of a major attack. Each group was designed to be capable of assuming control over the government in the event of massive fatalities, functionally creating three contingent presidencies. Since then, few things have changed concerning the CoG protocols for the Federal

[93] Department of Homeland Security, http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/factsheet.shtm, 2009
[94] Department of Homeland Security. http://www.dhs.gov/xnews/releases/pr_1179773665704.shtm, 2007
[95] Mann, James. *The Armageddon Plan*, March, http://www.commondreams.org/views04/0318-14.htm, 2004

Government. Fears of Russian annihilation have diminished over time, but they have now been replaced by rouge nations and terrorism. September 11th, 2001 illustrated our current incapacity to maintain CoG during a massive terrorist attack. Without a clear policy in effect, Dick Cheney personally initiated the same contingency plans that he had helped to develop during the Regan Administration. Luckily, the U.S. did not experience massive governmental causalities during the 9-11 attacks. Mobilization in the mist of chaos was slow, ill-prepared, and unpracticed. Without a clear and updated contingency plan, it is highly probable that the nation would be thrown into anarchy due to lack of governmental succession.

In an effort to update CoG operations, the Continuity of Government Commission (CoGC) was created in 2002 shortly following the September 11, 2001 terrorist attacks. Publishing their first report in 2003, the commission has continued to advocate a complete overhaul of current CoG strategies. Their proposals serve as the core of this particular topic area and provide valuable insight into the status and impact of various proposals.

The 2002 CoGC report has been recently supplemented by a 2009 report focusing on the succession of the presidency in the even of a catastrophic attack. The CoGC stipulates that the current presidential succession system is inadequate in a world of weapons of mass destruction:

> **Continuity of Government Commission, 09**
> (Preserving Our Institutions The second report of the continuity of Government commission The continuity of the presidency, June 2009, http://www.continuityofgovernment.org/SecondReport.pdf)
> **Unlike the current provisions for congressional continuity which do not include any institutional protections in the case of an attack causing mass vacancies** or mass incapacitations, **there is a Presidential succession system in place. However,** it is the finding of this commission that **the current system would be inadequate in the face of a catastrophic attack that would kill or incapacitate multiple individuals in the line of succession. The current system must be corrected to ensure continuity in the executive branch.**

In relation to this topic paper, the CoG provides unique ground on both sides of the debate. The state of CoG planning is an issue that incapulates questions of democracy, representation, terrorism, coercion, and international perception. The following sections will provide a brief examination of some core aff and neg ground concerning the CoG.

Affirmative Ground

Depending on the topic wording, affirmatives in this topic area could update the CoG protocols for one or all of the three branches of the USFG. This section will focus on the different affirmatives available under any given topic wording, focusing on specific and general plan action options.

Congressional CoG

As stated early, the CoGC has strongly recommended a Constitutional amendment addressing the succession of Congress in the event of mass causalities or incapacitation. Given the language of the Constitution in relation to Congressional succession, an amendment is likely to be the only means of

topical plan action when dealing with Congressional CoG[96] [97]. As would be might expect for a domestic topic area, CoG affirmatives would access large democracy advantage ground. One such example is provided by the CoCG:

> **Continuity of Government Commission, 03**
> (The Congress. Preserving our institutions: The first report of the continuity of government commission, May 2003
> http://www.continuityofgovernment.org/report/FirstReport.pdf)
> **If anyone doubts the importance of Congress in times of crisis, it is helpful to recall that in the days after September 11th, Congress authorized the use of force in Afghanistan; appropriated funds for reconstruction of New York** and for military preparations; **and passed major legislation granting additional investigative powers and improving transportation security. In a future emergency, Congress might also be called upon to confirm a new vice president**, to elect a Speaker of the House who might become president of the United States**, or to confirm Supreme Court justices for lifetime appointments. In the event of a disaster that debilitated Congress, the vacuum could be filled by unilateral executive action—perhaps a benign form of martial law. The country might get by, but at a terrible cost to our democratic institutions**.

Docket-based advantages another potential area of aff ground. In the event of a cataclysmic attack, any given issue relevant to Politics DAs would be derailed, meaning that advantages of this nature would continue to develop as new bills reach Congress.

Executive CoG

It is common knowledge that whenever the President addresses Congress that all but one of the Cabinet members are in attendance. The single member that is whisked away to an undisclosed location is charged with assuming the presidency in the event that the president and remainder of the cabinet were to be killed or incapacitated. Unfortunately, the single absent member is determined randomly, meaning that Department of Veterans Affairs Secretary Eric K. Shinseki could find himself assuming the presidency in the event of a national emergency. While Secretary Shinseki might prove to be a capable executive, he is hardly the most qualified option within the cabinet.

In a world of telecommunications and instantaneous data transfer, affirmatives could focus on altering the rules dictating who is in attendance during executive speeches such as the State of the Union. This type of affirmative would be uniquely interesting since it would draw upon other areas of the topic, such as telecommunications networks.

Regardless of the specific affirmative, executive CoG is a topic that has a large literature base. One such example in the status quo CoG protocols concerns the questionable nature of congressional separation of powers in the event of an unexpected presidential vacancy. The current wording of succession law dictates that if the President and Vice President were to be killed executive authority would transfer to the Speaker of the House or the President pro tempore. Under the current guidelines, these officers would technically retain their positions within Congress while serving as president, meaning

[96] Specific policy proposals available at: http://www.continuityofgovernment.org/report/FirstReport.pdf
[97] Continuity of Government Commission, The Congress. Preserving our institutions: The first report of the continuity of government commission, May 2003, http://www.continuityofgovernment.org/report/FirstReport.pdf

that separation of power would completely disappear[98]. There are multiple affirmatives that could solve for these harms, as argued by M. Miller Baker of the Federalist Society:

> **Baker,** former counsel to Senator Orrin G. Hatch, **03**
> (Fools, Drunkards, & Presidential Succession, December 1, 2003, http://www.fed-soc.org/publications/PubID.123/pub_detail.asp)
> In the long run**, the solution to** the problem of the **concentration of presidential successors** in Washington **is a constitutional amendment that allows the President to nominate**, subject to Senate confirmation, **statutory presidential successors** (in addition to the cabinet) **who are not "Officers" of the United States,** but nevertheless are eminently qualified**, to act as President in the extreme situation that the nation would face following the destruction of Washington, D.C., and the elimination of the President, the Vice President, and the statutory cabinet successors. For example, President Bush might nominate former President George H.W. Bush** and former Vice President Dan Quayle, both of whom no longer live in Washington**, to serve in the line of succession. Similarly, a future President Daschle might nominate former Vice Presidents Al Gore** and Walter Mondale to serve in the statutory line of succession (Baker 2003).

In addition to SoP advantage ground, affirmatives that alter the line of succession would also be able to run political advantages based upon the personal agendas of those that would gain power in the event of presidential succession, including arguments based on a potential president needing to replace the entire Supreme Court in the event of deadly attack on the Judiciary[99]. This brings us to the final branch of the Federal Government susceptible to CoG harms; the Supreme Court.

Judicial CoG

The threat of an attack on the judiciary is comparatively minimal. Lack of international perception and vulnerabilities of (perceptually) more important targets makes alternations to the judicial CoG a low priority. In addition to these perceptual barriers against an attack, Court justices have noted that the decentralized nature of the court system makes disruption of the legal system unlikely:

> **Washington Post, 02**
> (Charles Lane, After Sept. 11, judiciary rethinks the unthinkable, April 12, 2002, http://www.continuityofgovernment.org/pdfs/020412post.PDF)
> But despite what some consider a close call at the court Sept. 11, **the view among judges is that the security situation at the federal judiciary is different from,** and in some ways more favorable than, that of **the other two branches of government**. Although an attack on the Supreme Court when some or all of the nine justices were there could decapitate the judiciary, **the decentralization of the lower courts renders them relatively invulnerable to a Doomsday scenario**, judges say. "We wonder about the necessity" of being part of the shadow government, **Justice** Anthony M. **Kennedy**, who was the only other justice at the court Sept. 11, **told a House subcommittee** March 13. "**All . . . district and circuit judges are courts of general jurisdiction and can issue writs under the All Writs Act. So we are already dispersed nationwide**," he said.

[98] Baker, Miller M., Fools, Drunkards, & Presidential Succession, December 1, 2003, http://www.fed-soc.org/publications/PubID.123/pub_detail.asp
[99] Washington Post, Charles Lane, *After Sept. 11, judiciary rethinks the unthinkable*, http://www.continuityofgovernment.org/pdfs/020412post.PDF, April 12, 2002

Any potential affirmative ground concerning the judiciary would likely stem from claims that the status quo illustrates a false sense of security. Few (unclassified) protective measures are currently in place for the judiciary, meaning that any attack against the Court would have a reasonable risk of succeeding and spurring U.S. war escalation scenarios.

General CoG

Depending on the topic wording, affirmatives could focus on altering the CoG protocols for the entire Federal Government. An example of one such affirmative would be to alter the conditions in which governmental leaders can meet with each other. The CoGC isolates Presidential Inauguration ceremonies as being a uniquely dangerous moment for the CoG:

Continuity of Government Commission, 03
(The Congress. Preserving our institutions: The first report of the continuity of government commission, May 2003 http://www.continuityofgovernment.org/report/FirstReport.pdf)
It is 11:30 A.M., **inauguration day. Thousands await** the noon hour when a new president will **take the oath of office in the presence of members of Congress, the Supreme Court, family, and supporters. The outgoing president is** meeting at the White House **with his cabinet and top aides** for a final farewell before attending the swearing in ceremony where the reins of power will switch hands. Television networks have their cameras trained on the West Front of the Capitol, beaming live coverage of the event into millions of homes around the world. **Suddenly the television screens go blank! Al Qaeda operatives have detonated a small nuclear device** on Pennsylvania Avenue halfway **between the White House and the Capitol**. A one-mile-radius circle of Washington is destroyed. **Everyone present at the Capitol, the White House, and in between is presumed dead, missing, or incapacitated.** The death toll is horrific, the symbolic effect of the destruction of our national symbols is great, but even worse, **the American people are asking who is in charge, and there is no clear answer. The incoming president and vice president are** surely **dead, so the presidency passes** through the line of **succession to the Speaker of the House and** then to **the President Pro Tempore** of the Senate. **But both of them were at the inaugural ceremony, as protocol requires, so the presidency passes to the cabinet officers—but which cabinet? The president-elect never took office and never confirmed a cabinet. The presidency passes** through the line of succession **to the cabinet officers of the departing administration, assuming they have not resigned** by January 20th, **as is standard procedure, and assuming that they were not at the White House** bidding farewell to the outgoing president. Perhaps the Secretary of Veterans Affairs, or another lesser known cabinet member, was not in the area; then he or she would become president. Or **maybe no one in the line of succession is alive, and a number of generals, undersecretaries, and governors claim that they are in charge.** Congress has been annihilated as well, with only a few members who did not attend the ceremony remaining. It will be many months before Congress can function. Our Constitution requires a majority of each house of Congress to constitute a quorum to do business, and no such majority of the House or Senate exists. In addition, because of a series of past parliamentary rulings, there is confusion about whether there are enough members to proceed. The House's official interpretation of the quorum requirement is a majority of the living members, a proposition that scholars have questioned. Under this interpretation, if only five House members survive, a group of three might proceed with business and elect a new Speaker who would become president of the United States, bumping any cabinet member who had assumed the presidency and remaining in office for the rest of the four-year term. Because the House of Representatives can fill vacancies only by special election, the House might go on for months with a membership of only five. On average, states take four months to hold special elections, and in the

> aftermath of a catastrophic attack, elections would likely take much longer. Under the Seventeenth Amendment governors can fill vacancies within days by temporary appointment, therefore the Senate would reconstitute itself much more quickly than the House. Imagine in this chaotic situation that all these events are taking place without access to normal organization, procedure, and communication channels. **The confusion might** very well **lead to a conflict over who would be president**, Speaker of the House, or commander in chief, and **a cloud of illegitimacy would** likely **hang over all government action**. **The institution that might resolve such disputes is the Supreme Court. However**, it is likely that **the entire Court would be killed in such an attack, leaving no final tribunal to appeal to for answers to questions about succession and legislative and executive action. A new court could be appointed by a new president and confirmed by a new Senate, but which president, which Senate, and how soon? Further, would we want the entire Supreme Court appointed for life tenure by a disputed or unelected president?**

The unique circumstances of a presidential inauguration are rare, but troubling in the event of a WMD attack. The CEDA topic committee would need to determine if this kind of affirmative would qualify as a substantial shift in policy. Even if such an affirmative would prove too small to be topical, it illustrates the negligence of current succession policies.

In order to avoid rehashing the nuclear topic next year, debaters should keep in mind that events of mass governmental incapacitation need not be nuclear in nature. The CoGC stipulates that biological, chemical, or conventional attacks would be equally destructive:

> **Continuity of Government Commission, 09**
> (Preserving Our Institutions The second report of the continuity of Government commission The continuity of the presidency, June 2009, http://www.continuityofgovernment.org/SecondReport.pdf)
> Because of the availability of chemical and biological agents, the possibility of mass incapacitation is real. **A chemical attack might leave thousands in burn units or with respiratory and neurological injuries. If such an attack were centered on Congress, many members could be in hospital intensive care units for months**. Or imagine **if the anthrax attack on the Senate had been undetected and particles had dispersed widely through the ventilation system. Senators** and their staffs **might have survived** the attack, **but the recovery period would have been many months. More troubling is** the possibility of an **infectious disease such as smallpox. If even a few members** of Congress **contracted the disease**, the **members might choose not to convene for fear of spreading the disease**. Finally, even **a conventional attack might leave hundreds of members in hospitals or burn units—alive, but unable to perform their duties for a significant period of time**.

An attack that debilitates but does not kill a large number of Congressional members is particularly troubling because the Constitution offers no contingency for an incapacitated representative (CoGC 2009). Legally deceased or missing Congressional representatives can be quickly and efficiently replaced, but individuals that are alive but incapable of continuing their post are technically not eligible for immediate replacement. This leaves a large loophole in governmental succession, since any attempt to replace these Congress members would likely face legal battles and widespread uncertainty.

As a final note on affirmative ground, it should be noted that this topic area should be particularly appealing to critical debaters. Much of the civilian literature pertaining to CoG deals directly with 9/11 and

the questionable actions of the Bush administration concerning civil liberties and separation of powers. One such analysis identifies the CoG as the root of Bush's executive abuse:

> **Scott and Hamburg, 09**
> Peter Dale Scott and Dan Hamburg, (COG) is martial law in effect since 9/11. March 24, 2009, http://robertscourt.blogspot.com/2009/03/continuity-of-government-cog-martial.html
> **On 9/11 the Bush administration declared a State of Emergency** (SOE), which was formally proclaimed on September 14, 2001, and **extended by Bush repeatedly thereafter**, most recently on August 28, 2008.**1 Under cover of this SOE, Bush secretly enacted many extreme measures, ranging from suspension of habeas corpus to preparations for martial law in America; all these were undertaken as part of secret so-called "Continuity of Government"** (COG) **procedures associated with the SOE, and first instituted on 9/11**.

Topic wording will affect the topical affirmative ground based on the above information, but any logical resolution would likely allow most of the above affirmatives. As stated previously, the CoG will likely be utilized in conjunction with other topic areas for most affirmatives.

Negative Ground

Some portion of the potential affirmative ground discussed above will likely fall to the negative depending upon the topic wording. This ground will also be supplemented by a substantial number of core arguments pertaining the domestic politics and international perceptions. It is difficult to foresee how specific negative ground will play out for this topic area given its heavy dependence on topic wording, but some generic areas will likely include democracy-based claims, amendment ground similar to that of the counterplans seen on the courts topic, and critical negative ground pertaining to the existence and function of the government in the status quo. Additionally, negatives could elect to focus on counterplans calling for temporary appointments of various types as they would pertain to the plan.

Most negative ground for this topic will derive from the specific mechanisms and individuals affected by the plan. We should expect incredibly specific politics disadvantages and PICs focusing on specific policy proposals stipulated in the 1AC.

Critical Manufacturing

Introduction

This paper advocates on behalf of the inclusion of the Critical Manufacturing (CM) sector within a Critical Infrastructure and Key Resources debate resolution. The paper will begin by identifying key challenges and controversies confronting this sector and will then identify affirmative and negative strategies for consideration.

The Critical Manufacturing sector is defined by the Department of Homeland Security as follows:

> **Department of Homeland Security**,10
> (2010, June 14, Critical Manufacturing Sector: Critical Infrastructure and Key Resources. Retrieved from http://www.dhs.gov/files/programs/gc_1226007062942.shtm)
> **The Critical Manufacturing** (CM) **Sector is crucial to the economic prosperity and continuity of the United States**. **U.S.** manufacturers design, produce, and distribute **products** that **provide more than one of every eight dollars of the U.S. gross domestic product and employ more than 10 percent of the nation's workforce**. **A direct attack on or disruption of** certain elements of t**he manufacturing industry could disrupt essential functions at the national level and across multiple other critical infrastructure and key resources sectors**. Based on the guidance provided by HSPD-7, **the following nine industries currently meet the CIKR criteria** of the CM Sector **and are not included within an existing sector**:
> Primary Metal Manufacturing
> **Iron and Steel Mills and Ferro Alloy Manufacturing**
> **Alumina and Aluminum Production and Processing**
> **Nonferrous Metal** (except Aluminum) **Production and Processing**
> Machinery Manufacturing
> **Engine, Turbine, and Power Transmission Equipment Manufacturing**
> Electrical Equipment, Appliance, and Component Manufacturing
> **Electrical Equipment Manufacturing**
> Transportation Equipment Manufacturing
> **Motor Vehicle Manufacturing**
> **Aerospace Product and Parts Manufacturing**
> **Railroad Rolling Stock Manufacturing**
> **Other Transportation Equipment Manufacturing**
> The products made by these manufacturing industries are essential in varying capacities to many other CIKR sectors. The CM Sector focuses on the identification, assessment, prioritization, and protection of nationally significant manufacturing industries that may be susceptible to terrorist attacks.

Right away, it should be apparent to readers that the economy will factor in as a prominent focal point for discussion of the CM sector. While this is evident, the specific internal link debates offered by this area provide the community with a plethora of diverse arguments and opportunities for in-depth discussions of many of the products that keeps America on its feet.

This economic impact can be examined through evidence analyzing the relationship between manufacturing, jobs and consumer spending:

> **McCormack, 09** (Richard. (2009, December 21). The Plight of American Manufacturing. *The American Prospect*. Retrieved from http://prospect.org/cs/articles?article=the_plight_of_american_manufacturing#.)

Something has gone radically wrong with the American economy. **A once-robust system of** "traditional engineering" -- the invention, design, and **manufacture of products** -- **has been replaced by financial engineering**. **Without a vibrant manufacturing sector**, **Wall Street created money it did not have and Americans spent money they did not have**. **Americans stopped making the products they continued to buy**: clothing, computers, consumer electronics, flat-screen TVs, household items, and millions of automobiles. **America's economic elite has long argued that the country does not need an industrial base**. The economies in states such as California and Michigan that have lost their industrial base, however, belie that claim. **Without an industrial base**, **an increase in consumer spending**, **which pulled the country out of past recessions**, **will not put Americans back to work**. **Without an industrial base**, **the nation's trade deficit will continue to grow**. Without an industrial base, **there will be no economic ladder for a generation of immigrants**, **stranded in low-paying service-sector jobs**. Without an industrial base, the United States will be increasingly dependent on foreign manufacturers even for its key military technology. **For American manufacturers**, **the bad years didn't begin with the banking crisis of 2008**. Indeed, the **U.S. manufacturing** sector **never emerged from the 2001 recession**, **which coincided with China's entry into the World Trade Organization**. Since 2001, the country has lost 42,400 factories, including 36 percent of factories that employ more than 1,000 workers (which declined from 1,479 to 947), and 38 percent of factories that employ between 500 and 999 employees (from 3,198 to 1,972). An additional 90,000 manufacturing companies are now at risk of going out of business. Long before the banking collapse of 2008, such important U.S. industries as machine tools, consumer electronics, auto parts, appliances, furniture, telecommunications equipment, and many others that had once dominated the global marketplace suffered their own economic collapse. Manufacturing employment dropped to 11.7 million in October 2009, a loss of 5.5 million or 32 percent of all manufacturing jobs since October 2000. The last time fewer than 12 million people worked in the manufacturing sector was in 1941. In October 2009, more people were officially unemployed (15.7 million) than were working in manufacturing. **When a factory closes**, **it creates a vortex that has far-reaching consequences**. The Milken Institute estimates that **every computer-manufacturing job in California creates 15 jobs outside the factory**. **Close a manufacturing plant**, **and a supply chain of producers disappears with it**. **Dozens of companies get hurt**: those supplying computer-aided design and business software; automation and robotics equipment, packaging, office equipment and supplies; telecommunications services; energy and water utilities; research and development, marketing and sales support; and building and equipment maintenance and janitorial services. The burden spreads to local restaurants, cultural establishments, shopping outlets, and then to the tax base that supports police, firemen, schoolteachers, and libraries.

Among the other controversy areas within the CM sector is the question of maintaining America's military hegemony:

Rizzo, 10
(Jennifer. (2010, September 22). Industry experts: Less 'made in USA' putting American security at risk. *CNN*. Retrieved from http://www.cnn.com/2010/POLITICS/09/22/manufacturing.security/index.html)
Washington (CNN) -- **The decline in American manufacturing is risking the country's security**, experts will tell a Congressional hearing on Wednesday. **Manufacturing industry experts** will appear at a National Security Oversight Subcommittee on Capitol Hill to **examine the effects the decades old downturn in U.S. manufacturing** may **have on the country's national security**. **The committee also will examine the problem of reliance on substandard and sometimes counterfeit foreign-made parts**, **a dependence stemming from the drop in U.S.-made products**, **a depleted manufacturing workforce**, **and outdated technology**. **That reliance could place the**

> **lives of American soldiers at risk**, according to information released by the subcommittee. "**We have allowed our industrial base to deteriorate for the last two to three decades**. **As a result**, just in national defense terms, **our supply lines for strategic parts and materials have been stretched around the world**," **said** Jeff **Faux**, **founding president** and distinguished fellow **of the Economic Policy Institute**. "**As you watch globalization move the manufacturing base offshore**, **in essence you are moving the defense base offshore**," **said** Robert **Baugh**, **executive director of the AFL-CIO**, "This is dangerous."

Additional research confirms not only the importance of manufacturing to national defense, but specific products, political debates and other CIKR as well:

> **Parks, 10**
> (James. (2010, September 22). Restoring U.S. Manufacturing Vital to National Security. *AFL-CIO Now Blog*. Retrieved from http://blog.aflcio.org/2010/09/22/restoring-u-s-manufacuturing-vital-to-national-security/*)*
> **The days when the United States could mobilize hundreds of factories and trainable workers to quickly produce what the nation needs to fight a war are gone**. **Thousands of factories are sitting idle and the workers who make our ammunition**, **GPS systems and build our planes are nearly all overseas**. Testifying today before a House subcommittee, several experts called for an immediate rethinking of our national economic policies so as to regain our global lead in manufacturing before it is too late. **As manufacturing goes abroad**, **so do the skills workers need to produce today's computer-driven**, **advanced technology weapons and the research and development that support them**, they warned. **It's time to make the "Made in America" label really mean something again**, Bob **Baugh**, executive director of the AFL-CIO Industrial Union Council, **told the House** Oversight and Government Reform **Subcommittee** on National Security and Foreign Affairs. We must stop importing most of what we consume and begin to manufacture more of it here, he said. **We have already lost our lead in some critical defense-related industries such as semiconductors**, **printed circuit boards**, **machine tools**, **advanced materials and aerospace**, Baugh said. The closure of the Avondale and Ingalls shipyards would cripple our ability to make ships. Michael **Wessel**, a **member of the U.S.-China Economic and Security Review Commission**, **told the panel the situation is so bad that we no longer have the domestic capacity to produce enough ammunition to supply our troops and law enforcement**. **There are waiting lists to fill the police departments here at home**, he said. Baugh and Jeff Faux, distinguished fellow at the Economic Policy Institute (EPI) said the U.S. government must craft **an industrial policy to rebuild our manufacturing**. Its key elements **should include taking away incentives for companies to move jobs overseas**, **reducing the huge U.S. trade deficit**, **pushing harder to force China to end its currency manipulation and using government procurement to encourage domestic production**. **The time is ripe for an industrial policy**, Faux said. Polls show that **majority of American think we need to rebuild manufacturing**. **And business leaders are starting to speak out in support of industrial revitalization**. Or, as Baugh said in his testimony: While the economic crisis that began in 2007 has done massive damage to our country, the truth is our problems run far deeper and none is more fundamental than catastrophic decline of U.S. manufacturing. **The health of the economy and our national security are inextricably tied to a vibrant and innovative manufacturing sector**. **We must revive U.S. manufacturing as a clear centerpiece of our nation's economic and security strategy**.

This debate can be further contextualized by examining the comparative advantage of China, allowing teams to explore the costs and benefits of China's rise to power:

> **Rizzo, 10**

(Jennifer. (2010, September 22). Industry experts: Less 'made in USA' putting American security at risk. *CNN*. Retrieved from http://www.cnn.com/2010/POLITICS/09/22/manufacturing.security/index.html)
The nation's manufacturers are being seduced by China where they can get more for their money due to an undervaluation of their currency, **illegal subsidies**, **and a lack of enforceable laws regarding**, **worker rights**, **and environmental and health standards**, Baugh told CNN. **China's manufacturing sector is on the brink of passing that of the United States**, **according to a report** released in June **by** the economic research firm **IHS Global Insight**. **The value of goods produced by China's factories reached about $1.6 trillion last year**, **compared to $1.7 trillion by U.S. manufacturers**. **The nation's capacity utilization**, **which compares the output of U.S. factories to their maximum potential production**, **fell to a record low of 68.2 percent in June of 2009**, as Chrysler and GM plants essentially shut down due to the bankruptcy process at the two companies, and as other automakers and suppliers scaled back due to overall weakness in demand. **U.S. output has been increasing steadily every month since** that reading, rising to 74.7 percent in August -- the latest month for which data is available -- **but is still down from the average reading**, **which is about 81 percent**. The subcommittee will be looking to hear recommendations from the panel of experts to open up discussions with officials responsible for making manufacturing sector policies. "**It is critical that we focus on modernizing and improving our industrial base** to improve our economy, provide better employment opportunities to Americans, and strengthen national security," **said** Rep. John **Tierney**, D-Massachusetts, **chairman of the subcommittee**. "**We have to start to think strategically** about the industrial challenges we face **and take aggressive action** to fully address them."

Finally, worker exploitation in countries were manufacturing jobs are outsourced provides an angle for teams desiring a critical perspective on the topic:

Elich, 10
(Gregory. (2010, May 16). Sweatshop Manufacturing: Engine of Poverty. Retrieved from http://globalresearch.ca/index.php?context=va&aid=19193)
On a global scale, **the reign of free market ideology has wrought deep changes**. **Manufacturing jobs in the developed nations are rapidly shrinking while abroad there has been a rise in sweatshop manufacturing**, **with conditions reminiscent of the worst of the 19th century**. **The effect has been to widen the gulf between the living conditions of the wealthy and those who labor for them**. **Inequality has reached such an astounding level that it requires an act of willful blindness on the part of Western media not to notice it**. Over half of the world's population subsists on less than $2 a day, while the 200 richest individuals own more wealth than 41 percent of the world's population, or in other words, more than 2.6 billion people. Such an extreme concentration of wealth in the hands of the few cannot be construed as a failure of global capitalism. Indeed, it is a mark of its success, for this is what the system is designed to do. Nor can the mass immiseration on which the system rests be dismissed as an unfortunate mistake or an unintended byproduct of the process. Pillage is the very engine that drives the accumulation of riches. **It is abroad where the repercussions of triumphant capital are at their most troubling**, especially in underdeveloped nations offering a pristine opportunity for unfettered exploitation. Even as the domestic workforce is being relentlessly driven into insecurity, the profits to be had from the exploitation of labor, markets and resources in the Third World are unsurpassed. Capitalism is a global system, and capital flows where it stands to reap the highest returns. It knows no boundaries. **Naked exploitation of labor is the hallmark of manufacturing jobs exported abroad**. **Giant corporations such as Wal-Mart constantly press suppliers to lower costs**, **causing plant managers to wring more production from already over-exploited workers**. At a typical plant in Honduras, managers blame Wal-Mart's continual demands for cheaper clothing for the need to drive their workers so hard. Isabel Reyes labors at this plant for ten hours a day, where she is expected to sew sleeves onto

1,200 shirts during a single shift, an average of one sleeve every 15 seconds. “There is always an acceleration,” she says. “The goals are always increasing, but the pay stays the same.” After eleven years at the plant, her Carpal Tunnel Syndrome has worsened to the point where she cannot lift a pot or hold her baby without first taking anti-inflammatory pills. In compensation for her toil, she earns about $35 a month.

Affirmative Options

Research & Development

Part of improving the resilience and protection of the CM market is opening the doors to new technologies within the existing manufacturing sectors. Among these technologies is hydrogen, an alternative fuel that can be used to create a more resilient transportation infrastructure:

Interagency Working Group on Manufacturing R&D, 08
(2008, March, Manufacturing the Future: Federal Priorities for Manufacturing R&D. Retrieved from http://www.manufacturing.gov/pdf/NSTCIWGMFGRD_March2008_Report.pdf)
The IWG technical priority area Manufacturing R&D for Hydrogen Technologies complements the President’s Hydrogen Fuel Initiative, which President Bush unveiled in 2003. **The Hydrogen Fuel Initiative commits $1.2 billion over five years** (2004–2008) **to reverse the Nation’s growing dependence on foreign oil** by developing the technology needed to establish commercially viable hydrogen-powered fuel cells — a means to power cars, trucks, homes, and businesses **without producing pollution or greenhouse gases**. The initiative is the largest component of a comprehensive R&D effort that will help pave the way to widespread use of hydrogen and fuel cell technologies. In addition to several other Federal programs, the effort leverages the FreedomCAR and Fuel Partnership, a joint undertaking involving U.S. automakers, five energy companies, and the Department of Energy. Also, the Interagency Working Group on Hydrogen and Fuel Cells, which involves twelve Federal agencies and is co-chaired by DOE and the White House Office of Science and Technology Policy, is coordinating Federal efforts to develop the advanced materials and many other enabling technologies integral to achieving the hydrogen economy.10 **Manufacturing R&D is one among many areas being addressed by the President’s Hydrogen Fuel Initiative** and the Hydrogen R&D Interagency Task Force. The IWG on Manufacturing R&D is working closely with both programs to complement their efforts and to sharpen the focus given to manufacturing R&D as a critical enabler for the widespread use of hydrogen as an energy carrier. Through such coordination, the IWG seeks to accelerate the development of the necessary technologies and infrastructure to enable manufacturing for hydrogen and fuel cell components and systems. **Many** scientific, technical, and institutional **challenges must be overcome before hydrogen can replace fossil fuels and be integrated into the Nation’s economic and energy infrastructures**. The complexity of these challenges is illustrated by the scope of the changes that will be required in the passenger segment of the Nation’s vehicular transportation system. These include lowering the cost of hydrogen production and delivery; lowering the cost and improving the capacity limitations of current hydrogen storage systems; lowering the cost and improving the performance and durability of current fuel cell systems; lowering the cost of integration and ensuring near-zero defect standards in manufacturing, all accompanied by appropriate institutional supports for high levels of safety over the lifetimes of all components. **Overcoming these obstacles will require progress in science and engineering on many fronts**. **Ultimately**, however, **achieving the vision of a hydrogen economy will depend largely on the Nation’s manufacturing capabilities**, that is, **on whether U.S. industry can develop highvolume**, **cost-effective processes for making the fuel cells** and related production, delivery, and storage technologies that are now in their infancy. **Given the pivotal role that manufacturing must play** if the United States is to realize the energy and environmental benefits of deploying hydrogen

> and fuel cell systems**, it is critical that manufacturing R&D occur simultaneously while the technologies are still being developed**. As critical hydrogen and fuel cell technologies become ready for commercialization, **manufacturing processes must be developed concurrently to** (1) **reduce the costs of hydrogen systems to levels that are competitive with today's petroleum-based systems**, (2) **build the necessary manufacturing infrastructure to support the hydrogen economy**, **and** (3) **to develop a domestic supplier base for hydrogen and fuel cell components**.

It should be noted that the same report where the above evidence appears also provides specific recommendations to improve nanotechnology and intelligent and integrated manufacturing as technologies in need of federal intervention to improve their role in the CIKR.

Tax Reform

Another way to improve the nation's manufacturing sector is to reform the taxation policies used to enable both R&D and educational partnerships:

> **Williford, 10**
> (Sam. (2010, December 10). Necessary Components of a Successful Manufacturing Policy. *Economy in Crisis*. Retrieved from http://www.economyincrisis.org/content/necessary-components-successful-manufacturing-policy)
> **To restore manufacturing** and create good jobs for the millions of Americans seeking work, **there are several changes Congress should implement**. For example, **making the R&D tax credit permanent would help maintain stability in a key sector of manufacturing**. Also, **keeping consistent tax policy**, and ending one-time write offs, or temporary tax cuts **will help companies plan long-term**, **strategic growth**. Next, **Congress must work to develop greater partnerships between research universities**, **the private sector**, **and federal technology transfer**. **Similar efforts led to the creation of the Internet and other important inventions**. **A program similar to the National Institute of Health**, **with respect to manufacturing, could reap great dividends**. **Taxation policies need to be changed so that our university students can pursue careers in manufacturing**, **instead of the financial sector**. **Either capital gains taxes should be increased, or income taxes in critical manufacturing sectors should be lowered so that we stop losing talented individuals to socially and economically worthless activities**, **such as the derivative trading that caused the financial meltdown**.

