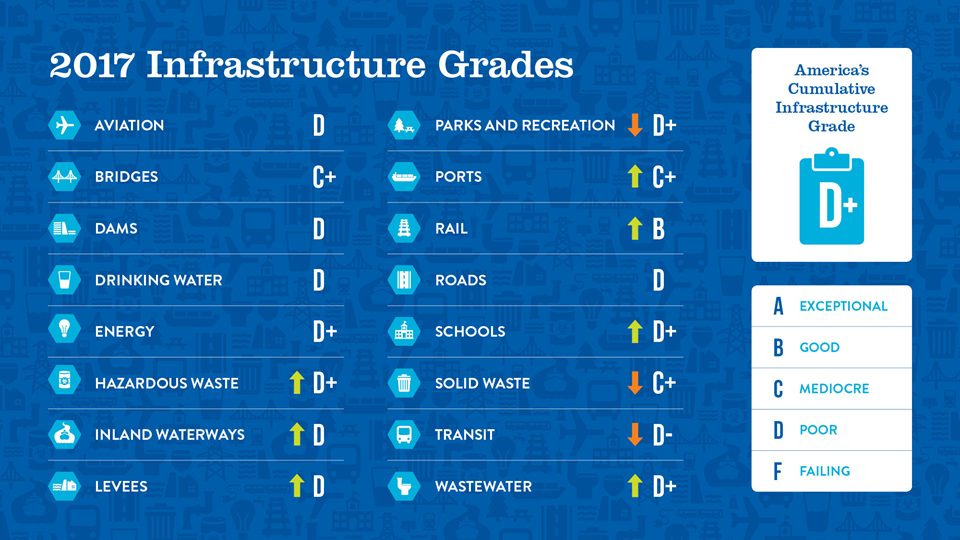
**Critical Infrastructure and Key Resources**

**2020-2021 Topic Proposal**



American Society of Civil Engineers, 2017, "America’s Grades," ASCE's 2017 Infrastructure Report Card, https://www.infrastructurereportcard.org/americas-grades///IC

Proposed to

The NFHS Debate Topic Selection Committee

August 2019

Proposed by:

Irene Caracioni and Dustin L. Rimmey

Topeka High School

Topeka, KS

# Acknowledgements

The ideas, background information and framing for this paper have come from a 2011-2012 proposal to the college topic selection committee. I would like to give credit to the original authors of the 2011-12 proposal: M. Archer, B. DeLong, T. Hahn, J. Kurr, N. Scjullo, A. Swanlek, and K. Young. A majority of the work is used throughout the paper is their original research and rhetoric and this would not exist without the hard work and effort they put into this proposal several years ago.

This paper has been updated since it was last presented by the author to the 2017 Topic Selection Meeting.

# Introduction

The nation's [critical infrastructure](https://www.dhs.gov/critical-infrastructure) provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family (DHS-CI). However, according to Cameron Mcwhirter from a 2017 Wall Street Journal article, our physical infrastructure has barely maintained a passing grade of D+. While our physical infrastructure is lacking, Ed Finkel argues that we “need to accelerate progress first of all for prevention and secondly to restore service,” if any of our Critical Infrastructure sectors were attacked or threatened by a natural disaster we would be relatively unable to function.

As a community, we have not taken the opportunity to debate infrastructure as a lynchpin of our social functioning. Yes, we have debated aspects of infrastructure like: Transportation (2012), Energy (1997,2008), and Water (1985) we have not looked holistically at the very real security challenges all of our “critical infrastructure” faces. While the Trump administration has promised to address infrastructure in his first term, his policies have either only looked at transportation infrastructure or have been stonewalled by partisan gridlock in Congress. Experts throughout the CIKR sectors agree more needs to be done to increase the resilience and security of all of our infrastructure sectors, justifying the need for debating this topic.

Depending on the sectors, affirmatives could debate protecting production, processing, and delivery of food or assisting banks in radical asset value drops or operational failure of the banking system to protecting dams, water quality, redundancies in governmental systems to curtailing the spread of pandemics. While negative teams would have access to a wide range of business and private industry disadvantages and counterplans, security criticisms, and inquiries into the best executive agency to implement changes to the resiliency of our Critical Infrastructure and Key Resources.

# Table of Contents

Table of Contents

[Acknowledgements 2](#_Toc13862998)

[Introduction 3](#_Toc13862999)

[Table of Contents 4](#_Toc13863000)

[Section 1: Introduction to CIKR 5](#_Toc13863001)

[A-1. The Definition of and Importance of U.S. Critical infrastructures and Key Resources (CIKR) 6](#_Toc13863002)

[A-2. The “Trumpdate”—How has Trump Altered CIKR since 2017? 11](#_Toc13863003)

[B. Nature of the Threats to CIKRs 15](#_Toc13863004)

[Section 2: CIKR Sectors for Debate 27](#_Toc13863005)

[2A—Areas that make for Great Debate 28](#_Toc13863006)

[Banking and Finance 29](#_Toc13863007)

[Chemical 34](#_Toc13863008)

[Communication 40](#_Toc13863009)

[Critical Manufacturing 44](#_Toc13863010)

[Dams 48](#_Toc13863011)

[Emergency Services 53](#_Toc13863012)

[Energy 62](#_Toc13863013)

[Healthcare and Public Health 68](#_Toc13863014)

[Information Technology 74](#_Toc13863015)

[Nuclear Reactors, Materials and Waste 82](#_Toc13863016)

[Water 87](#_Toc13863017)

[2B—CIKR Areas that Exist, but May Not Be Timely/Have Lit 92](#_Toc13863018)

[Agriculture and Food 93](#_Toc13863019)

[Commercial Facilities 98](#_Toc13863020)

[Continuity of Government 101](#_Toc13863021)

[Defense Industrial Base 106](#_Toc13863022)

[Government Facilities 111](#_Toc13863023)

[Transportation Systems 115](#_Toc13863024)

[Section 3: Definitions/Topicality 118](#_Toc13863025)

[Section 4: Resolutions 124](#_Toc13863026)

[Section 5: Limiting the Resolutions 125](#_Toc13863027)

[Section 6: Negative Ground 126](#_Toc13863028)

[Section 7: Why this Topic 134](#_Toc13863029)

[Section 8: Works Cited 136](#_Toc13863030)

# Section 1: Introduction to CIKR

### A-1. 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 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. 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:

Department of Homeland Security, “Critical Infrastructure and Key Resources,” Last Updated: Feb 19, 2010, http://www.dhs.gov/files/programs/gc\_1189168948944.shtm.

**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.

#### More specifically, CIKR’s are listed by the DHS as the following 18 sectors:

Department of Homeland Security, “Critical Infrastructure and Key Resources,” Last Updated: Feb 19, 2010, http://www.dhs.gov/files/programs/gc\_1189168948944.shtm.

* 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

As will be discussed later in the definitions 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. 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 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.

**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.**

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

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

**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 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**.

#### 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:

Department of Homeland Security, “National Infrastructure Protection Plan: Partnering to enhance protection and resiliency”, 2009, http://www.dhs.gov/xlibrary/assets/NIPP\_Plan.pdf.

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**.

#### 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,

Andrew W. Herrmann, “America’s Infrastructure,” CIP Report, October 2009, http://cip.gmu.edu/archive/cip\_report\_8.3.pdf

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**.

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.

#### In 2013 President Obama signed PPD-21 attempting to define roles for all levels of government and increase levels of security and communication.

White House, 2-12-2013, "Presidential Policy Directive," whitehouse.gov, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery. This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

#### **Homeland Security followed PPD-21 by introducing the National Infrastructure Protection Plan with several goals**

Department of Homeland Security, 2013 “NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,” https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

The National Plan continues to focus on risk management as the foundation of critical infrastructure security and resilience and promotes partnerships as the key mechanism through which risks are managed. In doing so, it reaffirms the role of various coordinating structures including Sector Coordinating Councils, Government Coordinating Councils, and cross-sector councils. Building on progress made toward critical infrastructure security and resilience by those councils and others over the past 10 years, this National Plan: • Elevates security and resilience as the primary aim of critical infrastructure homeland security planning efforts; • Updates the critical infrastructure risk management framework and addresses alignment to the National Preparedness System, across the prevention, protection, mitigation, response, and recovery mission areas; • Focuses on establishing a process to set critical infrastructure national priorities determined jointly by the public and private sector; • Integrates cyber and physical security and resilience efforts into an enterprise approach to risk management; • Affirms that critical infrastructure security and resilience efforts require international collaboration; • Supports execution of the National Plan and achievement of the National Preparedness Goal at both the national and community levels, with focus on leveraging regional collaborative efforts; and • Presents a detailed Call to Action with steps that will be undertaken, shaped by each sector’s priorities and in collaboration with critical infrastructure partners, to make progress toward security and resilience.

#### The 2013 NIPP had mixed levels of success, but is branded by “aspirational happy talk without action”, in response the only area of “critical infrastructure” the Trump administration is focused on is cybersecurity elements

Morgan Chalfant, 3-29-2017, "Trump pressed to secure US critical infrastructure," TheHill, <http://thehill.com/policy/cybersecurity/326218-trump-pressed-to-secure-us-critical-infrastructure>

The Trump administration appears to be taking the hint. President Trump’s proposed fiscal 2018 federal budget allocates $1.5 billion for Homeland Security to tackle cybersecurity, including protecting critical infrastructure. The budget proposal also directs the agency to ramp up cyber information sharing with federal agencies and the private sector for faster response times to attacks on federal networks and critical infrastructure. White House homeland security adviser Thomas Bossert emphasized at a recent conference that protecting critical infrastructure at greatest risk will be a priority of the new administration on cybersecurity, second only to safeguarding federal networks. He said that the new administration plans to partner with the owners and operators of critical infrastructure to achieve this goal. Brenner warned that previous administrations have engaged in “aspirational happy talk” about defending critical infrastructure without taking action.

#### However, more needs to be focused on than just cybersecurity. Elements of DHS reform could happen in the name of protecting critical infrastructure

Todd M. Rosenblum, 1-27-2017, "Reform Agenda For The Department Of Homeland Security," Forbes, https://www.forbes.com/sites/realspin/2017/01/27/reform-agenda-for-the-department-of-homeland-security/#5765b8972a31

Newly confirmed Homeland Security Secretary John Kelly will have a full plate. He needs to be postured in these first days to respond to all conceivable man-made or natural events in the homeland, prevent threats from entering the homeland, and continue to harden critical infrastructure against physical and network threats. Reforming the Department seems like a second-tier priority, but it is not. Success depends on maximizing the Department’s capabilities. Investment in internal reform will posture the Secretary—and the nation—for long-term success. Previous Secretaries, especially Michael Chertoff and Jeh Johnson, deserve great credit for making DHS a stronger whole. They increased cross-component collaboration, invested in strategic planning, and advanced seemingly mundane management concepts like establishing joint requirements and program review processes.

### A-2. The “Trumpdate”—How has Trump Altered CIKR since 2017?

#### In 2017, Trump issued EO 13800 focusing only on cybersecurity of critical infrastructure and data sharing through the government and private sectors.

Department of Homeland Security, 5-11-2017, "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," <https://www.dhs.gov/cisa/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure>

President Trump issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11, 2017, to improve the Nation’s cyber posture and capabilities in the face of intensifying cybersecurity threats. EO 13800 focuses Federal efforts on modernizing Federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies. The work undertaken to implement EO 13800 reflects the strong partnership across the Federal Government and with industry partners to safeguard the security of critical infrastructure and reduce national cybersecurity risk.

#### However, EO13800 has not been effective enough to transform the resilience of any of our CIKR networks.

Michael S. Rogers, the 17th director of the National Security Agency and 2nd Commander of U.S. Cyber Command., 6-9-2019, "Protecting our critical infrastructure in the digital age," TheHill, <https://thehill.com/opinion/cybersecurity/447596-protecting-our-critical-infrastructure-in-the-digital-age>

Faced with these circumstances, some are calling for a retreat into technological isolation — reverting from digital to analog and automated to manual, thus supposedly rendering hacking techniques obsolete. This prescription misses the point and it neuters America’s edge for innovation, a competitive advantage that supports both economic and national security priorities. On the contrary, America’s critical infrastructure is not vulnerable because it’s digital or automated; it’s vulnerable because the attackers understand the terrain better than the defenders. The security of our critical infrastructure, therefore, depends in large part on our ability to invert the visibility gap, obscuring our most sensitive assets to attackers and exposing them to defenders. We must transform what is an opaque attack surface into a transparent defense architecture. The aforementioned Pew study also polled citizens on the question of their country’s cyber preparedness. About half of Americans say their country is ready to deal with a major cyberattack. Our view is a more optimistic one informed by those who are at the tip of the spear. For the first time in the history of modern warfare, industry — not government — is on the front lines. The unfair advantage of America’s position in cyberspace is rooted not in government or industry alone, but rather in the harmonious partnership of the two. With nearly 90 percent of America’s critical infrastructure residing in the private sector, the primary burdens of defense rest with the same men and women who, for generations, have kept the industrial sector running. Now their mission has shifted from one of reliability to resilience — running under attack. As government sits in the crow’s nest monitoring the horizon of cyberspace for incoming threats, it is necessarily incumbent upon industry to surveil and rid their own networks of the adversaries who’ve already made it ashore. The circumstances of this digital battlefield — paired with deepest deference to civil liberties — has conscripted American industry into action. Indeed, this delicate division of labor is our greatest advantage.

#### Experts in the field have reached two conclusions: First, the Trump Administration has failed to meet the goals of its executive order, Secondly, Congressional and/or additional Executive action is needed to upgrade our digital ecosystem.

Joseph Marks, 5-13-2019, "Analysis," Washington Post, <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/05/the-cybersecurity-202-trump-s-efforts-failed-to-make-critical-infrastructure-safer-from-cyberattacks-experts-say/5c7d6c5b1b326b2d177d5fbd/?utm_term=.afa7c869f04c>

Some experts among the 78 percent who said U.S. critical infrastructure is not more secure today said the administration hadn’t done enough to achieve the goals outlined in its own [executive order](https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/). That order called for agencies across government to use every authority at their disposal to help industry protect critical infrastructure. But most of the efforts in support of the order are still in their early stages — including a Homeland Security Department-led process to map industry’s most critical functions that are in need of the greatest protection. “To make a major improvement in cybersecurity, the U.S. will have to make some strategic changes to how its digital ecosystem operates,” said former White House cybersecurity coordinator Michael Daniel. “That's not something that can be accomplished through an executive order alone,” said Daniel, who now leads the Cyber Threat Alliance, a cybersecurity information-sharing group. Yet many also said it wasn’t just the Trump administration’s fault. Any improvements the United States had made in protecting critical infrastructure, several experts said, were simply outpaced by adversaries who were able to improve their digital attacks even more. Dan Geer, the top cybersecurity official at the intelligence community venture capital firm In-Q-Tel, said critical infrastructure was less secure “but not because of any failure of diligence on the part of either the private or public sectors … Rather, [it’s] because our attack surface is growing faster than our diligence can grow.” Anup Ghosh, a managing director at Accenture Security and a former DARPA official, said that threats against critical infrastructure — especially against energy utilities — are proliferating “and the industry is playing catch-up.” Critical infrastructure is an official term DHS uses to describe [16 sectors](https://www.dhs.gov/cisa/critical-infrastructure-sectors) where a physical or cyberattack would be particularly devastating for U.S. national and financial security. The list includes energy, communications, financial services and transportation, among others.