Buy American

Another policy proposal would extend the Buy American provisions requiring defense industries to purchase the components used to manufacture their products from domestic producers:

> **Farrell, 04**
> (Lawrence. (2004, February). State of Manufacturing Base is Cause for Concern. *Defense Magazine*. http://www.nationaldefensemagazine.org/archive/2004/February/Pages/State_of3657.aspx)
> **One lesson** that we **learned from the "Buy America" debate** last year **was the need for a thorough** and detailed **discussion on a national level about the state of the U.S. industrial base**, particularly the capabilities of American industry to manufacture sophisticated components for weapon systems. **The Buy America provisions** passed by the House of Representatives as part of the Fiscal Year 2004 Defense Authorization Bill ultimately **were defeated**, given the strong resistance from the Bush Administration and defense industry leaders, who successfully argued that protectionist laws only would

hurt the competitiveness of the industry and the ability of the Defense Department to obtain state-of-the-art technology from the most competitive suppliers. The problem that needs more analysis and concerted action, however, is the decline in U.S. manufacturing capabilities. If the decline continues, it could have an impact on our ability to access competitive sources in the military market. A strong industrial base is essential to competitive sourcing and a cornerstone of national security. **The state of manufacturing capabilities in the United States today gives cause for concern** about the health of those manufacturers that produce highly sophisticated weapons and components for the armed forces. **In objecting to the Buy America legislation**, **the Administration acknowledged the need to take a detailed look at the U.S. industrial base, its critical capabilities, and its ability to meet demands for advanced military technology and components** at competitive prices. **What we are seeing today is that large defense firms gradually are outsourcing much of their manufacturing business**. Most manufacturing now is done by small and medium-sized enterprises. Large manufacturers have downsized their workforces and are outsourcing production of final parts and components. Mark Huston, of the National Center for Defense Machining & Manufacturing, points out that these **smaller manufacturers typically lack the resources to invest in research and development**. "The technologies they use today in many cases are not even state-of-the-market, let alone state-of-the-art," says Huston. His organization, NCDMM, has worked with defense contractors to help them upgrade outdated technology, improve processes and incorporate new tooling. In recent years, says Huston, "we've fallen behind the curve." A lot of know-how was lost as people retired, companies went out of business and cut back investments in R&D. **Government programs designed to fund advances in U.S. manufacturing technology**—such as Mantech, the Advanced Technology Program and the Manufacturing Extension Program—**are helpful**, **but their budgets have been shrinking**. "It's not sufficient to close the gap we need to close here," says Huston. The numbers are sobering. According to the Association for Manufacturing Technology, as of August 2003, the manufacturing sector had sustained 37 consecutive months of job losses. More than 2.7 million manufacturing jobs disappeared in the United States during the three-year period beginning in mid-2000. The impact of these changes can be seen most clearly in the loss of traditional machine tool companies, says AMT. More than 30 closed shop between January 2002 and July 2003, representing nearly 10 percent of the companies in the entire industry. As we try to envision what lies ahead for the defense industrial base, one thought that comes to mind is that we cannot continue to lose ground, and get to the point where we cannot manufacture critical items that the military services require for their weapon systems. **The debate that surrounded the Buy America bill**—and the resulting studies—**should prompt us to take a hard look at our manufacturing capabilities**, and see what can be done to increase competitiveness in this vital industrial arena. **The bottom line is that the United States has to have machine tools**, **technology and manufacturing capability to remain internationally competitive**. **Protectionism is not the answer**, **but there is a compelling case to be made that both the federal government and the private sector need to step up their investments in manufacturing technology**, **so we can stay on par with countries such as Japan**, **Germany and China**, which is poised to become the world's manufacturing powerhouse of the 21st century.

Negative Ground

Protectionism Disadvantage

One of the major negative objections to many CM affirmatives would be the Protectionism disadvantage. Plans like Buy American would be susceptible to trade retaliation on the part of countries like China:

Zhongzhou, 09

(Li, (2009, March 16). 'Buy American' means trade protectionism. China Daily. Retrieved from http://www.chinadaily.com.cn/bw/2009-03/16/content_7580665.htm)
The US Congress has finally passed the American Recovery and Reinvestment Act of 2009 which contains a protectionist "**Buy American**" **clause**. **All funds authorized by the Act must be used to buy American** made iron, steel and **manufactured goods** for public works projects even though they cost 25 percent more than imported goods. **It is regrettable that American politicians seem to have forgotten the bitter lesson of** the Smoot-Hawley Act of **the 1930s**, **which sparked off the Great Depression**. In line with the Act, the US imposed high tariffs on some 20,000 imported goods, which immediately invited retaliatory measures from Europe. World trade suffered an almost complete stop. The Smoot-Hawley Act was thought to be the biggest mistake the US made in the 1930s. This new act says that the "Buy American" clause should be applied in a manner consistent with US obligations under international agreements. It would actually exempt NAFTA members Mexico and Canada and signatories to the WTO Government Procurement Code such as the EU and Japan. China, Brazil and India, which are not signatories to the Code, would be the main targets. "**Buy American" is protectionist and discriminatory in nature**. **China seems to be one of the few singled out for such discrimination**, **and will probably need to consider an appropriate response**. The argument that American taxpayers' money can only be used to create jobs for American workers is totally wrong. All major economies have adopted economic stimulus programs with taxpayers' money. They are free to emulate the "Buy American" policy, but if they do so, **the outcome may backfire on American lawmakers and may even lead to a global trade war**.

Free Market Counterplan

Rather than increasing government protection and resilience of CM, some advocate a free market approach which would allow the negative to avoid links to the Protectionism disadvantage:

Crews, 10
(Wayne. (2010, March 23). More government means less manufacturing. *Washington Times*. Retrieved from http://www.washingtontimes.com/news/2010/mar/23/more-government-means-less-manufacturing)
"**Doing something**" **about manufacturing doldrums is about more than spending money**. **Legislation like the bipartisan America Competes Act might scrounge a few scarce billion dollars**. **But so what? The real gains can come only if we "liberate to stimulate," if we separate state and economics**. Here's how: c **Rather than trying to improve speeds by picking the particular R&D horses** to run on the racetrack, **improve the business and regulatory track so everyone can go faster**, and let jockeys keep more of their earnings. c **Allow freer trade in skilled labor**: Bright foreign workers want to stay and create U.S. jobs after graduating here. That's a better way to address global competition. c **Avoid safety regulation that makes us less safe**: Many frontier technologies like nanotech can make our environment cleaner. Exaggerating risks overlooks hazards of stagnation. c **Liberalize capital markets**: Capitalism ranks among the world's great democratizing forces, but post-Enron Sabanes-Oxley regulation has severely distressed smaller companies. So, exempt firms with small market capitalizations (for starters). c **Privatize**: During the 1990s, it was proposed that commercial aspects of federal labs be offered to the industries they benefit, or to allow research employee buyouts. Do that. c **Award "prizes" rather than grants** as one element of a transition to private funding. c **Relax predatory and anti-consumer antitrust activism**: Markets emphasize competition, but sometimes "collusion" is merely a "partial merger" instead of a full one. Constraining productive firms in ways the market never intended hobbles entire industry sectors, and undermines the wealth creation process itself. c **Reduce overregulation generally**: More than 60 agencies issue 4,000 regulations a year within some 70,000 Federal Register pages. Congress should get busy implementing a bipartisan "regulatory reduction commission"; sunsetting old rules

and putting an expiration date on new ones; requiring fast-track congressional approval for controversial agency rules; adding flexibility for smaller business; requiring supermajority points of order for unfunded mandates; and creating a basic regulatory report card to accompany the federal budget. **There's a way to stimulate the economy from the halls of Congress but it is not enacting wonderful new programs**. **It is acting to get government out of the way**.

Global Warming Disadvantage

Ramping up domestic production of manufactured products would contribute more greenhouse gases that cause global warming:

Tropical-Rainforest-Animals.com, 09
(2009, October Global Warming Causes. Retrieved from http://www.tropical-rainforest-animals.com/Global-Warming-Causes.html)
We have some other industry-related activities (usually called **industrial processes**) which **are** also **significant sources of greenhouse gases** such as fluorocarbons, carbon dioxide as well as small amounts of methane (CH4) and nitrous oxide (N2O). The products whose manufacturing causes the emission of these gases include cement, minerals, chemicals, metals. **Many activities related to industrial processes use large amounts of energy and thus produce significant amounts of greenhouse gas emissions through fossil fuel combustion**. **But industrial processes also produce greenhouse emissions not related to fossil fuel combustion but rather related to the use of specific methods and materials for the manufacture of the products** mentioned above.

States Counterplan

Although the federal level can create favorable conditions for CM, state level action can also capture many of these benefits:

Tanoos, 09
(Jim. (2009, August). Manufacturing The Politics of American Industry. Business Intelligence Journal. Retrieved from http://www.saycocorporativo.com/saycoUK/BIJ/journal/Vol2No2/article8.pdf.)
It has become increasingly important for a governor to serve as an ambassador that can best take advantage of the weak dollar to help bring economic activity specifically to his community. **The federal government can create favorable, across-the-board corporate tax rates, attempt to deregulate, and make sure the EPA doesn't overly burden industry across the country, but national politicians aren't in the habit of courting specific multinational companies**. **While Congress is busy with its own legislation, the job of marketing a workforce and region solely rests in the hands of the governors**.

Conclusion

If a CIKR resolution is found desirable by the debate community, the community would be well advised to include Critical Manufacturing within the resolution. Due to its contribution to the American economy and national security, it is incumbent upon us to consider improvements to the protection and resilience of this vital sector of the Critical Infrastructure. Including CM in the CIKR debate will give students opportunities to learn about vital industries that continue to suffer while globalization continues its march forward.

Dams

Although debating the merits of dams might not appear to be an exciting debate topic, the DOHS highlights the relevance of Dams to the rest of critical infrastructure perfectly:

> **Department of Homeland Security, 08**
> ("National Infrastructure Protection Plan: Dams Sector", 2008, http://www.bhs.idaho.gov/Pages/Plans/CIKR/Dams.pdf)
> The Dams Sector comprises the assets, systems, networks, and functions related to dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, or other similar water retention and/or control facilities. The Dams Sector is a vital and beneficial part of the nation's infrastructure and continuously provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation. The Dams Sector has dependencies and interdependencies with a wide range of other sectors, including: The Agriculture and Food Sector, as a continued source of water for irrigation and water management; The Transportation Systems Sector uses dams and locks to manage navigable waters throughout inland waterways; The Water Sector, by supplying potable water to concentrated populations and commercial facilities in the U.S.; The Energy Sector, by providing approximately 8 to 12 percent of the nation's power needs with hydropower dams; and The Emergency Services Sector, which relies on Dams Sector assets for firefighting water supply, emergency water supply, and waterborne access in the event of a significant disaster.

For these reasons listed above, Dam infrastructure should be in consideration for the 2011-2012 debate resolution. The main benefit of Dams is their ability to produce hydroelectric clean energy. Dams have been the only consistent clean energy resource that the United States has relied upon heavily for its energy production, although "Unlike Africa, Asia, and Latin America, the United States has made only feeble and generally unsuccessful efforts to increase hydroelectric production."[100] This observation is compounded by states made by the 2010 National Research Council, arguing that "the future of hydropower will play out in the public policy debate, where the benefits of the electric power are weighed against its effects on the ecosystem."[101]

In the Endangered Species Act (ESA) Congress made it near impossible to do any more major damn construction because of the negative environmental impact dams may have to particular animals. Although at a first glance it seems that an affirmative through normal means would be forced to modify it (probably solidifying any sort of politics link), Congress has loopholes which allow it to bypass said act:

> **Hager,** JD Candidate @ American University Washington College of Law, **2009**
> [Fall, "FEATURE: TENSION BETWEEN HYDROELECTRIC ENERGY'S BENEFITS AS A RENEWABLE AND ITS DETRIMENTAL EFFECTS ON ENDANGERED SPECIES Sustainable Development Law & Policy, 10 Sustainable Dev. L. & Pol'y 50, Lexis]

[100] Tarlock, Professor of Law @ Chicago-Kent College of Law, 11 ["SYMPOSIUM ON ENERGY LAW: ARTICLE: THE LEGAL-POLITICAL BARRIERS TO RAMPING UP HYDRO" 86 Chi.-Kent L. Rev. 259, Lexis
[101] America's Energy Future Panel on Electricity from Renewable Resources, National Research Council, "Electricity from renewable resources: status, prospects, and impediments," 2009

> **Renewable energy has come to the forefront politically as one of the means of achieving energy independence, addressing** the problem of **climate** change, **and restoring the economy**. n1 Although renewable energy sources will be a crucial tool in the fight against climate change, they often create other environmental problems. n2 A recent Ninth Circuit Court of Appeals decision, National Wildlife Federation v. National Marine Fisheries Service, exemplifies how one form of renewable energy, hydroelectric power, has been challenged by the environmental community for its detrimental effect on endangered fish species. n3 **The case demonstrates that, asCongress moves to incentivize hydroelectric power, there may be a temptation for Congress to exploit a judicial loophole to make the Endangered Species Act** ("ESA**") inapplicable to dam operations.**

Additionally, the role of Congress in this sector is readily apparent, since they are the only federal entity capable of exempting their actions from the ESA:

> **Hager**, JD Candidate @ American University Washington College of Law, 20**09** [Fall, "FEATURE: TENSION BETWEEN HYDROELECTRIC ENERGY'S BENEFITS AS A RENEWABLE AND ITS DETRIMENTAL EFFECTS ON ENDANGERED SPECIES Sustainable Development Law & Policy, 10 Sustainable Dev. L. & Pol'y 50, Lexis]
> One issue in NWF that will continue to be relevant in other actions against dam projects is whether the Congressional mandate of flood control, irrigation, and power production created a nondiscretionary duty. **n22Nondiscretionary duties of agencies need not meet the requirements of section 7 of the ESA. n23 In NWF the Ninth Circuit determined that, while the broad Congressional goals were mandatory, Congress did not mandate that the goals be accomplished in any particular way; thus the agency actions in implementing the goals were discretionary and subject to requirements of the ESA**. n24 **Thus, Congress could exempt the actions of an agency engaged in dam operations from the ESA by specifically dictating by statute the manner in which the agency is to carry out the construction and operation of the dam**. n25 **As a result of the recent growing political interest in hydroelectric power, there will likely be a substantial increase in the nation's hydroelectric energy capacity.** n26 Although Congress could facilitate its goal of increasing hydroelectric power by exempting the operation of hydroelectric facilities from the ESA, the better solution would be to mitigate the effects of hydroelectric facilities on fish populations with advanced technology. n27 The DOE's decision to incorporate the reduction of environmental impacts into its plan for the modernization of the nation's hydropower infrastructure lends hope that the DOE will make environmental mitigation a priority during the expansion of hydroelectric projects. n28

This also means you can say goodbye to agent CP's or at least any coherent net benefit they would garner off of them. Is that good? You decide.

Affirmative Ground

There is much room for dam reconstruction since the end of the "big dam era". The core affirmative ground deal with issues pertaining to renewable energy. These affirmatives would require a more compressive approach in actions pertaining to dams. There are a number of advantage areas that affirmative teams could address in this sector. These include hydroelectricity, terrorism, and the environment.

Hydroelectricity

The continued need to provide reliable energy to the United States is becoming increasingly problematic in an age of oil scarcity and resource conflicts. Upgrading turbines and construction of new hydroelectric Dam cites bring clean electricity to the table.

> **Tarlock,** Professor of Law @ Chicago-Kent College of Law**, 11**
> ["SYMPOSIUM ON ENERGY LAW: ARTICLE: THE LEGAL-POLITICAL BARRIERS TO RAMPING UP HYDRO" 86 Chi.-Kent L. Rev. 259, Lexis]
> **The United States currently generates over 300 billion kW h of electricity from hydro** plants. n8 The **Department of Energy estimates that up to 30,000 MW of electricity could be generated from undeveloped sites.** n9 **The Electric Power Research Institute estimates that untapped hydro capacity could increase production by twenty-four to twenty-seven percent**. n10 **The Energy Information Administration puts that total potential increase in hydroelectricity for new and upgraded plants at forty terawatts.** n11 **Additional hydroelectric capacity could come from the construction of new dams and reservoirs, by increasing the generating capacity of existing facilities or placing hydrokinetic devices in a stream**. n12 **At existing dams, turbines could be upgraded, more water could be put through existing ones, or new pump storage facilities could be constructed**. n13 For example, the Bonneville Power Authority has installed a new turbine at Chief Joseph Dam on the [*261] Columbia River, and the upgrade will generate enough power for 30,000 homes in the Pacific Northwest. n14

Dams are also crucial components for storing waters in areas of high droughts which are a prerequisite for civilization itself.

> **World Energy Congress, 04**
> (Managing the social and environmental aspects of hydropower, http://www.energy-network.net/resource_center/launch_documents/documents/Managing%20the%20social%20&%20environmental%20aspects%20of%20hydropower%2020.pdf)
> **Water is the vital resource to support all forms life on earth. Unfortunately, it is not evenly distributed over the world by season or location**. **Some parts of the world are prone to drought making water a scarce and precious commodity, while in other parts of the world it appears in raging torrents causing floods and loss of life and property. Throughout the history of the world, dams and reservoirs have been used successfully in collecting, storing and managing water needed to sustain civilization.**

Terrorism

Another potential affirmative can deal with Dam security. After 9/11 Dams have been listed as a potential site for a terrorist attack.

> **Copeland and Cody, 03**
> (Resources, Science, and Industry division at FAS, 5-23-3 [Claudia, Betsy, "Terrorism and Security Issues Facing the Water Infrastructure Sector", http://www.fas.org/irp/crs/RS21026.pdf)
> **Damage to or destruction of the nation's water supply and water quality infrastructure by terrorist attack could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. Interest in such problems has increased since the September 11, 2001, terrorist attacks**. Across the country, **water infrastructure systems extend over vast areas, and ownership and operation responsibility are both public and private but are overwhelmingly nonfederal**. **Since the attacks, federal dam operators and water and wastewater utilities have been under heightened security conditions and are evaluating security plans and measures. Policymakers are considering a number of options, including enhanced physical security, better communication and**

coordination, and research. **A key issue is how additional protections and resources directed at public and private sector priorities will be funded. In response, Congress has approved $410 million in funds for security at water infrastructure facilities** (P.L. 107-117, P.L. 108-7, and P.L. 108-11) **and passed a bill requiring drinking water utilities to conduct security vulnerability assessments** (P.L. 107-188). **Congress also created a Department of Homeland Security with responsibilities to coordinate information to secure the nation's critical infrastructure, including the water sector** (P.L. 107-297). **Continuing attention to these issues in the 108 th Congress is anticipated. Current interest is focusing on bills concerning security of wastewater utilities** (H.R. 866, S. 1039**). This report will be updated as warranted**

Environment

The environmental debate structuring dams is also a highly contentious issue. Dam debates would most likely be centered on the environmental impact they have, and what exactly they do to biodiversity. While the negative environmental impacts of dams have been loudly proclaimed, affirmatives will also have a literature base arguing that dams have positive impacts on the environment:

Tarlock, Professor of Law @ Chicago-Kent College of Law, **11**
["SYMPOSIUM ON ENERGY LAW: ARTICLE: THE LEGAL-POLITICAL BARRIERS TO RAMPING UP HYDRO" 86 Chi.-Kent L. Rev. 259, Lexis]
The end of the Big Dam Era ultimately changed our perception of rivers and dams in ways that pose major constraints for ramping up hydro. It replaced the conservation era vision of hard working rivers, the stewardship idea of a river that works for a wider variety of uses including aquatic ecosystem protection. n93 **The idea that most of our remaining high quality "natural" rivers should run wild has eventually evolved into the broader idea that maximum hydroelectric generation capacity should be subordinated** to the conservation of aquatic ecosystems and the promotion of white water rafting. And, **dams now are seen both as the source of the problem of degraded [*271] aquatic ecosystems and part of the solution. They can be re-operated to move the flow regime closer to pre-dam conditions.**

Negative Ground

Politics

The question of feasibility of Dams in the 21st will be a highly contentious issue, as illustrated by recent discussions:

Tarlock, Professor of Law @ Chicago-Kent College of Law, 11
["symposium on energy law: article: the legal-political barriers to ramping up hydro" 86 chi.-kent l. Rev. 259, lexis]
This article makes the positive argument that **increased hydroelectric generation is an unlikely component of the nation's energy future for four** [*263] **related reasons**. n28 **First**, **hydro's glory days are past in the United States**. n29 **The best sites have been developed or protected** from dams or smaller facilities. **Second**, **the environmental movement was born from fights to prevent dams and hydroelectric facilities and thus any move would have to reverse the end of the "Big Dam Era."** n30 Put differently, **the roots of hydro's inability to expand substantially can be traced to the reaction to the water policies of the Progressive Conservation Era** (1890-1920). Third, **environmental law has moved beyond dam prevention to river restoration**. One of the major water-related projects of environmental law is to conserve and restore the hydrographs of managed rivers and even to remove dysfunctional dams. n31 **To ramp up hydro, we would have to undo or substantially modify much of**

> **environmental law including the Endangered Species and Clean Water Acts**. n32 **Fourth, we are slowly beginning to appreciate the potential adverse impacts of global climate change on biodiversity**. Since these adverse impacts are likely to occur before any projected mitigation kicks in (if ever), we must adapt to climate change. n33Many adaptation strategies contemplate aquatic ecosystem restoration and conservation. n34 **As previously mentioned, the rub is that GCC may contribute to a decrease in river flows during times of high demand. Thus, both reliable flows for [*264] power generation n35 and aquatic biodiversity, including recent restoration efforts, will be imperiled.**

Additionally, much of the literature pointing to the controversy of dam-based policies simultaneously provides potential solvency takeouts:

> **Tarlock, Professor of Law @ Chicago-Kent College of Law, 11** ["SYMPOSIUM ON ENERGY LAW: ARTICLE: THE LEGAL-POLITICAL BARRIERS TO RAMPING UP HYDRO" 86 Chi.-Kent L. Rev. 259, Lexis]
> Hydro dominates electricity production in the Pacific Northwest, n59 but natural gas, coal, and nuclear are the major sources of electricity in the rest of the country. n60 At the present time, **hydro supplies between seven and [*267] nine percent of the nation's energy, and future projections hold that figure relatively constant**. n61 The **current non-carbon star is revived and safer nuclear power which already generates seventy percent of the nation's non-carbon energy**. n62 As mentioned earlier, **the two related reasons for hydro's decline are the exhaustion of good dam sites in the American West and elsewhere and public opposition to the loss of free-flowing rivers and scenic canyons which resulted from the Big Dam Era. n63**

Environment

As mentioned above, the environment debate is highly discussed in environmental circles, leading to an excellent literature base:

> **Tarlock,** Professor of Law @ Chicago-Kent College of Law, **11**
> ["SYMPOSIUM ON ENERGY LAW: ARTICLE: THE LEGAL-POLITICAL BARRIERS TO RAMPING UP HYDRO" 86 Chi.-Kent L. Rev. 259, Lexis]
> **No energy policy move is simple**, and **hydroelectric generation is no exception. Hydro is not completely clean and is an increasingly risky source of energy due to the projected impact of global climate change on river flows**.n15 Storage **reservoirs, especially those located in the tropics, n16 are a major source of methane emissions**. n17 Hydroelectric **generation causes other forms of more immediate, major environmental damage - primarily blocked fish runs, degraded downstream and upstream aquatic ecosystems due to temperature, flow changes, decreased downstream sediment transport, and the loss of access to scenic canyons.** n18 For example, t**he chain of Missouri River dams constructed since the 1930s have decreased downstream sediment transport to the detriment of endangered species along the Missouri and contributed to the loss of wetlands in the Mississippi Delta.** n19

It is also worth noting that much of the literature addressing the environmental impacts of dams also provides powerful literature for critical arguments on environmental managerialism and similar claims:

> **Luke, 99**
> Timothy W. Luke, Professor of Political Science at Virginia Polytechnic Institute and State University,1999, Discourses of the Environment, p. 138-140

> **Some take sustainable development to mean ecologically sustainable. Others just as rightly see it as economically sustainable, technologically sustainable or politically sustainable.** Chambers of commerce and ministries of industry in the 1990s glibly adopt sustainable development discourse as their own: **this dam, that factory, these highways**, those power lines **must be built to sustain, not nature, but job creation, population growth, industrial output or service delivery.** Such elements improve human life and enhance its ecosystems' carrying capacities. **This construction**, however, **clashes with ecological interpretations in which humans allegedly are seeking 'social and material progress within the constraints of sustainable resource use and environmental management'**; and, as a result, 'renewable resources (plants, trees, animals and soil) will be used no faster than they are generated; non-renewable resources (such as fossil fuels and metals) will be used no faster than acceptable substitutes can be found; and pollutants will be generated no faster than can be absorbed and neutralised by the environment' (McMichael 1993: 309). As a social goal, **sustainability is fraught with unresolved questions. Sustainable for how long: a generation, one century, a millennium, ten millennia?** Sustainable at what level of human appropriation: individual households, local villages, major cities, entire nations, global economies? Sustainable for whom: all humans alive now, all humans that will ever live, all living beings living at this time, all living beings that will ever live? **Sustainable under what conditions: contemporary transnational capitalism, low-impact Neolithic hunter-and-gather societies, some future space-faring global empire?** Sustainable development of what: personal income, social complexity, gross national product, material frugality, individual consumption, ecological biodiversity? For the most part, **few of these questions are even being adequately conceptualized, much less thoroughly addressed in the debates over sustainable development.**

Aquatic Restoration Trade off

As with most policy initiatives, affirmative action in the dam sector will trade off with other proposals. What is interesting is the specificity of these tradeoffs in the literature:

> **Tarlock,** Professor of Law @ Chicago-Kent College of Law, **11**
> ["SYMPOSIUM ON ENERGY LAW: ARTICLE: THE LEGAL-POLITICAL BARRIERS TO RAMPING UP HYDRO" 86 Chi.-Kent L. Rev. 259, Lexis]
> In 1968, the Sierra Club led a successful campaign to ban two cash register dams at either end of the Grand Canyon, n66 and in that same year **Congress passed the Wild and Scenic Rivers Act**. n67 **This Act protects most of the major undeveloped sites from hydroelectric dams**. n68 State wild and [*268] scenic river programs protect other rivers. n69 The dam building agencies, and the West in particular, did not initially appreciate the significance of these two events. Multiple purpose projects continued to be proposed until Jimmy Carter's infamous "hit list" in 1977 administered the "coup de grace. n70 " This and the Reagan Administration's interest in ending federal water development subsidies convinced the Western states that the federal money spigot was shut. n71 **Since the 1980s, the federal budget dollars devoted to water are increasingly being spent on aquatic ecosystem restoration rather than dam construction. n72**

Conclusion

The dam sector provides a valuable mode of engaging environmental questions and is one of the brightest points of critical ground available for both the affirmative and negative. Individuals considering this sector should also look towards the water sector, which has a substantial amount of intersection with the dam industry.

Defense Industrial Base

Introduction

The Defense Industrial Base (DIB) refers to a set private and public entities tasked with maintaining a national defense system for the United States. In an attempt to define the DIB the Department of Homeland Security, in cooperation with the Department of Defense, identifies this critical infrastructure as:

> "…the DoD, the U.S. Government, and the private sector worldwide industrial complex with capabilities to perform research and development (R&D), design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other Federal departments and agencies. Defense-related products and services provided by the DIB equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide." (DHS 2007)

The DHS has had to devote countless person-hours determining what is and is not a critical part of the DIB. Because the above definition could theoretically be applied to every entity within the United States, the DHS as explicitly stated that the DIB "does not include commercial infrastructure that provides, for example, power, communications, transportation, and other utilities that DoD war fighters and support organizations use to meet their respective operational needs".[102] Therefore, the DIB can be understood as the systems directly pertaining to our national defense, excluding support systems (many of which are other examples of critical infrastructures).

It will fall on the topic wording committee to determine how national security is understood in relation to the resolution, but there is no shortage of definitions provided by relevant government agencies. One of the most promising definitions, found in U.S. Code Title 50, identifies the national defense as:

> "…programs for military and energy production or construction, military assistance to any foreign nation, stockpiling, space, and any directly related activity. Such term includes emergency preparedness activities conducted pursuant to title VI of The Robert T. Stafford Disaster Relief and Emergency Assistance Act and critical infrastructure protection and restoration"[103].

To what extend the affirmative is granted authority over the broad area of the Defense Industrial Base will determine the ground on either side of these debates. We as a community will need to delineate between a critical core of affirmative plan options and a reasonable set of negative strategies. The author encourages the debate community to consider the possibility of limiting topical affirmatives to those that directly affect the categories of defense sectors later discussed in this section.

---

[102] Department of Homeland Security, Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. May 2007, http://www.dhs.gov/xlibrary/assets/DIB_SSP_5_21_07.pdf

[103] 50 U.S.C. app. [section] 2152(14) (2006)

While the last major official release pertaining to the DIB is from the DHS in 2007, the National Institute of Homeland Security will soon be hosting a conference on "Risk Reduction & Mitigation in the Defense Industrial Base" which will include focus on core topic issues discussed by national and local authorities.[104] The issues to be discussed at this conference are sure to provide an even more rich literature base in time for next year's debate season.

Affirmative Ground

While the DHS states that the DIB includes 'businesses of all sizes,'[105] the resolution would need to isolate only the major players as topical options (easily done with a 'substantial' or 'significantly' signifier). Another possibility is the remove the private sector as a topical part of this topic section, ensuring that the USFG would be the only topical actor.

External from the actor debate, there are questions concerning what is included under the DIB. The DHS provides an extensive review of military-based resources that might qualify as part of the DIB, including:

- Missiles
- Aircraft
- Troop Support
- Space Resources
- Combat Vehicles
- Ammunition
- Weapons
- Information Technology
- Shipbuilding
- Electronics

An affirmative interested in focusing on the DIB would need to significantly alter the current national policy pertaining to the research, development and/or deployment of these areas. The logical actor for these affirmatives would be the Defense Contract Management Agency, which is tasked with assigning contracts and overseeing DIB operations, but this agency need not work alone.[106] The Air Force in particular is very troubled by the current state of the DIB. In relation to cyber security, a recent Air Force law review argued that the current system faces a dwindling system of safeguards that must be rapidly updated in order to ensure domestic tranquility[107].

It should be easy to see the possible affirmatives and core advantage ground in this topic area. Briefly addressing multiple advantage areas, James Lewis of CSIS states:

> There are new areas of increased risk for the U.S. defense industry. These stem from larger trends where China is a symptom more than a cause. These larger trends are the

[104] National Institute for Homeland Security, 2010 DIBCIP Defense Industrial Base Critical Infrastructure Protection Conference, http://www.thenihs.org/calendar/2010/04/26/2010-dibcip-defense-industrial-base-critical-infrastructure-protection-conferenc, 2010.
[105] Department of Homeland Security, Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. May 2007, http://www.dhs.gov/xlibrary/assets/DIB_SSP_5_21_07.pdf
[106] Defense Contract Management Agency, 2010, http://www.dcma.mil/
[107] Brown, Todd A. Legal propriety of protecting defense industrial base information infrastructure. Air Force Law Review, Dec 22, 2009.

> ongoing international economic integration known as globalization, the related issue of the diffusion of scientific and technological capabilities around the world, and the general decline in demand for advanced conventional weapons. The effect of these trends is that if the United States relies solely on the policies and practices that made it strong in the 1980s and 1990s, it is likely to face increased risk to national security.[108]

Issues including U.S.-Sino relations, globalization, and weapons development each signify a strong advantage area available to most affirmatives. Provided that there is a specific solvency advocate, modification of the research, development, manufacture, or deployment of virtually any weapons system deemed 'critical' to national security may be topical. Teams that are interested in cutting-edge science might find unique affirmative ideas currently scheduled through the Defense Advanced Research Projects Agency (DARPA). The DIB also includes a sizable literature base focusing on critical arguments. The development and deployment of various munitions such as Depleted Uranium is a topic that has proven its argumentative viability during last years' topic. A resolution that included a call for modifying the current DIB is sure to offer unique possibilities to the debate community throughout the entirety of the season.

Negative Ground

Negative teams will enjoy a wide variety of options when dealing with DIB plans. Given the sheer magnitude of this specific critical infrastructure, virtually any BID affirmative can be answered with a specific counterplan, including precise solvency advocates for local and state governments. The DHS readily admits that these entities are crucial to the continued reliability and coordination of our defense system.[109] National policies also run the risk of severely altering fragile civil-military relations (CMR). Changes to the DIB have been identified as a major factor in CMR and it would be hard for an affirmative to completely avoid these links[110].

Generic negative ground can also be found through the international implications of modified DIB protocols. It is very likely that changes to the supply chain can create an unintended shift of power away from the U.S. For instance, a plan that increases our defense diversity while lowering cost by allowing for international bidding could forever alter U.S. leadership:

> **Lewis,** Director and Senior Fellow, Technology and Public Policy Program at CSIS, **05** (James A., Effect of U.S.-China Trade on the Defense Industrial Base: Testimony Before the U.S.-China Commission, June 23, 2005, http://csis.org/files/media/csis/pubs/050623_uschina.pdf)
>
> **There is** also some **concern that** new **risks** to security **could result from increased U.S. dependence on an international** (rather than national) **manufacturing** base. Western Europe and Japan have provided core manufacturing capabilities for many years, but **the U.S could find itself having to rely on suppliers, like China,** who are

[108] Lewis, James A., Effect of U.S.-China Trade on the Defense Industrial Base: Testimony Before the U.S.-China Commission, June 23, 2005, http://csis.org/files/media/csis/pubs/050623_uschina.pdf

[109] Department of Homeland Security, Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. May 2007, http://www.dhs.gov/xlibrary/assets/DIB_SSP_5_21_07.pdf

[110] Danopoulous, Constantine P., Vajpeyi, Direndra, and Bar-or Amir (eds.). Civil-military relations, nation building, and national identity, Praeger Publishers, Westport, CT. 2004.

> not allies. ‘Foreign dependency’ does not make the U.S. innately more vulnerable. U-boats are not going to blockade the Pacific Coast nor cut the global supply chain. **The long-term risk lies in the erosion of the U.S. high tech industrial base as foreign high tech companies enter and compete in the market. U.S. regulations and policies contribute to this erosion.** Many aspects of our export control system fail utterly to keep advanced technology out of foreign hands, yet put U.S. companies at a competitive disadvantage. The net effect is to reduce the number of U.S. defense and high tech suppliers.

The availability of off-case arguments such as these is reassuring, but is merely supplemental to the already sizable amount of negative arguments that will be available against specific plans, depending on which areas of DIB are affected. Additionally, much of the public sector literature that references the DIB identifies the contractors, agencies, and operations of this area as the key components of the Military Industrial Complex. Here, negatives can engage in a discussion of U.S. hegemony in both a policy and a critical framework.

When voting for a resolution area each debate squad should remember that many other topic proposals can be discussed through a C.I. resolution. For instance, teams interested in discussing space-based weaponry can do so VIA a DIB plan focusing on space assets. The broad umbrella of DIB policies ensures that debaters would be able to develop new arguments throughout the season, in opposed to having to rehashing old strategies in the spring.

Emergency Services

Introduction

This paper will advocate on behalf of the inclusion of the Emergency Services Sector within a Critical Infrastructure and Key Resources debate resolution. The following will begin by addressing the challenges facing this nation's emergency response personnel and use this information to detail the affirmative and negative strategies available in this area.

The Department of Homeland Security identifies the Emergency Services Sector as follows. Readers should note the overlap of this area with other areas of the topic, demonstrating the potential for this area of the topic to access other key areas of the Critical Infrastructure and Key Resources debate:

> **Department of Homeland Security**. (20**10**, June 21). Emergency Services Sector: Critical Infrastructure and Key Resources. Retrieved from http://www.dhs.gov/files/programs/gc_1189094187811.shtm.
> **The Emergency Services Sector (ESS) is a system of response and recovery elements that forms the nation's first line of defense and prevention** and reduction of consequences from any terrorist attack. **It is a sector of trained and tested personnel**, **plans**, **redundant systems**, **agreements**, **and pacts that provide life safety and security services across the nation** via the First-Responder Community comprised of federal, state, local, tribal, and private partners. **The ESS is representative of the following** first-responder disciplines: **emergency management**, **emergency medical services**, **fire**, **hazardous material**, **law enforcement**, **bomb squads**, **tactical operations/special weapons assault teams**, **and search and rescue**. **All first-responders within the ESS are individuals possessing specialized training** from one or more of these disciplines. **The ESS** has numerous interdependencies with all critical infrastructure and key resources (CIKR) sectors. Most significantly, it **is the primary protector for all other CIKR**, **including nuclear reactors**, **chemical plants**, **and dams**. **All other CIKR facilities depend on the ESS to assist with planning**, **prevention**, **and mitigation activities**, **as well as respond to day-to-day incidents and catastrophic situations**.

In the event of a natural disaster or terrorist attack, it will be the Emergency Services Sector who is called upon during this dark hour. Unfortunately, this sector currently suffers from not only a lack of resources, effective equipment and training, but also a misguided focus. The federal government presently neglects to establish a unified national framework to ensure that the needed resources and training are available to the emergency response personnel who need them:

> **Council on Foreign Relations**. (20**03**). Emergency Responders: Drastically Underfunded, Dangerously Underprepared. Retrieved from www.cfr.org/content/publications/attachments/Responders_TF.pdf.
> In the almost two years **since September 11**, **the U.S. federal government as well as state and local authorities** around the nation **have taken unprecedented steps to enhance preparedness** on multiple levels. The Department of Homeland Security (**DHS**) **was established** in March 2003; **federal**, **state**, **and local expenditures on emergency preparedness have increased**; **and personnel in the fields of emergency preparedness and response have undergone additional training**. Although **the United States** remains highly vulnerable to terrorist attack, the American public **is**, in some respects, **better prepared to address some aspects of the terrorist threat** now than it was two years ago. **But the United States has not reached a sufficient national level of emergency preparedness and remains dangerously unprepared to handle a**

catastrophic attack on American soil, particularly one involving chemical, biological, radiological, or nuclear agents, or coordinated high-impact conventional means. To offer a few examples: • **On average**, **fire departments across the country have only enough radios to equip half the firefighters on a shift**, **and breathing apparatuses for only one third**. **Only 10 percent** of fire departments in the United States **have the personnel and equipment to respond to a building collapse**. • **Most states' public health labs still lack basic equipment and expertise to respond adequately to a chemical or biological attack**. For example, only Iowa and Georgia have the technology to test for cyanide, even though the deadly compound is readily found both naturally and commercially in 41 states. Seventyfive percent of state laboratories report being overwhelmed by too many testing requests. • **Most cities do not have the necessary equipment to determine what kind of hazardous materials emergency responders may be facing**. • According to the International City/County Management Association (ICMA), **the average number of full-time paid police employees** for jurisdictions of 250,000 to 499,999 residents today **is 16 percent below the figure for 2001**. • **Police Departments** in cities across the country **do not have the protective gear to safely secure a site following an attack using** weapons of mass destruction (**WMD**). Although significant gaps in overall preparedness exist, there is currently an inadequate process for determining, and therefore addressing, America's most critical needs. **America's leaders have not yet defined national standards of preparedness**—**the essential capabilities that every jurisdiction of a particular size should have or have immediate access to**. **It is therefore not yet possible to determine precisely the gaps in each jurisdiction between how prepared it is now and how prepared it needs to be**. **The absence of a functioning methodology to determine national requirements for emergency preparedness constitutes a public policy crisis**. **Establishing national standards that define levels of preparedness is a critical first step toward determining the nature and extent of additional requirements and the human and financial resources needed** to fulfill them. National capability standards would, for example, determine the minimum number of people that cities of a certain size should be able to decontaminate, inoculate, quarantine, or treat after a chemical, nuclear, biological, or radiological attack. Local jurisdictions would then be allowed flexibility in reaching those levels over a fixed period of time. Standards would make it possible to use funding efficiently to meet identified needs and measure preparedness levels on a national scale. In some respects, there is no natural limit to what the United States could spend on emergency preparedness. The United States could spend the entire gross domestic product (GDP) and still be unprepared, or wisely spend a limited amount and end up sufficiently prepared. But the nation will risk spending an unlimited amount on emergency preparedness only if it fails to define requirements and determine national priorities. Without establishing minimal preparedness levels and equipment and performance standards that the federal government and state and local communities can strive to attain, the United States will have created an illusion of preparedness based on boutique funding initiatives without being systematically prepared. The American people will feel safer because they observe a lot of activity, not be safer because the United States has addressed its vulnerabilities. **The United States must rapidly develop a sophisticated requirements methodology to determine the country's most critical needs and allow for the setting of priorities in readiness training and procurement**. The United States does not, however, have the luxury of waiting until an overarching process is created to fund urgently needed enhancements to current capabilities. In the nearly two years **since the September 11 attacks**, **Congress has dangerously delayed the appropriation of funds for emergency responders**, **federal agencies have been slow getting funds to state and local jurisdictions**, **and states have hampered the efficient dissemination of much needed federal funds to the local level**. **The overall effectiveness of federal funding has been further diluted by the lack of a process to determine the most critical needs of the emergency responder community in order to achieve the greatest return on investments**.

A focus on the Emergency Services Sector is critical to an effective discussion of Critical Infrastructure and Key Resources because of the critical role played by individuals and groups within this area; indeed, emergency services are the "frontline" of any effective response measure to disasters and emergencies:

> **Council on Foreign Relations**. (20**03**). Emergency Responders: Drastically Underfunded, Dangerously Underprepared. Retrieved from www.cfr.org/content/publications/attachments/Responders_TF.pdf.
> **Emergency responders come from the fire**, **police**, emergency medical services (**EMS**), public **health**, **and other communities**, and the underlying strength of those general capabilities has a significant impact on the level of emergency preparedness within a given jurisdiction. While the focus of this report is on the cost of enhancing U.S. preparedness for terrorism, it must also be acknowledged that **many emergency response entities do not have the capability to adequately address basic emergencies**. For example, **two-thirds of fire departments do not meet the consensus fire service standard for minimum safe staffing levels**. Additionally, **public health systems across the country are dangerously underfunded and lack the capacity to do what is increasingly expected of them**. The building blocks of increased capabilities can only be laid upon a solid foundation. The United States must therefore both enhance the capabilities of its emergency responders and work to guarantee the overall health of police, fire, emergency medical, and public health systems. Enhancing responder capabilities will require inputs on multiple levels. **Providing response equipment is only one aspect of improving overall preparedness**. **Without appropriate staffing**, **training of personnel**, **and sustainment of equipment and capabilities over time**, **new equipment may contribute only marginally to greater preparedness**. Wherever possible, an all-hazards approach should be followed to ensure that, to the maximum extent possible, **resources devoted to responding to a terrorist attack can enhance underlying emergency preparedness capabilities for addressing natural disasters**. **With whatever capabilities they have**, however, **America's local emergency responders will always be the first to confront a terrorist incident and will play the central role in managing its immediate consequences**. **Their efforts in the first minutes and hours following an attack will be critical** to saving lives, reestablishing order, and preventing mass panic. Like the police, emergency medical services, and fire professionals who entered the World Trade Center on September 11, emergency responders will respond to crises with whatever resources they have. **The United States has a responsibility to provide them with the equipment**, **training**, **and other necessary resources to do their jobs safely and effectively**.

Some readers may wonder about this sector's vulnerability to the States and Localities Counterplan. However, experts in the field recognize the necessity for federal action to effectively coordinate responses to threats to critical infrastructure:

> **Council on Foreign Relations**. (20**03**). Emergency Responders: Drastically Underfunded, Dangerously Underprepared. Retrieved from www.cfr.org/content/publications/attachments/Responders_TF.pdf.
> This report does not prejudge how these critical needs should be met, but insists that they must be. **It is essential that federal**, **state**, **and local authorities come to a consensus on sharing responsibilities and make a commitment to meet them**. In this process, **it will be important to keep in mind that the threat of terrorism**, particularly international terrorism, **is a national security threat to the entire United States**. **Although state and local jurisdictions must maintain primary responsibility for funding basic levels of public health and safety readiness**, **the incremental costs of responding to the additional national security threat posed by terrorism**

> **are appropriately a federal responsibility**. **This federal responsibility is even more critical considering the current budget crisis faced by most state and local jurisdictions**, **which makes it more difficult to allocate sufficient resources for emergency response and to address other important needs**.

Indeed, current events only magnify the importance of this sector and its ability to access adequate and effective federal assistance, as the case study of Texas demonstrates:

> **CNN**. (20**11**, April 18). Fires burn across Texas with no end in sight. Retrieved from http://www.cnn.com/2011/US/04/18/texas.forest.fires/index.html?hpt=T2.
> **Dozens of large fires burned out of control** Monday **in Texas in what officials described as unprecedented conditions that show no signs of abating soon**. "We're experiencing conditions never seen in Texas before," said Marq Webb, a public information officer with **the Texas Forest Service**, which was devoting massive resources to the effort. "Yesterday, we had 1,400 people and that number will go up today," Webb said Monday in a telephone interview from the service's incident command center in Merkel just west of Abilene. In all, the Forest Service **has been asked to help battle fires covering some 700,000 acres**, he said. Thirty-one fires were being fought in East Texas; another 11 fires in West Texas, officials said. "**We've had 19 consecutive days of just super-dry weather**, **relative humidities in the single digits**," said Forest Service spokeswoman C.J. Norvell in Midland. "What we're seeing right now is **winds** that **are typical of spring**, **but everything else is typical of late summer** -- no rain, vegetation that's just super dry. When you combine those two, it really has not boded well." The Wildcat Fire just north of San Angelo has led to the evacuation of hundreds of people from their homes, Norvell said. The same fire threatens three small communities just north of Saint Angelo -- Robert Lee, Bronte and Tennyson, she said. **A predicted change in wind direction** from south to southwest **could worsen the prognosis**, she said. "**This little change is going to test some infrastructure and fire lines that we've set up**," she said. The fires have a variety of causes -- some of them acts of nature, such as lightning strikes -- but most of them acts of man, said Webb. Those include anything from fence welding to debris burning, despite the fact that burn bans are in effect for 195 of the state's 254 counties, he said. Texas authorities have made an arrest in connection with one of hundreds of blazes scorching the state in what a Forest Service official called the "perfect storm for wildfires." A man was arrested and charged with reckless endangerment, which is a felony under Texas law, Austin Fire Department Battalion Chief Palmer Buck said early Monday. The man, whom authorities did not immediately identify, was being held under a $50,000 bond. According to Buck, the man started a campfire at a homeless camp in a remote area, which got out of control and prompted evacuations. The fire burned about 60 acres. "We're experiencing conditions we've never seen in Texas before," he said. "We have a huge area of Texas with abundant fuels and they are tinder dry -- and I'm talking about probably half of the state." Monday's forecast was worse than Sunday's, "and tomorrow's supposed to be worse than today," he said. Though temperatures are expected to dip Wednesday, they were predicted to ramp back up on Thursday and Friday. **Such weather has taxed the resources available to fight the fires**. "We're stretched pretty thin right now," Webb said. Conditions this spring are the driest they've been in Texas since 1917, said a Texas Forest Service spokeswoman. **Authorities have responded to 7,807 fires across more than 1.5 million acres since this year's wildfire season began**, **Gov. Rick Perry** wrote over the weekend in a letter to President Barack Obama. Perry **requested that the federal government declare Texas a disaster area**. **Fires have affected all but two of the state's 254 counties**.

Affirmative Ground

A. Sector specific approaches

One of the benefits of including the ESS sector in the CIKR topic is affirmative flexibility. Indeed, due to the vast scope of actors involved in emergency response, it should come as no surprise that many of the organizations representing the disciplines within ESS publish reports and recommendations about how the federal government could better serve the interests of firefighters, police officers, paramedics, etc. While an examination of each discipline is beyond the scope of this paper, the author will attempt to use the Emergency Medical Services discipline to demonstrate the potential for affirmative creativity.

The Emergency Medical Services have currently been neglected in attempts to shore up this nation's disaster and terrorism response policies:

> **Center for Catastrophe Preparedness and Response**. (20**05**, March). Emergency Medical Services: The Forgotten First Responder. Retrieved from: http://www.nyu.edu/ccpr/NYUEMSreport.pdf.
> **Despite the lessons of September 11**, 2001, **the EMS system's homeland security and disaster preparedness efforts have received inadequate recognition and support**. EMS personnel, such as **EMTs and paramedics**, **lack vital response equipment**, **training and education and the EMS system receives little homeland security assistance**. **EMS personnel provide emergency medical care and transport to victims of terrorist attacks**, **disasters**, **and routine medical emergencies**. The emergency medical service and ambulance personnel who lost their lives responding to the terrorist attacks of September 11, 2001 reflect the diversity of EMS organizations across the country. The personnel who lost their lives were from the New York City Fire Department, a nonprofit private ambulance service, a for-profit private ambulance service, a volunteer fire department and hospital-based ambulance services. **A well-prepared EMS system is critical to homeland security**. **According to** a Department of Homeland Security (**DHS**) report, "**the readiness of EMS is vital to ensuring prompt and appropriate emergency care and transportation as a component of the overall response**. Therefore, it is essential that EMS agencies receive support and assistance to prevent, respond to and assist in the recovery from terrorist incidents." 6 **Despite acknowledgement by DHS and other Federal agencies of the importance of the EMS system's role** in homeland security preparedness, **to date the EMS system received little assistance from homeland security and bioterrorism grant programs. Of the billions of dollars distributed by** the Department of **Homeland Security**, **less than four percent** of "first responder funding" **was allocated to EMS** providers or EMS systems.7 In addition to receiving few homeland security resources, **EMS personnel lack emergency preparedness equipment**, **education and training**. **While EMS providers currently undertake preparedness efforts with limited federal assistance**, **further resources are necessary to ensure that EMS providers have the equipment and training they need to respond** to a terrorist attack or disaster. **If EMS personnel do not receive the equipment**, **education and training they need**, **their ability to provide care for patients during a disaster will be compromised**. There will be an inadequate medical first response.

This sector is of critical importance of the overall nation because of the frontline role it plays in bioterror response and response to other public health emergencies:

> **Center for Catastrophe Preparedness and Response.** (20**05**, March). Emergency Medical Services: The Forgotten First Responder. Retrieved from: http://www.nyu.edu/ccpr/NYUEMSreport.pdf.
> **The National Bioterrorism Hospital Preparedness Program**, administered by the Department of Health and Human Services (HHS), **provides funding to hospitals and health care systems**. **These grants help** hospitals and health care **systems to prepare**

> **for terrorism and other public health emergencies**. **Although HHS designated the preparedness of EMS systems as a critical area for improvement**, **the EMS system received only five percent of Bioterrorism Hospital Preparedness Grant Funding**.27 Four states did not involve the state EMS office in the application process for these grants28 and **some states provided no funding to EMS providers**.

This type of affirmative would demand federal action:

> **Center for Catastrophe Preparedness and Response**. (20**05**, March). Emergency Medical Services: The Forgotten First Responder. Retrieved from: http://www.nyu.edu/ccpr/NYUEMSreport.pdf.
> **No EMS-specific national bioterrorism or disaster preparedness standards or guidelines exist**. **The absence of these standards and guidelines is a significant barrier to the effective allocation of resources for improving the preparedness capabilities of the EMS system**. For example, there are currently no standards or guidelines to determine how many EMS personnel should have protective equipment, how many personnel should participate in mass casualty exercises or the kinds of information about what technology systems EMS should have. **EMS-specific national bioterrorism and disaster preparedness standards should be addressed through ongoing federal efforts**, such as Homeland Security Presidential Directive-8, regarding national preparedness. This directive outlines a series of goals, including the establishment of preparedness standards. As yet, however, the Federal government has developed few standards. **The Federal government must conduct a comprehensive assessment of the capabilities of the EMS system to respond to terrorism**, **public health emergencies and other disasters so that EMS-specific preparedness standards and guidelines will accurately reflect the capabilities needed to achieve effective levels of preparedness and response**.

The authors cited in these pieces of evidence included eight specific recommendations for federal action, including enacting legislation to establish a Federal Interagency Committee on Emergency Medical Services; funding efforts such as the National EMS Information System to allow the uniform collection of patient data; and increasing homeland security funding for EMS and coordinate grant guidance and funding priorities to improve the preparedness of the EMS system.

B. Interoperability

During large scale emergencies, it is not uncommon for multiple agencies at the federal, state and local level to respond simultaneously. With some many groups at work, communication problems are likely to arise. One potential affirmative within the ESS sector would improve interoperability by establishing a nation-wide network of interoperable frequencies, a debatable proposition from the perspective of the parties involved:

> **Jenkins, 06**
> William O. (2006, February 23). Emergency Preparedness and Response: Some Issues and Challenges with Major Emergency Incidents. Retrieved from http://www.gao.gov/new.items/d06467t.pdf.
> **The** first, and **most formidable**, **challenge in establishing effective interoperable communications is defining the problem and establishing interoperability requirements**. This requires addressing the following questions: Who needs to communicate what (voice and/or data) with whom, when, for what purpose, under what conditions? **Public safety officials generally recognize that effective interoperable communications is the ability to talk with whom you want**, **when you want**, **when**

authorized, **but not the ability to talk with everyone all of the time**. **Various reports**, including ours, have **identified a number of barriers to achieving interoperable public safety wire communications**, **including incompatible and aging equipment**, **limited equipment standards**, **and fragmented planning and collaboration**. However, **perhaps the fundamental barrier has been and is the lack of effective**, **collaborative**, **interdisciplinary**, **and intergovernmental planning**. The needed technology flows from a clear statement of communications needs and plans that cross jurisdictional lines. **No one first responder group or governmental agency can successfully "fix" the interoperable communications problems that face our nation**. **The capabilities needed vary with the severity and scope of the event**. In a "normal" daily event, such as a freeway accident, the first responders who need to communicate may be limited to those in a single jurisdiction or immediately adjacent jurisdictions. However, **in a catastrophic event**, **effective interoperable communications among responders is vastly more complicated because the response involves responders from the federal government—civilian and military—and**, as happened after Katrina, **responders from various state and local governments** who arrived to provide help under the Emergency Management Assistance Compact (EMAC) among states. **These responders generally bring their own communications technology that may or may not be compatible with those of the responders in the affected area**. **Even if the technology were compatible**, **it may be difficult to know because responders from different jurisdictions may use different names for the same communications frequencies**. **To address this issue**, **we recommended that a nationwide database of all interoperable communications frequencies**, **and a common nomenclature for those frequencies**, **be established**. Katrina reminded us that **in a catastrophic event**, **most forms of communication may be severely limited or simply destroyed**—land lines, cell phone towers, satellite phone lines (which quickly became saturated). **So even if all responders had had the technology to communicate with one another**, **they would have found it difficult to do so because transmission towers and other key supporting infrastructure were not functioning**. **The more comprehensive the interoperable communications capabilities we seek to build**, **the more difficult it is to reach agreement among the many players on how to do so and the more expensive it is to buy and deploy the needed technology**. **And an always contentious issue is who will pay for the technology**—purchase, training, maintenance, and updating.

C. FEMA Reform

Many felt that the creation of the Department of Homeland Security would effectively alleviate many of the challenges faced by first responders when confronting a terrorist attack. However, this consolidation of emergency management functions within the DHS structure has created coordination difficulties that have led some to call for the separation of the Federal Emergency Management Agency from the DHS:

Hugue and Bea, 06
Hogue, Henry B. & Bea, Keith. (2006, June 1). Federal Emergency Management and Homeland Security Organization: Historical Developments and Legislative Options. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33369.pdf.
Hurricane Katrina struck the Gulf Coast states of Louisiana, Alabama, and Mississippi on August 29, 2005, **resulting in severe and widespread damage to the region**. **The response of the federal government**, **especially the Federal Emergency Management Agency** (FEMA), in the aftermath of the storm **has been a matter of considerable controversy among elected officials and in the media**. **Some of the criticism has focused on FEMA's organizational arrangements at the time of the disaster. Prior to these events**, in July 2005, **Secretary Michael Chertoff had announced a reorganization of the Department of Homeland Security** (DHS), **including FEMA**. In the aftermath of Hurricane Katrina, the Administration proceeded

with the reorganization initiative after Congress signaled its approval. 1 **As a result of concerns about the effectiveness of the federal response after Hurricane Katrina**, **Congress is continuing to rethink the organizational arrangements for carrying out federal emergency management functions**. The release of reports by the House, Senate, and White House on the response to Hurricane Katrina may lead to further examination of these issues. **Legislation has been introduced in Congress bearing upon these arrangements**. **As of May 30, 2006**, **11 such bills had been introduced**. **Prior to its incorporation into DHS in 2003**, **FEMA was an independent agency, and eight of the 11 bills would reestablish FEMA as such**. **The three remaining bills would reorganize emergency management functions within DHS**, **bringing preparedness and response functions under one directorate**, as they were prior to the 2SR reorganization. This report provides background information about the establishment and evolution of federal emergency management and related homeland security organization since 1950. 2 Post-Katrina assessments of current arrangements by Congress and the White House are also discussed. Finally, the report provides a brief summary of related legislation that had been introduced as of May 30, 2006.

Negative Ground

1. Focus Tradeoff Disadvantage

Affirmatives would chose to focus upon improving the ESS sector's ability to respond to terrorism incidents would likely face tradeoff disadvantages which claim a focus on terrorism undermines preparedness for natural disasters:

Hugue and Bea, 06
Hogue, Henry B. & Bea, Keith. (2006, June 1). Federal Emergency Management and Homeland Security Organization: Historical Developments and Legislative Options. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33369.pdf.
At the outset of this report (see "Evolution of Organizational Arrangements") **issues concerning the scope of responsibility, types of threats, federalism concerns, and assignment of responsibility** were identified. These and other issues **will shape congressional debate over the future of FEMA**. An examination of the evolution of federal emergency management (now homeland security) policy since World War II reveals that some concepts have not changed. **Just as the debate over the federal role in civil defense affected executive and legislative branch decisions on organizational options 50 years ago**, **the current debate over whether a terrorism focus detracts from natural disaster preparedness and response is likely to affect present day policymaking**.

More evidence from the aftermath of Katrina discussing the proposed reorganization of FEMA confirms this possibility:

Democratic Staff of the House Committee on Science, 05
Failing to Protect and Defend: the Federal Emergency Response to Hurricane Katrina. (2005, October 20), Retrieved from http://democrats.science.house.gov/Media/File/Reports/katrina_response_updated_20oct05.pdf.
The planning efforts by DHS have produced endless documents, **but no more secure a public**. In fact, **the public may be less safe now than before 9/11 due to the shift in attention away from meeting the known threats that endanger our communities in exchange for a narrow concentration on threats that are frightful, but unknown**. This is not to say that **preparing to stop terrorists** or effectively respond should the unthinkable happen again are not priorities for the nation; but these efforts **should not be pursued at the expense of ignoring risks that we know we must face**

and that our science and technology often allow us to anticipate and prepare for. And the reality is that Katrina allowed the government more than two days to get ready. That time was squandered. **It is possible that FEMA** - **which has been through the turmoil of reorganization**, moved towards giving State and local governments more responsibility even in devastating situations and lost many senior employees - **cannot at present do better than it did**. In response to criticism about the government's response to Katrina, Russ Knocke, Mr. Chertoff's spokesman, said, "We pushed absolutely everything we could, every employee, every asset, every effort, to save and sustain lives. 80" We fear he is telling the truth and that should frighten everyone.

2. Private Action Counterplan

Many have criticized the ESS sector for its excessive focus on government delivered emergency response. These critics would advocate the expansion of incentives-based approaches which seek to increase the involvement of the private sector in disaster and terrorism preparedness and response. Net-benefits to such a counterplan would include a Coercion argument, Spending disadvantages or Politics.

Newt.Org, 06
A 21st Century Federal Emergency Response, Recovery and Reconstruction System. (2006, May 9), Retrieved from http://www.newt.org/newt-direct/21st-century-federal-emergency-response-recovery-and-reconstruction-system.
The vast majority of emergency response, **recovery and reconstruction capability will be outside the federal government**. **In fact the vast majority will be outside all governments**. **The government and bureaucracy centric model of the last 70 years overstates the role of bureaucrats and understates the capabilities and power of individuals and private sector organizations** (both for profit and non-profit). The federal government is only 18% of the total economy. Even that overstates its capabilities since much of that 18% is tied up in transfer payments, interest on the debt, and implementing existing programs. The mobilizable parts of the federal government are actually very tiny as a share of the total economy and society. State and local governments are not dramatically more flexible and capable (indeed they may be less so). It would be useful to analyze what percent of the resources going into response, recovery, and reconstruction after Katrina are private and what per cent are government. **Despite all the focus on government the private resources are vastly larger**. **Therefore planning should begin with an effort to understand how we can mobilize the entire society and use all the resources of citizens and civil society rather than merely passively waiting for bureaucracies** (whether federal, state, or local) to get things done. This principle of shifting from a bureaucrat and lawyer centered system to a citizen centered system has a number of implications which will be outlined below. **A citizen centered system will inherently be permissive**, **coordinating and flexible**. It will consistently seek reasons to say "yes, if" rather than "no because" when approached by volunteers. To a large degree this will be a self organizing system using information technology, expert systems, and citizen initiative, creativity and goodwill to identify and solve problems and develop opportunities at a rate faster than any industrial-bureaucratic system could possibly keep up. In some ways **the design of this new system** (deliberately NOT an 'administration") **will be a cross between E-Bay, Craig's List, and an online dating service**. **Those who need help will be signaling to those who have help to give and they will be mutually interacting with minimum bureaucratic interference**. In developing this 21st century citizen centered model it would be useful for the Congress to call in the developers of the most successful self organizing systems to learn what the new principles are and explore how they could be applied to this new Federal system (see Glenn Reynolds An Army of Davids for further insights in this area). A citizen-business-charity based system will work much better if there is a system of federal and state laws for application in a time of emergencies. **The bizarre behavior of FEMA** (for example keeping a donated childcare center locked for two months while

processing the paperwork**) is in part a function of 70 years of growing regulatory**, **legal and congressional complexity**. **A new set of laws should be written from the ground up at the federal and state level to maximize speed**, **flexibility and common sense and minimize litigation**, **regulatory processing and bureaucratic timidity**. An effective system will include five layers: federal, state, local, private sector (both profit and non profit) and citizen. The industrial-bureaucratic model we have inherited overstates the importance of the three government layers and understates the importance of the private sector and citizen layers. Hearings should be held centered on these two foundation layers and learning from institutions and leaders in those areas to develop a new citizen-centric rather than the bureaucrat- and lawyer-centric system we currently have. Future planning, organizing, training and exercising should have all elements of the system in the room and not merely have them waiting in the anteroom while the 'real' powers of the bureaucracy meet in secrecy. Involvement in implementation must begin with involvement in the planning and training phases. **A citizen centered system would begin with the recognition that the Immediate Responders** (in Congressman Reichert's phrase) **are the citizens**. **They are there even before the first responders**. **In a large crisis they have vastly more resources than the police and the firemen**. As David Hackett Fisher analyzes brilliantly in Paul Revere's Ride, **there is a very old and powerful tradition of citizen preparedness at the heart of the American experience**. A bold new effort must be made to create a 21st century citizenship in which people understand that their Creator endowed right to pursue happiness also has a corresponding responsibility to be an effective citizen. That effective citizenship has to include crisis preparedness. **The business community responded much faster than government during Katrina but was often blocked and inhibited from being as effective as it could have been**. **The new system should maximize business involvement in planning, training and exercising and should be designed to maximize business participation**. The current dismal failures in recovery in New Orleans should raise questions about new approaches to maximize private sector investment and maximize private sector job creation in the recovery and reconstruction phase. The work currently underway at BENS (Business Executives for National Security) is a good resource for the Congress to draw on in this area.

3. Politics & Spending Disadvantages

Decisions about proper disaster mitigation and response are politically controversial and subject to extreme budgetary pressures:

Kamarck, 07
Elaine, When First Responders Are Victims: Rethinking Emergency Response. *Harvard Law & Policy Review.* Retrieved from http://www.hlpronline.com/vol1no1/kamarck.pdf.
Second, **politics makes disaster prevention extremely difficult**. For instance, **following the 1993 flooding along the Mississippi River** that resulted in the evacuation of 70,000 people, **the Clinton Administration bought 7,700 properties along the river** at a cost of $56.3 million in order **to relocate people from the flood plains**. **But political and local development pressure meant that**, **by the time the Bush administration came into office**, **political support for mitigation had waned and the program was halted**. In fact, in a reversal of the policy of the 1990s, the population of the Mississippi Floodplains has increased, and 28,000 new homes have been built on land that was underwater just thirteen years ago. 43 **A short review of policies vis-a-vis New Orleans in the wake of Katrina illustrates again the political futility of treating natural disasters as preventable**. Wetlands are natural buffers between ocean and more solid land. In the case of hurricanes, wetlands act as natural sponges, absorbing some of the shock of the ocean before it hits dry land. The New Orleans levees "were built on the assumption that they would have forty or fifty miles of protective swamp between the city and the Gulf of Mexico."44 But successive

governments have allowed for development on wetlands, and thus the Gulf of Mexico is twenty miles closer to land than it was in 1965. Consequently, hurricanes are more destructive.45 The first step in trying to reduce the destructiveness of natural disasters should be to protect wetlands. “But rather than continue a ban on wetlands development instituted by previous administrations, the Bush administration overturned it.” 46 Banning wetland development means saying no to developers and, in some cases, voters. **The lack of political will is evident in another decision**. **When FEMA finally issued its long-awaited rebuilding guidelines**, **politics triumphed and common sense lost**. **The new federal guidelines required only that structures be rebuilt three feet above ground**. 47 Some houses in New Orleans had six feet of water in them. Of these, some had been built three feet above ground, and could thus be legally rebuilt without modification. The leniency of these new regulations was welcomed by all those anxious to get back home. **No one in the political system had the will to tell displaced residents they should not return home**. **The lack of political will to do anything serious about mitigation ex ante will produce significant ex post harm to federal taxpayers**, **as disaster relief consumes an increasing share of the federal budget**. **With costs rising at a rate that threatens to consume the remaining discretionary (nonentitlement) portion of the budget**, **spending on emergency response threatens to become a major federal entitlement program like Medicare and Social Security**. 48 Since the private market is not subject to political pressures, it will not insure much of what used to be New Orleans. It is left up to the National Flood Insurance Program which, instead of living up to its promise to reduce flood damage, is using old maps that significantly underestimate the danger from flooding. The cost of this short-sightedness will be borne by all taxpayers.49

4. States & Federalism

The effectiveness of federal action vis-à-vis the state is a debate ripe for investigation within the ESS literature:

Kamarck, 07
Elaine, When First Responders Are Victims: Rethinking Emergency Response. *Harvard Law & Policy Review.* Retrieved from http://www.hlpronline.com/vol1no1/kamarck.pdf.
Thus, we need a more complex and more subtle explanation of the government’s failure during Katrina. We can start by noting that **in the United States, disaster relief has never been seen as a task for which the federal government is primarily responsible**. **The design of our disaster mitigation institutions reflects this**. **However, in recent decades FEMA has been thrust into the role of director of emergency response, a role for which it was never designed**. Arnold Howitt and Herman “Dutch” Leonard of the Kennedy School of Government argue that **FEMA “has historically played a much larger role in pre-event planning and post-event recovery than in the management of a disaster in progress**.”21 **Historically, federal involvement in disaster prevention and relief is of recent vintage and has proceeded in an extremely incremental fashion**.22 In 1900, when Galveston Texas was decimated by a Hurricane, no substantial federal resources were deployed. In 1950, Congress set aside funding in anticipation of disasters, authorizing $5 million for the purpose, a pittance even then. 23 In 1955 the federal government covered only 6.2% of the total damages caused by Hurricane Diane. 24 Fourteen years later, Congress passed the Disaster Relief Act of 1969, which authorized the President to appoint Federal Coordinating Officers who would coordinate all federal disaster relief in a designated disaster area and “assist local citizens and public officials in promptly obtaining the assistance to which they are entitled.” 25 In the Stafford Act of 1974, Congress outlined the process by which the President declares and prepares for major disasters and emergencies and extended Federal disaster relief aid to individuals and families. 26 Finally, FEMA itself was not created until 1979, when President Carter, noting that more

> than 100 federal agencies were involved in aspects of disaster response, created the department by executive order.27 However, it was not until 1988 that Congress amended the Stafford Act, 28 formalizing the process for handling disasters in the United States. Ever since, the criteria for issuance of a disaster declaration have remained fairly constant. The Act assumes that **states and localities are first responders and that they can effectively assess the damage resulting from an event and, if necessary, ask the President for federal assistance**. **The Act does not assume that the Federal Government will be the primary actor in the event of an emergency, but rather specifies how it will supply help after the fact**. The relevant portion of the Act states: All requests for a declaration by the President that a major disaster exists shall be made by the Governor of the affected State. Such a request shall be based on a finding that the disaster is of such severity and magnitude that effective response is beyond the capabilities of the State and the affected local governments and that Federal assistance is necessary. As part of such request, and as a prerequisite to major disaster assistance under this Act, the Governor shall take appropriate response action under State law and direct execution of the State's emergency plan. The Governor shall furnish information on the nature and amount of State and local resources which have been or will be committed to alleviating the results of the disaster, and shall certify that, for the current disaster, State and local government obligations and expenditures (of which State commitments must be a significant proportion) will comply with all applicable cost-sharing requirements of this Act. Based on the request of a Governor under this section, the President may declare under this Act that a major disaster or emergency exists. 29 **Note the heavy reliance on state activity and the heavy burden placed on States—and by implication localities—before the Federal Government takes actio**n. **The law assumes that first responders are able to act and that the command and control apparatus of state and local government is intact**. **But in two instances where FEMA failed spectacularly, Hurricane Andrew and Hurricane Katrina, precious days and hours passed before people realized that the disaster was large enough that the first responders had themselves become victims and were therefore unable to file the statutorily mandated request for assistance**.