More recently, the Trump Administration has focused on creating responses to Electromagnetic Pulses (EMPs). While this has been a broader interagency taskforce than EO 13800, two quick conclusions can be reached. First, this may not be effective in creating change as his other EO’s on infrastructure policy have been unsuccessful. Secondly, this EO only calls for research on the impact of an EMP, which means there may be a long timeframe on implementation of any of the findings. However, the Trump Administration has used his emergency powers to potentially make the resolution more timely when it would be debated in 2020.

#### Trump’s national emergency on information and communication has created a one year time period on review and assessment of the communications chain to minimize external threats. This emergency creates a research priority which will give the government actionable intelligence within a year.

EMS Now, 5-16-2019, "President Trump Declares National Emergency to Secure the Information and Communications Technology Critical Infrastructure Supply Chain · EMSNow," EMSNow, <https://emsnow.com/president-trump-declares-national-emergency-to-secure-the-information-and-communications-technology-critical-infrastructure-supply-chain/>

WASHINGTON – President Trump signed an Executive Order: Securing the Information and Communications Technology and Services Supply Chain, declaring that threats to the information and communications technology and services supply chain by foreign adversaries are a national emergency. The Executive Order prohibits transactions that involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary whenever the Secretary of Commerce determines that a transaction would pose a threat to national security, as articulated in the Executive Order. The Secretary’s determination would be based on consultations with the Attorney General, the Secretaries of Treasury, State, Defense, and Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and the heads of other appropriate agencies. In carrying out this mission, the Department of Commerce will issue regulations within 150 days to establish procedures for reviewing such transactions. “President Trump is acting once again to protect U.S. national security. This Executive Order addresses the threat posed by foreign adversaries to the nation’s information and communications technology and services supply chain,” said Secretary of Commerce Wilbur Ross. “Under President Trump’s leadership, Americans will be able to trust that our data and infrastructure are secure.” Implementation and Reporting The Secretary of Commerce, in consultation with the Secretary of State, is authorized to submit reports to Congress on the national emergency declared in the Executive Order. The Director of National Intelligence is required to produce an assessment within 40 days of the Executive Order on the risks to the United States Government, critical infrastructure, and the American people from information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. The Secretary of Homeland Security, in coordination with sector-specific agencies and coordinating councils, must produce a written assessment within 80 days of the Order evaluating vulnerabilities in hardware, software, and services that threaten the national security of the United States. This assessment will also evaluate to what extent the hardware, software, or services are relied upon by service providers and critical infrastructure entities. Within one year of the Executive Order, the Secretary of Commerce, in consultation as appropriate with the Secretaries of Treasury, Homeland Security, State, Defense, the Attorney General, the United States Trade Representative, the Director of National Intelligence, and the Chairman of the Federal Communications Commission must report to the President whether the actions taken are sufficient and continue as necessary to mitigate the risks identified in the Order.

### 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. Most public discussions of Critical Infrastructure have focused on election security, but not other sectors. Below you will find a discussion of the general threats that exist at both an external and internal level to our CIKRs, while our discussions later about specific CIKR sectors will highlight more specific sector vulnerabilities.

#### 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.

#### We are in a state of daily attack against US infrastructure; Russia, China, Iran and North Korea in addition to dozens of other non-state actors graze our systems frequently.

Johnathan Tal, 9-20-2018, "America’s Critical Infrastructure: Threats, Vulnerabilities and Solutions," <https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions>//IC

Critical Infrastructure Threats

Security and government officials are concerned about the vulnerabilities of America’s critical infrastructure and the threats it faces now and in the foreseeable future. In a recent Reuters article, Dan Coats, Director of National Intelligence, said: “The system was blinking red. Here we are nearly two decades later and I’m here to say the warning lights are blinking red again,” Coats specifically marked Russia, China, Iran and North Korea as “daily” attackers of America’s computer networks, at federal, state and local government agencies level, in addition to U.S. corporations, and academic institutions. There are three classes of threats to critical infrastructures: Natural - earthquakes, tsunamis, land shifting, volcanic eruptions, extreme weather (hurricanes, floods, draught), fires. Human-Caused - terrorism, rioting, product tampering, explosions and bombing, theft, financial crimes, economic espionage. Accidental or Technical - infrastructure and hazardous material failures and accidents, power-grid failures, water-treatment facilities failures, water-mains ruptures, safety-systems failures and a host of other disasters of omission and/or commission. Cyber Threats The list of cyber threats increases rapidly, as the number of hacking-sensitive platforms and potential victims increase, attracting more and more individual, private and state actors into the fray. The following list represents a partial set of typical threats (Source: GAO): Terrorists and other non-state actors seeking to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Criminal groups, attacking systems, using spam, phishing, and spyware/malware, identity theft, online fraud, and computer extortion for monetary gain. Business intelligence operators, including criminal organizations, conducting voluntary and on-demand industrial espionage. Individuals and groups “grazing” the cyber world in search of victims, for a combination of thrill, monetary and “training” purposes. Bot-network operators, using networks, or botnets, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. Disgruntled insiders, poorly trained employees, incompetent contractors – all creating the opportunities for outsiders to penetrate networks. National intelligence and psychological operations organizations, using cyber tools for information gathering, regime destabilization and as another arm furthering strategic goals. Spammers using the above methods to distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service). National and/or commercial organization specializing in deploying spyware or malware against organizations or individuals, for political and commercial purposes.

#### Recent reports suggest that there is a rising threat posed by computer hackers and state-sponsored cyber-warfare.

CBS News, “Hack Threats Aimed at Power Plants,” Jan. 28, 2010, http://www.cbsnews.com/news/hack-threats-aimed-at-power-plants/

**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**.

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:

Siobhan Gorman, 4-8-2009, "Electricity Grid in U.S. Penetrated By Spies," WSJ, https://www.wsj.com/articles/SB123914805204099085

**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**."

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 personal injury, low investment, operate from nearly any location, few resources are needed. 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.

#### 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,

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

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.**

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

#### 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. 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:

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.

**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**.”

#### The Department of Homeland Security has recently deployed new technologies to help track storms and prepare for the damage, however their recent advancements only focus on spread of information and not physical protection of infrastructure

Department of Homeland Security, 6-3-2019, "Facing the Inevitable Storm," <https://www.dhs.gov/science-and-technology/blog/2019/06/03/facing-inevitable-storm#wcm-survey-target-id>

Natural disasters, like hurricanes, are unpreventable; however, the havoc they leave behind can, at least, be lessened. Over the years, S&T has developed a host of tools in preparation for the Atlantic hurricane season; the 2019 season officially began June 1. These tools prepare our communities, protect our nation’s critical infrastructure, and help us rebound from hurricane strikes. We worked with partners across federal, state, and local governments throughout the development lifecycle of these tools. We spent time with emergency managers and first responders as they prepared for hurricanes forecasted to make landfall, and learned from academic institutions, businesses, and local communities about the true costs of these seasonal threats. Many of our tools are field-tested and available now. The ADvanced CIRCulation (ADCIRC) storm surge model, which combines rain, atmospheric pressure, and wind forecasts to predict when, where, and to what extent flooding will inundate a coastal community with greater precision than other available models. This enables decision-makers to identify which locations to evacuate as a storm approaches and to plan for mitigation and response before severe storms occur. The Android Team Awareness Kit (ATAK), which supports the complex communication and coordination needs of multi-jurisdictional responders. ATAK was deployed during Hurricanes Harvey, Irma, and Maria. The HURREVAC-eXtended (HV-X) platform, which integrates forecast and planning data to provide emergency managers with decision support tools for use in advance of and during tropical weather. The ideas for these tools -- and many more -- came from seeing how those braving these storms operate, hearing what those suffering the aftermath needed – and then attempting to bridge this gap between established operational models and the resulting damage. We learned that – although preparation was still paramount to lessening the damage a storm causes – real-time and accurate information was the thread that tied together emergency response effectiveness from forecast to impact. Yet information alone is useless if it’s not conveyed quickly, precisely, and concisely, so tandem to information is communication. Our tools address these two lessons head on, incorporating aspects of both in their buildout and deployment during actual response missions. With much of the hurricane season still ahead of us, rest assured that these tools and many more are being used to ensure the safety of Americans and reduce the inescapable shock to devastated communities. Know, too, that we continue to enhance these tools based on advancements in technology and, perhaps most importantly, feedback from users and the communities who this technology was developed to protect.

#### The threat of natural disasters is magnified by two factors: climate change and infrastructure privatization, these in combination make disaster response impossible.

Braxton Bridgers, 7-27-2018, "Critical infrastructure and first responders," New America, https://www.newamerica.org/resource-security/phase-zero-blog/torrents-water-and-trickles-data/

This past May, stormwater raced down Main Street in Ellicott City, Maryland, [trapping](https://wtop.com/howard-county/2018/07/after-2-floods-ellicott-city-shop-relocates-from-main-street/) individuals in buildings and destroying shops all through the historic town’s commercial hub. It was the second “thousand year flood” to ravage the city in the span of only two years -- indeed, many of those small businesses were still recovering from the 2016 storm. This double occurrence was not just a bout of bad luck, as the Howard County Executive [claimed](http://www.baltimoresun.com/news/maryland/investigations/bs-md-ellicott-city-flood-next-steps-20180531-story.html). Instead, meteorologists have stated it is likely the changing climate played a role in the irregular [frequency and intensity of rainfall](https://www.washingtonpost.com/news/capital-weather-gang/wp/2018/05/28/the-second-1000-year-rainstorm-in-two-years-engulfed-ellicott-city-heres-how-it-happened/?noredirect=on&utm_term=.52a25594e76c) that caused the catastrophic flash floods. The floods in Ellicott City are just one local example of climate change’s effect on a slew of U.S. disasters that have occurred over the past year, from the [destructive wildfires](https://la.curbed.com/2018/6/5/17428734/wildfires-calfornia-risk-prediction) in California to the [devastating hurricanes](https://news.nationalgeographic.com/2017/11/2017-hurricane-season-most-expensive-us-history-spd/) in the Southeast. For the foreseeable future, America is set to face an [increase](https://science2017.globalchange.gov/chapter/1/) in severe weather events like these, and government officials, the fire and emergency services, police, voluntary organizations, and other first responders need to be ready for the rise in disasters. One way to do this is to ensure those responding to disasters are well informed with up-to-date, relevant information. When a disaster happens, there is information everywhere -- about where the damage is, what structures or systems are damaged, where the electricity is out, where there are still dangerous conditions, where there are risks to human safety, and so on. That great wealth of data, however, is not all in the same hands. In part, that's because roughly [80%](http://trajectorymagazine.com/security-and-resilience/) of all infrastructure in the United States is privately owned. So, emergency responders and local government officials may not have access to all the data they need in order to make good decisions about how to respond to a disaster to minimize the damage and protect human health and safety. Data play an integral role in enhancing efforts to protect citizens during disasters, allowing emergency management practitioners—local and federal officials, as well as first responders, involved in emergency response efforts—to assess the impacts of a disaster within their jurisdiction. Through the collection and analysis of data, practitioners are able to identify areas that are especially vulnerable to disasters and then where the damage is worst when a disaster does occur, allowing first responders to help communities most in need first. Practitioners are already [leveraging accessible data](https://datasmart.ash.harvard.edu/news/article/data-driven-emergency-response-learning-from-hurricanes-harvey-and-irma-113) in an attempt to increase the nation’s resilience to natural disasters. However, what is currently missing from the field of emergency management is readily available private sector data regarding critical infrastructure, and that hinders disaster response efforts.

While the government has been slowly working on some areas of data sharing and protection, or the creation of new models, they have clearly stalled in the area of resilience or streamlining the differences between public and privately-owned infrastructure. These are areas that are highly unlikely to change in the current political climate.

#### 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,

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

**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: 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.

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. What makes Brown’s assessment more terrifying, is in 2006 we were rated at a C- for our overall infrastructure, in a decade our grade has fallen, making internal failure all the more likely.

#### Our current aggregate grade is a D+, the only sector rated as good is rail, everything else is poor and on the verge of failing.

Cadie Thompson, 2-5-2019, "America's infrastructure is decaying — here's a look at how terrible things have gotten," Business Insider, https://www.businessinsider.com/asce-gives-us-infrastructure-a-d-2017-3//IC

There's speculation President Donald Trump will discuss infrastructure in his State of the Union address on Tuesday. America's infrastructure is desperately in need of investment, according to the American Society of Civil Engineers. The ASCE estimates the US needs to spend some $4.5 trillion by 2025 to fix the country's roads, bridges, dams, and other infrastructure. Trump reportedly "hates" major parts of the infrastructure plan he unveiled in 2018, which proposed $200 billion in federal funding designed to finance new projects and repairs while incentivizing private investment. President Donald Trump is expected to discuss infrastructure in his State of the Union address on Tuesday, but how exactly he plans to do so is unclear. The Washington Post reports that White House press secretary Sarah Sanders told CNN on Tuesday that infrastructure could be an area of compromise for Democrats and Republicans, but according to The Wall Street Journal, Trump Administration officials pushed for the removal of a call for Congress to pass Trump's infrastructure plan from an early draft of his State of the Union address. Trump reportedly "hates" major parts of the infrastructure plan he unveiled in 2018, which proposed $200 billion in federal funding designed to finance new projects and repairs while incentivizing private investment. Read more: Uber and Lyft are having a terrible effect on public transportation, new research shows No matter what Trump says about infrastructure during his State of the Union address, one thing is clear: America's infrastructure is in dire need of repairs. According to the American Society of Civil Engineers' 2017 Infrastructure Report Card, which is published every four years, US infrastructure gets a D+ grade. It got the same grade in 2013. The ASCE estimates the US needs to spend some $4.5 trillion by 2025 to improve the state of the country's roads, bridges, dams, airports, schools, and more. The report breaks down the state of infrastructure in 16 different categories. Here's a look at each category's final grade, according to the organization. Aviation: D Aviation: D Airports face a $42 billion funding gap between 2016 and 2025, according to the ASCE. Reuters/Lucas Jackson Airports and air traffic control systems are in serious need of an update, the report found. With some two million people per day coming through US airports, congestion is becoming a major problem. In fact, the report estimates that 24 out of the top 30 airports in the US could soon hit "Thanksgiving-peak traffic volume" one day a week. Bridges: C+ Bridges: C+ There are about 56,000 structurally deficient bridges in the US, according to the latest data from the Federal Highway Administration. Matt Rourke/AP Photo US bridges are aging. Out of the 614,387 bridges in the US, more than 200,000 are more than 50 years old. The report estimates it would cost some $123 billion just to fix the bridges in the US. Dams: D Dams: D Officials inspect Oroville Dam's crippled spillway Tuesday, Feb. 28, 2017, in Oroville, Calif. Rich Pedroncelli/AP Photo According to the report, there were some 15,500 high-hazard dams in the US in 2016. Drinking Water: D Drinking Water: D Los Angeles Department of Water and Power crews work to repair a juncture of a water main which ruptured near the University of California, Los Angeles on Sunset Boulevard. The pipe was 93 years old. Damian Dovarganes/AP Photo The pipes that carry America's drinking water are in critical need of attention. According to the report, many of the one million pipes have been in use for almost 100 years. The aging system makes water breaks more prevalent, which means there are about two trillion gallons of treated water lost each year. Energy: D+ Energy: D+ Most power lines in the US were built in the 1950s and 1960s. shes\_so\_high/Flickr Power interruptions could become more common if more attention isn't given to the US energy system, according to the report. The majority of the transmission and distribution lines were built in the mid-20th century and have a life expectancy of about 50 years, meaning that they are already outdated. Between 2016 to 2025, there's an investment gap of about $177 billion for infrastructure that supports electricity, like power plants and power lines. Hazardous Waste: D+ Hazardous Waste: D+ About 22 million acres of land are used for hazardous waste programs. Susan Montoya Bryan/ AP Photo The report describes the US infrastructure for hazardous waste as "generally adequate," however, it states that more than half of the US population lives within three miles of one of these waste sites. Inland Waterways: D Inland Waterways: D A barge travels down the Mississippi River. There are some 25,000 miles of inland waterways used for transport in the US. Shutterstock.com Inland waterways help transport goods to different parts of the country. But the infrastructure that supports these waterways, like dams and locks, are getting old and causing delays. In fact, about 50% of vessels using these waterways experience delays, according to the report. Levees: D Levees: D A worker walks across a levee near the Cedar River, Monday, Sept. 26, 2016, in Cedar Rapids, Iowa. Charlie Neibergall/AP Photo Levees play a critical role in protecting communities from flood waters, but they aren't currently getting the attention they need. During the next 10 years, there's a need for $80 billion to improve these structures, according to the report. Parks and Recreation: D+ Parks and Recreation: D+ National parks in the US are in need of billions of dollars for repairs. Thomson Reuters The infrastructure that supports local parks and national parks needs improvement. Roads, bridges, parking areas, trails, and campsites are just a few of the things that need repairs in our nation's parks. The National Park Service even estimates that it reached $11.9 billion in deferred maintenance costs in 2015, according to the report. Ports: C+ Ports: C+ There are 926 ports in the US. These ports are responsible for almost $5 trillion in economic activity, according to the ASCE. David J. Phillip/AP Photo Most overseas trade comes through US ports. And while our ports have a higher grade than most other infrastructure categories, there's still room for improvement. For example, as ships get bigger, ports will need to make deeper navigation channels. Also, as congestion in ports increases, the freight network that takes shipments to and from ports needs to be improved so that goods are transferred more efficiently with fewer delays. Rail: B Rail: B More than $25 billion is needed to repair and grow the railway system in the US. Getty Images/Tim Boyle While freight railroads are in relatively good shape, passenger rail could use some upgrades, especially in the Northeast Corridor. According to the report, the average age of Amtrak's backlogged projects in the Northeast Corridor is 111 years old. This includes bridges, tunnels, and a viaduct. Roads: D Roads: D Crumbling roads cost Americans about $160 billion in wasted fuel in 2014, according to the report. Mario Anzuoni/Reuters Roads in the US are in bad shape. About 32% of urban roads and 14% of rural roads are in poor condition. In fact, there's a $836 billion backlog of unmet capital needed to fix the highways and bridges in the US, according to a report by the US Department of Transportation. Schools: D+ Schools: D+ Public schools don't have the money they need to maintain their buildings. Scott Olson/Getty Images Schools in the US are not getting the funding they need to maintain public school buildings. About 24% of these buildings are in fair or poor condition, according to the report. Solid Waste: C+ Solid Waste: C+ Americans generated some 258 million tons of waste in 2014. Shannon Stapleton/Reuters While municipal solid waste systems are mostly in fair condition, the ASCE recommends increased promotion of developing better systems for recycling. Transit: D- Transit: D- According to the ASCE, only 51% of US households can travel to a grocery store in their area by using public transportation. Flickr / MTAPhotos Public transit is being used more and more, but it remains severely underfunded. According to the report, it would cost about $90 billion to fix the backlog of transit system projects and that cost is estimated to grow to $122 billion by 2032. Wastewater: D+ Wastewater: D+ The demand for more water treatment plants is expected to grow by 23% over the next 15 years. Wikimedia Commons Currently, there are about 15,000 wastewater treatment plants in the US, but it's estimated we will need 532 new systems by 2032, which means we need to be investing more in wastewater infrastructure now. The US needs to invest about $271 billion in the US wastewater infrastructure over the next 25 years, according to the report.

#### Maybe our infrastructure could be perceived as acceptable if it were on par with the rest of the world, however the developing world is outpacing the United States in both resilience and sustainability. Modernization is necessary to protect against contemporary threats.

Hiba Baroud, 7-28-2017, "Measuring up US infrastructure against other countries," Conversation, http://theconversation.com/measuring-up-us-infrastructure-against-other-countries-78164//IC

How does infrastructure in the U.S. compare to that of the rest of the world? It depends on who you ask. On the last two report cards from the American Society of Civil Engineers, U.S. infrastructure scored a D+. This year’s report urged the government and private sector to increase spending by US$2 trillion within the next 10 years, in order to improve not only the physical infrastructure, but the country’s economy overall. Meanwhile, the country’s international rank in overall infrastructure quality jumped from 25th to 12th place out of 138 countries, according to the World Economic Forum. On Feb. 12, the White House revealed its $1.5 trillion plan to rebuild U.S. infrastructure, financed through a combination of federal, local and private sectors. This is a long awaited plan, as the nation’s infrastructure quality continues to suffer. The quality of infrastructure systems can be measured in different ways – including efficiency, safety and how much money is being invested. As a researcher in risk and resilience of infrastructure systems, I know that infrastructure assessment is far too complex to boil down into one metric. For instance, while the U.S. ranks second in road infrastructure spending, it falls in 60th place for road safety, due to the high rate of deaths from road traffic. But by many measures, the U.S. falls short of the rest of the world. Two of these characteristics are key to our infrastructure’s future: resilience and sustainability. A new class of solutions is emerging that, with the right funding, can help address these deficiencies. Resilience Resilient infrastructures are able to effectively respond to and recover from disruptive events. The U.S. is still in the top 25 percent of countries with the most resilient infrastructure systems. But it falls behind many other developed countries because the country’s infrastructure is aging and increasingly vulnerable to disruptive events. For example, the nation’s inland waterway infrastructure has not been updated since it was first built in the 1950s. As a result, 70 percent of the 90,580 dams in the U.S. will be over 50 years old by 2025, which is beyond the average lifespan of dams. Vehicles at a business are surrounded by floodwaters from 2016’s Hurricane Matthew in Lumberton, North Carolina. AP Photo/Chuck Burton In addition, since the 1980s, weather-related power outages in the U.S. have become as much as 10 times more frequent. Several European countries – such as Switzerland, Germany, Norway and Finland – are ahead of the U.S. in the FM Global Resilience Index, a data-driven indicator of a country’s ability to respond to and recover from disruptive events. Though these countries are exposed to natural hazards and cyber risks, their infrastructure’s stability and overall high standards allow them to effectively survive disruptive events. The U.S. infrastructure was built according to high standards 50 years ago, but that’s no longer enough to ensure protection from today’s extreme weather. Such weather events are becoming more frequent and more extreme. That has a severe impact on our infrastructure, as cascading failures through interdependent systems such as transportation, energy and water will ultimately adversely impact our economy and society. Take 2016’s Hurricane Matthew, which was considered a 1,000-year flood event. The unexpectedly strong rainfalls broke records and caused damages equivalent to $15 billion. A better infrastructure that is modernized and well-maintained based on data-driven predictions of such events would have resulted in less impact and faster recovery, saving the society large damages and losses. As the country’s infrastructure ages, extreme weather events have a greater impact. That means the recovery is slower and less efficient, making the U.S. less resilient than its counterparts. Sustainability In terms of sustainability practices designed to reduce impact on human health and the environment, the U.S. does not make it to the top 10, according to RobecoSAM, an investment specialist focused exclusively on sustainability investing. Average CO₂ emissions per capita in the U.S. are double that of other industrialized countries and more than three times as high as those in France. The infrastructure in most EU countries facilitates and encourages sustainable practices. For example, railroads are mostly dedicated to commuters, while the bulk of freight moves through waterways, which is considered the most cost-effective and fuel-efficient mode of transportation. In the U.S., 76 percent of commuters drive their own cars. Reed Saxon/AP Photo In the U.S., however, 76 percent of commuters drive their own cars, as railroads are mostly reserved for freight and public transit is not efficient compared to other countries. American cities do not show up in the top cities for internal transportation, as do cities such as Madrid, Hong Kong, Seoul and Vienna. To promote sustainable practices, global initiatives such as the New Climate Economy and the Task Committee on Planning for Sustainable Infrastructure aim to guide governments and businesses toward sustainable decision-making, especially when planning new infrastructure. Smart infrastructure as a solution To address challenges of resilience and sustainability, future infrastructure systems will have to embrace cyber-physical technologies and data-driven approaches. A smart city is a city that is efficient in providing services and managing assets using information and communication technology. For example, in Barcelona, a city park uses sensor technology to collect and transmit real-time data that can inform gardeners on plant needs. While there is no official benchmark to grade countries in this aspect, a number of American cities, such as Houston and Seattle, are considered among the world’s “smartest” cities, according to economic and environmental factors. In order to prioritize dam restoration, the dam safety engineering practice is moving toward a data-driven process that would rank the dams based on how important they are to the rest of the waterway system. And last year, the U.S. Department of Transportation issued a call to action to improve road safety by releasing a large database on road fatalities, which researchers can study to answer important questions. Similarly, worldwide initiatives are seeking smart solutions that integrate communication and information technology to improve the resilience of cities such as 100 Resilient Cities and Smart Resilience. It’s imperative that we pursue these types of new solutions, so U.S. infrastructure can better and more sustainably withstand future disruptions and deliver better quality of life to citizens, too. Perhaps, by addressing these needs, the U.S. can improve its score on its next report cards.

#### 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.

#### 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,

Michael A. Vatis, “National Infrastructure Protection Center,” CALEA Online, 1999, http://www.calea.org/online/newsletter/No75/The%20National%20Infrastructure%20Protection%20Center.htm

**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**.

#### However, current trends show that insider threats are growing and might be an overlooked challenge to our critical infrastructure.

Brian Harrell, 9-1-2016, "Combating insider threats faced by utilities," CSO Online, http://www.csoonline.com/article/3113737/critical-infrastructure/combating-insider-threats-faced-by-utilities.html

Insiders pose the greatest threat, especially if they are working with a foreign state or other high level threat actors, because of their detailed knowledge of system operations and security practices. In addition, they often have legitimate physical and electronic access to key systems and the controls designed to protect them. Individuals with the highest level of access pose the greatest threat because they are already inside your organization, using legitimate credentials and permissions to access sensitive areas, thus evading detection from traditional security products. Furthermore, an individual with access to grid infrastructure could purposely or inadvertently introduce malware into a system through portable media or by falling victim to social engineering e-mails or other forms of communication. Current events have recently shown that people with legitimate access can produce substantial harm. Today, we are aware of [Edward Snowden](http://csoonline.com/article/2880486/data-protection/intelligence-community-works-to-get-beyond-snowden-stigma.html), who released classified information about national surveillance programs, U.S. Army P.F.C. [Bradley Manning](http://csoonline.com/article/2133876/malware-cybercrime/bradley-manning-sentenced-to-35-years-for-classified-document-leaks.html) who provided classified documents to WikiLeaks, and contractor [Aaron Alexis](https://en.wikipedia.org/wiki/Washington_Navy_Yard_shooting) who killed 12 people during a shooting at the Washington Navy Yard in 2013 while holding a security clearance.

#### Additionally, the multifaceted threats to Communications infrastructure make nearly all other sectors susceptible to sabotage.

Johnathan Tal, 9-20-2018, "America’s Critical Infrastructure: Threats, Vulnerabilities and Solutions," <https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions>//IC

The communications sector is huge and diverse, covering from traditional voice services, through all Internet-related services, to accessing all control devices in every other sector. Without properly functioning communications, it is difficult to imagine the smooth operation of business, public safety, transportation or government, to name but a few. Yet, the sector is vulnerable to extreme weather impact, as well as to the dangers of aging and terrorist attacks. In July of 2001, for example, a freight train caught fire inside a Baltimore tunnel. The fire resulted in damage to several telecommunications and Internet backbone lines. This, in turn, led to several days of total or partial loss of communications and Internet service between Washington, D.C. and New England. The 9/11 collapse of the World Trade Center towers resulted in flooding of one of the largest telecommunications nodes in the world. Millions of voice and data lines were disconnected, leaving thousands of businesses (including the New York Stock Exchange) and residential customers without service for days. With communications, an essential, integral part of every aspect of the U.S. economy, public safety and government, the economic and national security ramifications of a physical or cyber attack on even an isolated network are almost incalculable. These events come in conjunction with the increased vulnerability of this very same infrastructure due to inter-connectivity and growing complexity. With every signal light in every junction, every air-traffic control element interlinked though complex telecommunications networks, even an incidental interruption can easily mushroom into a colossal disruption of life and commerce. Of course, network designers and security experts are aware of these vulnerabilities and have developed mechanisms and procedures to contain and abate cyber and physical interferences with smooth operations, but the situation is far from secure. America’s cellular telephony network is one of the most vulnerable elements of the communications infrastructure. Cellular networks tend to collapse exactly when they’re needed most – in the aftermath of a disaster.

# Section 2: CIKR Sectors for Debate

## 2A—Areas that make for Great Debate

When this paper was originally written in 2011 the DHS list of CIKR was slightly larger than it is today. In updating the paper, the following sectors were omitted from a breakdown:

1. National Monuments and Icons. In checking new DHS policy and Presidential Directives, this sector is no longer listed in many major reports.
2. Postal and Shipping. Same Reasons as above

When this paper was updated in 2019, some sectors are included in the paper for background information, but not enough *good* literature exists for these areas to be the heart of a resolution. Those areas are located in Section 2B.

### Banking and Finance

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 clear, taking into account the 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”. 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. Literature stipulates that securing this sector does not require the continued reliability of physical assets, but rather of entire intangible assets.

**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.**

#### Additionally, we may not always think of banking and finance as crucial areas of our infrastructure, however it may be a key internal link to all other sectors.