Conclusion

Including the Emergency Services Sector within a Critical Infrastructure and Key Resources debate resolution will offer students an opportunity to learn about many of the practices and procedures that they often forget are necessary when and if the worst case materializes. Learning about how our everyday heroes struggle to carry out their jobs under less than ideal circumstances will give us a key appreciation of the role that citizens play in ensuring the safety of our communities. Due to the potential for affirmative creativity with stable negative ground, this author advocates includes of the ESS within the CIKR topic.

Energy

Introduction

Those of us that worked on the 2004-2005 energy topic know how important reliable energy distribution can be to the United States. While the development of energy failsafe systems has been considered by the USFG, there is a lot of room for improvement. What makes this specific topic area unique is that any failure in the energy sector is likely to cause a cascading effect across other areas of our critical infrastructure. The General Accounting Office of the United States points out that "within the energy sector, the electricity industry uses a combination of information technologies, including LAN, WAN, Internet, wireless networks, satellite, and radio".[111] In the event of a catastrophic energy shutdown, it is likely that all other forms of critical infrastructure protection would be crippled beyond repair.[112] This is particularly troubling because major military institutions such as the Pentagon depend upon the commercial energy grid, which is currently vulnerable to attack or malfunction.[113]

The Department of Energy stipulates that critical infrastructure in relation to Energy distribution relates to "electric power and the refining, storage, and distribution of oil and natural gas".[114] Depending on the topic wording, certain areas of energy distribution, exploration, and storage may or may not be topical. The Department of Homeland Security offers a slightly different analysis of critical infrastructures relating to energy, stating that the topic could include virtually anything relating to the creation and availability of electricity, petroleum, and natural gas.[115]

It is important to note that, depending on the topic wording, this section of the topic would include all means of energy distribution, storage, and exploration focused on the continued reliability of the grid. Additionally, the inclusion of natural gas indicates the possibility of Liquid Natural Gas (LNG) being a potential topic area (DHS 2010). It is also possible that the development of new and more stable sources of energy (renewables) might fall under certain resolution wordings.

Affirmative Ground

Affirmatives interested in addressing this topic area will find themselves enjoying a rich and diverse literature base. Questions of energy reliability in the event of a major crisis include calls for increased protection of resources[116], decreased foreign oil dependence[117,118] and calls for a

---

[111] General Accounting Office, Technology Assessment Cybersecurity for Critical Infrastructure Protection, http://www.oe.energy.gov/DocumentsandMedia/GAO_Tech_Assess_for_Cybersecurity_CIP.pdf, 2004
[112] Sheldon F., Potok, T., Krings, A. and Oman, P., Critical Energy Infrastructure Survivability, Inherent Limitations, Obstacles, and Mitigation Strategies, International Journal Of Power And Energy Systems, 2004.
[113] Defense Science Board Task Force, More Fight-Less Fuel, February 2008, http://www.acq.osd.mil/dsb/reports/2008-02-ESTF.pdf
[114] General Accounting Office, Technology Assessment Cybersecurity for Critical Infrastructure Protection, http://www.oe.energy.gov/DocumentsandMedia/GAO_Tech_Assess_for_Cybersecurity_CIP.pdf, 2004
[115] Department of Homeland Security, National Infrastructure Protection Plan: Energy Sector, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf, 2010
[116] Carafano, James J. and Beach, William W., July 25, 2007, http://www.heritage.org/Research/EnergyandEnvironment/cda07-03.cfm
[117] Marsh, Gerald E., Society for the Advancement of Education, Vol. 135, January2007
[118] Lauber, Volkmar, Switching to Renewable Power: a framework for the 21st century, ed. V., 2005

decentralized energy grid (renewables).[119] Any one of these areas would be a worthwhile topic in and of themselves. The resolution wording process will be a critical time to determine which, if any, of these subtopics would fall under topical ground for the affirmative. It is likely that whatever areas are not granted to the affirmative will be effectively ceded to the negative, as will be discussed later in this section.

Any affirmative choosing to engage this topic area will need to address their plan action in relation to Energy Infrastructure Survivability (EIS), which measures the effectiveness of our current reliability measures. EIS can be understood as "a hierarchical method used to assess and implement survivability mechanisms and mitigate common mode failures associated with three important areas of energy assurance: (a) securing cyber assets, (b) modeling and analysis to understand and enable fundamentally robust and fault- tolerant systems, and (c) systems architecture that can overcome vital limitations".[120] Applied to typical debate style and structure, this three-point guideline allows for affirmatives to focus on both cyber and physical limitations in the current system. Based on these two sections, affirmatives can focus on harms stemming from either malicious intent (terrorism or sabotage) or maintenance shortfalls (reliability or redundancy).

Concerning the harms debate, the energy section of this topic can borrow greatly from previous debate topics. Much of the relevant literature identified various types of terrorism as being a major threat to energy as a critical infrastructure. The most commonly identified threat is that of cyber terror, as identified by the DoE:

> **Department of Energy, 2010**
> (http://www.oe.energy.gov/controlsystems.htm)
>
> The U.S. energy sector operates the most robust and reliable energy infrastructure in the world. This level of reliability is made possible by the extensive use of SCADA, DCS, and other control systems that enable automated control of energy production and distribution. These systems integrate a variety of distributed electronic devices and networks to help monitor and control energy flows in the electric grid and oil and gas infrastructure. **Automated control has helped to improve the productivity, flexibility, and reliability of energy systems. However, energy control systems communicate with a multitude of physically dispersed devices and various information systems that can expose energy systems to malicious cyber attacks. A successful cyber attack could compromise control systems and disrupt energy networks and the critical sectors that depend on them**.

Other types of terrorism, such as plots to fly a plane into a nuclear reactor, remain a potential threat that could be addressed by an affirmative. Lack of proper funding for the protection and maintenance of critical gas pipelines within the United States is another major point of concern in the status quo.[121] Plans that focus on increased protection of facilities are likely to be a core plan focus for those debaters that are

[119] Morsella, Tracey, de, President Obama Awards $2.3 Billion for New Clean-Tech Manufacturing Jobs, http://greeneconomypost.com/president-obama-awards-2-3-billion-for-new-clean-tech-manufacturing-jobs-7444.htm
[120] Sheldon F., Potok, T., Krings, A. and Oman, P., Critical Energy Infrastructure Survivability, Inherent Limitations, Obstacles, and Mitigation Strategies, International Journal Of Power And Energy Systems, 2004.
[121] Gregory J. Lengyel, Colonel, USAF, 2007, DOD Energy Strategy: Trying to Teach an Old Dog New Tricks, h http://www.brookings.edu/~/media/Files/rc/papers/2007/08defense_lengyel/lengyel20070815.pdf

interested in the big impact debate. Cyber terrorism against critical energy facilities offers an additional internal link in to these scenarios, also spurring debates on the economy and environment, as described by the GAO:

> **GAO, 04**
> (General Accounting Office, Technology Assessment Cybersecurity for Critical Infrastructure Protection, http://www.oe.energy.gov/DocumentsandMedia/GAO_Tech_Assess_for_Cybersecurity_CIP.pdf, 2004)
>
> According to NIST, cyber **attacks on energy production and distribution systems**—including electric, oil, gas, and water treatment systems, as well as on chemical plants containing potentially hazardous substances—**could endanger public health and safety, damage the environment, and have serious financial implications, such as loss of production, generation, or distribution of public utilities; compromise of proprietary information; or liability issues**. When backups for damaged components are not readily available (e.g., extra-high-voltage transformers for the electric power grid), such damage could have a long-lasting effect.

Affirmatives based on energy as a critical infrastructure in need of updating will have no problem identifying multiple solvency mechanisms that would meet the resolutional burden. Additionally, this topic area proves that the critical infrastructure topic might be a domestic topic, but it still allows for international impact assessment.

Negative Ground

As stated earlier, virtually any energy policy that is not a topical option under the resolution can be considered ceded to the negative. Given the attention given to energy policy, virtually any competing policy option could be constructed as a counterplan, since perception would dictate that any sort of permutation would run the risk of supercharging a politics Disad. Additionally, the vast majority of energy initiatives currently being considered in the United States make their interests very clear, indicating that anything more than a single policy would likely derail true process in this sector. History has shown that major overhauls of critical infrastructures are extremely costly to the president:

> **Pernick and Wilder, 07**
> (Ron Pernick & Clint Wilder, Clean Edge, Inc., 2007, The Clean Tech Revolution: the next big growth and investment opportunity, p. 176-7)
>
> But the opportunities for companies, investors, governments, and entrepreneurs are still considerable. **"Right now the grid is held together by bubblegum and paper clips," says McDermott. He believes**, along with many others, **that the current grid needs significant investment and a coordinated push by a visionary leader, most likely from a visionary president in the White House. "**The example that's become the most telling for me is the interstate highway system in the US," he says. "**President Dwight Eisenhower used his political capital to build out the interstate highway system. This was done for national security,** in order to evacuate cities in the case of nuclear attack, and to spur the economy**. I believe there are a lot of parallels between the interstate highway of the 1950s and building out a smart grid today."**

In relation to specific counterplan ground, there is ample evidence available that the states might be the optimal actor in regard to the energy sector. One specific advantage available to the negative is

the argument that a decentralized energy program means that a system-wide blackout is less likely since no one single location is responsible for maintaining the entire national grid.

A resolution containing an energy-based policy option is also a core area for rich critical debates. Previous years have shown us that energy topics allow for a wide diversity of kritiks including Luke (consumption rhetoric), Global-Local, Commoditization and Deep Ecology to name a few. These options are in no way representative of the argumentative depth available through this topic area, but represent previous examples of kritiks run under similar resolutions.

Government Facilities

Introduction

Upon first noticing this sector on the list of CIKR assets, you might ask yourself what exactly constitutes a government facility. While this term seems vague, it is actually a very precise term used in contemporary literature and indicates facilitates maintained with the purpose of providing U.S. citizens a means of interacting with government at all levels. The Department of homeland security explains the areas covered by this sector:

> The Government Facilities Sector includes a wide variety of buildings, owned or leased by Federal, State, Territorial, local, or tribal governments, located domestically and overseas. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities. Others not open to the public contain highly sensitive information, materials, processes, and equipment. This includes general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment and systems, networks, and functions.[122]

Whereas the Continuity of Government sector is tasked with ensuring the continued functioning of the government through the protection of critical personal, the Government Facilities sector is tasked with maintaining the physical locations that the government requires to ensure that personal can conduct their business.

In addition to securing the physical locations critical to the functioning of government, this sector also includes certain cyber assets, such as secured government networks and access control systems.[123] Unlike most CIKR sectors, Government Facilities functions exclusively through the actions of the government, whereas most sectors require government actors to coordinate with private industry.[124] This makes action within this sector easier due to the lack of private interests, but simultaneously more difficult due to the lack of accountability and transparency.

Affirmative Ground

The type and amount of affirmative ground granted through this sector will depend greatly upon the particular wording of the resolution. For instance, including the clause 'within the United States' will limit the Government Facilities sector, excluding international resources hosted by other countries. Arguably, this wording would still allow affirmatives to effect certain U.S. embassies and military bases since some of these facilities are considered extraterritorial, meaning that they are considered to be sovereign U.S. soil.[125]

---

[122] Department of Homeland Security, "National Infrastructure Protection Plan: Government Facilities Sector," 2008, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_governmentfacilities.pdf
[123] Department of Homeland Security, "National Infrastructure Protection Plan: Government Facilities Sector," 2008, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_governmentfacilities.pdf
[124] "Critical Infrastructure Protection" Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics," October 2006, http://www.gao.gov/new.items/d0739.pdf
[125] Integrity Legal, "Law and Rules Regarding Extraterritoriality", July 14th, 2009, http://integrity-legal.com/legal-blog/miscellaneous/laws-and-rules-regarding-extraterritoriality/

Currently, this sector is in a state of repair; recent inspections have found that security protocols are rarely followed and fail to account for developing threats to government facilities. Joe Lieberman recently explained these harms:

> **Senate Committee on Homeland Security & Governmental Affairs, 11**
> ("Senators Introduce Legislation To Better Secure Federal Buildings And People Who Visit Them," April 11th, 2011, http://www.hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=45aeffcf-5056-8059-76b0-945b13e784f7)
> "**Poor management, serious budget shortfalls, and operational challenges have diminished FPS' effectiveness and undermined public trust** in the agency," **Lieberman said. "FPS guards were** famously caught **sleeping on the job, putting an infant** in its carrier **through an X-ray machine, and failing to detect bomb-making materials** on investigators who passed through security. **The agency must be turned around,** which is why we are introducing this legislation to strengthen its management, provide it with the necessary resources to fulfill its mission, and help it function at a higher level."

While the Senate is currently ways to improve this sector, no major changes have been made to date.

Despite these security shortfalls, the threat to government facilities is readily apparent; we need look no farther than the 1995 Oklahoma City bombing where the Federal Building was torn asunder, killing 20 people (6 of which were children) and wounding hundreds.[126] Since this tragic event, the government has devoted considerable time and money towards the securing of these assets. Currently, the government facilities sector is overseen by the Federal Protective Service (FPS) and the General Services Administration (GSA), responsible for assessing risk and reliability for all resources consider critical government facilities.[127,128]

While the GSA and FPS are responsible for assessing these resources, much of the actual work required to maintain this sector is outsourced to private corporations. Affirmatives interested in addressing this sector should consider how the selection of any particular contractor will influence the quality of solvency in addition to how the contract assigned through the plan will affect the company's ability to solve other issues. One such company, 4D Security Solutions, has been tasked with the protection of multiple critical infrastructure sectors including transportation, chemicals, and government facilities.[129] Choosing to solve through a particular actor might have negative consequences on one of these other operations.

Another continued problem in this sector is the nature of governmental facilities; many of which only rent or lease part of a building, leaving the rest open to the general public. This severely complicates security measures for these facilities since government offices are only capable of banning weapons

[126] ABC News, April 19, 1995, "World News Tonight With Peter Jennings," April 19, 1995.
[127] "Critical Infrastructure Protection" Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics," October 2006, http://www.gao.gov/new.items/d0739.pdf
[128] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, 2003.
[129] 4D Security, "Solutions," http://www.4-dsecurity.com/solutions.asp

within their own offices, not the entire building in which government assets are housed.[130] Solvency discussions on this issue are currently developing in the literature base due to the Supporting Employee Competency and Updating Readiness Enhancements for Facilities Act of 2011 (SECURE Facilities Act) which was presented to Congress in early April 2011.[131] This act is geared towards solving many of the problems currently hampering the sector, but does not go far enough to solve all concerns. For instance, in 2010, the Government Accountability Office found that all 7 of the 7 contractors paid to supply qualified security forces to government facilities were failing to do so.[132] Given these serious security loopholes, change is desperately needed in this sector. While the SECURE Facilities Act, if passed, will solve some issues, the GAO has proposed a far larger initiative which it claims is critical to ensuring security:

> **GAO, 10**
> ("Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards," April 2010, http://www.gao.gov/new.items/d10341.pdf)
> Recommendations for Executive Action
> **Given the long-standing and unresolved issues related to FPS's contract guard program and challenges in protecting federal facilities**, employees, and the public who use these facilities, **we recommend** that the Secretary of Homeland Security direct the Under Secretary of NPPD and the Director of FPS to take **the following eight actions:**
> • **identify other approaches and options that would be most beneficial and financially feasible for protecting federal facilities**;
> • **rigorously and consistently monitor guard contractors' and guards' performance** and step up enforcement against contractors that are not complying with the terms of the contract;
> • **complete all contract performance evaluations** in accordance with FPS and FAR requirements;
> • **issue a standardized record-keeping format** to ensure that contract files have required documentation;
> • **develop a mechanism to routinely monitor guards** at federal facilities outside metropolitan areas;
> • **provide building-specific and scenario-based training** and guidance to its contract guards;
> • **develop and implement a management tool for ensuring that reliable, comprehensive data on the contract guard program are available** on a realtime basis; **and**
> • **verify the accuracy of all guard certification and training data** before entering them into RAMP, and periodically test the accuracy and reliability of RAMP data to ensure that FPS management has the information needed to effectively oversee its guard program.

While no affirmative would necessarily have to initiative all of these proposals, they do lay out a significant amount of ground for teams interested in discussing this sector.

Negative Ground

---

[130] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf, 2003.
[131] Senate Committee on Homeland Security & Governmental Affairs, "Senators Introduce Legislation To Better Secure Federal Buildings And People Who Visit Them," April 11th, 2011, http://www.hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=45aeffcf-5056-8059-76b0-945b13e784f7
[132] Government Accountability Office, "Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards," April 2010, http://www.gao.gov/new.items/d10341.pdf

Government Facilities is one of the CIKR sectors which is currently getting a lot of attention in Congress. Similar to the way that Obama's immigration initiatives affected how the debate community debated visa policy last year, it is possible that the SECURE Facilities Act will affect how this sector is discussed.

Some controversial issues are slated to remain in effect, regardless of the SECURE Facilities Act. One such issue is the usage of new screening techniques such as Fully Body Scanners, the controversial technology primarily utilized by the TSA in airports. Used in various government facilities, the continued usage of technology provides negative teams with ample kritik ground focused on surveillance.[133]

Additional ground will likely stem from the security limitations due to government facility location. Affirmatives that do not address the security issues created through public access to buildings housing government facilities are likely to face solvency deficits and potentially counterplans calling for all governmental facilities to be housed in fully-secured buildings. Finally, negative teams should consider the merits of privatized security personal as opposed to military security, which is likely to offer a higher quality of protection.

[133] Fact Resource, 2010, http://factresource.com/2010/list-airports-with-full-body-scanners/

Healthcare and Public Health

Introduction

Health and public health critical infrastructure (HPH), provides fruitful ground for issues that impacts domestic interests (economic, health, workforce, medical care) and global issues (pandemics, bioterrorism, natural disaster). HPH constitutes 15 percent of the GNP, is owned by 85 percent of privately owned assets, and exists within a birds nest of legal and jurisdictional issues of federal, military, state, tribal, and local governments. Without question, HPH CIKR is an area of the controversy that is dynamic, with elapsing legal authority and 2011/2012 funding/budgetary issues, as well as a rich research base that would provide enough depth to justify a years' worth of policy debate research.

The uniqueness of HPH as an addition to the topic wording is in relation to how the DHS and HHS define the health care workforce, as well as research scientists, as constituting an essential and critical portion of the health care infrastructure. Millions of human beings existing within overlapping jurisdictions that have been identified by the government as critical infrastructure presents an interesting as well as difficult issue for policymakers. As policymakers project future health threats and attempt to prepare and prime trained groups of people for their realization, the method for lining up goals with actual policies opens up space for HPH's addition to the college debate topic.

Initial observations suggest advantages will be based in the area of disease, bioterrorism, natural disasters, federalism, and ethics in terms of inclusion/exclusion of care and resource allocation. The literature is saturated with potential doomsday scenarios of civilization as well visions of dystopic overreach of government control, and everything in between. As an issue of "critical infrastructure" the health of the public and the nation provides for internal links to rich impacts, critique links, and on-case debates.

A preview of agency responsibility and the ends of HPH CIKR:

The Department of Health and Human Services is largely responsibility for prioritizing and implementing the protection and resiliency of HPH. A report from HHS highlights the four major goals of the HHS: To "protect" the: 1) Continuity of Services, 2) Workforce, 3) Physical Assets, 4) Cyber Systems.[134] Each one of these major areas provides for decent case and solvency debate as well as other major advantage and disadvantage areas. Expanding on the 4 priorities:

1) Continuity of Services:

> **HHS, 09**
> (2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
> The HPH sector is highly reliant on its workforce and on its increasingly interdependent supply chain in order to deliver services. <u>During emergencies, the sector must not only sustain but also increase its capacity. The sector's goal for service continuity is to</u>

[134] HHS, 2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf

maintain the ability to provide essential health services during and after disasters or disruptions in the availability of supplies or supporting services (e.g., water, power). It advances this goal through objectives related to Health Care Continuity, Supply Chain Continuity, Supporting Services Continuity, and Workforce Family Member Protection. Among the sector's key RMAs addressing these objectives are the HHS Hospital Preparedness Program; The Joint Commission's Accreditation Programs; RxResponse; preparedness and response activities of the Centers for Disease Control and Prevention (CDC) Public Health Emergency Preparedness Cooperative Agreement; Project Public Health Ready; and the U.S Food and Drug Administration's Drug, Biologic, and Medical Device Shortage Program. The JAWG has developed R&D/MS&A priorities in this area under the categories of Medical Surge Management, Continuity of Operations Planning (COOP), Medical Supply Chain Management, and Policy and Legal Considerations.

Workforce protection:

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
The sector's goal for workforce protection is to protect the sector's workforce from the harmful consequences of all hazards that may compromise their health and safety and limit their ability to carry out their responsibilities. It advances this goal through objectives related to Mass Prophylaxis and Health Surveillance. Among the sector's key RMAs addressing these objectives are the CDC Public Health Emergency Preparedness Cooperative Agreement (Disease Detection, Investigation Activities, and Mass Prophylaxis) and the Cities Readiness Initiative. The JAWG has developed R&D/MS&A priorities in this area under the categories of Workforce Sustainability and Biosurveillance.

2) Workforce and Surge Capacity

A) Worker Shortage Issues

Lister, 11
(S. A., Management: Issues in the 112th Congress Specialist in Public Health and Epidemiology. http://www.fas.org/sgp/crs/misc/R41646.pdf)
"The response to a mass casualty incident requires additional health care workers, those who provide direct care to the injured. The response to health incidents in general typically requires additional public health workers to track illnesses and injuries, monitor food and water safety, and take such other actions as needed to ensure health and safety among affected populations. The means to achieve and sustain surge capacity in the health care and public health workforces, especially in a climate of budget constraint, is one of the more persistent challenges in emergency management."

B) Surge Capacity: Hospital Beds

Lister, 11
(S. A., Management: Issues in the 112th Congress Specialist in Public Health and Epidemiology. http://www.fas.org/sgp/crs/misc/R41646.pdf)
"Facing growing cost constraints for several decades, the largely private health care sector has sought to avoid having the unused, reserve capacity (such as empty beds) that would be needed in such situations. Since 2001, the federal government has sought to establish this capacity in the private sector, with mixed success. For example, the Hospital Preparedness Program, run by the HHS ASPR, has provided about $3.8 billion in cooperative agreement funds to state and territorial governments from FY2002 through FY2010, to work with private health care facilities and systems in ensuring regional surge capacity in the event of a mass casualty incident. 28 Appropriations for the program are displayed in Figure 2."

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
The sector's goal for workforce protection is to protect the sector's workforce from the harmful consequences of all hazards that may compromise their health and safety and limit their ability to carry out their responsibilities. It advances this goal through objectives related to Mass Prophylaxis and Health Surveillance. Among the sector's key RMAs addressing these objectives are the CDC Public Health Emergency Preparedness Cooperative Agreement (Disease Detection, Investigation Activities, and Mass Prophylaxis) and the Cities Readiness Initiative. The JAWG has developed R&D/MS&A priorities in this area under the categories of Workforce Sustainability and Biosurveillance.

C) Laboratory Capacity

Lister, 11
(S. A., Management: Issues in the 112th Congress Specialist in Public Health and Epidemiology. http://www.fas.org/sgp/crs/misc/R41646.pdf)
The 112th Congress may consider issues associated with domestic biodefense laboratories, such as the effectiveness of current oversight efforts, the appropriate balance between security and the transparency that fosters scientific discovery, and possible effects of domestic regulatory approaches on international collaboration. 105 Legislation introduced in the 111 th Congress (S. 485/H.R. 1225) 106 would have required the HHS Secretary to review and report to Congress regarding, among other things, the adequacy of laboratory capacity, and information sharing between the biodefense and infectious disease communities. The Secretary would also have been required to develop minimal training standards for personnel, and to establish a voluntary reporting system through which laboratory personnel could report accidents and other incidents.

3) Physical Assets

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
Internationally, the sector has faced threats to physical assets in recent years, including this year's attack on Cama Hospital in Mumbai, India. Sector facilities are often vulnerable to physical attack due to their open nature, and some contain select agents 2 that invite theft. **The sector's goal for physical asset protection is to mitigate the risks posed by all hazards to the sector's physical assets. It advances this goal through objectives related to Biosafety Level (BSL)-3 and BSL-4 Facility Protection, Countermeasure Facility Security, Healthcare and Public Health Protection, and Research Facility Protection**. Among the sector's key RMAs addressing these objectives are the CDC Select Agent Program, the HHS Biomedical Advanced Research and Development Authority Program Office, and Hospital Protection Activities. The JAWG has developed R&D/MS&A priorities in this area under the category of Healthcare Facility Security (HFS).

4) Cyber Security

The expansion of computers as essential devices for medical care (medical records, tracking and identifying threats, automated care, prescription evaluation etc.) makes cyber-security a key aspect of HPH CIKR:

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
The rapid expansion of health information technology and high reliance on these systems for sensitive health and claims data make the sector increasingly vulnerable to the consequences of cyber attacks. The sector's goal for cybersecurity is to mitigate the risks to the sector's cyber assets that may result in disruption to or denial of health services. It advances this goal through objectives related to Cyber Network, System, and Data Protection. Section 5.4 of this report details several activities the sector has undertaken to advance cybersecurity.

To answer the basic question of is policy change needed?:

Status quo HPH CIKR is not perfect. The CRS indicates that very difficult policy based decisions in terms of issues of future threats, authority of action, and funding allocations lie ahead for the federal government:

Gottron, and Shea, 10
(Gottron, F., & Shea, D. A. (2010). Federal Efforts to Address the Threat of Bioterrorism: Selected Issues for Congress Retrieved from http://fpc.state.gov/documents/organization/140765.pdf)
While no mass-casualty bioterrorism event has yet occurred, some experts and policymakers assert that terrorist organizations are attempting to develop such a capability. The federal government has been preparing for a bioterrorism event for many years. Multiple programs in many agencies attempt to prepare for and respond to a bioterrorism event. Whether these programs are sufficient, redundant, excessive, or need improvement has been a topic of much debate. Congress, through oversight activities as well as authorizing and appropriations legislation, continues to influence the federal response to the bioterrorism threat. Congressional policymakers will likely be faced with many difficult choices about the priority of maintaining, shrinking, or expanding existing programs versus creating new programs to address identified deficiencies. Augmenting such programs may incur additional costs in a time of fiscal challenges while maintaining or shrinking such programs may be deemed as incurring unacceptable risks, given the potential for significant casualties and economic effects from a large-scale bioterror attack.

T Definition Debate: Protection vs. Resiliency and Additions

I agree with the opening chapter of the topic paper that protection and resiliency do not have clearly defined and agreed upon distinctions within a large portion of relevant HPH-CIKR advocacy literature. A document provided by the HHS, and reprinted by a state government, provides a contextual distinction that is important to note for the topic committee:

"Protection":
CIKR Protection: Given the relatively large number of sector assets, particularly hospitals and clinics, protecting and preventing damage to any one asset is less vital than the ability to continue to deliver care. The focus is more on the sector as a system that must remain resilient in the face of all hazards. The HPH Sector focuses on consequence management as a form of risk reduction, integrating CIP principles with surge planning, response and recovery operations.[135]

[135] HHS. (No date). National Infrastructure Protection Plan: Healthcare and Public Health Sector. Retrieved from http://www.bhs.idaho.gov/Pages/Plans/CIKR/Public Health.pdf.

"Resiliency"

> The HPH Sector's vision is to achieve overall resiliency against all threats—natural and man-made. Implementing this vision will prevent or minimize damage to, or destruction of, the Nation's healthcare and public health infrastructure. It will also preserve the sector's ability to mount timely and effective responses to both routine and emergency situations as it strives to protect its critical workforce from harm resulting from terrorist or criminal activities, natural disasters, and serious infectious disease outbreaks, including those originating outside the United States.

More evidence:

> The Healthcare and Public Health SSP addressed resiliency. For example, in an emergency, healthcare capabilities are to be coordinated within the sector to ensure resiliency across other CIKR sectors because these sectors rely on the healthcare sector for their resiliency. According to an SSA representative, the 2010 SSP will be more in-depth than the 2007 SSP in certain sections. For example, the 2010 SSP will focus on workforce and supply network resiliency because the Healthcare and Public Health sector is generally made up of systems and networks. (GAO, March 2010, p. 34).

While a distinction is clear in the quoted text provided here, the 2009 HHS report uses the two terms under the umbrella of a "single mission" "R&D and Other CIKR Protection and Resiliency Mission Needs." Furthermore, and I think this is the clearest example in how "protection" and "resiliency" are used synonymously:

> **Public Health Emergency, No Date**
> (http://www.phe.gov/preparedness/planning/cip/Pages/default.aspx)
> The Healthcare and Public Health Sector Critical Infrastructure Protection Program, in the Office of the Assistant Secretary of Preparedness and Response, leads a unique public and private sector partnership in protecting the essential goods, services, and functions of healthcare and public health that, if destroyed or compromised, would negatively affect the Nation. …
> What we do:
> • Implement the NIPP sector partnership and risk management framework
> • Develop protective programs to protective actions to defend against, prepare for, and mitigate the consequences of a terrorist attack or other hazards
> • Provide guidance on sector critical infrastructure protection in line with NIPP
> • Measure the sector's performance toward sector protection priorities
> • Encourage information sharing among all sector partners
> • Submit an annual sector plan and an annual sector report.
> Key Initiatives
> The Critical Infrastructure Program is currently pursing a number of key initiatives centered around critical infrastructure protection, information sharing, research and development, and risk assessment. Learn More.
> Sector vision statement:
> • The Healthcare and Public Health Sector will achieve overall **resiliency** against all threats — natural and manmade
> • Prevent or minimize damage to, or destruction of, the Nation's healthcare and public health infrastructure
> • Preserve its ability to mount timely and effective responses to both routine and emergency situations
> • Strive to protect its critical workforce from harm resulting from terrorist or criminal activities, from natural disasters, and from serious infectious disease outbreaks, including those originating outside the United States.
> These snapshots provide concise overviews of various aspects of the Critical Infrastructure Protection Program and the Healthcare and Public Health Sector.

I believe a decent argument exists to include "resiliency" in the event HPH is included in the final topic wording. From limited research experience, the best literature in terms of availability and scholarly work does not contain a distinct resiliency vs. protection focus. Rather most articles fluidly move amongst issues of increasing worker/infrastructure surge capacity, and preventing worker attrition during a crisis. If protection is the key word in the final topic, the resolution may split hairs and limit action to security force detail for physical assets, detection of bio-pathogens, and cyber-security issues. The debate may be made stale at the cost of losing rich controversies in the literature on Medical and public health care during crisis situations.

Research also provides room for two more words to be included in the topic committee's inclusion of HPH:

"Preparedness" or "Response"

Additional suggested wordings may include "preparedness":

> **DHS 07**
> (Homeland Security Presidential Directive 21: Public Health and Medical Preparedness. Retrieved from http://www.dhs.gov/xabout/laws/gc_1219263961449.shtm.)
> Homeland Security Presidential Directive 21: Public Health and Medical Preparedness (October 2007)
> HSPD-21 establishes a National Strategy for Public Health and Medical Preparedness. The Strategy draws key principles from the National Strategy for Homeland Security (October 2007), the National Strategy to Combat Weapons of Mass Destruction (December 2002), and Biodefense for the 21st Century (April 2004) that can be generally applied to public health and medical preparedness. Implementation of this strategy will transform our national approach to protecting the health of the American people against all disasters.

While preparedness may seem awkward the term has precedence in use as it was in the title of a major piece of legislation: "Pandemic and All-Hazards Preparedness Act addresses public health security and all-hazards preparedness and response."[136]

Affirmative Ground

This section includes a few potential affirmative areas. The list is not exhaustive and should not be treated as such. As occurs every year, the community will need to determine what is a "substantial" increase in [select verb] would be. The quotations provided should provide a decent taste of what an HPH critical infrastructure topic would include.