David Cotney, 11-20-2018, "Financial Sector at Risk as Cyber Foes Target Critical Infrastructure," Homeland Security Today, <https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-financial-sector-at-risk-as-cyber-foes-target-critical-infrastructure/>

While many people think of defense, energy, and communications when they think of critical infrastructure, financial services is another crucial sector underpinning the nation’s health. A disruption in financial services could have devastating consequences both for individual consumers and small businesses, as well as our entire economy. Even if an attack is not widespread throughout the industry, a cyber attack against one or more financial institutions can prevent customers from accessing their account or their funds, thereby causing reputational damage and lack of confidence in the system as a whole. Protecting the safety of this critical infrastructure is a shared responsibility not only for the financial services industry, but also each and every one of us. It is something that must be prioritized during National Critical Infrastructure Security and Resilience Month, and every day of the year. Financial institutions collect and hold large amounts of personal information of consumers and small-business owners. Because of this, it should be no surprise that the financial industry is a frequent target of cyber attacks. Whether their motive is to disrupt the financial sector or the U.S. economy or simply to steal data, these criminals will exploit any weakness. Sometimes, the hackers will attack an institution directly through a system that has not been properly patched or through an employee who downloads malware. Similarly, if the hackers obtain the credentials of a bank employee, they can wreak havoc on the bank’s systems. Hackers will also attack an institution indirectly. Consumers regularly receive phishing scam emails from what looks like their financial institution asking them to change their account ID or password. Businesses and corporations can also become victims of such schemes in what is called corporate account takeover (CATO), resulting in the movement of funds out of a business account. Finally, third-party vendors are often connected to a bank’s systems, meaning that if the third-party fails to maintain controls as strong as the institution itself, the bank can be vulnerable.

**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.

#### While particularly advantages will be extremely diverse, there are two core areas that they are likely to stem from.

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)

**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 impacts 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.

In order to protect this sector against events that could take down the entire 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.

#### If the government were to work to increase the resilience of the Banking and Finance sector, it would spill over to broader sectors of the US economy. Borghard offers 5 suggestions.

Erica D. Borghard, 10-3-2018, "Banking on Cooperation: The U.S. Government and the Finance Industry Need to Work Together to Defend the Financial Sector from Cyber Threats," Lawfare, <https://www.lawfareblog.com/banking-cooperation-us-government-and-finance-industry-need-work-together-defend-financial-sector>

In a Carnegie working [paper](https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324), I propose that the U.S. government and key actors in the financial sector collaborate at the operational level to defend against major cyber threats. If implemented, the recommendations could be replicated across other critical sectors of the economy, taking into account their unique and specific risk and threat profiles, defensive requirements, and regulatory and compliance regimes. A program of operational collaboration between the U.S. government and key financial sector actors should contain five elements: sector-specific foreign intelligence collection institutionalized in the National Intelligence Priorities Framework (NIPF); side-by-side analytic collaboration and real-time data sharing between U.S. government and financial sector analysts; joint development of playbooks; routine exercising of playbooks; and deepening organizational connective tissue between the government and the sector. Reliable intelligence is essential to composing an accurate picture of the threat environment. However, both private-sector and government intelligence analysts lack a complete understanding of their adversaries. Open-source intelligence analysts in the private-sector lack the full range of authorities and capabilities to collect adequate foreign intelligence to defend their networks. Government intelligence agencies lack deep subject-matter expertise about the assets and systems at risk and the nature of the threat environment facing an industry, like financial. Two remedies might address this intelligence gap. First, the U.S. government should prioritize foreign-intelligence collection against finance-specific threats. But because expertise about the financial system within in the industry outpaces that of the government, the financial sector should be formally incorporated into every step of the intelligence cycle. For example, banks could help the intelligence community develop indicators and warnings of threats. Absent such collaboration, there is a strong chance that U.S. government intelligence collection against foreign threats will be rudderless. Second, there should be deeper and more routinized intelligence collaboration across classification lines between government and financial sector analysts. The likelihood of getting security clearances for all of the finance industry’s threat analysts is slim to none, but that shouldn’t stand in the way of collaboration with cleared personnel in the intelligence community. This collaboration should move beyond [existing information-sharing initiatives](https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/) to include side-by-side analytic collaboration and real-time data sharing. The dearth of cleared individuals in appropriate positions—like chief information-security officers, threat intelligence leads, and some threat analysts—within the financial sector should be remedied to support this effort.

**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.

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.

#### Additionally, there is great ground for the Public Private Partnerships CP in this sector.

Chuck Brooks, 5-6-2019, "Public Private Partnerships And The Cybersecurity Challenge Of Protecting Critical Infrastructure," Forbes, <https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#6b759aab5a57>

It's a global threat not just against the United States. In 2017, Hackers use Triton, a specialized malware to compromise critical safety systems at Schneider Electric. The malware is still being used to target industrial systems. Because of the sensitivity to the threats to national security and changing threat matrix of hackers augmented by newer technologies such as machine learning and artificial intelligence, the government is prioritizing the importance of the risk management approach to defend against more sophisticated malware and automated attacks targeting critical infrastructure. An effective risk management approach necessitates information sharing that helps allow government and industry to keep abreast of the latest viruses, malware, phishing threats, ransomware, insider threats, and denial of service attacks. Information sharing also establishes working protocols for lessons-learned and resilience that is critical for the success of mitigating incidents. A cornerstone of that approach is creating Public Private Partnerships (PPP) based upon risk management frameworks. A high level of public-private collaboration is needed to address growing cyber-threats. Preparation and commitment from both government and industry leadership is critical. Industry should collaborate with government to best utilize risk management models and prepare resiliency plans. The specifics of an industry security approach may vary according to circumstances, but the mesh that connects the elements is situational awareness combined with systematic abilities for operational management and critical communications in cases of emergency.

### Chemical

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”.

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.

#### 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”. 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 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**.

Where things get particularly interesting, is the lack of information sharing with first responders. If there were any sort of attack or system failure at a chemical plant or facility, the DHS cannot share information with first responders, which hinders effective response to crises.

GAO, 8-8-2018, "Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders," No Publication, <https://www.gao.gov/products/GAO-18-538>

Since 2013, the Department of Homeland Security (DHS) has strengthened its processes for identifying high-risk chemical facilities and assigning them to tiers under its Chemical Facility Anti-Terrorism Standards (CFATS) program. Among other things, DHS implemented a quality assurance review process to verify the accuracy of facility self-reported information used to identify high-risk facilities. DHS also revised its risk assessment methodology—used to assess whether chemical facilities are high-risk and, if so, assign them to a risk-based tier—by incorporating changes to address prior GAO recommendations and most of the findings of a DHS-commissioned peer review. For example, the updated methodology incorporates revisions to the threat, vulnerability, and consequence scoring methods to better cover the full range of security issues regulated by CFATS. As of February 2018, a total of 29,195 facilities—including all 26,828 facilities previously assessed and 2,367 facilities new to the program—were assessed using DHS's revised methodology. DHS designated 3,500 of these facilities as high-risk and subject to further requirements. DHS has also made substantial progress conducting and completing compliance inspections and has begun to take action to measure facility security but does not evaluate vulnerability reduction resulting from the CFATS compliance inspection process. In 2013, GAO found that the backlog of chemical facility security plans awaiting review affected DHS's ability to conduct compliance inspections, which are performed after security plans are approved. Since then DHS has made progress and increased the number of completed compliance inspections. As of May 2018, DHS had conducted 3,553 compliance inspections. DHS has also begun to update its performance measure for the CFATS program to evaluate security measures implemented both when a facility submits its initial security plan and again when DHS approves its final security plan. However, GAO found that DHS's new performance measure methodology does not measure reduction in vulnerability at a facility resulting from the implementation and verification of planned security measures during the compliance inspection process. Doing so would provide DHS an opportunity to begin assessing how vulnerability is reduced—and by extension, risk lowered—not only for individual high-risk facilities but for the CFATS program as a whole. DHS shares some CFATS information, but first responders and emergency planners may not have all of the information they need to minimize the risk of injury or death when responding to incidents at high-risk facilities. Facilities are currently required to report some chemical inventory information, but GAO found that over 200 CFATS chemicals may not be covered by these requirements. To improve access to information, DHS developed a secure interface called the Infrastructure Protection (IP) Gateway that provides access to CFATS facility-specific information that may be missing from required reporting. However, GAO found that the IP Gateway is not widely used at the local level. In addition, officials from 13 of the 15 Local Emergency Planning Committees—consisting of first responders and covering 373 CFATS high-risk facilities—told GAO they did not have access to CFATS data in the IP Gateway. By encouraging wider use of the IP Gateway, DHS would have greater assurance that first responders have information about high-risk facilities and the specific chemicals they possess.

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. Since 2006, the industry has seen continuous growth, seeing 1.6% growth in 2016 (1 trillion in total sales), with an anticipated 3.6% and 4.8% growth in 2017 and 2018.

#### 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. 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. 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. 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.

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. Some are led to believe that it is the chemicals manufactured and distributed that should be the classificatory 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

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”.

**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.

#### A. Vulnerability Assessment & Remediation Compliance Affirmatives

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.

#### 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. These policies are certainly amendable to switch-side debate:

#### 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.

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

### Communication

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. 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.” 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. 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. 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. In seeking to reinforce the communication sector, there are two security areas that must be considered: cyber and physical.

#### Cyber security

The communication sector prioritizes two types of cyber security threats: Denial of Service attacks (DoS) and Intrusion attempts. 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. Military networks are not doing much better, recently receiving a grade of ‘D’ 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.

#### Our critical infrastructure is more vulnerable than ever due to cyber threats – but implementing security controls and collaboration solves.

Michael K. Daly, 10-17-2018, "Our Critical Infrastructure is More Vulnerable Than Ever. Here's What We Can Do About It.," Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/our-critical-infrastructure-is-more-vulnerable-than-ever-here-s-what-we-can-do-about-it//IC

Critical infrastructure—from the electric grid to public transportation—is under assault as cyber attackers gain a foothold in the United States. When the US Department of Homeland Security (DHS) released its cybersecurity strategy in May, it laid out seven goals to help the government better defend the United States and its infrastructure against the constant onslaught of sophisticated cyber threats. These include: Assessing and understanding systemic cybersecurity risks Protecting critical infrastructure Responding effectively to cyber incidents Although these are similar to prior strategic goals, there is a new keyword: systemic. Putting this cybersecurity strategy into action requires three aggressive steps be taken across people, technology, and process. These are: Build deeper partnerships with industry to foster an aligned cybersecurity ecosystem Accelerate the use of innovative and emerging technologies such as artificial intelligence and machine learning Produce comprehensive playbooks to unify government actions across homeland security, law enforcement, intelligence, and state. In September, the US Department of Defense (DoD) delivered its own cybersecurity strategy in which it laid out how the department will implement the priorities outlined in the DoD National Defense Strategy. A few key objectives include: Deterring, preempting, or defeating malicious cyber activity that targets critical infrastructure in the United States Securing DoD information and systems, including on non-DoD-owned networks, against cyber espionage and malicious cyber activity Expanding DoD cyber cooperation with allies, partners, and private sector entities. The intersection of these two strategies—addressing critical infrastructure and calling for public-private partnership—opens the door to a powerful community of interested parties who are grappling with cybersecurity challenges. This is the foundation that will be required for a cybersecurity “moonshot” referenced by US Vice President Mike Pence in his speech at the DHS Cybersecurity Summit in July. At that summit, DHS unveiled its new National Risk Management Center. This hub will help drive toward the goal of managing systemic risk to critical national infrastructure. Cybersecurity is a shared responsibility for DoD, DHS, federal agencies, and the corporate world. Cyber criminals now target the commercial sector with as much force and skill as they do the government. Many attacks against the corporate world have national security consequences, a reality not yet fully appreciated by all businesses and citizens. As just a few examples: ransomware payoffs fund terrorists and nation states seeking to evade sanctions; compromised computers act as relays to disguise attacks on critical infrastructure and steal secrets; stolen intellectual property accelerates the build-out of competitive enterprises weakening our economy and influence. DHS and the DoD understand domain expertise is key and will involve individuals who have experience protecting and hardening systems at a federal level, or those who know how to bring together people and systems. Additionally, partners will need to have an understanding of the geopolitical implications around protecting national infrastructure. While it is not likely that an attack will create widescale impacts like shutting down the power grid, disrupting mass transit systems, or massively altering election results across the nation, if hackers could infect relatively few computers they could prevent effective emergency response in the midst of a crisis or sow seeds of doubt about the legitimacy of these systems. The United States, like many of its allies, is at a tipping point. We must step up and make it more difficult for our adversaries to breach our critical infrastructure. These breaches not only erode trust, but also impact our safety and lives. Of the sixteen critical infrastructure sectors as defined by DHS, election systems present a unique challenge to security professionals. US elections are managed through a hodgepodge of systems that vary from state to state, including paper ballots, electronic screens, Internet messaging, and even some Internet voting. As we move into midterm elections in November and with an eye to the 2020 presidential election, the following steps can help build confidence and combat threats to critical electoral systems: Election officials and cybersecurity staff should review the importance of cybersecurity controls, the threat vectors that are known to have been exploited in systems, and the long history of election tampering that has been occurring since World War II. Improperly informed stakeholders are our greatest vulnerability. Document the end-to-end election process with all of its systems, dependencies, and interfaces. Every community is different and faces somewhat different threat vectors. Engaging technology vendors and IT organizations (across the end-to-end chain) to conduct technical testing to ensure systems are secured should be a regular occurrence. As with any technology that you deploy in your homes or offices, patching, segmentation, monitoring, wireless configurations, hardening to remove unnecessary applications, and ensuring there are multiple redundancies and methods of validation are components of good cyber hygiene routines. Implement integrity features for electoral rolls, vote casting, counting, and communications systems, including redundant records and backups that guarantee every vote is counted and verified. We live in an interconnected world full of cyber threats and vulnerabilities. Our national security depends on the resilience of implementing effective security controls across all sectors of our critical infrastructure. Our strength in addressing these evolving threats will require a much more collaborative effort with far more active engagement by the private sector in matters of systemic risk and national security. Collectively, we have the people, processes, and technology needed to combat this threat and remain safe.

#### 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. 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 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.

#### Natural disasters and extreme weather pose great threats to the communication sector.

Department of Homeland Security, 2015, "Communications Sector-Specific Plan An Annex to the NIPP 2013," Homeland Security, <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf>//IC

Hurricanes, wildfires, and other extreme weather events have increased in frequency and severity in recent years, impacting local and regional communications infrastructure in the United States. On a national level, a geomagnetic solar super storm, such as the one in July 2012, could cause an electromagnetic pulse that collapses electric power grids and triggers a long-term outage (LTO) in national communications.9

#### The communication sector faces vulnerabilities due to its dependency on supply Chains.

Department of Homeland Security, 2015, "Communications Sector-Specific Plan An Annex to the NIPP 2013," Homeland Security, <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf>//IC

The Communications Sector depends on suppliers for the products and services that are necessary to deliver communication services to users. In particular, the sector is dependent on reliable hardware and software. This is an area the sector continues to scrutinize closely.

In order to maintain critical communication networks in a time of national crisis, updated and reinforced assets are desperately needed. This area of the topic also potentially becomes one of the largest and most important sectors for debate as nearly all other sectors of modern infrastructure rely on communication. This, in the author’s opinion is a must-include element of any resolution.

### Critical Manufacturing

#### 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.

#### In fact, since 2016 we have seen Russian cyberattacks against our manufacturing sectors

Larry O'Brien, 7-30-2018, "DHS Sounds the Alarm on Critical Infrastructure Cybersecurity," No Publication, <https://www.arcweb.com/blog/dhs-sounds-alarm-critical-infrastructure-cybersecurity>

A [Wall Street Journal article last week](https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110) revealed some new concerns from the Department of Homeland Security on cybersecurity in our critical infrastructure. DHS made headlines back in March when they specifically called out cyberthreats to our critical infrastructure back in March. Russia was the specific subject of this warning and here is the summary [description from the March Announcement](https://www.us-cert.gov/ncas/alerts/TA18-074A): “Since at least March 2016, Russian government cyber actors—hereafter referred to as “threat actors”—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. Analysis by DHS and FBI, [SIC] resulted in the identification of distinct indicators and behaviors related to this activity. Of note, the report Dragonfly: Western energy sector targeted by sophisticated attack group, released by Symantec on September 6, 2017, provides additional information about this ongoing campaign. [[1]](https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks)(link is external) This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as “staging targets” throughout this alert. The threat actors used the staging targets’ networks as pivot points and malware repositories when targeting their final intended victims. NCCIC and FBI judge the ultimate objective of the actors is to compromise organizational networks, also referred to as the “intended target.””

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."

#### 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.

#### Negative Ground

In terms of negative ground, there are a variety of options like business confidence, criticisms of hegemony or a variety of small counterplan options. For example:

#### PPP is a key area of counterplan competition

Michael Daly and Russ Schrader, 4-1-2019, "Protecting our infrastructure demands a critical public-private partnership," Federal News Network, <https://federalnewsnetwork.com/commentary/2019/04/protecting-our-infrastructure-demands-a-critical-public-private-partnership/>

While these investments are a positive sign, we need to recognize that the threats go well beyond these sectors to include water, pharmaceuticals, critical manufacturing and more. The reality is this: All of these interconnected systems are vulnerable, and we need to work together to develop protections at every level. Creating public-private partnerships So how can DHS and other federal agencies lead by example through security policy, and what can industry and the corporate world do to follow suit? Educating the public remains a hurdle. On the individual level, stronger, two-factor authentication is no longer a “nice-to-have” security measure, but an essential protective layer that all individuals and businesses need to employ. At the industry level, we need to understand the systemic risks to those industries, and model the cyber and real-world indicators that can warn of an attack. DHS has led the charge in this initiative with its National Risk Management Center, enabling the power of our government to be brought to bear on our adversaries. This not only empowers us to limit the damage of an attack, but deter one altogether. In addition, the creation of CISA will likely serve as a major asset for DHS in promoting these public-private partnerships, as an increase in funding and autonomy will enable the agency to continue its partnerships with technology companies that can help speed up the department’s efforts to protect our nation’s critical infrastructure. DHS already has important partnerships in place, like the [Silicon Valley Innovation Program](https://www.dhs.gov/science-and-technology/svip)(SVIP), which finds new technologies that strengthen national security with the goal of reshaping how government, entrepreneurs and industry work together to find cutting-edge solutions. As cyber hardening our critical infrastructure will involve a collaborative effort, programs like the [DHS InnoPrize](https://www.dhs.gov/science-and-technology/prize-competitions), which uses crowdsourcing to quickly find solutions to security issues, and the [Small Business Innovation Research](https://www.dhs.gov/science-and-technology/sbir)(SBIR) Program, which helps U.S. small businesses to develop solutions to homeland security needs, need to be expanded to continue to incentivize private sector action. On a national scale, the idea of a Cybersecurity Moonshot — a national initiative to shift the balance of cyber-power from attackers to defenders and regain trust in cyberspace — is gaining traction. In fact, the National Security Telecommunications Advisory Committee (NSTAC) recently presented a Cybersecurity Moonshot report to the White House, in an effort to make the U.S. a key player in making the internet safe in the next ten years. As government officials advance this initiative to make a fundamental change in cyberspace, they will address [six key pillars](https://www.dhs.gov/publication/2018-nstac-publications) to achieve a more secure internet within the next 10 years. One of the pillars is human behavior, which remains a hurdle as user, provider and employer actions continue to be one of the top causes of data breaches today. Another critical pillar the government seeks to address is education. The lack of cybersecurity awareness and regular education continues to be a challenge for businesses, organizations and consumers alike. The need to increase the availability, quality and diversity of cybersecurity talent is paramount to ensuring proper protection for years to come. Additionally, together with tech companies and other partners, organizations like DHS and the Defense Department (DoD) can develop compelling, minimally technical messaging to citizens to demonstrate that good cybersecurity practices are a part of our national security. The time for collaboration is now

### 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](http://www.dhs.gov/files/programs/gc_1188565256722.shtm), as a continued source of water for irrigation and water management; [The Transportation Systems Sector](http://www.dhs.gov/files/programs/gc_1188404440159.shtm) uses dams and locks to manage navigable waters throughout inland waterways; [The Water Sector](http://www.dhs.gov/files/programs/gc_1188399291279.shtm), by supplying potable water to concentrated populations and commercial facilities in the U.S.; [The Energy Sector](http://www.dhs.gov/files/programs/gc_1189013411585.shtm), by providing approximately 8 to 12 percent of the nation’s power needs with hydropower dams; and [The Emergency Services Sector](http://www.dhs.gov/files/programs/gc_1189094187811.shtm), 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 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.” 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."

#### 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]

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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#n1) Although renewable energy sources will be a crucial tool in the fight against climate change, they often create other environmental problems. [n2](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#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, 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]

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. [n22](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#n22)Nondiscretionary duties of agencies need not meet the requirements of section 7 of the ESA. [n23](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302617393983&returnToKey=20_T11722137830&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.899146.4340541934#n28)

**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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#n8) The Department of Energy estimates that up to 30,000 MW of electricity could be generated from undeveloped sites. [n9](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#n9) The Electric Power Research Institute estimates that untapped hydro capacity could increase production by twenty-four to twenty-seven percent. [n10](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#n10) The Energy Information Administration puts that total potential increase in hydroelectricity for new and upgraded plants at forty terawatts. [n11](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1302614198971&returnToKey=20_T11721395576&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.230774.27396727112#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.

#### The aff could also implement these Dam Safety Plan initiatives

Association Of State Dam Safety Officials, 2019, "Dam Security," No Publication, <https://damsafety.org/dam-owners/dam-security>

The DHS Dams Sector has established goals to improve awareness, prevention, protection, response, and recovery. The eight Dams Sector goals are driven by a desire to reduce the risks to critical assets within the Dams Sector, and to ensure the continued economic use and enjoyment of this nationally critical infrastructure. The eight goals of the Dams Sector are as follows: Build Dams Sector partnerships and improve communication among all critical infrastructure partners Identify Dams Sector composition, consequences, and critical assets; Improve the Dams Sector's understanding of viable threats; Identify Dams Sector vulnerabilities; Identify the risks to Dams Sector critical assets; Develop guidance on how the Dams Sector will manage risks; Enhance the security and resilience of the Dams Sector through research and development (R&D) efforts; and Identify and address interdependencies.

### Emergency Services

#### 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** **U**nited **S**tates 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** **U**nited **S**tates **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**.

#### The federal government has consistently recognized the importance of its role in emergency preparedness.

Rebecca Katz, September 2017, "Funding Public Health Emergency Preparedness in the United States," PubMed Central (PMC), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5594396///IC

In the last 15 years, the federal government reframed the roles and responsibilities for emergency preparedness and response, particularly for biological events. After the terrorist attacks of September 11, 2001, Congress approved the creation of the Department of Homeland Security (DHS) to act “as a focal point regarding natural and manmade crises and emergency planning” for the federal government.[3](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5594396/#bib3)Following the 2001 anthrax assaults, Congress also granted new resources and authorities to the Department of Health and Human Services (HHS) and its operating divisions, including the Centers for Disease Control and Prevention (CDC), to coordinate preparedness and response for bioterrorism and other events.[4](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5594396/#bib4) Widespread coordination failures during Hurricane Katrina in 2005, including in the federal response to complex public health challenges that followed the storm, underscored the limited capabilities of the DHS to organize federal response activities as well as ambiguities in national guidance for “all-hazards” emergency preparedness and response. The Katrina experience, coupled with concerns over the emergence of potentially pandemic influenza, prompted Congress to establish the office of Assistant Secretary for Preparedness and Response within the HHS and to strengthen federal programs to mobilize assistance to states for immediate and extraordinary action to protect public health.[5](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5594396/#bib5) In addition to the establishment of new offices, the federal government created a series of planning and guidance documents to better coordinate preparedness and response efforts. The National Response Framework defines the general roles, responsibilities, and coordination structures for federal, state, and local entities during all types of disasters or emergencies.[6](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5594396/#bib6) The Emergency Support Function and Support Annexes to the National Response Framework outline how federal agencies will provide coordinated assistance in core areas commonly required for disaster response. The Incident Annexes to the Federal Interagency Operational Plan similarly address coordination of the federal response to specific risks and threats. Both the Public Health and Medical Services Annex (Emergency Support Function #8) and the Biological Index Annex designate the HHS the coordinating agency for federal preparedness and coordination regarding public health events.

**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**.

*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.

#### FEMA lacks resources to effectively respond to disasters – increasing its resiliency is crucial.

Christopher Flavelle, 9-6-2018, "U.S. Report Says Lack of Staff, Resources, Planning Hurt FEMA's 2017 Disaster Response," Insurance Journal, <https://www.insurancejournal.com/news/national/2018/09/06/500272.htm//>IC

The federal government’s chief watchdog slammed the Federal Emergency Management Agency’s response to the hurricane that killed thousands of people in Puerto Rico last year, saying it was unprepared and failed to deploy enough qualified staff. The U.S. Government Accountability Office’s report issued Tuesday said FEMA struggled with a record year for disasters on the mainland and Puerto Rico. Overall, the agency failed to adequately house disaster victims, distribute financial assistance in a timely fashion or do enough to prevent fraud. For instance, scammers implemented “a well-organized and coordinated identity theft fraud scheme” in Texas, Florida, Puerto Rico, the U.S. Virgin Islands and California that hadn’t shown up following previous disasters, according to the report. The report’s criticism was especially pointed when it came to Hurricane Maria’s strike on Puerto Rico last September. “They were not prepared to respond to an event like that,” said Chris Currie, the lead author of the report. “They were having a lot of trouble getting people there. And not just people, but qualified people.” A report by George Washington University commissioned by Puerto Rico Governor Ricardo Rossello and released last week found that 2,975 people on the island died as a result of the storm. Other estimates have ranged as high as 5,000, but Rossello said the GWU figures would be used as the official tally. President Donald Trump said last week that his administration “did a fantastic job in Puerto Rico” after Maria devastated the island. The GAO report acknowledged factors outside of FEMA’s control that contributed to the poor response, including the island’s distance 1,000 miles from the U.S. mainland, its outdated infrastructure and the “limited local preparedness for a major hurricane.” But the response was also hindered by FEMA’s lack of adequately trained staff — including those who speak Spanish — the report found. “FEMA did not have enough bilingual employees to communicate with local residents or translate documents,” the GAO wrote, which “resulted in further delays while staff were reshuffled from other disasters to Puerto Rico.” Even the fitness of those personnel was a problem. According to FEMA’s leadership, some of the personnel sent to the island weren’t physically able to handle the extreme environment. The report described an agency stretched beyond its resources by an unprecedented sequence of storms and wildfires. Its staffing was down by about a third before Hurricane Harvey hit Texas — which was followed in rapid succession by Hurricane Irma striking Florida and then Maria. At the height of the deployments, in October, more than half of FEMA staff were serving in a capacity for which they weren’t designated as “qualified.” “By the time Maria hit Puerto Rico, they were down to the bottom of the barrel,” Currie said on a call with reporters. Wildfires The ripple effect eventually reached California. FEMA encountered initial delays in deploying personnel to the wildfires there last year because a majority of its workforce was already dispatched to support hurricane recovery efforts, according to the report. It could take years for FEMA to dole out funding for long-term projects to rebuild storm-damaged infrastructure and other facilities. That is on top of $1.5 billion FEMA had obligated in public assistance grants to three states and two territories recovering from Harvey, Irma and Maria. Administrative challenges in awarding those public assistance grants were tied to delays in removing debris, though the GAO highlighted bright spots where local and federal officials collaborated to overcome the problems. For instance, in Texas, officials arranged to have military personnel help move debris when they encountered problems. In response to the GAO’s findings, the Department of Homeland Security, which includes FEMA, said the agency “is constantly reviewing its program delivery, decision-making processes, and response efforts to ensure that it can improve, minimize errors, and better serve survivors.” In July, FEMA released its own report on its response to last year’s disasters, and the policy changes the agency was making as a result. Tuesday’s report said it’s “too soon to assess the adequacy of these actions as part of this review and whether the actions will have the intended impact.” In a press conference Tuesday, Rossello said there were joint initiatives underway with FEMA to ensure a better response to a future hurricane. But he said it’s unreasonable to expect a drastic change in the island’s preparedness so long as Puerto Rico isn’t a state. Puerto Rico is a territory whose residents are U.S. citizens by birth but lack voting representation in Congress. “We have to address the root of the problem,” Rossello said. Since the start of his political career, Rossello has repeatedly pushed for Puerto Rico to become the 51st state, and he addressed the matter directly with Trump at a lunch with other governors earlier this year. But as Trump himself has acknowledged, political realities are likely to prevent that from happening anytime soon: Puerto Ricans tend to support Democrats.

#### The Emergency services sector is facing a plethora of threats – increasing its protection/resiliency is key

Department of Homeland Security, 2015, "Emergency Services Sector-Specific Plan," Homeland Security, https://www.dhs.gov/sites/default/files/publications/emergency-services-ssp-fact-sheet-2015-508.pdf//IC

Current Risks Natural disasters and extreme weather; cyberattacks or disruptions; violent extremist and terrorist attacks; and chemical, biological, radiological, and nuclear incidents are persistent risks to the sector. Risks associated with cyberattacks continue to grow as sector reliance on cyber systems for emergency operations communication, data management, biometric activities, telecommunications, and electronic security systems increases. Increased public expectations for ESS expertise and rapid response capabilities and reduced grant funding constraining State and local resources both contribute to the risk profile of the sector.

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

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”. In the event of a catastrophic energy shutdown, it is likely that all other forms of critical infrastructure protection would be crippled beyond repair. 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.

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”. 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.