1) Establish mechanisms for compensation and preparation of medical surge related issues during pandemics

> **Lister, 07**
> (S. A., The Public Health and Medical Response to Disasters: Federal Authority and Funding. Retrieved from http://lieberman.senate.gov/assets/pdf/crs/publichealthdis.pdf)
> ESF-8 Funding Needs During a Flu Pandemic. While a severe flu pandemic may constitute a national catastrophe, requiring a robust ESF-8 public health and medical

[136] CRITICAL INFRASTRUCTURE PROTECTION Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. http://www.gao.gov/new.items/d10296.pdf) March 2010

response, funding needs may not be readily addressed through existing assistance mechanisms pursuant to the Stafford Act (to the extent that they apply), and could outstrip existing government and private resources. While the need for public health and medical services could be considerable, extensive damage to public or private infrastructure is not anticipated. Costs associated with workforce surge capacity (e.g., overtime pay) and consumption of certain supplies (e.g., for public health laboratory tests) could increase substantially. Presuming a surge of patients in the healthcare system, non-urgent procedures (which are often more lucrative) could be postponed for weeks or months at a time. This has raised questions regarding whether there would be shifts in overall revenue to providers for services rendered during a pandemic, and how such shifts could affect providers and insurers. Finally, the cost of providing healthcare services during a pandemic, when almost 46 million Americans lack health insurance, is of concern to many. Some are concerned that disease control efforts could suffer if some subgroups of the population were unwilling, because of their insurance status or for other reasons, to seek care or otherwise interact with disease control authorities during a pandemic. As previously noted, following Hurricane Katrina, Congress provided $2.1 billion to states to cover the states' usual share of Medicaid and SCHIP costs for storm victims for a defined time period, and the cost of uncompensated care for the uninsured. This federal assistance mechanism required legislative action and took nearly six months to enact, in the absence of a pre-existing mechanism to provide such federal assistance. Whether this could serve as a model for federal assistance during a flu pandemic is unclear. An important element of the discussion regarding the Katrina assistance was the desire to help both states that had been directly affected, and states that had assumed fiscal liability by accepting evacuees. While the element of victim displacement would not likely be seen during a pandemic, Congress may nonetheless debate the merits of expanding federal assistance for healthcare costs during a flu pandemic, and the model developed following Hurricane Katrina may serve as a useful starting point for discussion.

2) Clarity in special circumstances and "temporary suspension" of jurisdiction during crisis

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
Through the examination of such past events as 9/11 and Hurricane Katrina, the need to address obstacles to response activities due to existing policy frameworks is clear. For example, the function of privileging to provide vaccinations is State regulated. However, if a response is regional – that is, it crosses State boundaries – the privileging of various healthcare professionals may be restricted, hindering a response function that may be critical. The R&D/MS&A CIPAC JAWG made the following recommendations to address these obstacles: Conduct policy research regarding existing logistics, mobilization, and distribution practices in the face of major disasters or disruptions. The focus should be on State and Federal laws and processes that influence the supply chain during a disaster. Research the effectiveness of temporary suspension of certain Federal, State, and local laws, rules, and regulations governing response functions. The results of this research could be best demonstrated by leveraging modeling and simulation tools to predict the successes and/or failures of a response under the "temporary suspension" framework.

3) Federal Quarantine Law Expansion:

Clarkson, 10
J. T. (2010). Phase Six Pandemic: A Call To Re-Evaluate Federal Quarantine Authority Before The Next Catastrophic Outbreak. *Georgia Law Review*
"It is indeed not well for Congress to wait with the passage of a national quarantine law until anarchy again, as it did last summer, threatens the commercial relations of the states." This proposal did not come from a 2009 newspaper or scholar but rather from an

article written in the aftermath of an outbreak of yellow fever in 1905. Dean William Walz's view may have been ambitious in his time; however, his prescient call to action is even more relevant today in light of modern health threats. In order to fully protect against dangerous pandemics, the federal government should have the ability to enact large-scale quarantines in the event of an inadequate local response.

Clarkson continues…

This Part will outline constitutional arguments to support reform, review the shortcomings of the current framework, and conclude with a legislative solution. a. constitutional underpinning for large-scale federal quarantine As stated earlier, the Commerce Clause is the enumerated power that provides the basis for federal quarantine authority ... If we can successfully reform quarantine laws now, then we can prevent unwanted shifts in power and we can avoid straining to justify large- scale quarantine authority under the vague and broad current authority. … it is clear that Congress should revise § 264 of the PHSA in order to give the federal government power to institute large-scale quarantines in a pandemic crisis. ... Reform is necessary to acknowledge that the federal government may be best positioned to respond to national health threats and to create limits on federal power to ensure a proper balance of power between the states and the federal government.

4) Military involvement: Posse Comitatus

Batlan, 07
(F. j. Law In The Time Of Cholera: Disease, State Power, And Quarantines Past And Future. *Temple Law Review*.)
The Plan is not comforting. Some current models predict that avian flu could lead to the deaths of between 200,000 and 2,000,000 people in the United States. Absentee rates of up to forty percent of the work force could cause the disintegration of the nation's infrastructure, threatening the ability to supply and access critical goods and services and crippling the economy. At least for some, "the avian influenza outbreaks have provoked fears of an influenza pandemic reminiscent of the great plagues in world history." The Plan addresses the possibility of a variety of different types of quarantines, significant domestic [*58] travel restrictions, and the closure of U.S. borders. President Bush has endorsed the use of the military to maintain quarantines. As George Annas wrote in October 2005: We have moved quickly in the past month, at least metaphorically, from the global war on terror to a proposed war on hurricanes, to a proposed war on bird flu.

More…

Sciarrino,06
(A. J. (2006). The Grapes of Wrath and the Speckled Monster, Part III: Epidemics, Natural Disasters and Biological Terrorism-The Federal Response. Journal of Medicine and Law)
Without doubt, the present NRP "creates confusion about federal active duty military involvement due to unresolved tension between the possible need for active duty military assistance when state and local officials are overwhelmed, and the presumption that a governor will use his or her understanding of the situation on the ground to decide whether and when to ask for active duty military support," for the support that can be given by the military is substantial.

5) Funding and transparency of preparedness programs

Levi, Vinter, and Segal, 07
(Levi, J., Vinter, S., & Segal, L. M. (2007). Ready or Not? Protecting the Public's Health from Diseases, Disasters and Bioterrorism. Retrieved from http://healthyamericans.org/reports/bioterror07/BioTerrorReport2007.pdf)

The report also evaluates federal progress in preparing the country for bioterrorism, disasters and disease. TFAH finds that the passage of the Pandemic and All-Hazards Preparedness Act (PAHPA) of 2006, issuance of presidential directives, and start-up of the new Office of the Assistant Secretary for Preparedness and Response (ASPR) are significant steps forward. Major challenges that remain include assuring adequate funding for the ASPR's key programs, such as the Biomedical Advanced Research and Development Authority (BARDA), and delivering on the requirements of PAHPA to increase transparency and accountability in all federally-funded preparedness programs.

6) Increase workforce hires and staff capacity

Lister, 11
(S. A., Management: Issues in the 112th Congress Specialist in Public Health and Epidemiology. http://www.fas.org/sgp/crs/misc/R41646.pdf)
The CDC PHEP cooperative agreements, discussed earlier, provide funds that state and territorial grantees can use to pay for recruitment, training, and salaries. However, grantees have had difficulty recruiting and retaining qualified personnel with these "soft" funds, and may face other impediments, such as hiring freezes, that are not ameliorated by the federal funds. In addition, the amount of funding limits the extent to which it can effectively bolster the public health workforce at the local level. (The extent to which funds "pass through" from states to localities for this or any other purpose is unclear.) It is reported that the recent recession has led to significant staff contraction in local health departments.

7) Risk Assessment Methodology reform

For example, the SSA representative for the Healthcare and Public Health sector told us that his agency planned to contact DHS to discuss a change that is designed to make the SSP risk assessment methodology consistent with the NIPP, but could be impractical for the SSA to implement. The Healthcare sector representative said a single risk assessment methodology would not be feasible for the Healthcare and Public Health sector because it is composed of different kinds of partners, such as emergency medical personnel, doctors, and hospitals and is made up of systems— transportation, communication, personnel—as opposed to other sectors which he said may be made up predominantly of facilities. The SSA representative said this makes the use of a single risk assessment methodology difficult for the Healthcare sector. (GAO, March 2010, p. 20).

8) Pandemic/Bioterror attacks: Need for consistent/well defined and ethical hierarchy of who received limited health care supplies

Katz, 08
(M., Bioterrorism and Public Law: The Ethics of Scarce Medical Resource Allocation in Mass Casualty Situations. Journal of Legal Ethics)
The threat of bioterrorism poses formidable ethical and legal challenges. In the event of a bioterror attack, medical providers and public **health** officials may be called upon to deliver or administer medical resources to vulnerable populations. If those resources are insufficient in quantity to treat these populations, many people who vitally need aggressive medical care will not have access to it. Public **health**officials will have to allocate [n1] scarce medical resources and devices within these vulnerable populations, implicitly opting to save certain lives at the expense of others. [n2] **Health** care providers will be in the conspicuous and unfortunate [*796] position of turning away many deathly ill people. [n3] Under intense pressure, **health** care providers operating without proper guidance may make inconsistent decisions that do not reflect sound public **health** policy. Accordingly, to guide allocation and to ensure that it does not disrupt or undermine recovery efforts, it is imperative that clear plans for medical resource allocation are made in advance of bioterrorism and other mass casualty situations. … In sum, decision-

makers need a system that is capable of clearly answering a most difficult question: Who shall live when not all can live?[137]

9) Improving Government Sharing/Tracking information – to determine outbreak. An aff could deal with biosensors as well as trading vital medical records.

Smith, 09
(G. P. (2009). Re-shaping the Common Good in Times of Public Health Emergencies: Validating Medical Triage. Annals of Health Law)
On July 17, 2007, the government issued an update [n210] on the Pandemic Influenza Implementation Plan originally released on November 1, 2005. [n211] **This new assessment of progress shows - rather strikingly - the weakness in the federal government's ability to both detect an outbreak of the flu or to even track the progress of it as it moves throughout the country**.

More:

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
The sector has determined that information sharing is a critical priority. This presents both opportunities and challenges. Much of the information that is helpful to non-Federal agency partners in their CIP efforts is sensitive. It may relate to sector vulnerabilities or intelligence gathering and must therefore be kept secure. Much of this information is controlled under the FOUO designation, while other information is PCII or Classified information. Some information relevant to the HPH sector is also protected under HIPAA. The sector must share information efficiently and effectively while keeping it secure. Valuable information should be easily accessible to individuals who need it. However, not all information is valuable to all individuals; its dissemination must be targeted to reduce information overload. When information is shared through mechanisms such as HSIN, it must be categorized in a way that makes it easy to retrieve. During an emergency response, this categorization becomes especially critical due to the urgency of the situation and time sensitivity of incident-related information. The sector must ensure that it shares targeted information without imposing an overly burdensome information collection process that slows information sharing.

10) Priority lists of mission critical locations/assets, triage and priority lists of anti-viral medications.

Smith, 09
(G. P. (2009). Re-shaping the Common Good in Times of Public Health Emergencies: Validating Medical Triage. Annals of Health Law)
Overtime, the government will refine the priority list for individuals who will receive the flu vaccine first when an outbreak occurs and - as well - will develop more fully and then release plans for coordinated school [*28] closings between state and local governments. [n215] On July 17, 2007, the government issued an update [n210] on the Pandemic Influenza Implementation Plan originally released on November 1, 2005. [n211]

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
The sector has encountered challenges related to the prioritization of assets through the Tier 1/Tier 2 and CFDI processes. These challenges emerge primarily because of the

[137] Also See Berkman, B. E. (2009). Incorporating Explicit Ethical Reasoning Into Pandemic Influenza Policies. Journal of Contemporary Health Law & Policy for more on ethics and crisis health care
.

unique characteristics of the sector. Although the sector as a whole is critically important to protecting the life and health of every American, it is distributed geographically and across functional areas in such a way that it is rare for any one component to rise to the level of national criticality. For example, a large urban hospital might be critically important for a specific large city, but its criticality as part of the national healthcare infrastructure is much less clear. Any impact on a particular hospital would have a negligible effect on the delivery of healthcare in other parts of the country, and local impacts could be mitigated through mutual aid. Some HPH infrastructure assets are critical because of the secondary consequences they prevent. For example, vaccine manufacturers are critical in the prevention of death and disease from seasonal influenza, as well as by providing protection from tropical diseases and biological weapons to military personnel. The criticality of other assets varies depending on circumstances. For example, the destruction of a sole-source manufacturer of a countermeasure to pandemic influenza would not in itself have a catastrophic, immediate impact on lives and health. However, the national impacts would be catastrophic if this were to happen in conjunction with an actual pandemic. To prioritize assets of this type most accurately requires an additional level of analysis that **remains to be fully developed**.

11) Funding for anti-virals

Smith, 09
(G. P. (2009). Re-shaping the Common Good in Times of Public Health Emergencies: Validating Medical Triage. Annals of Health Law)
The HHS Plan recommendations take into great consideration the limited supply of medications that would be available in a pandemic, as well as the strain on healthcare systems when patients flood the hospitals. One goal of the plan is to target vaccination toward groups that are most susceptible to illness to keep those individuals out of hospitals. In the event that those who are less susceptible to the virus fall ill and come to the hospital, there will be beds, nurses, antiviral medications, and other medical necessities available to them. Also, those individuals with compromised immune systems not likely to be protected by a vaccine will not be provided one, because vaccinating those individuals would be futile and others who may benefit from the vaccination would not receive one. E. Implementation Plan Update On July 17, 2007, the government issued an update [n210] on the Pandemic Influenza Implementation Plan originally released on November 1, 2005. [n211] **This new assessment of progress shows - rather strikingly - the weakness in the federal government's ability to both detect an outbreak of the flu or to even track the progress of it as it moves throughout the country**.

12) Federal-State unification of priorities

Lister, 11
(S. A., Management: Issues in the 112th Congress Specialist in Public Health and Epidemiology. http://www.fas.org/sgp/crs/misc/R41646.pdf)
Second, states and localities, rather than the federal government, are the seats of most authority and responsibility for the oversight of both health care and emergency management. For example, state laws generally authorize governors to order and enforce the evacuation of residents in emergency situations. Except under extraordinary circumstances, the federal government generally does not dictate the conduct of either health care or emergency management activities to state or local officials, or to health care providers. **The federal government can, however, attach conditions to the expenditure of federal grant funds, in furtherance of national goals.**

Negative Ground

1) Resource Tradeoff

The government is trending towards cutting and reducing the reserve of what on-face is perceived to be unnecessary preparation for future threats. I believe the HHS resource tradeoff DA will be well developed by the first tournament of the year.

HHS, 09
(2009 Sector CIKR Protection Annual Report for the healthcare and public health sector.http://www.phe.gov/Preparedness/planning/cip/Documents/2009_sar_annual_rpt.pdf)
The government and private sector partners within the HPH sector face a number of competing demands on resources. The healthcare industry must find ways to serve patients in an increasingly challenging business environment. Government public health agencies must continue to develop preparedness and response capabilities in an environment of diminishing resources. While some sector partners embrace the value of the sector's CIP efforts, those efforts must be prioritized against important patient service and emergency response missions that continue to demand more time and resources.

2) Court counterplans and locality backlash

O'Leary, 06
(N. P. M. (2006). Bioterrorism or Avian Influenza: California, The Model State Emergency Health Powers Act, and Protecting Civil Liberties During a Public Health Emergency. California Western Law Review)
In addressing these types of threats, it is important to note that in the United States the responsibility for safeguarding public **health** falls largely to the states under their police powers. [n20] Under the Tenth Amendment, "powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." [n21] Accordingly, in attempting to draft legislation necessary to protect the public safety during either a bioterror attack or during a large-scale outbreak of an infectious disease, planners focused on the powers of state officials to quell the threat.[n22] The result was the Model State Emergency **Health** Powers Act (Model Act), upon which many states now base their legislation. [n23] Although many see the Model Act as a significant attempt to protect the public, opponents view it as a monumental threat to the civil liberties of all Americans, including Californians. [n24] The power to isolate or quarantine individuals simply thought to be infected, compel the collection and reporting of a person's private **health** information, appropriate vaccines and medications, and even force persons identified as **health** risks to undergo treatment is too much for many who criticize the broad authority granted under the Model Act.

3) Referendum CP

Katz, 08
(M., Bioterrorism and Public Law: The Ethics of Scarce Medical Resource Allocation in Mass Casualty Situations. *Journal of Legal Ethics*.)
Once the dialogue between the government and the public progresses to the point that public **health** officials and policy-makers are satisfied that allocational plans have been refined, the proposals ought to be submitted for a public vote in the form of a national nonbinding referendum. **[n167]** Members of the public will have the opportunity to formally express their opinions on each of the various [*821] proposals.**[n168]** All of the proposals submitted for referendum are likely to be efficacious and the product of good public **health** policy because they will have previously passed through the extensive processes of drafting, critique, and refining discussed above. Just as there may be no correct decision, **[n169]** it is unlikely that any of the options put forth in this referendum will be incorrect. Nonetheless, the process of referendum is uniquely valuable; the people will feel that they, not the government, are ultimately deciding how to allocate scarce medical resources. If the chosen plan achieves desirable results, the people will feel a sense of accomplishment and the communitarian ethic surrounding recovery efforts will be

strong. [n170] Although a strong communitarian ethic will not render the decision to take an elderly patient off a ventilator to supply it to an ill fifteen-year-old any easier for the unfortunate healthcare worker who is chosen to do this or for the family of the elderly patient to hear about the decision later, hopefully the public as a whole will be understanding and relatively supportive, even if devastated. Alternatively, if the plans prove less than successful, the public, having gone through the process of referendum, will hopefully accept that its fate was not preventable. In either case, the public will not resent the government and wish to rebel against it, but will rally around it in opposition of those who used the terrible weapon of bioterrorism against them.

4) Public/Private Cooperation

The Healthcare and Public Health Sector-Specific Plan (SSP) was created to complement the National Infrastructure Protection Plan (NIPP) by developing efforts to improve the protection of the sector in an all-hazards environment. The Healthcare and Public Health SSP establishes a relationship between government and the private sector to foster the cooperation necessary to improve the protection of the sector from a natural or manmade disaster. The plan sets a path forward for the sector to collectively identify and prioritize its assets, assess risk, implement protective programs, and measure the effectiveness of its protective programs. This document reflects the collaborative efforts between government stakeholders and public and private sector members who are dedicated to the protection of key resources within the Healthcare and Public Health Sector. The Department of Health and Human Services (HHS), in its role as Sector-Specific Agency (SSA), and in collaboration with government and private sector security partners, developed this SSP. The sector is highly diverse in its composition and relationships with its many systems, networks, services, facilities, functions, and roles, both public and private, needed to prevent disease and disability, treat patients, foster public health, and respond to incidents requiring medical and public health services. The private sector, as well as various Federal, State, and local agencies, provide healthcare and public health services and participate in ongoing surveillance and detection of potentially devastating threats to the Nation's critical infrastructure and key resources (CI/KR) from terrorism and other manmade and natural threats. If these threats were realized, the result could seriously impact public health and economic vitality. In addition, many other sectors rely on Healthcare and Public Health Sector assets and services to ensure resiliency in the face of threats that may result in serious public health consequences (e.g., pandemic influenza). The SSP is divided into eight sections based on guidance promulgated by the Department of Homeland Security (DHS) to ensure some consistency across all sectors. All sector specific plans are re-written on a tri-annual basis with the next iteration due in 2010. The Healthcare and Public Health Sector Specific Plans seek to accomplish the following. Reflects unprecedented coordination among the Sector's public and private partners. Our Sector Partnership Model encompasses Federal, State, local, Tribal, Territorial, and private sector organizations, including owners, operators, and large trade organizations and national associations. Provides the road map for strengthening vital infrastructure and reducing vulnerability to all hazards-terrorist attacks and natural disasters alike. Establishes a sector-specific risk-reduction consultative network to exchange best practices and to facilitate rapid threat-based information sharing among the sector's security partners. (HHS, p http://www.phe.gov/Preparedness/planning/cip/Pages/ssp.aspx)

5) "Process CPs" and solvency questions of Public Trust

Smith, 09
(G. P. (2009). Re-shaping the Common Good in Times of Public Health Emergencies: Validating Medical Triage. Annals of Health Law)

The HHS Plan does provide for the vaccination of those who are in regular contact with individuals with compromised immune systems. [n162] Pregnant women are in a high priority group of those vaccinated because it was observed from past pandemics that pregnant women were at high risk, and that vaccinations will also protect infants who cannot be vaccinated. [n163] Since children less than six months of age cannot be vaccinated, those in household contact with children of that age are to be vaccinated. [n164] In prioritizing these groups of individuals, the triage system is fulfilling the parent role principle because both the caretakers and pregnant women have others who are dependent upon them for survival. [n165] It would therefore be in the best interests of the community to allow for those individuals to continue caring for their dependents so as to conserve the resource of the **health** care system. Finally, public **health** officials are playing a critical role in the pandemic response; thus key government leaders making decisions and implementing the response are to be vaccinated to maintain its continuity. [n166] Tier 2 protects healthy individuals aged sixty-five and older, healthy infants aged six to twenty-three months and those six months old to sixty- [*23] four years old with high-risk conditions of influenza. [n167]These groups are at less of an increased risk than those in Tier 1; nevertheless, they are still at a high risk for influenza. [n168] Here, the HHS Plan continues to try to solve the problem of the scarcity of **health**care resources by providing these high-risk groups with preventative vaccination. [n169] Hopefully, it will eliminate the need for future treatment in hospitals by conserving the resources for others. [n170] Included in this Tier are other public **health** emergency responders, public safety workers (police, fire, 911 dispatchers and correctional facility staff), utility workers (power, water, and sewage), transportation workers (fuel, water, food, and medical supplies), and telecommunications workers. [n171] These workers are important for maintaining the continuity of societal functions and **critical infrastructure,** and thus are valued contributors to society. [n172] Here, the HHS Plan is providing a federal guideline for the states, which the states must modify to suit the needs of their communities and citizens. [n173] In order for a state to determine effectively which social functions are essential, the affected populations in the community must be encouraged to cooperate, so that state officials may understand the values and priorities of the affected communities. [n174] However, when a state or locality develops a plan to maintain the social order in a time of crisis, it is important that the public is encouraged to cooperate and participate in its development so the public perceives the triage standards as fair. [n175] When the public is regarded as a partner and an ally in the planning effort, public confidence and trust in the process is established. [n176]When the public understands the rationale and has participated in the process by contributing their values and priorities, social disruption will be minimized during the pandemic. [n177] Prior to a **health** emergency, the government must maintain the public's trust, and achieving this trust will be more likely if the public "participates in setting [the] procedures and material criteria and ... in determining what to emphasize [*24] in medical utility, which functions and roles are essential in judgments of narrow social utility."

6) Jurisdiction issues - Indigenous Peoples

See: (Burleson, 2007)

7) Business Confidence

Lister, 11
(S. A., Management: Issues in the 112th Congress Specialist in Public Health and Epidemiology. http://www.fas.org/sgp/crs/misc/R41646.pdf)
Finally, while most public health functions—broad, population-based programs, such as restaurant inspections to ensure food safety—are inherently governmental, the nation's health care system—which delivers professional health care services to individuals—is primarily private and for-profit. Providers and facilities operate in an increasingly competitive marketplace in which emergency planning is not always seen as a necessary

expense. For example**, hospitals may be reluctant to maintain empty beds or to stockpile costly medical products to be ready for incidents that may not occur.**

Also see Joseph P. McMenamin, “Pandemic Influenza: Is There A Corporate Duty To Prepare?” *www.ncbi.nlm.nih.gov/pubmed/19998573*

Information Technology

> Imagine the lights in this room suddenly go out, and we lose all power. We try to use our cell phones, but the lines of communication are dead. We try to access the Internet with our battery-powered laptops, but the Internet, too, is down. After a while, we venture out into the streets to investigate if this power outage is affecting more than just our building, and the power is indeed out as far as the eye can see. A passer-by tells us the banks are closed and the ATMs aren't working. The streets are jammed because the traffic lights are out, and people are trying to leave their workplaces en masse. Day turns to night, but the power hasn't returned. Radio and TV stations aren't broadcasting. The telephone and Internet still aren't working, so there's no way to check in with loved ones. After a long, restless night, morning comes, but we still don't have power or communication. People are beginning to panic, and local law enforcement can't restore order. As another day turns to night, looting starts, and the traffic jams get worse. Word begins to spread that the US has been attacked- not by a conventional weapon, but by a cyber weapon. As a result, our national power grid, telecommunications, and financial systems have been disrupted- worse yet, they won't be back in a few hours or days, but in months. The airports and train stations have closed. Food production has ceased. The water supply is rapidly deteriorating. Banks are closed so people's life savings are out of reach and worthless. The only things of value now are gasoline, food and [*321] water, and firewood traded on the black market. We've gone from being a superpower to a third-world nation practically overnight.[138]

Introduction

The above scenario highlights the pervasive nature of our dependence on Information Technology (IT) and its security. Should this critical infrastructure fail due to intentional attack or accidents, every aspect of our daily lives would be greatly affected. According to the DHS National Infrastructure Protection Plan, the IT critical infrastructure sector is defined as,

> The Information Technology (IT) Sector has a key role in securing the Nation's cyberspace. **The IT Sector is composed of entities**—owners and operators and their respective associations—**who produce and provide hardware, software, and IT systems and services, including development, integration, operations, communications, and security**. **The IT Sector is comprised of, but not limited to, the following: Domain Name System root and Generic TopLevel Domain operators; Internet Service Providers; Internet backbone providers; Internet portal and e-mail providers; networking hardware companies; and other hardware manufacturers, software companies, security services vendors, communications companies that characterize themselves as having an IT role, edge and core service providers, and IT systems integrators**. In addition, **Federal State, and local governments participate in the IT Sector as providers of government IT services that are designed to meet the needs of citizens, businesses, and employees**.[139]

The significance of these IT networks are great, as every aspect of our economy and our military systems would be affected by a major attack on or failure of the IT sector. As Rebecca McFadyen explains in 2009,

---

[138] Rebecca C.E. McFadyen, 2009, "Article: Protecting the Nation's Cyber Infrastructure: Is the Department of Homeland Security Our Nation's Savior or the Albatross Around Our Neck?," I/S: A Journal of Law & Policy for the Information Society, Summer, pp. LN

[139] "Information Technology Sector," No Date, http://www.dhs.gov/xlibrary/assets/nipp_it.pdf

> **According to Richard Clarke, the former Chair of the President's Critical Infrastructure Protection Board, the threat to cyberspace is "really very easy to understand. If there are major vulnerabilities in the digital networks** that make our country run, **then someday, somebody will exploit them in a major way doing great damage to the economy**." n113 Clarke explained that the exploitation of such vulnerabilities will likely be devastating. "**Transportation systems could grind to a halt. Electric power and natural gas systems could malfunction. Manufacturing could freeze. 911 emergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled . . . our forces [will be] at great risk by having their logistics system fai**l." n114 **The potential for panic among the American people is real, and it is frightening**. Accordingly, this article explores the persistent threats to the nation's cyber security and the Department's efforts to combat those threats, and concludes that **the current organizational infrastructure of the [DHS] is ill-conceived and ill-equipped to secure the nation's cyber infrastructure**.[140]

Even more problematic is that every one of our CIKRs depends on the IT sector, making it one of the most important CIKRs. As a 2004 GAO report notes,

> **Our nation's critical infrastructures include those assets, systems, and functions vital to our national security, economic need, or national public health and safety**. Critical infrastructures encompass a number of sectors, including many basic necessities of our daily lives, such as food, water, public health, emergency services, energy, transportation, information technology and telecommunications, banking and finance, and postal services and shipping. **All of these critical infrastructures increasingly rely on computers and networks for their operations. Many of the infrastructures' networks are also connected to the public Internet. While the Internet has been beneficial to both public and private organizations, the critical infrastructures' increasing reliance on networked systems and the Internet has increased the risk of cyber attacks that could harm our nation's infrastructures**.[141]

As a result, potential affirmative advantage ground in this sector is almost limitless. Additionally, these impacts fall into two types of scenarios: civilian and military attacks. The previous evidence illustrates the broad range of civilian scenarios that are possible, which could include:

- Banking/financial system collapse/attack
- Energy sector collapse/attack
- Transportation collapse/attack
- Manufacturing collapse/attack
- Health care system collapse/attack

The second type of scenarios includes cyber-attacks on U.S. military systems. Currently, there are almost constant cyber-attacks against U.S. military information systems. And these attacks are increasing in intensity and precision. As Rebecca McFadyen in 2009 explains,

> Carpenter's description of the cyber hackers' proficiency and sense of purpose is not an exaggeration. **Consider this series of coordinated attacks on American interests. On November 11, 2004**, at 10:23 PM Pacific Standard Time ("PST"), **Chinese hackers**

[140] Rebecca C.E. McFadyen, 2009, "Article: Protecting the Nation's Cyber Infrastructure: Is the Department of Homeland Security Our Nation's Savior or the Albatross Around Our Neck?," I/S: A Journal of Law & Policy for the Information Society, Summer, pp. LN
[141] "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," May, http://www.gao.gov/new.items/d04321.pdf

> **detected a vulnerability at the United States Army Information Systems Engineering Command** at Fort Huachuca, Arizona. n147 **At 1:19AM** PST, **hackers then attacked the same vulnerability in computers at the military's Defense Information Systems Agency in Arlington, Virginia**. n148 **Again, at 3:25 AM** PST, **the hackers hit the Naval Ocean Systems Center**, a defense department installation in San Diego, California. n149 **And again, at 4:46 AM** PST, **the hackers penetrated the Army's Space and Strategic Defense Installation** in Huntsville, Alabama. n150 Regarding these attacks, Allen Paller, director of the SANS Institute, stated: **The precision of the attacks, the perfection of the methods and the 24-by-seven operations over two and a half years, and the number of workstations involved are simply not replicated in the amateur criminal community** . . . . **[T]his is an order of magnitude more disciplined than anything I have seen out of the hacker or amateur criminal community**. n151 Paller noted that "[t]hese attacks come from someone with intense discipline . . . . [These hackers] were in and out with no keystroke errors and left no fingerprints, and created a backdoor in less than [*347] thirty minutes. How can this be done by anyone other than a military organization?" n152 **More recently, in June 2007, cyber hackers attacked the computer networks servicing the Pentagon**. The Pentagon acknowledged that this particular cyber attack forced officials to shut down computers that served the office of Defense Secretary Robert Gates. n153 **Although the Pentagon did not confirm the exact number of affected computers, estimates placed the number around 1,500**. n154 Regarding the attacks, Secretary Gates stated, "Elements of the OSD unclassified e- mail system were taken offline yesterday afternoon, due to a detected penetration." n155 Characterized as the most successful cyber attack to date on the United States Defense Department, n156 a person familiar with the attack said the officials believe with a "very high level of confidence . . . trending towards total certainty" that the People's Liberation Army of China ("PLA") perpetrated the June 2007 attack. n157 Gates also offered this sobering comment: "**The reality is that the Defense Department is constantly under attack . . . hundreds of attacks" per day**. n158 For example, **in 2005, the Pentagon recorded more than 79,000 attempted intrusions. Approximately 1,300 of such attempts were successful**, including the penetration of systems linked to the Army's 82nd and 101st Airborne Divisions and the 4th Infantry Division. n159 **Furthermore, more attempts to scan the systems that** [*348] **serve the Defense Department originate in China than in any other country in the world**.[142]

There is great concern that these Denial of Service (DoS) attacks will be used preemptively to cripple U.S. defenses for more catastrophic attacks on U.S. soil and resources.[143] In addition to these kinds of DoS attacks by other nation-states, there is a growing threat that terrorists and organized crime groups will also target information systems to cripple U.S. civilian and military systems. As the GAO reports,

> For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security, during a Senate hearing, when he stated that **although to date none of the traditional terrorists groups, such as al Qaeda, had used the Internet to launch a known assault on an American infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan**. Also, in February 2002, the Director of Central Intelligence testified before the Senate Select Committee on Intelligence on the possibility of cyber warfare attacks by terrorists. **He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and**

[142] "Article: Protecting the Nation's Cyber Infrastructure."

[143] Michiko Kakutani April 26, 2010, The Attack Coming From Bytes, Not Bomb, The New York Times, http://www.nytimes.com/2010/04/27/books/27book.html

> **other foreign adversaries become more familiar with these targets and the technologies required to attack them**. According to the FBI, **terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping programs** ("sniffers") **that can destroy, intercept, degrade the integrity of, or deny access to data** (see table 9).[144]

There are a couple of scenarios that might stem from these DoS attacks on military systems. The first involves immobilizing U.S. forces that are in the field. As modern military forces are more dependent on information systems to coordinate troop movement and battle, they are increasing vulnerable to cyber-attacks that seek to stop them.[145] Second, and the greater nightmare scenario, is that these attacks could be directed at U.S. nuclear forces, which risks accidental nuclear launch and retaliation.[146]

While the federal government has implemented a host of policies and programs since 9-11 to counter the threat of cyber-attacks, these policies have done little to solve the problem and cannot keep up with innovations in hacker techniques and technology. For example, The Federal Information Security Management Act (FISMA) is frequently criticized as nothing more than a "paperwork exercise" that has no impact on security.[147] Also, the Homeland Security Act of 2002 and the DHS has failed to comprehensively protect private and public information systems. Additionally, a number of CIKR sector specific regulations to deal with cyber-security are criticized as slow and lacking authority to actually improve information system security.[148]

Affirmative Ground

An affirmative in this sector can take a number of approaches to significant improve the protection of the information technology sector.

Technology

One affirmative approach to increasing IT sector protection is to increase access to a number of control technologies, system integrity technologies, cryptography, audit and monitoring tools, and configuration management and assurance technologies.[149]

For instance, there are a number of ways that federal legislation and policy could be changed in order to increase protection for both civilian and government information systems. One such approach, as described by Kenneth Dam, Professor of Law at the University of Chicago and former deputy secretary of

---

[144] GAO, "Technology Assessment."