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, decreased foreign oil dependence, and calls for a decentralized energy grid (renewables). 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”. 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. Plans that focus on increased protection of facilities are likely to be a core plan focus for those debaters that are 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.

#### There is also a growth in human error in the energy sector, making resilience an important and timely topic for debate.

Taylor Armerding, 4-4-2019, "Despite Ongoing Warnings, U.S. Critical Infrastructure Remains Vulnerable," Forbes, <https://www.forbes.com/sites/taylorarmerding/2019/04/04/despite-ongoing-warnings-u-s-critical-infrastructure-remains-vulnerable/#5ee9a9061fa8>

A lengthy national or even regional collapse of critical infrastructure – the kind envisioned in multiple past warnings of a [“cyber Pearl Harbor”](https://nakedsecurity.sophos.com/2017/08/18/how-likely-is-a-digital-pearl-harbor-attack-on-critical-infrastructure/) or in former Nightline anchor Ted Koppel’s 2015 book [Lights Out](http://www.csoonline.com/article/3004819/business-continuity/ted-koppel-apocalypse-likely.html) – remains hyperbole, they say. But it also doesn’t mean significant disruption couldn’t happen on a smaller scale. Last September a series of seemingly random [natural gas fires and explosions](https://www.wbur.org/tag/gas-explosions-lawrence-andover-north-andover) upended the lives of thousands of residents in three communities in the Merrimack Valley of Massachusetts. Dozens lost their homes entirely. Thousands more, without gas or heat for months, had to move to motels and trailers. Now, more than six months later, supplier Columbia Gas reports that the cost of the disaster has topped $1 billion and is still rising. Keep in mind, this was in just three communities in a small corner of a small state. An investigation concluded the cause was human error – a failure to transfer a regulator pressure sensor during a pipe replacement project, which led to catastrophic excess pressure in gas lines. But, as numerous experts said at the time, a cyberattacker who was able to take control of the system and “fool” pressure sensors would achieve similar results.

#### Most human error or lack of detection does not come from intentional incompetence, many engineers who work in the energy sector are not required to take cybersecurity courses, which is a threat to nearly all sectors.

Taylor Armerding, 4-4-2019, "Despite Ongoing Warnings, U.S. Critical Infrastructure Remains Vulnerable," Forbes, <https://www.forbes.com/sites/taylorarmerding/2019/04/04/despite-ongoing-warnings-u-s-critical-infrastructure-remains-vulnerable/#5ee9a9061fa8>

In a recent [podcast with Momenta Partners](https://www.momenta.partners/edge/control-systems-cybersecurity-a-grim-gap-a-conversation-with-joe-weis?utm_campaign=Podcast&utm_content=86509424&utm_medium=social&utm_source=linkedin&hss_channel=lcp-6407713), he said “Cybersecurity is normally taught in computer science, and they don’t require you in most cases to take any engineering classes. Meanwhile, the engineering domains – electrical, mechanical, chemical, systems, nuclear, industrial – don’t really require you to take any cybersecurity training.” And it is not enough to protect the network in an ICS system, he said. “You can keep lights on even if the network is down, but if the lights are off, the network isn’t going to be on anyway. We’re looking at the wrong things,” he said. “IT can’t kill anybody, but engineering can and has.” In a [blog post last month](https://www.controlglobal.com/blogs/unfettered/the-need-to-train-control-system-engineers-and-monitor-process-sensors-for-possible-cyber-attacks/), Weiss wrote that the 2017 [Trisis attack](https://www.synopsys.com/blogs/software-security/triton-attack-failure/) in 2017 on a Saudi petrochemical plant illustrated that training gap. “The plant engineers had no training to identify unexpected events as possibly being cyber-related,” he wrote. “Consequently, the first time the plant tripped, it was simply considered a malfunction and the plant restarted without cyber security considerations.” It wasn’t until the plant shut down again, two months later, that the malware was discovered. Fabian has said previously that he doesn’t foresee an effort to take down a major part of U.S. infrastructure because even hostile nation-states are wary of U.S. power. “We’re not going to just sit there and take it,” he said, “and I think our [cyber] capabilities are probably more significant than those of others.” Still, even smaller-scale attacks, if there are enough of them, could start to feel like death by a thousand cuts.

In addition to focusing on some cybersecurity threats, there is heavy demand for increased use of “smart” upgrades. These smart upgrades allow for constant re-evaluation of weaknesses in both human and machine interfaces. Both traditional and alternative forms of energy all have a variety of security issues:

Trend Micro, 10-30-2018, "Critical Infrastructures Exposed and at Risk: Energy and Water Industries," No Publication, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries#RealWorldThreatScenariosForTheWaterSector

Real-world threat scenarios for the energy sector Since energy is one of the more central sectors of critical infrastructure, disruption in this sector can have cascading effects to other industries that depend on the continuous flow of energy to function. Here are some theorized scenarios using the results of our research on exposed HMIs. Oil and gas structures We found gas wells whose controllers were exposed. An interested attacker could shut down or reset wells, possibly affecting the state or national energy supply, which even small or medium organizations have a hand in providing. Solar energy devices Exposed HMIs in this industry included home solar panels as well as solar farms. An attacker hijacking the controls could affect the capability of individual homes to generate their own supply of energy, or affect the total available power on the larger national level since the excess energy from home solar panels is sold to the national grid. Power plants We found different kinds of power plants exposed online, from biogas to hydro plants. An attack in such facilities could mean affecting the energy supply for homes and organizations alike. Hydroelectric Plants We found a hydroelectric plant exposed in a different way: through its security cameras. An exposed camera could reveal possibly sensitive information that cybercriminals can use for other attacks.

Two final areas of threats to energy infrastructure are climate change and industrial technology shifts. While we have been the most on top of anticipating threats to energy systems, a failure to adapt to either of these issues will also create continued threats to the sector as a whole.

#### To solve any of the major issues in the energy sector, here are some specific mechanisms affirmatives could focus on:

Chuck Brooks, 2-16-2019, "Protecting Energy Critical Infrastructure a Key Challenge for DHS," Homeland Security Today, <https://www.hstoday.us/subject-matter-areas/infrastructure-security/protecting-energy-critical-infrastructure-a-key-challenge-for-dhs/>

Risk management incorporates that “whole-of-society” approach and is a guiding path to pursue. In cooperation with the recently established DHS Critical Infrastructure Task Force, there have been legislative initiatives to promote collaborative efforts – among federal, state, and private stakeholders of the electricity sector – to assess and improve the physical security and cybersecurity of electric utilities. There are several compelling themes I recommend to help mitigate risk. These include: Invest in hardening the National Grid to make it resilient to solar flares, or EMP attacks. This is an urgent imperative. Peter Pry, a member of the Congressional EMP Commission and executive director of the Task Force on National and Homeland Security, put the threats in frightening perspective: “Natural EMP from a geomagnetic super storm, like the 1859 Carrington Event or 1921 Railroad Storm, and nuclear EMP attack from terrorists or rogue states, as practiced by North Korea during the nuclear crisis of 2013, are both existential threats that could kill 9 of 10 Americans through starvation, disease and societal collapse.” Remain vigilant and continually analyze and game the energy cyber-threat landscape, as the methods, means and malware variants are constantly morphing. The specifics of a security approach may vary according to circumstances, but the mesh that connects the elements is situational awareness combined with systematic abilities for critical communications in cases of emergency. These guidelines are represented in the U.S. government’s National Institute of Standards and Technology (NIST) mantra for industry: “Identify, Protect, Detect, Respond, Recover.” Share and communicate cybersecurity information between the public and private sectors (a majority of the energy infrastructure is owned by the private sector). DHS is already expanding this program via the National Risk Management Center (NRMC) at the newly stood-up Cybersecurity and Infrastructure Security Agency (CISA). According to the CISA website: “The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions — the functions so vital that an attack or interruption to services within the government and the private sector could have devastating consequences to our national security, economic security, national public health and safety, or any combination thereof.” Follow and enforce industry security protocols, especially related to Supervisory Control and Data Acquisition (SCADA). The Internet was not built for security at its inception; it was built for connectivity. Following industry and government protocols derived from lessons learned is essential for protecting vital infrastructure. Invest in next-generation technologies. This includes physical security controls and cybersecurity technologies. Technology development continues to evolve with the introduction of new innovations to address the cybersecurity framework that includes networks, payloads, endpoints, firewalls, antivirus software, and encryption. This framework will provide for better resiliency and also forensic analysis capabilities. Some newer areas of cybersecurity spending will be in the areas of cloud, authentication, biometrics, mobility, and automation, including self-encrypting drives. And, of course, super-computing and quantum computing. Automation, including via artificial intelligence, is an emerging and future cybersecurity pathway. Protecting critical infrastructure, and specifically the energy sector, is just one area of the many security challenges we need to address in the increasingly interconnected work in 2019. The risks associated with vulnerabilities make it an especially urgent and key priority.

**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.

#### 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. In addition to the States, Public Private Partnerships are necessary due to the massive levels of private ownership.

Kevin Randolph, 2-12-2019, "Energy infrastructure security requires continuous industry-government collaboration," Daily Energy Insider, https://dailyenergyinsider.com/featured/17597-energy-infrastructure-security-requires-continuous-industry-government-collaboration/

The energy sector is one of 16 critical infrastructure sectors, as designated by Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience. “It has been — this partnership between the electricity subsector and the government — has been looked at as best in class among the 16 critical infrastructure sectors,” Scott Aaronson, vice president of security and preparedness at EEI, said. Kate Marks of the Department of Energy gave the committee an overview of the Office of Cybersecurity, Energy Security and Emergency Response (CESER) within DOE, which U.S. Secretary of Energy Rick Perry established in February 2018. “CESER was stood up to ensure that DOE was working with industry and government to secure U.S. energy infrastructure against all hazards, reduce the risks of and impacts from cyber events and other disruptive events and assist with restoration activities,” Marks said. Marks noted that DOE is the sector-specific agency for energy as well as for cybersecurity in the energy sector. She also noted that DOE leads the Energy Government Coordinating Council (EGCC), which engages with the energy industry through the electricity subsector coordinating council (ESCC) and Oil and Natural Gas Sector Coordinating Council (ONG SCC). CESER has set three priorities for its work this year, Marks explained. These priorities include improving understanding of risks and how to mitigate them, clarifying industry and government roles in cybersecurity and building capacity across industry and government. Information sharing, Marks said, is an important part of the office’s efforts. DOE shares threat information through conference calls, reports, and quarterly threat briefings. It shares updates through ISERnet, a secure website managed by the Infrastructure Security and Energy Restoration (ISER) Division of DOE’s Office of Electricity Delivery and Energy Reliability, with points of each contact identified in each state through the Energy, Emergency and Assurance Coordinators (EEAC) list. Marks offered as an example an incident in December in which the administration announced that a group of cyber actors known as APT10 is running a cyber-enabled theft campaign. DOE, she said, organized two conference calls — one with industry and state regulators — to share information about the threat. “So, while seemingly a small act to just stand up two conference calls, we really think this helps to demonstrate CESER’s commitment that providing energy information at the same to both industries and states with actionable information will allow us to improve coordination across the industry…” Marks said.

### Healthcare and Public Health

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 bird’s 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 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. 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. During emergencies, the sector must not only sustain but also increase its capacity. The sector’s goal for service continuity is to 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.”

#### 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.

**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 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.

#### 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.

#### 5) 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.

#### 6) 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](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1303501365267&returnToKey=20_T11808378216&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.800730.5398670872#n1) scarce medical resources and devices within these vulnerable populations, implicitly opting to save certain lives at the expense of others. [n2](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1303501365267&returnToKey=20_T11808378216&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.800730.5398670872#n2) **Health** care providers will be in the conspicuous and unfortunate  [\*796]  position of turning away many deathly ill people. [n3](http://www.lexisnexis.com/lnacui2api/frame.do?reloadEntirePage=true&rand=1303501365267&returnToKey=20_T11808378216&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.800730.5398670872#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?

### Information Technology

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

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.

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,

Information Technology Sector,” No Date, <http://www.dhs.gov/xlibrary/assets/nipp_it.pdf>

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.

#### 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,

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

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 fail." 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.

#### 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,

“Technology Assessment: Cybersecurity for Critical Infrastructure Protection,” May, <http://www.gao.gov/new.items/d04321.pdf>

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.

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,

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

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 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.

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. 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 bring down U.S. civilian and military systems.

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. 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.

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. 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.

**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.

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 state, and Herbert Lin, study director for the NRC’s Committee to Study National Cryptography Policy, argues:

#### We Should increase the use of advanced cryptography technology throughout the U.S.

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

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.

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.

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 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.

***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. Even more problematic is that the DHS has no authority to direct cyber-security regulations for the private sector. 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. 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 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.

*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,

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

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.

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.

### Nuclear Reactors, Materials and Waste

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

#### 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](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "n123) For example, Canada has [\*336] nuclear energy, but no nuclear weapons. [n124](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "n124) Conversely, Israel has a relatively weak nuclear energy program, but is an (unofficial) member of the nuclear weapons club. [n125](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "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](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "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](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046#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](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046#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](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046#n162) This is the one area that cannot change quickly without governmental support.

*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](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "n93) as well as reducing coal burning's environmental impact by using nuclear power plants to power coal gasification techniques, [n94](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "n94)aiding in the sterile insect technique to reduce pests' crop destruction, and irradiating food to prevent food-borne diseases. [n95](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "n95) Research and development have already shown strong promise for these techniques, and the nuclear industry holds the potential for many more. [n96](http://www.lexisnexis.com.navigator-clarion.passhe.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1303611268016&returnToKey=20_T11811805911&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.312677.46345985046" \l "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.

*Cybersecurity of plants*

#### Affirmatives could work throught the Nuclear Regulatory Commission to prevent breaches of both active and decommissioned nuclear facilities and/or test reactors

NRC, 3-28-2019, "NRC: Backgrounder on Cyber Security," No Publication, https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html

In June 2013, the NRC centralized oversight of the regulatory agency’s activities related to cyber security. Today, within the Office of Nuclear Security and Incident Response, the Cyber Security Branch is responsible for planning, coordinating, and managing all agency activities related to cyber security for NRC licensees and applicants. This includes all rulemaking, guidance, licensing, policy issues and oversight related to cyber security requirements. Cyber security is an element of decommissioning activities for nuclear facilities. Cyber security rulemaking is in progress for fuel cycle facilities, using the lessons learned from power reactor cyber security program implementations. Currently there are no cyber security requirements for Independent Spent Fuel Storage Installations, and research and test reactors. The NRC is considering the need for cyber security requirements for non-power production or utilization facilities and materials licensees. The NRC works on cyber security issues with other regulators and organizations, including FERC and the North American Electric Reliability Corporation, whose mission is to ensure the reliability of the North American power grid. In 2010, the NRC signed a Memorandum of Understanding with NERC to clarify the roles and responsibilities of each organization, including inspection protocols and enforcement actions. Additionally, the NRC participates with other federal regulators and Executive branch agencies on the Cyber Security Forum for Independent and Executive Branch Regulators. Established in 2014, the forum brings together regulators to share best practices and lessons learned in cyber security protection for critical infrastructure.

*Waste*

#### The US Government still has no idea what to do with nuclear waste, and each day without action, it becomes a larger threat.

Jane C. Hu, 6-7-2019, "Someday the U.S. Will Have to Actually Deal With Its Nuclear Waste Problem," Slate Magazine, <https://slate.com/technology/2019/06/department-of-energy-nuclear-waste-reclassification-yucca.html>

In addition to the waste we already have sitting around at Hanford and other old nuclear weapons facilities (charmingly called “legacy waste”), nearly 100 commercial nuclear reactors at 60 facilities around the U.S. are creating new waste every day. The type of waste produced by those two types of facility contains different radioactive materials with varying half-lives, but the same storage issues remain: What will we eventually do with all this radioactive stuff? The lack of solution is not from lack of discussion. There have been all sorts of wacky ideas floated about where to store nuclear waste. Some have proposed we shoot it all into space, maybe have it orbit [Venus](https://space.nss.org/media/Space-Manufacturing-conference-12-111-Disposal-Of-High-Level-Nuclear-Waste-In-Space.pdf). But given how spacecraft are prone to explosions, which would effectively mean showering the world with bits of radioactive waste, that idea stalled. In the ’90s, the idea of burying waste in deep ocean seabeds seemed [promising](https://www.theatlantic.com/magazine/archive/1996/10/the-sub-seabed-solution/308434/), but it never really got off the ground. And some countries tried storing barrels of waste in [ice sheets](https://www.igsoc.org/journal/19/81/igs_journal_vol19_issue081_pg607-617.pdf), which turns out to be less than ideal given that ice both moves and melts. As the earth thaws out, old waste becomes [uncovered](https://grist.org/article/melting-ice-could-unleash-hazardous-waste-from-abandoned-cold-war-project/). Here in the U.S., we’re running out of space, and experts are concerned about the lack of long-term solutions. “Instead of a planned, coherent system, we have the confusion of an unplanned, less than optimal system,” nuclear experts wrote in [a 2018 report](https://cisac.fsi.stanford.edu/research/projects/reset-nuclear-waste-policy) on nuclear waste management strategy and policy, calling the U.S. program “an ever-tightening Gordian Knot” subject to technical, scientific, logistical, regulatory, legal, financial, social, and political challenges. “This is not a situation that builds public confidence.”

### Water

International incidents including terrorist attacks in France and South Africa have illustrated that terrorist organizations are increasing their focus on attacking water-based resources. 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.”

#### 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:

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.

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).

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.

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.

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.”

#### 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) 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. 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.

These issues have not gotten any better since 2003, Trend Micro highlights current threats to both Water and Wastewater treatment plants:

Trend Micro, 10-30-2018, "Critical Infrastructures Exposed and at Risk: Energy and Water Industries," No Publication, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries#RealWorldThreatScenariosForTheWaterSector>

Real-world threat scenarios for the water sector One of the greatest concerns for organizations in this sector is the possible effect of direct cyberattacks on their operations, thereby leading to a disruption of supply to and from the plant. This is especially true for water facilities that either purify water for distribution or use water in their operations. Here are theorized scenarios, taken from our research findings: Water treatment plants The main HMI controls for a certain seawater-to-drinking water treatment plant were found exposed through our publicly available methods. An attacker could discover the exposure and launch an attack that could affect the supply of drinking water in the area. Industrial water facilities The HMI controls for a water heating facility used for various industrial processes were exposed to the public internet. An attacker could gain access and use such controls to cause serious industrial accidents in a similar facility by manipulating temperatures.

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 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.

#### 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. Damage 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.

There are also several large cybersecurity issues in the area of water and wastewater treatment, and may be one of the most overlooked areas of vulnerability because of older technology and shrinking budgets.

Pieter Arntz, 4-1-2019, "Compromising vital infrastructure: water management," Malwarebytes Labs, <https://blog.malwarebytes.com/security-world/business-security-world/2019/04/compromising-vital-infrastructure-water-management/>

The report goes on to say that getting cybersecurity right is not an easy mission and many organizations have limited budgets, aging computer systems, and personnel who may lack the knowledge and experience for building robust cybersecurity defenses and responding effectively to cyberattacks. In cyberwarfare, a mass shutdown of computers controlling waterworks and dams could result in flooding, power outages, and shortage of clean water. In the long run, this could lead to famine and disease. In March and April 2018, the US Department of Homeland Security and Federal Bureau of Investigation [warned](https://www.us-cert.gov/ncas/alerts/TA18-074A) that the Russian government is specifically targeting the water sector and other critical infrastructure sectors as part of a multi-stage intrusion campaign. Malware One of the major threats to water-energy plants is Industroyer, aka [CrashOverRide](https://www.wired.com/story/crash-override-malware/), an adaptable malware that can automate and orchestrate mass power outages. The most dangerous component of CrashOverride is its ability to manipulate the settings on electric power control systems. It also has the capability of erasing the software on the computer system that controls circuit breakers. CrashOverRide clearly was not designed for financial gain. It’s purely a destructive tool. Another malware that many industrial plants are threatened by is called [Stuxnet](https://blog.malwarebytes.com/threat-analysis/2013/11/stuxnet-new-light-through-old-windows/). This threat is designed to spread through Windows systems and go after certain programmable controllers by seeking out their related software. Near the end of 2018, the Onslow Water and Sewer Authority (ONWASA) said it would have to completely restore a number of its internal systems thanks to an outbreak of [Emotet](https://blog.malwarebytes.com/cybercrime/2019/03/emotet-revisited-this-pervasive-persistent-threat-is-still-a-danger-to-businesses/) and [one of the ransomware variants](https://blog.malwarebytes.com/cybercrime/malware/2019/01/ryuk-ransomware-attacks-businesses-over-the-holidays/) it is known to deliver. Earlier in 2018, the first cryptocurrency mining malware impacting industrial controls systems and SCADA servers was found in the network of a [water utility provider in Europe](https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack). This was not seen as a targeted attack, but rather the result of an operator accessing the Internet on a legacy Human Machine Interface (HMI). Not that SCADA systems are free of targeted attacks. A [honeypot](https://www.cso.com.au/article/456486/honeypot_phony_waterworks_gets_hammered_internet/) that mimicked a water-pump SCADA network was found by hackers within days and soon became the target of a dozen serious attacks.

#### These threats are urgent, Colorado warded off an attack months ago, and they are just an example of what the over 70,000 water utility providers face throughout the nation.

Blake Sobczak, News Reporter Energywire, 3-28-2019, "SECURITY: Hackers force water utilities to sink or swim," No Publication, <https://www.eenews.net/stories/1060131769>

Last month, hackers tied computers into knots at a small Colorado water utility. It wasn't the first time the Fort Collins-Loveland Water District and its wastewater counterpart had been hit by "ransomware," a type of malware that encrypts victims' computer files and demands online payment to unlock them. While operations weren't harmed, the infection prompted the water district to switch out its information technology service provider and call in the FBI. The case, first reported by the [Coloradoan](https://www.coloradoan.com/story/money/2019/03/14/cyberattacker-demands-ransom-colorado-utility/3148951002/), remains under active investigation. FCLWD and the South Fort Collins Sanitation District treat and distribute water to 45,000 customers in northern Colorado. Colorado water officials aren't alone in their cybersecurity woes. The nation's nearly 70,000 water and wastewater utilities are struggling to keep their heads above a rising tide of online threats, based on interviews with security experts and water company operators. As one IT manager at a midsize water utility put it, "It's not a question of if, it's a question of when" hackers disrupt vital U.S. water systems. "Most small and midsize utilities are overstressed," said the manager, who requested anonymity. Some larger utilities are well-positioned to thwart an attack by hackers backed by a foreign government, said Michael Arceneaux, managing director for the Water Information Sharing and Analysis Center, the industry's clearinghouse for getting the word out about the latest hacking threats and vulnerabilities. But in a sector that encompasses tens of thousands of local water systems, securing America's vast and disparate drinking water supply remains a significant challenge. "Drinking water utilities run the gamut in terms of cybersecurity preparedness," Arceneaux said. "What we try to do to compensate for that is make sure people are aware of the threats, so they have some motivation to invest the resources that should be invested."

#### 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 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 harm the industry. 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.

## 2B—CIKR Areas that Exist, but May Not Be Timely/Have Lit

### Agriculture and Food

Choosing to debate critical infrastructure during the 2018-19 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.

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

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.

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:

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

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.

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.

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.” 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.

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”.

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.

**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”. Affirmatives 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.

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

**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.

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.

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.

### Commercial Facilities

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).

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. 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 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.

#### 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, 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.

### Continuity of Government

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”. 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’. 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. 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 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 was 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.

**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***

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.

#### As would be expected 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.

***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 that separation of power would completely disappear.

#### 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).

***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.

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.

**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.

### Defense Industrial Base

This area could be fascinating, however, I believe it should be exculuded as this will be a LARGE portion of the Arms Sales debates we will have in 2019-2020.

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”. 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”.

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.

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. 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,’ 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. 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.

#### 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 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.

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. 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.

#### 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 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.

### Government Facilities

Upon first noticing this sector on the list of CIKR assets, you might ask yourself what exactly constitutes a government facility. This term is 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:

Department of Homeland Security, “National Infrastructure Protection Plan: Government Facilities Sector,” 2008, http://www.dhs.gov/xlibrary/assets/nipp\_snapshot\_governmentfacilities.pdf

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.

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 ensuring 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. 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. 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 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 sovereign U.S. soil.

#### 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.”

Despite these security shortfalls, the threat to government facilities is clear; we need look no further than the 1995 Oklahoma City bombing where the Federal Building was torn asunder, killing 20 people (6 of which were children) and wounding hundreds. 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.

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 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. 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 within their own offices, not the entire building in which government assets are housed. 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. 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. Given these serious security loopholes, change is desperately needed in this sector.

#### While the SECURE Facilities Act, if passed (multiple versions have stalled in committee), 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**

Some controversial issues are slated to remain in effect, regardless of the SECURE Facilities Act or other potential policies.

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.

### Transportation Systems

In looking at this section for debate in 2018-19, some people may say “didn’t we just debate transportation infrastructure in 2012?” Yes, but including transportation as a sector of CIKR would create functionally different debates than things like CAFÉ standards, or solar highways from that topic. 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 shortages).”[[1]](#footnote-1) While there will easily be some overlap, the debates are different enough to warrant debating this portion of a topic so close to the transportation incentives topic.

#### 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].” 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.

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.

#### 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.

#### 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/paper9>

4cb.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 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 can 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.

# Section 3: Definitions/Topicality

#### 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:

http://www.dhs.gov/xlibrary/assets/NIPP\_Plan.pdf.

**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**.

#### 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:

http://cip.gmu.edu/cip/

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**.

#### However, Daniel Overbey, 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.[[2]](#footnote-2)

#### 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:

http://www.gao.gov/new.items/d10296.pdf

**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 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**.

#### 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,

http://www.gao.gov/new.items/d10296.pdf

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**).

[**https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil**](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

[**https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf**](https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf)

Resilience, as defined in PPD-21, is “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” Having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience. • Security and resilience are strengthened through risk management. Risk refers to the “potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood [a function of threats and vulnerabilities] and the associated consequences;” risk management is the “process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.”

#### c. Recent turns in policy have turned to use the phrase security:

**https://www.dhs.gov/what-security-and-resilience**

[Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)defines security as reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

#### d. Final opinion on the verbiage/mechanism issue:

The literature does not appear to make a significant distinction between “protection” and “resiliency.” There has also been the modification in recent policies to replace the term protection with security. However, 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 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:

http://www.gao.gov/new.items/d0739.pdf

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.

#### As mentioned in Sections 1 and 2 of this paper, CIKR’s are listed by the DHS as the following 18 sectors:

http://www.gao.gov/new.items/d0739.pdf

* 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

[**https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil**](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

#### B. Eliminate Key Resources

Many people may 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 provides a much narrower list of just Critical Infrastructures (CI) without Key Resources. This narrows the list to eight CI sectors:

http://www.irational.org/APD/IPC/criticalinf.htm

* 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, which established the President’s Commission on Critical Infrastructure Protection, outlines a similar list of eight critical infrastructures:

http://www.fas.org/irp/crs/RL31556.pdf

* 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.

# Section 4: Resolutions

1. Resolved: The United States federal government should substantially increase the protection and/or resiliency of one or more of the following Critical Infrastructure Sectors in the United States: Communications; Emergency Services; Nuclear Reactors, Materials, and Waste; Water and Wastewater Systems.

(This is the resolution we ended on when the topic was last proposed in 2017).

2. Resolved: The United States federal government should substantially increase the protection and/or resiliency of one or more of the following Critical Infrastructure Sectors in the United States: Banking and Finance; Communications; Nuclear Reactors, Materials, and Waste; Water and Wastewater Systems.

(Adds Banking and Finance and drops Emergency Services)

3. Resolved: The United States federal government should substantially increase the protection and/or resiliency of one or more of the following Critical Infrastructure Sectors in the United States: Banking and Finance; Critical Manufacturing; Communications; Nuclear Reactors, Materials, and Waste; Water and Wastewater Systems.

(Adds Critical Manufacturing to #2)

4. Resolved: The United States federal government should substantially increase the protection and/or resiliency of one or more of the following Critical Infrastructure Sectors in the United States: (Pick the best 4-5 sectors that you like).

5. Resolved: The United States federal government should substantially increase the protection and/or resiliency of its Critical Infrastructures and Key Resources in the United States.

(Does not limit to sectors)

6. Resolved: The United States federal government should substantially increase the protection and/or resiliency of its Critical Infrastructures in the United States.

(Drops key resources)

# Section 5: Limiting the Resolutions

#### A. Narrow by Eliminating “Key Resources”

The initial wording suggestion provided by resolution 5 is admitted large in scope. We prefer to start with a broader wording as it is most likely that the Marshall Subcommittee and Wording Committee will seek to narrow the topic.

If there is a desire to have a much narrower topic that does not include a list, then the phrase “Key Resources” should be eliminated from the topic and just include “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.

Neither the original authors nor the current author 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.”

# Section 6: 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 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, as are any increase in regulations. Second, various infrastructure projects would benefit different regions, which means they have support by various Congresspersons. Third, there have been battles on the “infrastructure bill” in Congress. Depending on the infrastructure sector, politics 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.

We will be in the midst of a Presidential election during this topic. Therefore, depending on if/what action has been taken it could either give ground for the GOP to claim wins, increasing their mandate or it gives the Dems a win, threatening the ability for the Dems to take any ground back in the House and/or the Senate.

#### Business Confidence DA

Biz con 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 biz con 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://www.heritage.org/defense/report/building-infrastructure-resiliency-private-sector-investment-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]](http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security" \l "_ftn33" \o ") The Act provides liability protections for companies that develop technologies or invest in homeland security projects.[[34]](http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security" \l "_ftn34" \o ") 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://www.heritage.org/defense/report/building-infrastructure-resiliency-private-sector-investment-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]](http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security" \l "_ftn35" \o ") 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]](http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security" \l "_ftn19" \o ") 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]](http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security" \l "_ftn20" \o ") 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]](http://heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security" \l "_ftn21" \o ")

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.