[145] Owens, Dunn & Lin (Eds.) (2009), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capacities," National Research Council, http://www.nap.edu/openbook.php?record_id=12651&page=9

[146] Stephen Cimbala, professor of political science at the Pennsylvania State University Delaware County Campus, Summer 1999, Armed Forces & Society: An Interdisciplinary Journal

[147] John Grant, 2010, Minority Counsel for the Senate Committee on Homeland Security and Governmental Affair, "Cybersecurity Symposium: National Leadership, Individual Responsibility: Will There Be Cybersecurity Legislation?," Journal of National Security Law & Policy, pp. LN.

[148] Grant, 2010, "Cybersecurity Symposium."

[149] GAO, "Technology Assessment."

state, and Herbert Lin, study director for the NRC's Committee to Study National Cryptography Policy, is to increase the use of advanced cryptography technology throughout the U.S.:

> Because cryptography is an important tool for protecting information and because it is very difficult for governments to control, **policymakers must recognize that the widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run**. **The proper role of national cryptography policy, therefore, is to facilitate a judicious transition from today's world of information vulnerability to a future world of information security, while meeting to the extent possible the legitimate needs of law enforcement, national security, and foreign policy**. **U.S. cryptography policy should be built on three principles: · The broad availability of cryptography to all legitimate elements of U.S. society; · Continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy**, including but not limited to U.S. computer, software, and communications companies; · **Public safety and protection against foreign and domestic threats**. The first two objectives argue for a policy that places few government restrictions on the use of cryptography and actively promotes the use of cryptography on a broad front. The third argues for some kind of government policy role in the deployment and use of cryptography. **One aspect of federal policy that is slowing progress in the use of cryptography is the uncertainty it creates for vendors and potential users. Users are reluctant to take actions that might be made obsolete by subsequent policy decisions**. For example, businesses are unlikely to purchase products with sophisticated encryption capabilities when it is possible that government will later mandate or unduly favor the use of an incompatible product. **As a first step, policymakers should set some clear boundaries on the reach of federal regulations and establish a coherent structure for policy development that ensures that the needs of nongovernment cryptography users are respected. Specifically: No law should bar the manufacture, sale, or use of any form of encryption within the United States**. The administration has wisely rejected the option of banning unescrowed encryption. Such a ban would be easily circumvented technically and would also raise a number of constitutional issues whose outcome is highly uncertain. National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and should be governed by the rule of law. **Only a national discussion of the issues involved in national cryptography policy can result in the broadly acceptable social consensus that is necessary for any policy in this area to succeed**. **A consensus derived from such deliberations, backed by explicit legislation when necessary, will lead to greater public acceptance and trust, a more certain planning environment, and better connections between policymakers and the private sector.** National policy affecting the development and use of commercial cryptography should be more closely aligned with marketforces. As cryptography has assumed greater importance to nongovernment interests, national cryptography policy has become increasingly disconnected from market reality and the needs of parties in the private sector. **To harness market forces to promote widespread use of cryptography, federal policy should emphasize the freedom of domestic users to determine cryptographic functionality, protection, and implementation according to their security needs as they see fit; encourage the adoption of cryptographic standards by the federal government and private parties that are consistent with prevailing industry practice; and support the use of algorithms, product designs, and product applications that are open to public scrutiny.** For example, the administration has argued that escrowed encryption would benefit private users by making it possible to recover encrypted stored data to which access has been inadvertently lost. To the extent that this is true, market forces should be sufficient to generate a growing market for products that provide escrowed encryption services for stored data, and aggressive government promotion of this particular application is not necessary. **Today, U.S. firms compete and operate in a global**

> **market. Many U.S. firms have close relationships with foreign suppliers, customers, and strategic partners. Under such circumstances, a U.S. firm will inevitably need to share some of its sensitive or proprietary information with these parties, and protecting this information abroad is as necessary as protecting it within the United States**. **Some relaxation of today's export controls on cryptography is warranted.**[150]

Other technologies can be used to help improve IT systems and networks protection. Federal government promotion and implementation of these technologies can help stimulate the use of these technologies. The GAO outlines these technologies,

> • **Access controls** restrict the ability of unknown or unauthorized users to view or use information, hosts, or networks. Access control technologies can help protect sensitive data and systems. Access controls include boundary protection, authentication, and authorization technologies.
> • **System integrity controls** are used to ensure that a system and its data are not illicitly modified or corrupted by malicious code. Antivirus software and integrity checkers are two types of technologies that help to ensure system integrity….
> • **Audit and monitoring controls** help administrators to perform investigations during and after an attack. We describe four types of audit and monitoring technologies: intrusion detection systems, intrusion prevention systems, security event correlation tools, and computer forensics.
> • **Configuration management and assurance controls** help administrators to view and change the security settings on their hosts and networks, verify the correctness of security settings, and maintain operations in a secure fashion under duress conditions. We discuss five types of configuration management and assurance technologies: policy enforcement, network management, continuity of operations, scanners, and patch management.[151]

Even though the private sector owns 85% of the nation's critical infrastructures, particularly information systems and networks, federal government action to better protect its systems can lead to further research and development, diffusion and implementation of these technologies throughout the private sector. As the GAO also explains,

> **Because about 85 percent of the nation's critical infrastructure is owned by the private sector, the federal government cannot by itself protect the critical infrastructures. There are three broad categories of actions that the federal government can undertake to increase the usage of cybersecurity technologies. First, the federal government can take steps to help critical infrastructures determine their cybersecurity needs, and hence their needs for cybersecurity technology**. These actions include developing a national CIP plan, assisting infrastructure sectors with risk assessments, providing threat and vulnerability information to sector entities, enhancing information sharing by critical infrastructures, and promoting cybersecurity awareness. These activities can help infrastructure entities determine their needs for cybersecurity technology. This information can help the federal government to prioritize its actions and to assess the need to take further action to encourage the use of cybersecurity technology by critical infrastructure entities. Because the security needs of critical infrastructure could differ from the commercial enterprise

[150] Kenneth Dam & Hebert Lin, "NATIONAL CRYPTOGRAPHY POLICY FOR THE INFORMATION AGE," Issues in Science & Technology, Summer, 1996, http://bss.sfsu.edu/fischer/IR%20305/Readings/national.htm
[151] GAO, "Technology Assessment."

> needs of infrastructure entities, the federal government could assess the needs for grants, tax incentives, regulations, or other public policy tools to encourage nonfederal entities to acquire and implement appropriate cybersecurity technologies. **Second, the federal government can take actions to protect its own systems, including parts of the critical infrastructure. These actions could lead others to emulate the federal government or could lead to the development and availability of more cybersecurity technology products**. **Third, the federal government can take long-term actions to increase the quality and availability of cybersecurity technologies available in the marketplace.** Table 4 highlights many of the federal policy options and some examples of the current or planned activities undertaken by the federal government that implement these options.[152]

DHS Reorganization/Leadership

There are a number of criticism of the Department of Homeland Security (DHS) and its complete lack of leadership on cyber-security and information sector protection issues. Due to a revolving door of cyber-security leaders within the DHS, there is very little federal leadership on information protection.[153] Even more problematic is that the DHS has no authority to direct cyber-security regulations for the private sector.[154] One proposal currently circulating in Congress to solve these problems is the "Protecting Cyberspace as a National Asset Act of 2010." It would create a new DHS agency and appoint a White House-level authority leader or czar to specifically oversee and organize federal cybersecurity efforts. However, the bill also includes a very controversial element that will likely doom its chances of passing: it provides the President authority to declare a state of emergency that would effectively act as a "kill switch" to shut down the internet in the case of an attack.[155] Affirmatives could implement something similar to the "Protecting Cyberspace" law through reorganizing existing agencies, developing new ones, or including a "kill switch." For example, John Grant in 2010 calls for a new cyber-security regime that has direct authority in both the public and to some extent the private sectors:

> **The most dramatic and arguably the cleanest approach to establishing a new cybersecurity regime would be the creation of a single new entity to oversee the security of the information infrastructure**. **This new cybersecurity "agency" would be responsible for coordinating the federal government's entire approach to information infrastructure security. Such authority would go beyond mere strategy development, and include the authority to direct action both at the agency level and to some extent within** [*115] **the private sector. The agency would have the authority to set security standards that would be binding on agencies and on the information infrastructure controlled by the private sector**. The agency would be both seizing authorities from other Cabinet-level departments and directing those departments in securing their own networks, as well as regulating information technology systems in private sector industries that are otherwise subject to the regulatory authorities of the departments. **The agency would**, therefore, **need ways to compel action. Such mechanisms would likely include the authority to write and rewrite**

[152] GAO, "Technology Assessment."
[153] McFadyen 2009 "Protecting the Nation's Cyber Infrastructure."
[154] Molly Bernhart Walker, "Cyber bill would reform FISMA, instate new DHS agency and appoint White House-level authority," Fierce Government, January 20, 2011, http://www.fiercegovernmentit.com/story/cyber-bill-would-reform-fisma-instate-new-dhs-agency-and-appoint-white-hous/2011-01-20
[155] Minority Counsel for the Senate Committee on Homeland Security and Governmental Affair, "Cybersecurity Symposium: National Leadership, Individual Responsibility: Will There Be Cybersecurity Legislation?," Journal of National Security Law & Policy, pp. LN

> **agency information security budgets, access to agency enterprise architecture, access to the intelligence and law enforcement information necessary to identify threat signatures, the authority to isolate compromised systems from the network or take them offline completely**, and the authority to conduct operational evaluations of federal and private sector information infrastructure. **An agency given these strategic responsibilities and broad operational authorities over cybersecurity would necessarily be of considerable size. If it were assembled in the same way as the DHS - by, in most cases, joining disparate components of existing departments under a single umbrella** - large chunks of the Department of Commerce, OMB, and the DHS would be uprooted and placed under the new agency. Assuming that national security systems remained within the purview of the intelligence community and the Department of Defense, it would still be necessary to develop mechanisms by which they could coordinate with the new agency. **Such an agency would require a substantial budget.**

Or the affirmative could take a much smaller action to coordinate authority on protection, which avoids the more controversial elements of creating a new agency with broad powers.[156]

Offensive Cyber-attack Capabilities as Protection

For those that find the idea of talking about organization restructuring and development of new computer technologies unattractive, one of the more interesting affirmative areas of this sector is to bolster U.S. offensive cyber-attack capabilities as information system protection. As Owens, Dunn, and Lin suggest in 2009,

> **Given the importance of information technology to many societal functions, it is not surprising that there has been much public debate about cybersecurity (i.e., protection of information technology systems and networks** and the programs and information within them from hostile actions) **and about how the United States might improve its cybersecurity posture in the face of hostile actions** perpetrated by an adversary, such as a terrorist group, criminals, or another nation. **Although in many other domains, security has always had both defensive and attack components, cybersecurity has been somewhat anomalous, in the sense that its purely defensive side has been the primary focus of attention over the years. But, in fact, it is possible to imagine that cyberattacks might be used to support cyber defensive objectives. It is further possible to imagine that cyberattack would naturally be part of a robust U.S. military posture.** The possibility that the United States might choose to engage in cyberattacks to serve its own national interests is, however, rarely discussed in public. **For the record, the U.S. government has acknowledged that it has an interest in such capabilities as a possible instrument of national policy**,1 **but this is virtually all that it acknowledges publicly**. At least one press report has indicated the existence of a still-classified National Security Presidential Directive, NSPD 16, issued in July 2002, that reportedly ordered the U.S. government to develop national-level guidance for determining when and how the United States would launch cyberattacks against enemy computer networks.2 The National Strategy to Secure Cyberspace, published in February 2003, is entirely silent about an offensive component to U.S. cybersecurity efforts.[157]

[156] Ibid
[157] Owens, Dunn & Lin (Eds.) (2009), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capacities," National Research Council, http://www.nap.edu/openbook.php?record_id=12651&page=9

Owens, Dunn and Lin also raise the possibility that any action that imposes high enough costs on attacker's to deter attack – such as the use of economic sanctions - could be a protection (although depending on the wording of the eventual resolution seems rather extra-topical). Additionally, they outline offensive options like initiating an kinetic or EMP military strike or counter-cyber-attack attacks as defensive protections:

> As suggested in the previous section, cyberattack sometimes arises in the context of defending U.S. computer systems and networks. Passive defensive measures such as hardening systems against attack, facilitating recovery in the event of a successful attack, making security more usable and ubiquitous, and educating users to behave properly in a threat environment are important elements of a strong defensive posture.7 Nevertheless, for the defense to be successful, these measures must succeed every time the adversary attacks. The adversary's attack need succeed only once, and an adversary that pays no penalty for failed attacks can continue attacking until he or she succeeds or chooses to stop. This places a heavy and asymmetric burden on a defensive posture that employs only passive defense. **If passive defense is insufficient to ensure security, what other approaches might help to strengthen one's defensive posture? One possibility is to eliminate or degrade an adversary's ability to successfully prosecute an attack. In that case, the attack is ultimately less successful than it might otherwise have been because the defender has been able to neutralize the attack in progress** (or perhaps even before it was launched). **A second possibility is to impose other costs on the adversary, and such a strategy is based on two premises. First, the imposition of these costs on an attacker reduces the attacker's willingness and/or ability to initiate or to continue an attack. Second, knowledge that an attack is costly to an attacker deters other parties from attempting to attack—and advance knowledge of such a possibility may deter the original adversary from attacking in the first place**. **There are in general many options for imposing costs on an adversary, including economic penalties such as sanctions, diplomatic penalties such as breaking of diplomatic relations, and even kinetic military actions such as cruise missile strikes. In-kind military action—a counter-cyberattack—is also a possibility**.

For those bold enough to advocate offensive capabilities to stop enemy attacks, there would be obvious hegemony, deterrence, and other similar advantages.

Negative Ground

There are a variety of negative options to counter affirmatives in the IT sector. At the most basic level, there is very rich case debate ground, particularly concerning the probability of cyber-terror attack. At their core, most of negative options contend that federal action or certain agent action is bad and that these actions harm or panic businesses. Also, there are a host of advantage counterplans that can solve the threat of cyber-terrorism that do not require increased infrastructure protection.

Politics Links

Many of the affirmative options will provoke political opposition from members of Congress and congressional lobbies. For instance, given that national security protection is shrinking as a priority on Congress' agenda, there will be little desire to debate cyber-security issues during a busy agenda full of budget and economy issues. As Grant explains,

> In the course of just a few decades, information technology has become an essential component of American life, playing a critical role in nearly every sector of the economy. Consequently, government policy affecting information technology currently emanates from multiple agencies under multiple authorities - often with little or no coordination. The White House's Cyberspace Policy Review (the Review) wisely recognized that the first priority in improving cybersecurity is to establish a single point of leadership within the federal government and called for the support of Congress in pursuit of this agenda.**Congressional involvement in some form is inevitable, but there is considerable uncertainty as to what Congress needs to do and whether it is capable of taking action once it decides to do so. With an agenda already strained to near the breaking point by legislation to address health care reform, climate change, energy, and financial regulatory reform - as well as the annual appropriations bills - the capacity of Congress to act will depend, in some part, on the necessity of action. For the last eight years, homeland security has dominated the congressional agenda. With the memory of the terrorist attacks of September 11 becoming ever more distant, there may be little appetite for taking on yet another major piece of complex and costly homeland security legislation**.[158]

Additionally, any perceived mandatory requirements on private businesses – which almost all affirmatives will order – will face stiff business lobby opposition in Congress.

> **As with any piece of legislation, a key factor in determining the likelihood of passage is the level of opposition. In general terms, the most significant lightning rod in any cybersecurity legislation is likely to be the imposition of mandatory standards on privately owned information technology infrastructure**. n41 It has frequently been claimed that the Internet is free from regulation and that any attempt to impose a mandatory regime could stifle the innovation that has turned information technology into an economic engine. n42 **Any bill that is perceived - rightly or wrongly - as imposing regulation on the Internet will draw substantial opposition**. [*113] **An example of potential opposition can be seen by the reaction to** Senators Jay **Rockefeller and** Olympia **Snowe introduction of the Cybersecurity Act of 2009**. **The bill includes provisions establishing cybersecurity standards for both government and private sector information infrastructure, requiring the licensing and certification of cybersecurity professionals, and designating the Department of Commerce as the clearinghouse for cybersecurity threat and vulnerability information**. n43 Reaction to the bill was initially muted but gives an indication of potential future opposition. **TechAmerica, a leading industry trade association, warned that "some provisions of the Rockefeller-Snowe bill may impose prescriptive regulations on the private-sector that could inhibit the very technology innovation** needed for greater prosperity and security." n44 Phil Bond, President of TechAmerica, added that "the last thing we need is cybersecurity innovation that moves at the speed of government." n45 Larry Clinton**, President of the Internet Security Alliance, criticized the bill's vagueness and stated that without clarification his organization** - which has close ties to Verizon, Nortel, and other key industry stakeholders - **could not support the bill**. **n46 In addition to industry opposition, the Rockefeller-Snowe bill drew concern from the privacy and civil liberties community as well**. The Center for Democracy and Technology expressed concern that the bill would give "the federal government extraordinary power over private sector Internet

[158] John Grant, 2010, Minority Counsel for the Senate Committee on Homeland Security and Governmental Affair, “Cybersecurity Symposium: National Leadership, Individual Responsibility: Will There Be Cybersecurity Legislation?,” Journal of National Security Law & Policy, pp. LN

> services, applications and software." n47 The Electronic Frontier Foundation argued that provisions of the bill "could eviscerate statutory protections for private information."[159]

Also, any affirmative will cause congressional committee infighting as information technology falls within almost all of their jurisdictions:

> **Information technology has become part of nearly every major industry and service in the United States. Consequently, most - if not all - of the congressional committees could seek jurisdiction over cybersecurity**. [*114] Already in the Senate, the Chairman and Ranking Member of the Commerce Committee have introduced two bills, n49 several prominent members of the Judiciary Committee have introduced data breach bills n50 with significant cybersecurity implications, and the Chairman and Ranking Member of the Homeland Security and Governmental Affairs Committee have announced their intention to develop comprehensive cybersecurity legislation. n51 **Given the prominence of the issue and the economic power of the information technology industry, it is unlikely that the aforementioned committees - among the most powerful in the Senate - will cede jurisdiction without considerable reluctance. Similar jurisdictional tensions can be found in the House of Representatives as well**.

More specifically, businesses will oppose any requirements to report cyberattacks on their businesses[160], the creation of new government agencies or the expansion of presidential authority over information technologies.[161]

Business Confidence/Economy

Most affirmatives will need to mandate guidelines or regulations to provide a clear signal to solve for both private and public systems. The real and perceived impacts on businesses will undermine business confidence and potentially disrupt innovation and investment. As the lobbies politics link above suggests, businesses greatly fear many of these potential affirmative actions.

Counterplans

Given the potential business opposition to federal mandates, voluntary compliance counterplans that provide incentives for acquiescence to the plan's provisions would solve both politics and business confidence. Because most of the information systems are owned by the private sector, cooperative compliance measures may solve better than federal action.

Additionally, the negative can run a host of counterplans that solve the advantage areas that link to cyber-attacks/cyber-terrorism. One such measure would include consulting with NATO and other allies to coordinate cyber protection policies. As Owens, Dunn and Lin (2009) suggest,

---

[159] Ibid.

[160] Matthew Hicks, "Trade Groups Launch Security Assessment Tools," EWEEK, Dec 13, 2003, http://www.eweek.com/c/a/Security/Trade-Groups-Launch-Security-Assessment-Tools/

[161] Grant

> **Recommendation 3: The U.S. government should work to find common ground with other nations regarding cyberattack**. **Such common ground should include better mutual understanding regarding various national views of cyberattack, as well as measures to promote transparency and confidence building**. **The committee believes that most other nations are no farther along in their understanding of the key issues than is the United States. It is therefore important for the United States to begin to find common ground on this topic with allies, neutrals, and potential adversaries**. In this context, "common ground" is not a euphemism for treaties or arms control agreements regarding cyberattack. It is rather a term that denotes a common understanding of its significance for policy—and common ground is important for allies and adversaries alike if misunderstandings are to be avoided. **Consultations with allies of the United States (such as the NATO countries) are likely to be the easiest to undertake. Such consultations should take two tracks—between the governmental entities that would be responsible for executing cyberattacks in these nations and between the cognizant policy decision makers**. At the very least, those with opera- tional responsibility for attack execution need to develop mechanisms for coordinating cyberattacks so that they do not interfere with each other. **And policy makers must be able to discuss issues related to cyberattack in an informed manner, without having to learn about them in the middle of a cyber crisis.** As an example of such consultation, NATO established in March 2008 the Cyber Defence Management Authority, which will manage cyberdefense across all NATO's communication and information systems and could support individual allies in defending against cyberattacks upon request.23 One press report indicates that "the Authority will also develop and propose standards and procedures for national and NATO cyberdefence organisations to prevent, detect, and deter attacks," but will focus on defense "whether an attack comes from state, criminal or other sources."24 Similar efforts to reach common understandings regarding cyberattack (and on the relationship of cyberattack to cyberdefense) would be helpful as well.[162]

Also, the negative can have the U.S. make declaration policy that clarifies our use of cyberattacks in order to deter other nations and powers from initiating these attacks:

> 1.the DOD Information Operations Roadmap of 2003 recommended that the U.S. government should have a declaratory policy on the use of cyberspace for offensive cyber operations. As the committee has been unable to find any such statement of declaratory policy, it concurs with and reiterates this call. a. For example, the United States could declare its commitment to abiding by the laws of armed conflict with respect to cyberattack. Such a posture could well affect the willingness of other nations to make similar declarations. Another related example concerns the national military strategy of the United States.[163]

Critical Arguments

There are a number of critical arguments that the negative can deploy against Information Technologies sector affirmatives. First, there are links to federal regulation of info technologies as a form of capitalist panoptic surveillance of the internet. As Tom Burghardt in 2011 explains,

> **A reflexive power-grab by the Pentagon is not however, a sign that the internet and related telecommunications' platforms are being absorbed by that scarecrow beloved by neoliberals, libertarians and other "free market" fanatics: "big government." As Marxist social media critic Christian Fuchs points out: Foucault**

[162] "Technology, Policy, Law, and Ethics."
[163] Ibid

> **characterized surveillance in the following way: "He is seen, but he does not see; he is the object of information, never a subject in communication." With the rise of "web 2.0," the Internet has become a universal communication system, which is shaped by privileged data control by corporations that own most of the communication-enabling web platforms and by the state that can gain access to personal data by law**. … By being subjects of communication on the Internet, users make available personal data to others and continuously communicate over the Internet. **These communications are mainly mediated by corporate-owned platforms, therefore the subjects of communication become objects of information for corporations and the state in surveillance processes**. … In web 2.0, **corporate and state power is exercised through the gathering, combination, and assessment of personal data that users communicate over the web to others, and the global communication of millions within a heteronomous society produces the interest of certain actors to exert control over these communications**. In web 2.0, **power relations and relationships of communication are interlinked**. The users are producers of information … but this creative communicative activity enables the controllers of disciplinary power to closely gain insights into the lives, secrets, and consumption preferences of the users. (Christian Fuchs, "Web 2.0, Prosumption, and Surveillance," Surveillance & Society, Vol. 8, No. 3, p. 304) **In this light, the Pentagon's obsessive secrecy, particularly as it relates to "cybersecurity" and programs designed for offensive cyber war, its management-driven cult of controlling informational flows and pathological aversion to democratic decision-making processes are anything but antithetical to a neoliberal regime that commodifies everything and values nothing. Rather, the broader militarization of society and social relations as a whole, characterized by endless imperial wars and a system of generalized plunder must be viewed as an expression, albeit a sinister one, of capitalism's drive to privatize and commodify the state itself as a profit-generating center**.[164]

The advantage areas of critical infrastructure protection, cyberterrorism and national security naturally link to Terror Talk and Security critiques. For instance, as the King's College Seminar on Contemporary Biopolitical Security suggests in 2011,

> **"There is no liberalism without a culture of danger."** (Foucault) **Threats and risks have become the preferred categories for imagining contemporary security. Practices such as defence, border control and the surveillance of populations, insurance, risk profiling to identify suspicious subjects, and risk assessments to protect objects and systems such as critical infrastructure, rely heavily on well-established paradigms of security**. **Discourses and practices of threats and risks, with their allied technologies of measurement and calculation, however, relate to the wider problem of danger and its allied concept of 'uncertainty'. Thinking 'danger' relates to understandings of uncertainties, otherness of being, and spaces and environments of protection in excess of those accounted for in the language and metrics of discourses of threats and risks**. What happens, then, if the analysis of security resorts to understandings of 'danger', 'dangerousness', and processes of 'endangerment'? Is it possible to think security by referring ideas of danger to understandings of life, livelihoods and lifestyles, instead of ready-made 'objects' of security such as sovereignty, territory, the nation-state, citizens, borders, and sociological categories such as class and gender? **Is it possible to think security in relation to danger away from utilitarian economic categories such as cost-benefit analysis, risk calculus, and rational choice**? The workshop aims to explore these questions and to challenge participants to wonder if current policy security priorities such as terrorism, climate change, weapons proliferation, resilience and migration can be thought in relation

[164] Tom Burghardt, "Pentagon Demands Billions in 'Cybersecurity' Handouts,", April 4th, 2011, http://www.americanpendulum.com/2011/04/tom-burghardt-pentagon-demands-billions-in-cybersecurity-handouts/

> to 'danger' outside discourses of threats and risks. In the first three workshops of this seminar series we began to explore an agenda for contemporary biopolitical security research around problems such as mobilities and circulations, resilience, values and processes of valuations in relation to the technologies through which lifestyles and livelihoods are treated as referents of security. In this fourth workshop we intend to spark a conversation around the implications of thinking dangerousness in relation to security and life. The workshop is based on participants' work and invites a reflection on the following questions: - **How are ideas of danger constituted? What forms of 'data', 'information', and 'knowledge' are involved in constituting a dangerous subject or a dangerous environment? - What are the preconditions for understanding endangerment in and how do they question the 'new security challenges' of for example, terrorism (and cyber-terrorism), proliferation of weapons of mass destruction, climate change, and health pandemics? - Can discourses and practices of security be different if reflections on the consequences of endangerment are advanced**?[165]

In addition, there are a number of scholars that contend that cyber-terrorists are forms of cyber-cultural resistance that resist dominate norms, rules and laws. Thus, attempts to control this type of activism risks undermining the public space and a variety of movements that could be labeled "cyber-terrorists".[166]

Conclusion

There are a wide range of affirmative options with large impacts and negative counterplan, disadvantage and critical arguments in the Information Technology sector. Given its interrelationship with all of the other CIKR areas, we recommend that the IT sector be included as a resolution area. In many ways, the affirmative/negative ground for this area overlaps with the Communication sector area and could replace it if the topic committee was looking for an easy way to reduce the number of sectors in the topic.

[165] http://backdoorbroadcasting.net/2011/02/problematising-danger/
[166] Pramod K. Nayar, An Introduction to New Media and Cybercultures, John Wiley & Sons, 2010.

National Monuments and Icons

Introduction

In order to appreciate how national monuments and icons could relate to the kinds of arguments seen in policy debate, it is important to re-clarify a few key terms. The National Strategy for Homeland Security defines "key assets" as:

> Individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. Key assets include symbols or historical attractions, such as prominent national, state, or local monuments and icons. In some cases, these include quasi-public symbols that are identified strongly with the United States as a Nation.... Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community. [167]

This sheds some light on what is meant by National Monuments and Icons. The Office of the President clarifies slightly

> One category of key assets comprises the diverse array of national monuments, symbols, and icons that represent our Nation's heritage, traditions and values, and political power. They include a wide variety of sites and structures, such as prominent historical attractions, monuments, cultural icons, and centers of government and commerce....[168]

This sector provides ground for Affirmatives to topically engage the Resolution and Negatives to respond on case. Because the definition of National Monuments and Icons is imprecise, this should encourage important topicality debates.

Affirmative Ground

Affirmatives may make cases and plans that address any number of monuments and icons (Lincoln, Washington, Gateway Arch, etc.). They may also address other historically significant areas. An Affirmative could design a plan that protects U.S. parks, for example, or even museums like the Smithsonian Institution.

The United States Department of Homeland Security makes several limiting remarks regarding the scope of the National Monuments and Icons classification.[169,170] This clarification seems to reduce the initial Affirmative ground provided by The National Strategy for Homeland Security.[171]

DHS 10

---

[167] U.S. Office of Homeland Security. The National Strategy for Homeland Security. July 16, 2002.
[168] Office of the President. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. February, 2003.
[169] U.S. Department of Homeland Security, National infrastructure Protection Plan: National Monuments and Icons Sector, 2010, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_nationalmonuments.pdf
[170] U.S. Department of Homeland Security, National Monuments and Icons Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, 2010, http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf
[171] U.S. Office of Homeland Security. The National Strategy for Homeland Security. July 16, 2002.

(Department of Homeland Security, National infrastructure Protection Plan: National Monuments and Icons Sector, 2010, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_nationalmonuments.pdf)
NMI sector assets share three common characteristics:
•Are a monument, physical structure, or object;
•Are recognized both nationally and internationally as representing the Nation's heritage, traditions, and/or values or are recognized for their national, cultural, religious, historical, or political significance; and
•Serve the primary purpose of memorializing or representing significant aspects of our Nation's heritage, traditions, or values and as points of interest for visitors and educational activities. They generally do not have a purpose or function that fits under the responsibility of another sector.

The threat is real, as indicated in recent new articles on the subject.

AFP 08
Agence France Press, US monuments vulnerable to terrorist attacks: report, February 4, 2008, http://afp.google.com/article/ALeqM5hzdfHg4kI50ar-IbpEfw3avROAxQ
Major US monuments are vulnerable to terrorist attacks because the US Park Police is disorganized, under-staffed and ill-equipped, the Washington Post reported Monday, citing a government audit. The Park Police, a branch of the Interior Department, is in charge of securing landmarks like the Statue of Liberty in New York and the Lincoln Memorial in Washington. The 40-page report from the Department's inspector general's office includes the photograph of what is apparently an officer sleeping in a patrol car at the Jefferson Memorial in the US capital, and describes another officer filling out a crossword puzzle, the Post reported. The Park Police "has failed to adequately perform either mission, which has resulted in deficient security at national icons and monuments and an inability to effectively conduct police operations," the Post reported, citing a copy of the report to be made public Monday. The report was based on more than 100 interviews and surveillance the inspectors carried out in 2007, the Post said.

Advantage ground for the Affirmative will be difficult to define precisely, but there are some interesting political theory arguments to be made that hint at advantages of liberty, freedom, republicanism, etc.

US DHS 10
U.S. Department of Homeland Security, National Monuments and Icons Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 1 (2010), http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf
The NMI Sector is committed to ensuring that the symbols of our Nation remain protected and intact for future generations. Because access to monuments and icons is a hallmark of life in a free and open society, the sector will strive for an appropriate balance between security, public access, and aesthetics. The sector will promote protective measures to dissuade adversaries from affecting the national psyche by damaging or destroying these important symbols.

Negative Ground

There will be on case arguments to be made regarding the level of threats to our National Monuments and Icons. There will also be plenty of room to run one-off on case positions on specific monuments.

Believe it or not, National Monuments and Icons are a politically divisive issue. The maintenance, establishment, and funding of National Monuments and Icons can be contentious. As such, politics disadvantages should be a viable Negative strategy.

HCN 10
Jonathan Thompson, The Trouble With Monuments, High Country News, March 1, 2010, http://www.newwest.net/topic/article/the_trouble_with_monuments/C559/L559/
Last week, Western conservative congressmen found a great excuse to get all worked up, apoplectic, and downright angry in the gleeful way that Western conservatives seem to have a premium on. President Obama, they said, was ready to make a massive land grab that would turn huge swaths of Western states into federal fiefdoms, off-limits to gas drilling, off-road-vehicles, grazing, coal mining and all kinds of other God-given rights. The kerfluffle was over an Interior Department secret list of places worthy of protection, either by national monument designation, other conservation designations, or by buying up private land that checkerboards federal holdings. Fourteen sites are on the national monument list, with another ten or so on the other lists, all spread out across the 11 Western states. The document emphasizes, in the short preamble: "The areas listed below may be good candidates for National Monument designation under the Antiquities Act; however, further evaluations should be completed prior to any final decision, including an assessment of public and Congressional support." That tone, which is hardly "unilateral," as opponents claim, hasn't eased the backlash. The U.S. Chamber of Congress – notorious for its climate change denials—sent a letter to Congress urging it to remand the president's authority to create any new national monuments. The Congressional Western Caucus – led by nouveau sagebrush warrior Rep. Rob Bishop, R-Utah – ran no fewer than eight articles on its Web site bashing the document and its alleged intent, with titles like "War on the West II." The reference was clear: The first "War on the West" being President Bill Clinton's executive order establishing Grand Staircase Escalante National Monument in Utah in 1996.

Current legislation in Congress to require congressional approval of monuments is politically divisive.

Missoulian 3/11
John Todd, Rehberg needs to give divisive monument bashing a rest, The Missoulian, March 11, 2011, http://missoulian.com/mobile/article_03627d70-4bf2-11e0-91f9-001cc4c03286.html
This January marked the tenth anniversary of the Upper Missouri River Breaks National Monument designation. Since its creation, many Montanans have enjoyed floating the river, exploring the Breaks and meeting residents of nearby communities.
For the past nine years, I've enjoyed working on the Missouri River as a field-based educator and guide. Monument designation pointed out to the entire world that this place is special-that this place is worth protecting. Montana is proud of the monument. So why isn't Rep. Denny Rehberg? These days, when Rehberg talks about monuments, it's as if he's ashamed of this great state's natural heritage and history. Rehberg's new anti-monument bill sends the message that we aren't proud of past efforts to conserve Montana's unique places. The bill is a shallow political stunt and waste of the public's time. It would require Congress to approve any new national monument in Montana that a president might designate under the Antiquities Act. In other words, it robs Montanans of an influential voice and the power to steer monument designation from the local level. It is simply not true that past monuments in Montana were created without public support. But if Rehberg's bill passes, Montanans could have less of a say about protecting the state's remaining special places. Instead, the decision will be taken out of local meeting halls in Fort Benton, Lewistown and other communities, and replaced with Washington D.C. partisan politics.