# Section 7: Why this Topic

#### Resources Available

As seen throughout the paper, there is a wide variety of resources available to help students research the topic. Not only is there literature from an engineering perspective in terms of looking at our infrastructure, this paper proves that CIKR taps into the economy, defense networks, and nearly all aspects of our life, making research relatively easy to find to justify this topic.

#### Topic Balance

The original authors and I have tried to show potential divisions of ground throughout this area, while the topic may seem large in terms of affirmative ground, it is easily checked by broad-reaching, competitive negative strategies like the states or private actor counterplans. There is also a depth of research in terms of analyzing each sector of CIKR which should ensure robust debate for both sides in any area of the topic.

#### Timeliness

A recent analysis of the United States infrastructure, conducted in 2017, gave the nation an average grade of a D. This grade has not improved since then. 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. You have seen 2020 Presidential candidates talk about the need for improved infrastructure and security. Also, the cybersecurity element of this topic is HUGE, which is an area of growing political and social concern. Also, New York just suffered a major blackout and a lot of people, including Presidential candidate Andrew Yang tweeted about it:

A screenshot of a cell phone

Description automatically generated

Each day we go without addressing our infrastructure, the threats only continue to grow in number and magnitude. Students will be debating one of the most important challenges of their time in both infrastructure and cybersecurity. As the focus on STEM continues to grow in the United States, the number of students interested in our activity and a variety of science and/or engineering fields will be huge.

#### Interest

Previous topics that have addressed issues relevant to CIKR, such as the 2012-13 transportation topic or the 2008-9 alternative energy topic, were built in a fashion that separated the resolution from some of the most accurate and important aspects of the 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.

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.

There has also been a growing interest in debating a cybersecurity topic in the past several years, however the concern has been that the topics will become TOO technical. I believe the cybersecurity literature in the realm of CIKR is easier to understand for novice debaters, non-tech savvy folks or people who are not experts. All of this cybersecurity literature is written in a clearer area of policy, than dealing with all cybersecurity threats in general.

# Section 8: Works Cited

\*Definitions are excluded from the works cited

\*\*Some sources might be missing, but there are full citations for every card as well

American Chemistry Council. "Outlook: U.S. Chemical Industry Continues to Outpace Industrial Output; Accounts for More Than One-Half of Construction Spending by Manufacturing Sector." *American Chemistry Council*. N.p., 2016. Web. 14 July 2017. <https://www.americanchemistry.com/Media/PressReleasesTranscripts/ACC-news-releases/US-Chemical-Industry-Continues-to-Outpace-Industrial-Output.html>.

Armerding, Taylor. "Despite Ongoing Warnings, U.S. Critical Infrastructure Remains Vulnerable." *Forbes*. Forbes Magazine, 04 Apr. 2019. Web. 12 July 2019.

Arntz, Pieter. "Compromising Vital Infrastructure: Water Management." *Malwarebytes Labs*. Malwarebytes, 28 Mar. 2019. Web. 12 July 2019.

"Backgrounder on Cyber Security." *USNRC*. N.p., 28 Mar. 2019. Web. 12 July 2019.

Bagby, John W. "Evolving Institutional Structure and Public Policy Environment of Critical Infrastructures." (n.d.): n. pag. *Speaker’s Journal Volume 9.14*. 2010. Web. <http://www.pahouse.us/SpkrJournal/documents/9/v9\_a14.pdf>.

Baroud, Hiba. "Measuring up US Infrastructure against Other Countries." *The Conversation*. N.p., 28 July 2017. Web. 12 July 2019.

Borghard, Erica D. "Banking on Cooperation: The U.S. Government and the Finance Industry Need to Work Together to Defend the Financial Sector from Cyber Threats." *Lawfare*. N.p., 10 Oct. 2018. Web. 12 July 2019.

Bridgers, Braxton. "Critical Infrastructure and First Responders." *New America*. N.p., 27 July 2018. Web. 12 July 2019.

Brooks, Chuck. "Protecting Energy Critical Infrastructure a Key Challenge for DHS." *Homeland Security Today*. N.p., 16 Feb. 2019. Web. 12 July 2019.

Brooks, Chuck. "Public Private Partnerships And The Cybersecurity Challenge Of Protecting Critical Infrastructure." *Forbes*. Forbes Magazine, 06 May 2019. Web. 12 July 2019.

Brown, Kathi Ann. "Critical Path: A Brief History of Critical Infrastructure Protection in the United States." (n.d.): n. pag. 2006. Web. <http://cip.gmu.edu/archive/CIP\_CriticalPath.pdf>.

Bryan, William N. "Facing the Inevitable Storm." *Department of Homeland Security*. N.p., 03 June 2019. Web. 12 July 2019.

Carafano, James Jay. "Resiliency and Public-Private Partnerships to Enhance Homeland Security." *Family Security Matters*. N.p., 26 June 2008. Web. 12 July 2017. <http://www.familysecuritymatters.org/publications/id.467/pub\_detail.asp>.

Chalfant, Morgan. "Trump Pressed to Secure US Critical Infrastructure." *TheHill*. N.p., 29 Mar. 2017. Web. 13 July 2017. <http://thehill.com/policy/cybersecurity/326218-trump-pressed-to-secure-us-critical-infrastructure>.

Clarkson, J. T. "Phase Six Pandemic: A Call To Re-Evaluate Federal Quarantine Authority Before The Next Catastrophic Outbreak." *Georgia Law Review* (2010): n. pag. 2010. Web.

Cotney, David. "Financial Sector at Risk as Cyber Foes Target Critical Infrastructure." *Homeland Security Today*. N.p., 20 Nov. 2018. Web. 12 July 2019.

"Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders." *U.S. Government Accountability Office (U.S. GAO)*. N.p., 08 Aug. 2018. Web. 12 July 2019.

"Critical Infrastructure Security." *Critical Infrastructure Security | Homeland Security*. DHS, 19 Feb. 2010. Web. <http://www.dhs.gov/files/programs/gc\_1189168948944.shtm>.

"Critical Infrastructures Exposed and at Risk: Energy and Water Industries." *Security News - Trend Micro USA*. N.p., 30 Oct. 2018. Web. 12 July 2019.

Daly, Michael K. "Our Critical Infrastructure Is More Vulnerable Than Ever. Here's What We Can Do About It." *Atlantic Council*. N.p., 17 Oct. 2018. Web. 12 July 2019.

Daly, Michael, and Russ Schrader. "Protecting Our Infrastructure Demands a Critical Public-private Partnership." *Federal News Network*. N.p., 02 Apr. 2019. Web. 12 July 2019.

"Dam Security: Association of State Dam Safety." *Dam Security | Association of State Dam Safety*. N.p., 2019. Web. 12 July 2019.

"Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." *Department of Homeland Security*. N.p., 11 May 2017. Web. 12 July 2019.

Finkel, Ed. "Critical Infrastructure Sector Battles Growing Variety of Security Threats." *Security Magazine RSS*. N.p., 1 Aug. 2016. Web. 14 July 2017. <http://www.securitymagazine.com/articles/87302-critical-infrastructure-sector-battles-growing-variety-of-security-threats>.

Flavelle, Christopher. "U.S. Report Says Lack of Staff, Resources, Planning Hurt FEMA's 2017 Disaster Response." *Insurance Journal*. N.p., 06 Sept. 2018. Web. 12 July 2019.

Gorman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies." *The Wall Street Journal*. Dow Jones & Company, 08 Apr. 2009. Web. 13 July 2017. <http://online.wsj.com/article/SB123914805204099085.html>.

Gunter, Paul. "Natural Disasters and Safety Risks at Nuclear Power Stations." *Nuclear Information and Resource Service*. Nuclear Information and Resource Service, Nov. 2004. Web. 12 July 2017. <https://www.bing.com/cr?IG=72674333BE474082B94F034617B0733D&CID=0C725E953EEC691B11D4542B3FEA68A9&rd=1&h=pqMkwCS\_BAKo0WcpqXzXAdHb-d1b1aLH3NzwK9Uszu4&v=1&r=https%3a%2f%2fwww.nirs.org%2fwp-content%2fuploads%2ffactsheets%2fnaturaldisaster%26nuclearpower.pdf&p=DevEx,5062.1>.

"Hack Threats Aimed at Power Plants." *CBS News*. CBS Interactive, 28 Jan. 2010. Web. 12 July 2017. <http://www.cbsnews.com/news/hack-threats-aimed-at-power-plants/>.

Harrell, Brian. "Combating Insider Threats Faced by Utilities." *CSO Online*. CSO, 01 Sept. 2016. Web. 13 July 2017. <http://www.csoonline.com/article/3113737/critical-infrastructure/combating-insider-threats-faced-by-utilities.html>.

Heisler, Autumn. "7 Critical Risks Impacting the Energy Industry." *Risk & Insurance*. N.p., 26 July 2018. Web. 12 July 2019.

"Homeland Security Presidential Directive / HSPD-9: Defense of United States Agriculture and Food." *Homeland Security Presidential Directive / HSPD-9*. N.p., 3 Feb. 2004. Web. 13 July 2017. <http://www.fas.org/irp/offdocs/nspd/hspd-9.html>.

Homeland Security. "National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency." (n.d.): n. pag. 2009. Web. 12 July 2017. <http://www.dhs.gov/xlibrary/assets/NIPP\_Plan.pdf>.

Hu, Jane C. "Someday the U.S. Will Have to Actually Deal With Its Nuclear Waste Problem." *Slate Magazine*. Slate, 07 June 2019. Web. 12 July 2019.

Katz, Rebecca, Aurelia Attal-Juncqua, and Julie E Fischer. "Funding Public Health Emergency Preparedness in the United States." *American Journal of Public Health*. American Public Health Association, Sept. 2017. Web. 12 July 2019.

Lister, S. A. (n.d.): n. pag. *The Public Health and Medical Response to Disasters: Federal Authority and Funding.* 2007. Web. <http://lieberman.senate.gov/assets/pdf/crs/publichealthdis.pdf>.

Listes, Mark. "CI Scoop: History of Critical Infrastructure Designation." *U.S. Election Assistance Commission (EAC)*. N.p., 17 May 2017. Web. 14 July 2017. <https://www.eac.gov/ci-scoop-history-of-critical-infrastructure-designation/>.

Luke, Timothy W. *Discourses of the Environment*. Ed. Eric Darier. Oxford: Blackwell, 1999. 141-42. Print.

Marks, Joseph. "The Cybersecurity 202: Trump's Efforts Failed to Make Critical Infrastructure Safer from Cyberattacks, Experts Say." *The Washington Post*. WP Company, 05 Mar. 2019. Web. 12 July 2019.

McNeill, Jena Baker. "Building Infrastructure Resiliency: Private Sector Investment in Homeland Security." *The Heritage Foundation*. N.p., 23 Sept. 2008. Web. 12 July 2017. <http://www.heritage.org/defense/report/building-infrastructure-resiliency-private-sector-investment-homeland-security>.

McWhirter, Cameron. "U.S. Infrastructure Gets 'D+' Grade From Civil Engineers." *The Wall Street Journal*. Dow Jones & Company, 09 Mar. 2017. Web. 14 July 2017. <https://www.wsj.com/articles/u-s-infrastructure-gets-d-grade-from-civil-engineers-1489069827>.

O'Brien, Larry. "DHS Sounds the Alarm on Critical Infrastructure Cybersecurity." *ARC Advisory Group*. N.p., 30 July 2018. Web. 12 July 2019.

Owens, Lin, and Dunn. "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capacities." *National Research Council*. N.p., 2009. Web. 14 July 2017. <http://www.nap.edu/openbook.php?record\_id=12651&page=9+>.

"President Trump Declares National Emergency to Secure the Information and Communications Technology Critical Infrastructure Supply Chain · EMSNow." *EMSNow*. N.p., 16 May 2019. Web. 12 July 2019.

"Presidential Policy Directive -- Critical Infrastructure Security and Resilience." *National Archives and Records Administration*. National Archives and Records Administration, 12 Feb. 2013. Web. 13 July 2017. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

Quinn, Hal. "Op-ed: Infrastructure Plan Could Be Stymied by Lack of Key Resources." *DeseretNews.com*. Deseret News, 27 June 2017. Web. 14 July 2017. <http://www.deseretnews.com/article/865683761/Op-ed-Infrastructure-plan-could-be-stymied-by-lack-of-key-resources.html>.

Randolph, Kevin. "Energy Infrastructure Security Requires Continuous Industry-government Collaboration." *Daily Energy Insider*. N.p., 12 Feb. 2019. Web. 12 July 2019.

Rogers, Michael S., and Dave Weinstein. "Protecting Our Critical Infrastructure in the Digital Age." *TheHill*. The Hill, 10 June 2019. Web. 12 July 2019.

Rosenblum, Todd M. "Reform Agenda For The Department Of Homeland Security." *Forbes*. Forbes Magazine, 27 Jan. 2017. Web. 13 July 2017. <https://www.forbes.com/sites/realspin/2017/01/27/reform-agenda-for-the-department-of-homeland-security/#5765b8972a31>.

Sobczak, Blake. "SECURITY: Hackers Force Water Utilities to Sink or Swim." *SECURITY: Hackers Force Water Utilities to Sink or Swim -- Thursday, March 28, 2019*. N.p., 28 Mar. 2019. Web. 12 July 2019.

Spring, Baker. "Electromagnetic Pulse Weapons: Congress Must Understand the Risk." *The Heritage Foundation*. N.p., 3 Mar. 2010. Web. 12 July 2017. <http://www.heritage.org/Research/Reports/2010/03/Electromagnetic-Pulse-Weapons-Congress-Must-Understand-the-Risk+>.

Tal, Johnathan. "America's Critical Infrastructure: Threats, Vulnerabilities and Solutions." *Www.SecurityInfoWatch.com*. N.p., 20 Sept. 2018. Web. 12 July 2019.

"The Clinton Administration's Policy on Critical Infrastructure Protection." *First Gov*. N.p., May 1998. Web. <http://clinton4.nara.gov/WH/EOP/NSC/html/documents/NSCDoc3.html.>.

Thompson, Cadie. "America's Infrastructure Is Decaying - Here's a Look at How Terrible Things Have Gotten." *Business Insider*. Business Insider, 05 Feb. 2019. Web. 12 July 2019.

Trump, Donald. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." *The White House*. The United States Government, 11 May 2017. Web. 14 July 2017. <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.

"What Is Critical Infrastructure?" *What Is Critical Infrastructure? | Homeland Security*. DHS, 12 July 2017. Web. 14 July 2017. <https://www.dhs.gov/what-critical-infrastructure>.

1. 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 [↑](#footnote-ref-1)
2. Personal Email, March 31, 2010. [↑](#footnote-ref-2)