Counterplan ground will consist mainly of Plan Inclusive Counterplans (PICs). Negative teams may wish to relinquish control of a certain monument or monuments in a certain state. Relinquishing control in a certain state may provide a valuable politics disadvantage as a net benefit to the counterplan.

Critical ground will be strong as monuments and icons are at the center of national projections of history, pride, virtue, decadence, and advancement. All generic criticisms of the state should still apply to this sector.

A link to racial discrimination in the building of at least one monument can be found.

Moore 94/95
Robert J. Moore, Jr., Showdown Under the Arch: The Construction Trades and the First "Pattern or Practice" Equal Employment Opportunity Suit, 1966, Gateway Heritage, 1994-1995, 6
Percy Green told the story of his protest in this way in a 2004 essay: "We spoke to the general contractor, MacDonald Construction Company, which said that they had tried but could not find qualified black contractors to do the work. Regarding skilled workers, the contractor said that there were only a few blacks and they were all working on other construction jobs; and that the unions were responsible for the fact that there were so few skilled black construction workers. We did not find these excuses acceptable. The question became: How could we expose to the world that this national monument, the Arch, was guilty of racial discrimination using federal tax dollars? "During a strategy session, it was determined that an exploratory reconnaissance was necessary. Richard Daly, a European-American, joined me, an African-American, to test the waters by seeing how far we could explore the Arch site without confrontation. A few days later we visited the site at lunchtime. We were dressed like construction workers, in Levis, T-shirts, and boots. We walked up to the North leg of the Arch, and seemed to be viewed as regular workers. We walked around the grounds and left without incident. "At the next strategy session, we reported our experience, and after some discussion, a direct-action protest plan was adopted. We decided to climb the Arch to expose the fact that federal funds were being used to build a national monument that was racially discriminating against black contractors and skilled black workers.

Ticketing policies may also discriminate against families, providing additional unique ground.

Walker No Date
Jed Walker, Statue of Liberty Discrimination, No Date Given, http://tinky2jed.wordpress.com/my-thoughts/statue-of-liberty-discrimination-against-u-s-citizens/
Did you know that access to the Statue of Liberty's crown prevents many U.S. families from visiting it together as family, even though non U.S. citizens can visit it? We are planning on taking a trip to New York and found out that you can not book more than four tickets for Crown access per household. I find it very disheartening that they would discriminate against U.S. Citizens in such a way. Their reasoning is that "if the NPS did not have this 4 ticket limit in place, the tickets would not be available at all to most families because they would sell out much faster." I find that pretty poor reasoning. Per http://factfinder.census.gov/servlet/SAFFFacts the median U.S. Family size is 3.14, wow that is as American as apple Pi (yes, pi). So, I guess that is how they determine it, maybe you have to be an "average" U.S. Family to have the privilege of visiting such an important part of our history. It did get me wondering, what if it was a total of five or six people. Wow, that would probably cover a large majority of families in the U.S., but how would it affect visits to the statue. According to http://en.wikipedia.org/wiki/Statue_of_Liberty about 240 people ascend to the crown per day, so instead of a total of 60 families visiting it in a day, a total of 40 families could if every family had six members. I don't know, but that doesn't seem bad, and given the average of 3.14 per family, I imagine it would be higher. It is sad to see that a U.S. Monument would discriminate in such a way.

Conclusion

The literature base for National Monuments and Icons is relatively thin, but a thoughtful Affirmative team should be able to craft a compelling case and plan. Negative teams will find politics disadvantages a relatively easy position to run. Negatives may also find critical arguments a useful strategy. This section, despite the lack of literature, presents an even array of arguments for the Negative and the Affirmative.

Nuclear Reactors, Materials and Waste

Introduction

The Nuclear (section) of the topic would include these areas: "nuclear power plants; non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; decommissioning reactors; and the transportation, storage, and disposal of nuclear material and waste"(Department of Homeland Security). What we get here is a domestic nuclear energy topic that has potential to stay fresh and intriguing all year long. The debate community is also the perfect forum for this discussion, as illustrated by Gray in 2009:

> **Gray, 09**
> (John, J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 "Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development", Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis)
> Although energy policy is about choices, policymakers still require that circumstances provide the right context and support for their decisions. An effective energy policy requires that the right circumstances make certain energies viable and that policymakers recognize these opportunities. **For the first time in nearly thirty years, nuclear power has the opportunity to expand and to change United States energy policy forever. Public opinion may provide a brief window for nuclear power to reemerge**

Yes we did do a topic that had the word nuclear attached to it, and no we did not do a topic which dealt with the nuances of the actual nuclear material, energy, and management of said energy. The nuclear weapons topic was in many ways an international topic as compared to the domestic policies of what roll nuclear energy/material has in the United States. Affirmatives will have to argue an increase in protection/resiliency of the nuclear infrastructure instead of decreasing of the United States' weapons. These discussions are unique, both in argument and literature base.

> **Gray, 09**
> (John, J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 "Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development", Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis)
> **First, contrary to popular belief, no inherent connection exists between civilian and military nuclear technology. n123 For example, Canada has [*336] nuclear energy, but no nuclear weapons**. n124 **Conversely, Israel has a relatively weak nuclear energy program, but is an (unofficial) member of the nuclear weapons club**. n125 **Technologically, the processes used for civilian nuclear energy and nuclear weapons development are different; the uranium enrichment process differs, meaning a natural connection separates civilian from military technology**. n126 If a natural connection between civilian and nuclear energy actually existed, as critics claim, then global proliferation should have mirrored civilian nuclear energy changes much more closely.

Taking these examples into account, parts of the debate community might wonder if this topic area is too large. Yes, there are a slew of potential affirmative and negative arguments, are they substantial, no. Most scholars identify that piecemeal tactics in the form of nuclear energy etc… will fail without a substantial reform limiting the ability for the affirmative team to run to the margins. My

recommendation would be if the nuclear section would be included it should be a part of a more limited resolution, or (everybody's favorite) a list-type resolution.

Affirmative Ground

By no means is this "the" list of all available affirmative arguments, but the following should provide insight into the types of arguments available in this sector.

Reactors

Nuclear reactor affirmatives will be particularly intriguing because of the potential benefits that arise from more/better funded sites. This area is uniquely dynamic because public skepticism towards nuclear technology has caused inaction on behalf of the US.

> **Gray, 09**
> (John, J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 "Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development", Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis)
> **Nuclear energy is the only alternative that combines current economic viability with environmental protection. Skeptics note that nuclear energy accounts for only about twenty percent of the nation's energy and that no nuclear plants currently in use have been ordered since 1973.** [n71] However, [*328] these disappointing facts indicate only a historical lack of political support and capital construction initiative. **As other energies become decreasingly economical and as the public becomes more supportive of alternative energy, alternative energies, such as nuclear energy, become prime targets for expansion.**

In conjunction with the above evidence, there is a strong literature base indicating that government action will be key to maintaining the nuclear sector.

> **Gray, 09**
> (John, J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 "Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development", Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis)
> Aside from political opportunity, which may, for the first time in thirty-five years, be in nuclear power's favor, nuclear power's capital and short-term costs have prevented industry expansion. n161 **Although nuclear power is more economically efficient and beneficial in the long term, high capital costs of nuclear plants, unfettered devotion to the fossil fuel industry, and high nuclear plant licensing and registration costs decrease nuclear power's short-term competitiveness. n162 This is the one area that cannot change quickly without governmental support.**

There is a strong argument that affirmatives dealing with this area will qualify as being substantial due to the massive funding and upgrades required to solve.

> **Gray, 09**
> (John, J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 "Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development", Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis)

> In the electricity sector, **expanded nuclear power could quickly displace coal, oil, and natural gas. n74 Even given decades of public and governmental admonishment, nuclear power still comprises about twenty percent of the nation's energy consumption. n75 Nuclear energy's true potential could be realized by building new nuclear power plants, which could compensate for growing energy demand, especially given today's efficiency standards. Furthermore, unlike renewable energies, nuclear power's high generating capacity means that nuclear power can provide a major portion of the country's energy in only a few square miles, avoiding costly expansion** over large areas of land. n76

There is also a plethora of advantages available to affirmatives stemming from reactor-based affirmatives.

> **Gray, 09**
> (John, J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 “Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development”, Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis)
> Perhaps most importantly, **nuclear power is both a short and long-term solution. In the short-term, it can currently provide for the country's growing energy demand, with cost-efficient technology already in place. Nuclear technology currently exists to provide powerful and efficient energy; the fact that nuclear power is already developed to this efficiency gives it a unique advantage over other alternative energies, which are still in their infancy and thus unable to provide a large amount of power in a cost-effective manner at this time. In the long-term, nuclear power is a critical part of a cost-effective and sustainable energy economy. Nuclear power's many advantages and opportunities make it an essential energy alternative capable of providing for the country's changing needs in an environmentally-safe manner. It can prevent the pending economic collapse caused by oil and natural gas shortages, avoid the pollution and global warming dangers of fossil fuel emissions, and fill the energy gap quickly and efficiently, before fossil fuel's dangers become irreversible.** n81

> **Gray, 09**
> **(**J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 [John, **“**Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development”, Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis]
> **Nuclear energy, if given the opportunity to compete in a fair market, could provide a substantial part of the country's energy economy, alleviating many of the public health and environmental concerns caused by fossil fuel energy.** Critics' arguments are based more in fear and rumor than in logic and fact. However, merely answering these critics is not enough; actively supporting the industry is the next step.

The above evidence indicates a legion of potential advantages available through rector-based plan action. These advantages are diverse in nature and dynamic in their impacts. Some examples include:

A) Energy and the environment

> **Gray, 09**

(J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, **Spring 2009** [John, “Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development”, Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis]
With nuclear plants' high energy capacity and operating efficiency, **nuclear power could fill the energy demand currently met by fossil fuels, thus lowering the adverse economic and environmental impacts that coal, oil, and natural gas present. Currently, 104 licensed nuclear power plants exist in the United States, producing over 95,000 net megawatts of electricity**. n72 **Additionally, although new plants have not been built, nuclear plants are becoming more efficient, improving nuclear power's capability to meet the nation's energy demand. n73 Even without the benefit of strong governmental support, the nuclear industry has already proven its capacity to comprise a large portion of the nation's energy.**

B). Oil Spikes

Gray, 09
(J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 [John, **“**Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development”, Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis]
In addition to its "land efficiency," nuclear power has extremely cost-efficient operation. For example, **even accounting for the costs of uranium enrichment, management, and disposal, the average nuclear power plant is approximately three times more cost-efficient than a typical coal plant**. n77 **Nuclear power technology also continually improves**, such as with power uprates, n78 new fuels, n79 or other methods of improving power and efficiency, **therefore making the technology viable both today and in the future**. Additionally, **nuclear power has the most stable operating budget because its costs are more predictable**; for example, **uranium supply is plentiful and inexpensive, while oil and natural gas prices are volatile and increasingly expensive. n80 This stability makes nuclear power less vulnerable to price spikes that could damage the industry's viability and strain businesses.**

C). International Coop/E.U. Relations

Gray, 09
(J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 [John, **“**Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development”, Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis]
Nuclear power also offers various extraneous advantages, only tertiary to the energy grid. One major advantage is nuclear power's capacity to create a shift to a sustainable energy mindset. **The United States could frame a renewed commitment to nuclear power as a renewed commitment to environmental protection. This could gain favor with allies, who are already upset with the United States about its position on global warming and other environmental issues.** n82 Although renewable energies are more often hailed as the "green" technologies, the United States' allies, especially in Europe, have already recognized that nuclear energy can lower emissions. n83 In fact, **many European countries draw a substantial portion of their energy from nuclear power. n84 This preexisting ideology against fossil fuels and toward nuclear power could set the stage for the United States to use a strong nuclear industry as a point of cooperation and improved relations with its European allies.**

D). Water Wars

Gray, 09
(J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, Spring 2009 [John, **"**Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development", Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis]
Another example deals with perhaps the only resource more precious than oil and gas: Water. Utilizing nuclear power plants for water desalinization would provide a solution to the world's water supply shortage. By some estimates, fifty percent of the global population, mostly in Asia and Africa, already lack a sufficient water supply, and studies suggest this figure will grow substantially by 2025. n85 **As the global population continues to increase, the earth's usable water supply remains, at best, constant; at worst, continued pollution of the earth's precious fresh [*331] water actually decreases usable water supply even as demand increases. n86 Similar to oil and natural gas, the apocalyptic impact of water shortage occurs long before supply actually falls to zero. As water supply decreases, countries could be willing to fight for the few remaining drops, creating a slew of water wars across Asia and Africa. n87 These wars will not solve the underlying resource competition, however. Conflicts eventually become larger, more frequent, and more likely to become global**.

E). Electricity

Whitman 7
(Christine Todd, EPA Administrator, http://www.msnbc.msn.com/id/20730356/)
The cost of failing to meet these needs will be steep…. **prices over the past three years, industry production costs have remained low**, at less than 2 cents per kilowatt-hour (a quarter of those at gas-fired plants).

Transportation

Transportation of materials is overseen by the NRC (Nuclear Regulatory Commission) and the DOT (Department of transportation). These sites are particularly interesting because of the potential harmful consequences that can happen when transferring such materials. Transportation of nuclear materials includes the following sub-sectors: Regulations, Guidance, and Communications, Package Certification, Shipping Requirements, and Oversight.

Affirmatives can deal with issues of terrorism as well as potential impacts of an accident during transportation.

Ballard, Assistant Professor Grand Valley State University, **98**
[James David, July, "A PRELIMINARY STUDY OF SABOTAGE AND TERRORISM AS TRANSPORTATION RISK FACTORS ASSOCIATED WITH THE PROPOSED YUCCA MOUNTAIN HIGH-LEVEL NUCLEAR FACILITY", http://www.state.nv.us/nucwaste/trans/jballard.htm]
The Nevada Agency for Nuclear Projects was created by the Nevada Legislature to oversee federal high-level radioactive waste activities in the state. **As part of its oversight role, the Agency has contracted for this preliminary study of the risk of terrorism against shipments of high-level nuclear waste and spent nuclear fuel**. This study continues the Agency's assessment of socioeconomic and transportation risks/impacts associated with the proposed Yucca Mountain repository. This study was funded using Federal Nuclear Waste Funds appropriated by Congress for the State of Nevada through the U.S. Department of Energy. **This study begins by identifying the potential risk of terrorism against waste shipments to the proposed repository. Section Two examines Rand Corporation records of international terrorist activity**

to help establish that a risk exists. Additional data sources (FBI, ATF, etc.) **are examined to assess risks of terrorism domestically and/or within the state of Nevada**. **The report finds that a potential risk of terrorist attack exists for the transportation of nuclear waste. Section Three analyzes the economic, environmental, social, and moral consequences of a terrorist attack. Drawing from the existing research on the potential consequences of a severe transportation accident, the report finds that significant consequences could result from a successful terrorist attack using armor-piercing weapons**. In **addition to the human health, environmental, and economic consequences, a terrorist attack may exacerbate public perceptions of the risks of nuclear waste transportation.** This report suggests that, **as a result of these potential consequences, shipment safeguards and prevention countermeasures become a vital part of any risk reduction strategy for the proposed Yucca Mountain facility**. **Section Four analyzes various methodologies for risk reduction (e.g., safeguards). The report pays particular attention to counter-terrorism intelligence systems, transportation engineering designs, transportation plans, and relevant regulations**. The **report concludes with recommendations for additional research including studies of the preparedness level of Nevada's law enforcement and emergency management agencies, consequences of attacks using armor-piercing weapons, and rural impact studies**. Funding for these independent research projects should become a priority for the Department of Energy and the Nuclear Regulatory Commission. DOE should incorporate the results of these research efforts into the transportation planning for the proposed Yucca Mountain repository and the Environmental Impact Statement that must be submitted to the NRC.

Non-Power Options

New technologies have enabled us to see the potential for a slew of exciting new technologies and innovations that affirmatives could potentially turn into advantages:

Gray, J.D. Candidate, Sandra Day O'Connor College of Law at Arizona State University, **Spring 2009**
[John, “Comment: Choosing the Nuclear Option: The Case for a Strong Regulatory Response to Encourage Nuclear Energy Development”, Arizona State Law Journal, 41 Ariz. St. L.J. 315, Lexis]
Finally, a strong nuclear industry would help in a wide variety of other areas outside the energy sector. These include assisting in district heating, industrial processes, ship propulsion, and space travel applications, n93 as well as reducing coal burning's environmental impact by using nuclear power plants to power coal gasification techniques, n94aiding in the sterile insect technique to reduce pests' crop destruction, and irradiating food to prevent food-borne diseases. n95 Research and development have already shown strong promise for these techniques, and the nuclear industry holds the potential for many more. n96 The key is that policymakers cannot and should not view nuclear power's benefits as confined only to the electricity sector. [*332] The industry holds promise in a variety of other areas, each independently sufficient to justify support of the industry.

Negative Ground

There is a slew of literature addressing the harmful consequences of a United States which relies more heavily on its nuclear infrastructure (Plus most affirmative teams will have inherent tension claiming nuclear tech good and nuclear war bad). The list below is just to illustrate that there is negative ground. The fact that the United States hasn’t bought into Nuclear power after thorough understanding of its benefits shows that there are legitimate concerns to be dealt with on the issue of nuclear safety.

Natural Disasters

The Toronto Star, March 19
[Sarah Barmak, “Is nuclear power safe?;
The earthquake in Japan and its effects 'have reminded the whole world of the risks'”, Lexis]
Dr. Rianne Teule, Greenpeace anti-nuclear activist and radiation scientist, quoted by CNN: "Despite their assurances, the nuclear industry is not prepared for this kind of disaster - even with state-of-the-art technology, and even in Japan, a country well prepared for earthquakes. I hope that governments will take this incident as a serious warning and rethink their strategy, choosing less risky energy options instead."

Terrorism

The Toronto Star, March 19
[Sarah Barmak, “Is nuclear power safe?;
The earthquake in Japan and its effects 'have reminded the whole world of the risks'”, Lexis]
Sheldon Filger,Huffington Post: "In effect, a nuclear power reactor located within 20 or 30 kilometres of a major population centre is the ultimate radiological bomb. Its promise of cheap, safe and supposedly clean electricity exists only in a parallel universe, where human failings and mistakes do not occur, **terrorism is non-existent and natural disasters such as earthquakes and tsunamis do not happen**

Politics

NPR, 5/26
[PETER OVERBY, “Amid Scrutiny After Spill, Oil Lobby Weighs Response”, http://www.npr.org/templates/story/story.php?storyId=127122334]
Tyson Slocum, the energy policy program director of the progressive group Public Citizen, says he isn't counting the oil industry out. "Big Oil's legislative agenda is still able to function, even after a devastating event like we've got going on in the Gulf of Mexico right now," Slocum said. An industry lawyer was more direct. Speaking on background, after his boss told him not to, he said: "Never, ever, ever, ever underestimate the influence of the oil industry in Congress."

Reuters, March 13
[Jeff Mason and Will Dunham, “Japan nuclear woes cast shadow over U.S. energy policy”, http://www.reuters.com/article/2011/03/13/us-nuclear-usa-idUSTRE72C2UW20110313]
Since the 1979 accident at the Three Mile Island nuclear plant in Pennsylvania, many Americans have harbored concerns about nuclear power's safety. Controversy has also dogged the nuclear power industry due to its radioactive waste, which is now stored on site at reactor locations around the country.

International Coalition Counterplans

Maarbjerg, University of Baltimore J.D. Candidate, **2009**. [Martin Peder, “THE GLOBAL NUCLEAR ENERGY PARTNERSHIP: IS THE CURE WORSE THAN THE DISEASE?”, University of Baltimore Journal of Environmental Law, 16 U. Balt. J. Envtl. L. 127, Spring, Lexis]
Because GNEP falls short of the goals it is trying to accomplish, the GNEP countries should come together with the new U.S. presidential administration to

more completely analyze the nuclear fuel cycle and the environmental and nuclear weapons proliferation issues that arise with reprocessing/recycling and the storage of nuclear power plant wastes, as well as to analyze the future of nuclear energy. Although GNEP is not the answer to these problems, nuclear energy should hold a significant place in future international and national programs erected to combat the problems caused by greenhouse gas emissions.

Postal and Shipping

Introduction

We all use the postal system, so it's easy to see the importance this sector has for the everyday functioning of the United States. What is less apparent is the massive amount of organization required to keep this system running. The department of homeland security reports that the Postal and Shipping sector employs over 1.8 million people, bringing in over $213 billion a year[172]. Despite its importance, this sector is a somewhat recent addition to the CIKR list, only having been added in 2002.

The postal and shipping sector operates under the umbrella of the Transportation Security Administration (TSA) and accounts for all small and medium-class shipping[173].

Affirmative Ground

Affirmatives seeking to address the postal and shipping sector are likely to be focused on probability rather than magnitude-based impact claims. The Department of Homeland Security notes that it would be incredibly simple for terrorists to insert dangerous materials into the system through any of the hundreds of unmonitored access points across the nation[174]. Adding to the threat of terrorism, the DHS has indicated that the postal and shipping sector would be essential to the survival of the nation in the event of a disease epidemic[175]. While it is incredibly likely that the continued degradation of our postal and shipping sectors will one day spur a national emergency through terrorism or other impact areas, those affirmatives that are looking for multiple nuclear war scenarios will need to look elsewhere. That being said, there are a plethora of internal links available that might make this topic area a lynchpin for other solvency claims:

> **Department of Homeland Security, 2008**
> (http://www.dhs.gov/xlibrary/assets/nipp_snapshot_postal.pdf)
> **Every sector of the economy depends on the** service providers in the **Postal and Shipping Sector** to deliver time-sensitive letters, packages and other shipments. These **time-sensitive delivery needs are critical to the Banking and Finance, Government Facilities, Commercial Facilities, and Healthcare and Public Health Sectors, who all rely heavily on the** Postal and Shipping **Sector for the shipment and delivery of critical documents and packages**.

Affirmatives interesting in addressing this topic section will likely focus on the postal industry's influence on other key sectors of the economy. The literature base for this topic area is diverse and extensive; benefiting from the works of the Postal and Shipping Sector Coordinating Council. This council includes

---

[172] DHS 2008, National Infrastructure Protection Plan: Postal and Shipping Sector, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_postal.pdf
[173] DHS 2009, National Infrastructure Protection Plan, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
[174] DHS 2008, National Infrastructure Protection Plan: Postal and Shipping Sector, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_postal.pdf
[175] DHS 2008, Pandemic Influenza Preparedness, Response, and Recovery Guide for critical infrastructure and key resources Annex: Postal and Shipping Sector Pandemic Guideline. http://www.dot.gov/pandemicflu/pdf/postalshipping.pdf

representatives from UPS, USPS, FedEX and DHL, all of whom provide extensive reports on the reliability and security of the sector.

Negative Ground

In the event that there are affirmatives addressing only this sector, the negative can employ some specific strategies in addition to the negative ground discussed earlier. One feasible option would be a private agent counterplan (either through consult or direct action), employing the Postal and Shipping Government Coordination Council (GCC). The GCC mission statement states that it seeks to "promote effective government coordination of postal and shipping security strategies; identify gaps and activities; establish policies and standards, program metrics, and performance reporting criteria; and foster effective communications and partnerships across government and between government and the private sector"[176]. The GCC includes representatives from all major shipping corporations in addition to representatives from various federal agencies.

What is more likely is that this topic will be addressed by affirmatives in conjunction with other areas that garner larger solvency claims. Negative teams will need to be aware of how the postal sector functions, but it seems unlikely that this area will be a focal point for debate-style arguments throughout the academic year.

[176] DHS 2008, National Infrastructure Protection Plan: Postal and Shipping Sector, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_postal.pdf

Transportation Systems

Introduction

The National Consortium on Remote Sensing in Transportation clearly describes the ripeness of the controversy with respect to Transportation Systems:

> **NCRST 05**. National Consortium on Remote Sensing in Transportation, US DOT, Spatial Information Technologies in Critical Infrastructure Protection, 2, 2005, http://www.ncgia.ucsb.edu/ncrst/research/cip/CIPAgenda.pdf
> **The transportation infrastructure of the United States**, like every country in the world, **has been vulnerable to attack, disruption, damage and destruction for many years. Although these disruptions have been caused principally by natural disasters such as floods, storms, fires or earthquakes, deliberate attacks on transportation facilities have occurred with increased frequency in the past 10 years** [Everett]. The terrorist attacks of **September 11**, 2001 have **created a new awareness of the critical role and vulnerability of transportation fleets and facilities.**

The national consciousness about transportation is as high as it has ever been. Ever since September 11, combined with the constant threat of national disasters; transportation policy has become an area of intense national focus.

Affirmative Ground

The NCRST defines Critical Transportation Infrastructure (CTI) as "Major arterial highways and bridges comprising the National Highway System (NHS), including the Strategic Highway Network (STRAHNET) and National Intermodal Connectors, International marine harbors, ports and airports, Major railroads, including depots, terminals and stations, Oil and natural gas pipelines, and Transportation Control Systems (e.g., air traffic control centers, national rail control centers) [Everett]."[177] This provides considerable core Affirmative ground. The United States Department of Homeland Security (DHS) provides a slightly different definition isolating aviation, highways, maritime transportation systems, mass transit, pipeline systems, and freight rail.[178]

Conceivable the Affirmative could select any one of these areas, or support funding for all areas. There are a number of ways to operationalize advocacy. Tax incentives, tolling, public-private partnerships (P3's) are all available options. P3s may also be Negative counterplan ground.

The NCRST isolates a number of Affirmative focus areas that provide ample Advantage ground including: "Natural Disasters (Fires, Floods, Storms, and Earthquakes), Human Caused Disasters (HAZMAT spills and releases and Major traffic crashes), Social, Criminal and Terrorist Activities (Vandalism, Sabotage, Civil unrest/riots/strikes, Attacks using chemical, biological, nuclear or explosive weapons), and Other Threats (Deferred maintenance and neglect and Energy and material

[177] National Consortium on Remote Sensing in Transportation, US DOT, Spatial Information Technologies in Critical Infrastructure Protection, 2, 2005, http://www.ncgia.ucsb.edu/ncrst/research/cip/CIPAgenda.pdf
[178] United States Department of Homeland Security, Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan May 2007, http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

shortages)."[179]

Several examples of Affirmative advantages exist, such as environmental and economic claims:

> **Peterka 10**
> Amanda Peterka, U.S. Transit Spending Key to Boosting Manufacturing Economy, E&E News, October 10, 2010, http://unitedstreetcar.com/press/2010/11/585/u-s-transit-spending-key-to-boosting-manufacturing-economy.html
> **Increased investment in public transit and intercity and high-speed rail would boost a lagging U.S. manufacturing sector and reduce greenhouse gas emissions and air pollution**, according to a report released today by a group of labor, business, environmental and community leaders. The Apollo Alliance is urging the federal government to invest $30 billion a year in public transit and $10 billion a year in high-speed rail to create 3.7 million jobs within six years, the group estimates in its Transportation Manufacturing Action Plan. More than 600,000 jobs would be in the manufacturing sector, the report says, as more investment in transit would create the need for more homegrown transit vehicles, track and supporting equipment. **"Investments in public transit done correctly are a critical piece of much-needed comprehensive national strategy to rebuild America's manufacturing sector and middle class,**" the alliance's executive director, Cathy **Calfo, told reporters** in a conference call. The report is based on research conducted by the Economic Policy Institute, Duke University, Northeastern University, the Worldwatch Institute, and business and labor leaders. The Apollo Alliance also found that since the last reauthorization of the U.S. transportation-funding law in 2003, more than $10 billion have gone overseas toward purchasing those vehicles, tracks and equipment.

Rail also has many environmental advantages relative to fuel efficiency and emissions.

> **CER 08**. Community of European Railways, Rail Transport and the Environment: Meeting the Challenge, May 28, 2008, http://www.cer.be/publications/books/1796
> **Placing environmental criteria at the forefront of transport policy has never been more important than it is today, with cutting emissions of greenhouse gases becoming one of the biggest political issues** in Europe. **Yet transport is proving the most intractable area to change, with emissions continuing to rise relentlessly. As the most efficient mode of major transport, rail has a key role to play in reducing the impact of transport and ensuring a more sustainable future**. With this in mind, CER has put together the book 'Rail transport and the environment: meeting the challenge' that puts the railways' environmental strengths into context, using contributions from over a dozen experts in the transport field.

Strong transportation systems also provide redundancy, which is key to addressing natural disasters and malevolent acts.

> **TPRSC 07**
> Transportation Policy and Revenue Study Commission, Final Report - Volume III: Section 1 - Technical Issues Papers, Analysis of Future Issues and Changing Demands on the System, Part E. Security and Emergency Management, January 10, 2007, http://transportationfortomorrow.com/final_report/volume_3_html/technical_issues_papers/paper94cb.htm?name=4e_02
> **Redundancy among transportation modes is discussed** separately **in** Commission **Briefing Paper 4E-03,** EVALUATION OF THE POTENTIAL USE OF ALL MODES IN EVACUATIONS DURING TIMES OF EMERGENCIES. **This paper** recognizes the importance of multiple transportation modes but **stresses primarily the role of other elements in achieving redundancy.** It provides information on the transportation

[179] National Consortium on Remote Sensing in Transportation, US DOT, Spatial Information Technologies in Critical Infrastructure Protection, 2, 2005, http://www.ncgia.ucsb.edu/ncrst/research/cip/CIPAgenda.pdf

> system's ability to support local, State, Regional or Federal authorities in planning for and executing safe evacuations during disasters or emergencies. **It notes that implementation of safe and effective evacuations triggered by either manmade** (e.g., hazardous materials incidents, transportation accidents or malevolent acts) **or natural disasters** (e.g., earthquakes, hurricanes, tsunamis, floods) **depends upon** local knowledge of the capabilities and **availability of both public and private response and recovery resources**.

Further, a strong transportation network supports many homeland security priorities.

> **ASCE 08**
> American Society of Civil Engineers, Authorization of the Nation's Surface Transportation program: A Blueprint for Success, March 14, 2008, http://www.asce.org/Content.aspx?id=7690&css=print
> Support and assist homeland security initiatives**. Transportation operations and homeland security share many of the same goals and functions. Resource sharing** (e.g. communications infrastructure, traffic control centers) **and joint planning are appropriate. Transit security and preparedness, international border security, asset security and tracking, vulnerability assessment, planning, and creation of system redundancy are important transportation priorities for homeland security.**

The clearly defined ground of this sector should provide ample room for Affirmatives to topically engage the Resolution. The alternate definitions also provide room for the Negative to engage in a substantive Topicality debate.

Negative ground

The Negative is able to make on case arguments against each Affirmative case area as well as each advantage area. The literature base is strong and all teams should be able to find on case positions on all plans and cases.

As mentioned above, topicality is a viable position for the Negative as well. Definitions for critical transportation infrastructure vary, with definitions containing different groups of transportation infrastructure. A savvy Negative team should be able to articulate why a certain category subcategory of transportation infrastructure falls outside the scope of the Resolution. Arguments about substantial changes to transportation infrastructure should also be relatively easy to make. Does affecting only one sector constitute a substantial change? Must all sectors be affected? The interconnectedness of transportation sectors also means Effects- and Extra-Topicality arguments will be plausible strategies.

Politics disadvantages are strong in this infrastructure sector. The uncertainty over the passage of the Transportation Reauthorization Bill (SAFETEA-LU, P.L. 109-59) allows for several complex political scenarios. Republicans and Democrats are struggling with funding priorities, the use of continuing resolutions (CR's) vs. a multi-year bill, and myriad other issues from tax incentives to environmental issues.

The Uniqueness story is currently that a multi-year bill is likely before the end of the year, despite the history of continuing resolutions:

> **Press-Republican 4/14**
> (Dan Heath [Press-Republican], Optimism refuels desire for multi-year transportation bill, Plattsburgh Press-Republican, April 14, 2011,

http://pressrepublican.com/0100_news/x1041535164/Optimism-refuels-desire-for-multi-year-transportation-bill)
There is optimism in Washington, D.C., that a new multi-year federal transportation reauthorization bill will be crafted by the end of the year. There has been no multi-year bill since the last one expired in October 2009. Congress has authorized a series of short-term authorizations since then.

New investments in transportation infrastructure will cost political capital:

New York Times 4/5
(Elena Schor [Greenwire], Budget Drama Casts Fresh Doubt on Transportation Funding, New York Times, April 5, 2011, http://www.nytimes.com/gwire/2011/04/05/05greenwire-budget-drama-casts-fresh-doubt-on-plan-for-tra-57096.html)
A new long-term transportation bill is dearly sought by many in the capital -- Democrats, Republicans, business and labor -- but the Hill's spending stalemate is laying bare the political challenge of selling significant new infrastructure investment to a Congress consumed by thrift.

Economy stories will also be popular. Transportation funding, at the root of many possible Affirmative plans and cases, is a complex issue that dramatically affects other spending decisions and the economy at large. Furthermore, transportation projects are often described in terms of economic development, which may or may not provide further linkages into an Economy story. The fact is that the Highway Trust Fund is broke:

Providence Journal 4/9
Bruce Landis [staff writer, Providence Journal], Highway Trust Fund is 'broke,' expert tells R.I. officials, Providence Journal, April 9, 2011, http://www.projo.com/news/content/TRANSPORTATION_FORUM_04-09-11_BUNDRJ8_v7.1864c8e.html
Jack Basso, **a top official at the national organization representing state departments of transportation, said the Highway Trust Fund,** the backbone of the federal transportation financing system, **is "broke." Moreover, he said, there is no support in Washington, D.C., for an increase in highway user fees, like the federal gasoline tax, to restore it. Like the state gasoline tax, the purchasing power of revenue from the federal tax is declining.**

Counterplan ground will likely consist of several Plan Inclusive Counterplans (PICs) where a Negative may seek to remove a certain subcategory or even a specific piece of funding in a subcategory. Counterplans may also include commission counterplans, and actor counterplans (Department of Homeland Security vs. Department of Transportation for example. The most likely Counterplans will be PICs, however, which are most strongly supported in the literature base.

State counterplans are also possible, although the literature base seems to suggest that comprehensive federal legislation is needed. States have been known to engage in innovate practices including tolling, bonding, transportation banks, and other policies to fund transportation. Additionally, public-private partnerships may be a plausible counterplan strategy.

Rall 11
Jamie Rall, Public-Private Partnerships for Transportation, 19.16 NCSL LegisBrief (March 2011), http://www.ncsl.org/?TabId=22325
A combination of deteriorating infrastructure, growing travel demand and declining public revenue is creating a crisis for America's transportation system. In this

> **context, public-private partnerships** (PPPs or P3s) **are** receiving new emphasis as **one alternative** that may help states achieve much-needed transportation improvements. Public-private partnerships are contractual agreements between public and private sector partners. **They allow private companies to assume traditionally public roles in infrastructure delivery, but keep ultimate ownership, oversight and responsibility in public hands. As many as a dozen types of such partnerships exist.** In some, facilities are built, financed, renovated or operated by private companies in return for the right to collect user fees such as tolls. In others, the state pays a private company directly, sometimes based on how well certain performance goals have been met.

The critical ground for this sector offers several interesting possibilities. The clearest link story is to issues of race and Whiteness. The placement of transportation infrastructure has long been a way to segregate populations.

> **Bullord 05**
> Robert D. Bullord [Director, Environmental Justice Resource Center, Clark Atlanta University], Transportation Policies Leave Blacks on the Side of the Road, The Crisis, January/February 2005, http://findarticles.com/p/articles/mi_qa4081/is_200501/ai_n9522085/
> **Transportation is one of the most significant aspects of our lives, yet few people realize the historical civil rights struggle associated with it. In fact, the modern Civil Rights Movement has its roots in transportation**. In 1896, the U.S. Supreme Court upheld Louisiana's segregated “White” and “Colored” seating on railroad cars. The case, Plessy v. Ferguson, ushered in the infamous doctrine of "separate but equal.” **Plessy not only codified apartheid in transportation facilities, but also served as the legal basis for racial segregation in education**. The ruling was overturned in 1954 by the historic Brown v. Board of Education of Topeka decision, in which the Supreme Court declared that the “doctrine of ‘separate but equal’ has no place.”

Suburbia also provides a strong link to critical race and whiteness position.

> **Holmes 97**
> Henry Holmes, Just and Sustainable Communities, in Just Transportation: Dismantling Race and Class Barriers to Mobility 22, 24 (Robert D. Bullard & Glenn S. Johnson eds., 1997).
> **Suburbia, as we know it today, became the preferred middle- class lifestyle. With it came patterns of economic development, land use, real estate investment, transportation and infrastructure development that reflected race, class and cultural wounds deeply embedded in the psyche and history of the United States. Jim Crow**—institutionalized segregation and apartheid against African Americans and other nonwhites— was reflected in urban and suburban zoning codes, restrictive racial covenants in real estate investment and lending practices, redlining by financial institutions, discriminatory private business practices, and the distribution of public investments. All these **served the interests of the policy-makers, usually the corporate elite who were typically European-American and middle class or wealthy**.

Federal highway spending may provide the strongest link.

> **Mandell 08**
> Bekah Mandell, Racial Reification and Global Warming: A Truly Inconvenient Truth, 28 Boston College Third World L. J. 289, at 322 (Spring 2008)
> **Racist federal transportation policy has reified race in American society in a number of ways**.189 First and foremost**, federal transportation policy contributed to**

> **racial segregation in American society through decades of spending on an interstate highway system,** which made private car transportation possible.190 **Beginning with legislation in 1916 that made state and federal cooperation in highway funding possible, a combination of state and federal dollars eventually paid to build the extensive interstate highway system** that now crisscrosses the nation.191 This federal and state financial commitment to passenger car travel contrasts sharply with its laissez-faire attitude towards funding public transport.192 According to the Federal Highway Administration, the federal subsidy of passenger car travel on the interstate highway system had cost more than $119 billion by 1996.193

Further research will provide numerous other links to standard criticisms of capitalism and the state. Transportation is ripe for these sorts of arguments as transportation is often seen as the backbone of the economy and transportation systems are often used, again with funding constrains, to exert federal government control over states and citizens.

Conclusion

The transportation sector provides plausible options for both the Affirmative and the Negative. Transportation is an important issue on the forefront of many political discussions. There is ample ground for topically engaging the Resolution, and also ample ground for Negatives to engage both on and off case arguments. Transportation is an active issue at the federal, state, and local levels. The literature base continues to develop almost daily and as the U.S. federal government grapples with funding issues as well as legislation, there should be a changing terrain that keeps both the Affirmative and Negative engages in this sector throughout 2011-2012.

Water

Introduction

Recent international incidents including terrorist attacks in France and South Africa have illustrated that terrorist organizations are increasing their focus on attacking water-based resources.[180] While there have been no widespread attacks on the United States' water resources in recent history, literature shows that an attack is inevitable if current water systems are not updated and better protected. Realizing this threat, J. Edgar Hoover observed in 1941 that "among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace."[181]

Despite Hoover's observations, the water sector remains vulnerable to attack and breakdown. In coming years, these problems are likely to become exasperated due a number of developing factors:

> In the U.S., a recent AwwaRF study listed a number of other future utility issues which are projected to consume our attention in coming years. These include: (1) population and demographic changes. (2) political environment complexity, (3) increasing regulations, (4) workforce issues, (5) technology improvements. (6) total water management. (7) changing customer expectations, (8) utility finance constraints, (9) energy cost and supply reliability, and (10) increased risk profile (Means et al. 2006).[182]

Currently, most of the responsibility for assessing the vulnerability of the water sector falls on local operators. These operators were forced to double their efforts in the months prior to January 2000, fearing a system-wide collapse due to Y2K computer glitches. Upgrades in preparation for Y2K were a double-edged sword, as they increased focus on digital systems security but subsequently drew resources away from physical protection of water resources.[183]

The need for a holistic revamping of the water sector has been reiterated time and again in Congressional records, appealing to the need of reliable water services in order to sustain other critical infrastructures. Unfortunately, current strategies continue to favor an ad hoc localized initiative, meaning that while some facilities are extremely secure others remain woefully neglected.[184]

Covering a great number of resources and facilities, the water sector includes a wide variety of technologies, each dedicated to the continued operation of the United States:

---

[180] Lorenz, Frederick M., The Protection of Water Facilities Under International Law, 2003.
[181] Copeland, C. and Cody, B., Terrorism and Security Issues Facing the Water Infrastructure Sector, CRS Report to Congress, 2003.
[182] Haskins, S. "Report: Risk management: current states, gaps, and looking ahead." In *Strategic Asset Management of Water Supply and Wastewater Infrastructure,* Alegra, H. and Céu Almeida, M. (eds.), 2009.
[183] Copeland, C. and Cody, B., Terrorism and Security Issues Facing the Water Infrastructure Sector, CRS Report to Congress, 2003.
[184] Department of Homeland Security, Water: Critical Infrastructure and Key Resource Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.amwa.net/galleries/securityinfo/Water_SSP-Open.pdf, 2007.

> "water infrastructure systems include surface and ground water sources of untreated water for municipal, industrial, agricultural, and household needs; dams, reservoirs, aqueducts, and pipes that contain and transport raw water; treatment facilities that remove raw water contaminants; finished water reservoirs; systems that distribute water to users; and wastewater collection and treatment facilities. Across the country, these systems comprise more than 75,000 dams and reservoirs; thousands of miles of pipes, aqueducts, water distribution, and sewer lines; 168,000 public drinking water facilities (many serving as few as 25 customers); and about 16,000 publicly owned wastewater treatment facilities."[185]

The wide spectrum of issues pertaining to the continued reliability of the water sector indicate that affirmatives should have no trouble isolating how best to increase the reliability and security of this topic area.

Affirmative Ground

Affirmative teams seeking to address the water sector do not need to solve all of the facilities listed above. Recent congressional records have specified that only portions of the water sector qualify as 'critical,' particularly "the 340 large community water supply systems which each serve more than 100,000 people."[186] The potential vulnerability of these systems has been well illustrated:

> **Copeland & Cody, 03**
> (Terrorism and Security Issues Facing the Water Infrastructure Sector, Claudia Copeland and Betsy Cody, Resources, Science, and Industry Division, http://www.fas.org/irp/crs/RS21026.pdf)
> While some experts believe that risks to water systems actually are small, because it would be difficult to introduce sufficient quantities of agents to cause widespread harm, concern and heightened awareness of potential problems are apparent. **Characteristics that are relevant to a biological agent's potential as a weapon include its stability in a drinking water system, virulence, culturability in the quantity required, and resistance to detection and treatment**. Cyber-attacks on computer operations can affect an entire infrastructure network, and **hacking in water utility systems could result in theft or corruption of information or denial and disruption of service.**

The Clean Water Act (CWA) currently provides safeguards against any leaks that might result due to malicious intent or human error, but these stopgaps only go so far. The EPA has no federal jurisdiction to control or upgrade the security systems; they merely operate in an advising capacity, encouraging plant operators to institute voluntary initiatives[187,188] Affirmatives can solve these harms by increasing the regulatory power of the EPA, either through the CWA to include or other relevant forms of legislation. Additionally, an increase in funding as a means of implementing EPA proposals could solve many of the ills currently plaguing the water sector.[189]

While the threat to drinking water has been well-documented, considerably less attention has also been paid to the protection of wastewater treatment facilities. This disproportion allocation of resources

---

[185] Copeland, C. and Cody, B., Terrorism and Security Issues Facing the Water Infrastructure Sector, CRS Report to Congress, 2003.
[186] Copeland, C. and Cody, B. Terrorism and Security Issues Facing the Water Infrastructure Sector, CRS Report to Congress, 2003
[187] Copeland, C. and Cody, B. Terrorism and Security Issues Facing the Water Infrastructure Sector, CRS Report to Congress, 2006.
[188] U.S. Environmental Protection Agency, Office of Inspector General, EPA Needs a Better Strategy to Measure Changes in the Security of the Nation's Water Infrastructure, Report No. 2003-M-00016, September 11, 2003.
[189] Copeland, C., Terrorism and Security Issues Facing the Water Infrastructure Sector, CRS Report to Congress, 2010.

makes sense given the potential impact of attacks on drinking water (millions dead) versus the impact of wastewater (release of untreated sewage into the ecosystem). This discrepancy provides ample ground for critical affirmatives, arguing that the prioritization of human cities over the earth's nature resources is akin to ecocide.[190] Additionally, there is ample political-based ground in the wastewater subsection, stemming from non-secure facilities.

> **Copeland & Cody, 03**
> (Terrorism and Security Issues Facing the Water Infrastructure Sector, Claudia Copeland and Betsy Cody, Resources, Science, and Industry Division, http://www.fas.org/irp/crs/RS21026.pdf)
> **Vulnerabilities do exist**, however. **Large underground collector sewers could be accessed by terrorist groups for purposes of placing destructive devices beneath buildings or city streets**. D**amage to a wastewater facility prevents water from being treated and can impact downriver** water **intakes. Destruction of containers that hold large amounts of chemicals at treatment plants could result in release of toxic chemical agents**, such as chlorine gas.

Whether affirmative teams chose to address these issues individually or under a single umbrella policy, ample solvency exists for each of these water subsectors, including a candid governmental analysis indicating that an increase in federal control over risk assessment would greatly improve the security of the sector:

> **Department of Homeland Security, 07**
> (Water: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, http://www.amwa.net/galleries/securityinfo/Water_SSP-Open.pdf)
> **The Water Sector does not use a formal screening process to identify which assets should or should not perform risk assessments**. EPA, in collaboration with the sector, continues to encourage all utilities to take security concerns into consideration. The **different risk assessment methodologies developed for use by utility owner/operators allow them to choose the methodology most applicable** to their security requirements depending on utility size, treatment method, and population served. Given the large number of Water Sector utilities throughout the Nation and the limited resources available to address their security, the objective of the RAMCAP process is to prioritize at the national level those sector assets that warrant more in-depth risk analyses. **The entire sector**, especially owner/operators, **may benefit from coordination within the sector on development of a screening process to determine the need for detailed risk assessments.** Risk assessments are iterative; therefore, **exploring development of screening methodologies could help identify assets that are significant enough to require further assessment**. Because not all utilities face the same level of risk, the sector may want to limit more detailed assessments to only those assets with the highest risk. Specifically, a screening process that may use a standard form containing a few simple questions could be developed in collaboration with Water Sector security partners, EPA, and DHS. The screening would enable owner/operators to quickly look at potential consequences associated with attacks on theirs asset and determine whether those consequences are significant enough to warrant additional assessments.

Negative Ground

Much of the negative ground available through the water sector focuses on arguments pertaining to the cost and political uncertainty of increasing federal regulation over private actors such as water plant

[190] Luke, Timothy. Discourses of the Environment, 1999.

operators. Previous attempts to increase EPA control over threat assessment have failed in Congress due to intense lobbying on behalf of the private sector that is afraid that increased regulation will cripple the industry.[191] These uncertainties concerning government regulation have manifested in the form of intense lobbying, but they have also spurred the formulation of privatization proposals which provide access to private-actor counterplans:

> **Underhill**, Founder of Capital Innovations LLC, 20**10**
> (The Handbook of Infrastructure Investing, Water and Wastewater Infrastructure, 2010)
> **Improving water delivery, minimizing costs and increasing effectiveness of water recycling necessitates infrastructure investments** moving forward. **The investment can come in multiple forms, the most prevalent being the privatization of the urban water delivery and wastewater management** sector. At the beginning of the decade, the global market for water and wastewater treatment was estimated at $160.8 billion, with Australia, Canada, the United States, and the counties of Western Europe accounting for 87 percent of this market. 'This market will continue to grow, even in the countries already listed. Challenges to access arc no longer a concern in these areas, but **the water supply needs to be repaired, water treatment Technologies expanded, and water storage practices enhanced.** For example, the Environmental Protection Agency (EPA) estimates That the current U.S. water infrastructure requires $334.8 billion capital investment over the next 20 years, broken down as follows: transmission and distribution (60 percent), treatment 122 percent), storage (1 percent), sourcing (6 percent), and other (I percent). The long-term need is driving a steady increase in spending; The European Union (EU) estimates that $75 billion per year is currently spent on water and wastewater services, and capital is expected to increase by 7 percent annually. As is typical in infrastructure spending, the developed world requires refurnishing and maintenance costs, and the developing world's spending will target the construction of new infrastructure, fueled by the demand for greater water access. The UN's Millennium Development Mal (MDG) sets out a lofty objective for environmental sustainability number of people without access to safe drinking water and basic sanitation in half by 2015. In order to achieve this annual water services spending needs to be increased to $180 billion from $75 billion. Even without achieving the UN's MDG, access to water for drinking and sanitation purposes will require spending in the developed world due to rapid urbanization and a lack of infrastructure to support it. As evidence of this Trend, private water and sanitation projects in developing countries increased more than fifteenfold (from $2 billion to $35 billion) over the eight-year period between 1992 and 2000. **Private sector participation can lead to new thinking on best-cost solutions in the management of catchment areas and in water supply solutions**.

While much of the water sector has undergone privatization in recent decades, the influence of governmental actors remains an unsettling factor for investors. The relationship between public and private actors in the water sector is far more volatile than you will find in most CIKR sectors. This is due in part to the developing fear of global water scarcity, leading to a vast literature base on the merits of various water plans.

[191] Copeland, C., Terrorism and Security Issues Facing the Water Infrastructure Sector, CRS Report to Congress, 2010.

VII. GENERIC NEGATIVE GROUND

Overview

Generic negative ground for critical infrastructure has a number of possibilities. After researching various ideas, the strongest generic policy 2NRs against most, if not all, affs would be one of the following:

1. Politics DA and Agent CP
2. Agency Overstretch DA and Plausible Agency CP
3. Business Confidence DA and Private Industry CP or Regulatory Negotiation CP

These strategies are considered the strongest as the literature base is very diverse and strong. In addition, links and solvency mechanisms do not have to be tailored to specific affirmative action in order to solve. This makes these strategies probably the core of most negative teams absent a smart specific strategy. In addition, they are viable for even small schools given the strength of the evidence for each mentioned strategy.

There is other possible negative ground, but the literature was either not as in depth or not as widely applicable. These strategies are included in the "Possible Negative Ground" subsection.

For critical ground, negative teams can look forward to a wide spectrum of arguments that will be pertinent to individual cases, but may also be applicable on a resolution-wide scale. Though most of the critical ground that is relevant to individual areas has been embedded into the appropriate sector discussions, it is important to briefly mention the generic kritiks afforded through this topic area.

Kritiks

Some of the mainstays of kritik debaters, such as various versions of the capitalism kritik, are clearly able to fit into the CIKR topic. This is particularly true given that two of the sectors (Banking and Commercial Facilities) unapologetically encourage affirmative teams to focus their attention on capital gains and economic signifiers rather than individuals.

Beyond the kritiks that are available on a yearly basis, a number of arguments will be available through generic negative ground, yet these generic kritiks can also be tweaked depending on the sectors being discussed. One such example is the consumption/environmental managerialism kritik, primarily authored by Timothy Luke:

> **Luke 99**
> Timothy W. Luke, Professor of Political Science at Virginia Polytechnic Institute and State University,1999, Discourses of the Environment, p. 141-42
> In some sectors or at a few sites, **ecologically more rational participation in some global commodity chains may well occur as a by-product of sustainable development**. Over-logged tropical forests might be saved for biodiversity-seeking genetic engineers; over-fished reefs could be shifted over to eco-tourist hotel destinations; over-grazed prairies may see bison return as a meat industry animal. **In the time—space compression of postmodern informational capitalism, many businesses are more than willing to feed these delusions with images of**

> **environmentally responsible trade**, green industrialization, **or ecologically sustainable commerce, in order to create fresh markets for new products**. None the less, **do these policies contribute to ecologically sustainable development? or do they simply shift commodity production from one fast track to another slower one, while increasing opportunities for more local people to** gain additional income to **buy more commodities that further accelerate transnational environmental degradation**? or do **they empower a new group of outside experts following doctrines of engagement to intervene in local communities and cultures so that their geo-power may serve Global Marshall Plans**, not unlike how it occurred over and over again during Cold War-era experiments at inducing agricultural development, industrial development, community development, social development and technological development? Now that the Cold War is over, as the Clinton/Gore green geopolitics suggests, **does the environment simply substitute for Communism as a source and site of strategic contestation, justifying rich/powerful/industrial states' intervention in poor/weak/agricultural regions to serve the interests of outsiders who want to control how forests, rivers, farms or wildlife are used?**

Other critical arguments that will apply to most plans include rhetoric-based arguments such as terror talk and securitization, both of which can be argued against nearly all CIKR sectors. On a meta-level, the entire CIKR section falls into the type of thinking outlined by the risk kritik, illustrated in the Chemical sector earlier in this topic paper.

The particular kritiks developed through this topic will largely depend on the particular resolution wording chosen by the debate community. Regardless of which sectors are included in the final resolution, it remains clear that there will be a large spectrum of critical arguments available to the negative, ensuring the ability to discuss philosophical and moral questions as they pertain to the topic.

Politics/Elections DA

Politics is interesting for a couple reasons. First, increasing spending is unpopular right now with the GOP. Second, various infrastructure projects would benefit different regions, which means they have support by various Congresspersons. Depending on the infrastructure sector, politic disads could fall into two categories.

The first type is where the GOP backlashes over the plan due to increased spending and fails to support a Democrat measure in the House. The second is where the Democrats appease the GOP by conceding on GOP measures. The problem with identifying how these would work out is of course dependent on the political climate come the fall and spring.

Debates in the spring on politics on spending issues would be far more interesting. Assuming Congress passes the 2012 budget by October, Congress typically debates the budget issue early in the year (this year was a bit late as they hadn't passed the 2011 budget). That means for January until March, negative would have good negative ground on spending horse-trades either with other infrastructure programs or with other politically contentious programs.

> **Snyder,** Editor of Streetsblog Capitol Hill, a daily news source focusing on transportation and infrastructure issues, **4/19/2011**

> (Tara, “A Two-Year Transportation Bill? Some Say It’s a Better Deal,” Streetsblog Capitol Hill, http://dc.streetsblog.org/2011/04/19/a-two-year-transportation-bill-some-say-it%E2%80%99s-a-better-deal/)
> Given that projected trust fund revenues diminish steadily into negative territory over the next six years, looking only at the next two years would allow for slightly higher expenditures, but still nothing close to the robust investment needed to start addressing the nation’s massive infrastructure backlog. **And a Congress filled with deficit hawks won’t consider spending more than the Highway Trust Fund brought in — even for just two years**. Besides, the construction industry and the states are on their knees begging for a long-term bill. Donna Cooper, who served as Pennsylvania Governor Ed Rendell’s secretary of policy, said **short term reauthorizations are very inefficient ways to do infrastructure spending**. “You need the multi-year horizon to go from design to construction,” she told Streetsblog. “Otherwise you interrupt that process and you can’t keep your construction pipeline going.” She said the stimulus bill “cleaned out the closet of all the projects that could be done quickly” and now it’s time for a multi-year bill to plan, design, and build longer-term projects. **And then there’s the political calculation. Many political pundits predict that the Senate will fall to the GOP in 2012, meaning that by putting off negotiations on a long-term bill by two years, Democrats will find themselves in the minority in not one but two houses, and the only power they’ll have is the presidential veto.**

The other reason the spring is more interesting is the elections disad. The deficit and economy is on the public’s radar. Depending on the timeliness of economy/job impacts and perception of various infrastructures, there could be interesting debates on how the public perceives infrastructure spending. If short term jobs are actually created, elections would shift more towards Democrats winning more seats. If programs are perceived as a waste of money, then elections would shift more towards the GOP, as Democrats are the ones who are pushing generic infrastructure spending.

> **Snyder,** Editor of Streetsblog Capitol Hill, a daily news source focusing on transportation and infrastructure issues, **4/19/2011**
> (Tara, “A Two-Year Transportation Bill? Some Say It’s a Better Deal,” Streetsblog Capitol Hill, http://dc.streetsblog.org/2011/04/19/a-two-year-transportation-bill-some-say-it%E2%80%99s-a-better-deal/)
> But Cooper has a different perspective. She said **having an unfinished infrastructure bill could help the Democrats in the 2012 election. If I was the Republicans I’d try to get it done ahead of time because i don’t think this is a good election issue for the Republicans. The American public wants to see responsible, smart infrastructure investment** and I think they’ll worry, with the Republican party as it stands now, having such a strong anti-investment approach, “these guys aren’t going to build my road; I’m going to continue to sit in traffic; I’m not going to get that rail system.”

Business Confidence DA

Bizcon functions in tandem with the private industry counterplan. Affirmatives would require increasing government control of infrastructure or forcing directions for businesses via new regulations. Both actions would hinder profitable business opportunities. A more detailed analysis of bizcon is with the private industry counterplan given the interconnectedness between the two.

Private Industry CP

Instead of the government directing infrastructure development, private industry can direct it. A counterplan could encourage private industry development through the use of tax incentives, eliminating governmental oversight for certain infrastructure investment, etc.

Various mechanisms exist for encouraging private investment. The main issue for these generic counterplans would be having specific solvency evidence for how the affirmative increases protection or resiliency of infrastructure. Like the affirmative ground, there exists various ways to deal with this. For example, counterplans could model private industry incentives on the SAFETY Act, which gave exemptions to private company investments in anti-terror projects.

> **McNeill,** Senior Policy Analyst, Homeland Security, **08**
> (Jena Baker, September 23, "Building Infrastructure Resiliency: Private Sector Investment in Homeland Security," Heritage, http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security)
> Strengthen and promote the SAFETY Act. The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, **the SAFETY Act, is a model for how the government can increase private-sector investment**.[33] **The Act provides liability protections for companies that develop technologies or invest in homeland security projects**.[34] Absent such liability protections, the private sector is less likely to invest because of fears over lawsuits in the event of an attack. Congress and the new Administration must not forget the benefits of the SAFETY Act. Furthermore, **DHS must do more to market the Act to new and existing companies interested in investing in infrastructure. Absent the entrepreneurial energy of the private sector, the deficiency of infrastructure will continue to plague the path to resiliency**.

In addition to these exemptions, counterplans would be able to provide direction by changing regulations that the Committee on Foreign Investments in the United States (CIFUS) has for infrastructure investment. This would allow counterplans to direct private industry to solve the affirmative with the private industry as a net benefit.

> **McNeill,** Senior Policy Analyst, Homeland Security, **08**
> (Jena Baker, September 23, "Building Infrastructure Resiliency: Private Sector Investment in Homeland Security," Heritage, http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security)
> Re-evaluate CIFUS regulations. **The Committee on Foreign Investments in the United States (CIFUS), the group that reviews foreign investments in U.S. infrastructure, has the ability to reject foreign investments that might be a threat to national security**.[35] Although foreign investors do possess ownership of some U.S. structures, **critics of CIFUS argue that it has often been slower than preferred in confronting the national security element of foreign investment in infrastructure**(as evidenced by the Dubai Ports World debacle -- where CIFUS frustrated a foreign investor to the point that the investor forfeited its ownership of several U.S. ports). This is bad news for infrastructure because investors have vast sums of money capable of improving infrastructure quickly, without U.S. government intervention. The notion that precluding foreign ownership of U.S. assets offers a measure of security is flawed. Of course, CIFUS should have the ability to consider national security when it reviews foreign investments. But **it must be careful not to use national security as a means of economic protectionism. Such protectionism would ensure that infrastructure continues to deteriorate, and that real security is not achieved**.

There's good evidence from conservative think tanks (Heritage, Cato, Mises, etc.) on why the private industry is better: no bureaucracy, speed of investment, and direction of investment.

> **McNeill,** Senior Policy Analyst, Homeland Security, **2008**
> (Jena Baker, September 23, "Building Infrastructure Resiliency: Private Sector Investment in Homeland Security," Heritage, http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security)
> **The free market can improve and maintain infrastructure while stimulating economic growth**. Wise investment by the private sector can lead to dollar gains to investors. This translates into more capital for these private-sector entities to reinvest in the market. **The more the government spends, the less the private sector can engage in investment. A decrease in government spending can have an enormous effect on the economy. When Washington is too large, the "high spending undermines economic growth by transferring additional resources from the productive sector of the economy to government, which uses them less efficiently.**"[19] In other words, federal spending is associated with significant transaction costs not experienced by the private sector. For example, the government must take money from individuals, meaning the U.S. population, before it can spend it.[20] Instead of wasting time on the bureaucratic struggles and wasting American tax dollars on transaction costs, **Washington should look past the Beltway and rely on the entrepreneurial energy of the private sector**. As Secretary Chertoff stated, "What **these businesses do need is information and guidance about the best way they can carry out what they're already motivated to do**, which is to make sure that their investments are secured and that the people who work to carry out their businesses are safe."[21]

What about the perm? Well, the above piece of evidence illustrates the spending trade off. More government spending necessarily trades off and interferes with private spending, which acts as a disad to the perm. Even if the permutation were to capture the private industry net benefit, depending on the link to politics or spending, those disads would also be net benefits to a private industry counterplan.

Regulatory Negotiations CP

This is obviously very similar to the private industry counterplan. However, instead of providing direct incentives to private industries, this counterplan would negotiate with private industry about the roles and regulations for a given infrastructure. Part of this literature is based on the idea that since infrastructure is owned by private industry, they should have a say in what happens to it.

> **Carafano,** leading expert in defense affairs, intelligence, military operations and strategy, and homeland security at The Heritage Foundation. He was an Assistant Professor at the U.S. Military Academy in West Point, **2008**
> (James Jay, June 26, "Resiliency and Public-Private Partnerships to Enhance Homeland Security" Family Security Matters, http://www.familysecuritymatters.org/publications/id.467/pub_detail.asp)
> **Determining the criticality of assets, however, should be a shared activity**. In many cases, the private sector owns or is responsible for managing both private and public infrastructure that provide vital goods and services for the society. Meanwhile, **only the national government has the overall perspective to determine national needs** and priorities during disasters and catastrophic threats. **The private sector and the national government ought to work together to determine what is truly critical** to maintaining the heartbeat of the nation at a time of adversity. The issue of vulnerability should be the primary responsibility of the partner that owns, manages, and uses the infrastructure, so

it is largely the private sector's duty to address vulnerability by taking reasonable precautions in much the same way that society expects the private sector to take reasonable measures for safety and environmental protection. Equipped with these assessments and a commonsense division of roles and responsibilities, public-private partnerships ought to be able to institute practical measures to reduce risk and enhance resiliency. **Governments should participate in defining "reasonable" as a performance-based metric and in improving information sharing to enable the private sector to perform due diligence** (i.e., protection, mitigation, and recovery) in an efficient, fair, and effective manner. **A model public-private regime would define what is reasonable through clear performance measures, create transparency and the means to measure performance, and provide legal protections to encourage information sharing and initiative.**

Alternative Executive Agency CPs

For each specific sector, there are various agencies in charge of maintaining the infrastructure (e.g. Agriculture is run by the Department of Agriculture). These agencies could be argued by the aff, via the plan, or neg, via a-spec, as normal means. That leaves plausible/alternative agencies as potential counterplan ground. Here is a table summarizing these:

Bagby, – Professor of Information Science and Technology The Pennsylvania State University, **2010**
(John W., Spring 2010, "Evolving Institutional Structure and Public Policy Environment of Critical Infrastructures," Speaker's Journal Volume 9.14, http://www.pahouse.us/SpkrJournal/documents/9/v9_a14.pdf)

Table 1: Critical Infrastructure: the Sectors and Current or Plausible/Alternate Lead Agencies		
Critical Infrastructure Sector (& sub-sectors)	**Current Lead Agency**	**Plausible/Alternate Agency**
Agriculture	Dept. of Agriculture (USDA)	Environmental Protection Agency (EPA); State Depts. of Agric.
Food	USDA	Dept. of Health & Human Services(HHS); EPA; State Depts. of Agric.
Meat, Poultry	USDA	HHS; EPA; State Depts. of Agric.
All Other Ag.	Dept. of Health & Human Services (HHS)	USDA; EPA; State Depts. of Agric.
Banking, Finance	Dept. of Treasury	Security & Exchange Commission; Fed. Reserve Bd.; Comptroller; Federal Deposit Insurance Corp.; State Banking or Insurance Agencies
Chemical	Dept. of Homeland Security (DHS)	EPA
Commercial Facilities	DHS	
Communications	DHS's Office of CyberSecurity & Communications	Fed. Communications Comm. (FCC); State Public Utility Regulators
Defense Industrial Base	Dept. of Defense	Dept. of Commerce
Dams	DHS	Dept. of Interior; U.S. Army

		Corps. of Engineers
Emergency Services	DHS	Dept. Health & Human Services, State EMS Licensing Agencies
Energy (electric power, petroleum)	Dept. of Energy	State Public Utility Regulators
Government Facilities	DHS's Immigration & Customs Enforcement and DHS's Federal Protective Service	State Police
Information Technology	DHS's Office of CyberSecurity & Communications	FCC
Manufacturing (critical)	DHS	Dept. of Commerce
National Monuments & Icons	Dept. of Interior	DHS
Nuclear Power (commercial: reactors, materials, waste)	DHS	Dept. of Energy; Nuclear Regulatory Comm.
Postal & Shipping	DHS's Transportation Security Administration	Dept. of Transportation (DOT)
Public Health & Healthcare	HHS	
Transportation Systems	DHS's Transportation Security Administration & U.S. Coast Guard (maritime)	DOT; State Transportation Agencies
Water (drinking) & Water Treatment	EPA	

Net benefits for these various counterplans could either be overstretch disads for the current lead agency or advantages for the plausible alternative agency. The specific overstretch disads are included in the specific sector sections in the paper. Perms could possibly share the burden between the two, but the theoretical legitimacy of that debate would be the reason A-spec or a normal means procedural would need to be ran. However, the perm would require coordination between multiple agencies and would probably be less effective due to the rise in bureaucracy. I was unable to find specific evidence for an example, but I'd assume generic evidence about agency coordination would suffice.

Other Possible Generic Ground

Coercion DA – The scenario is simple enough. Improving infrastructure would require government expenditure, which hinders taxpayers' ability to maintain their property rights and have a say in where the money goes. It would function mainly as a possible add-on to a private industry counterplan. Since no evidence specifically speaking to whether improving infrastructure was coercive, the link is tentative at best.

Court Clog DA – This scenario is based on private industry and individuals reacting to the aff. To avoid compliance with standards, companies are likely to go to the courts. Individuals would also get involved depending on how the government goes about implementing the plan. The problem with this disad is that its highly dependent on the wording of the resolution. For instance, if the resolution is "improving protection and/or resiliency" then this disad doesn't apply, as the mechanism is about increasing government expenditure not about new regulations on companies.

Workers Union Backlash DA – There are various stipulations for working on government contracts than on private contracts primarily for construction but also applicable to other industries. Depending on the industry, these regulations might be less favorable to workers, namely in the form of benefits. The problem with this ground is it requires the affirmative's implementation mechanism to be based on subcontracting to private industry, which moots out the private industry counterplan/disad strategy.
Resource-Based DAs – Depending on the infrastructure being improved and the improvements, various commodities/resources would be used. While this was initially thought to be generic, there aren't very many, if any, generic links. Much of the literature is based on specific resources and the most generic grouping is for things like rare earth metals. Despite these shortfalls, this disad could become very prevalent depending on commodity price levels and availability to other nations.
States CP – It's a domestic topic, so the states counterplan is definitely in play. The issue with the viability of this option is state budgets are very tight right now and require balanced budgets, which means there'd be strong disads against various states from enacting the aff.