2013

Stunted Growth: Institutional Challenges to the Department of Homeland Security's Maturation

Dana James Fronczak

STUNTED GROWTH:

INSTITUTIONAL CHALLENGES TO THE DEPARTMENT OF HOMELAND SECURITY'S MATURATION

A Thesis

Submitted to the Graduate Center for Social and Public Policy

McAnulty College & Graduate School of Liberal Arts

Duquesne University

In partial fulfillment of the requirements for

the degree of Master of Arts

By

Dana Fronczak

May 2013

STUNTED GROWTH:

INSTITUTIONAL CHALLENGES TO THE DEPARTMENT OF

HOMELAND SECURITY'S MATURATION

By

Dana Fronczak

Approved March 20, 2013

_____	_____
Dr. Lewis Irwin Professor of Political Science (Committee Chair)	Dr. Kent Moors Professor of Political Science (Committee Member)
_____	_____
Dr. James Swindal Dean, McAnulty School of Liberal Arts Professor of	Dr. Charles Hanna Director, Graduate Center for Social and Public Policy

ABSTRACT

STUNTED GROWTH: INSTITUTIONAL CHALLENGES TO THE DEPARTMENT OF HOMELAND SECURITY'S MATURATION

By

Dana Fronczak

May 2013

Thesis supervised by Dr. Lewis Irwin

Scholars have proposed numerous explanations as to why the Department of Homeland Security has struggled to mature as an organization and effectively conduct its core mission. We propose an alternative viewpoint that the department lacks key legal authorities and necessitates key organizational transfer in order to rationalize its portfolio. We examine these points through review of legal authorities in select mission areas and through a resource analysis of activities conducted throughout the federal government to execute the homeland security mission. The analysis leads to specific recommendations for transfers and authorities and suggestions as to how the political environment might coalesce around engendering these changes.

TABLE OF CONTENTS

Page

I. Introduction

Drug Interdiction. Infrastructure Assessments. Commodities Stockpiling. Disaster Response Search and Rescure. Currency Investigations. Passenger Screening. Cyber Security. Immigrant Processing.Virus Detection. Communications Interoperability. Border Checkpoints.

What do these seemingly incoherent functions have to do with one another? They are all responsibilities of the Department of Homeland Security (DHS), the enormous government agency created in the wake of the September 11, 2001 attacks. In the course of one day, DHS screens over 2 million people at over 300 international and domestic airports; it will also screen 71,000 cargo containers at sea and land ports; it will apprehend 1,983 people who cross the border illegally and accept more than 3,200 who become legal citizens[1]. It will analyze and try to prevent cyber attacks, prepare for emerging natural hazards such as hurricanes and earthquakes and protect the President, Vice-President and any visiting heads of state from harm[2].

Melded from 22 federal agencies and 170,000 employees, DHS assumed responsibility for an enormous number of diverse and complex missions, a portfolio that requires a widely dispersed focus. The department further expanded its missions and functions in its first seven years due to mandates from Congress and the Office of the President. The Department now comprises over a dozen different components and over 216,000 employees[3].

In addition to its own resources, DHS requires the cooperation of an enormous number of other federal agencies, state and local governments and private-sector partners. All of this must happen in order to get the “homeland security” mission right’

consequently, at times there are overlapping and sometimes conflicting roles within that panoply of groups.

But that's not all DHS does.

Collecting tariff revenue. Protecting against exploited children. Polar icebreaking. Training other federal agents. Environmental cleanups. Recreational boating safety. Preventing international piracy. Another set of missions that belong to DHS, in some capacity, but ones that don't fit easily with protecting the United States from a terrorist attack and responding when a catastrophic event occurs. These also require coordination, money and effort. In many cases DHS is required by law to carry them out. In fact, when the Department was created, it was specifically charged to maintain the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland[4].

All of the DHS missions, whether core "homeland security" missions or not, are completed under the glare of public, political and media scrutiny. These missions are also completed under the sometimes conflicting principles of preserving freedom and facilitating the free flow of commerce while ensuring safety and security.

The department has suffered nearly constant criticism for its handling of many key events, most notably its response after the city of New Orleans's levee system failed in the wake of Hurricane Katrina, which was seen as a manifestation of the Department's failure to take its disaster preparedness, response and recovery mission seriously[5] [6]. But other issues, including its struggles to secure the United States' borders, effective screening of airport passengers, apprehending and removing illegal immigrants, and disseminating grants to state and local entities to prepare for a terrorist attack have also

come under controversy. In part because of these problems, the department has both instituted and been subjected to numerous reorganizations in its short history[7].

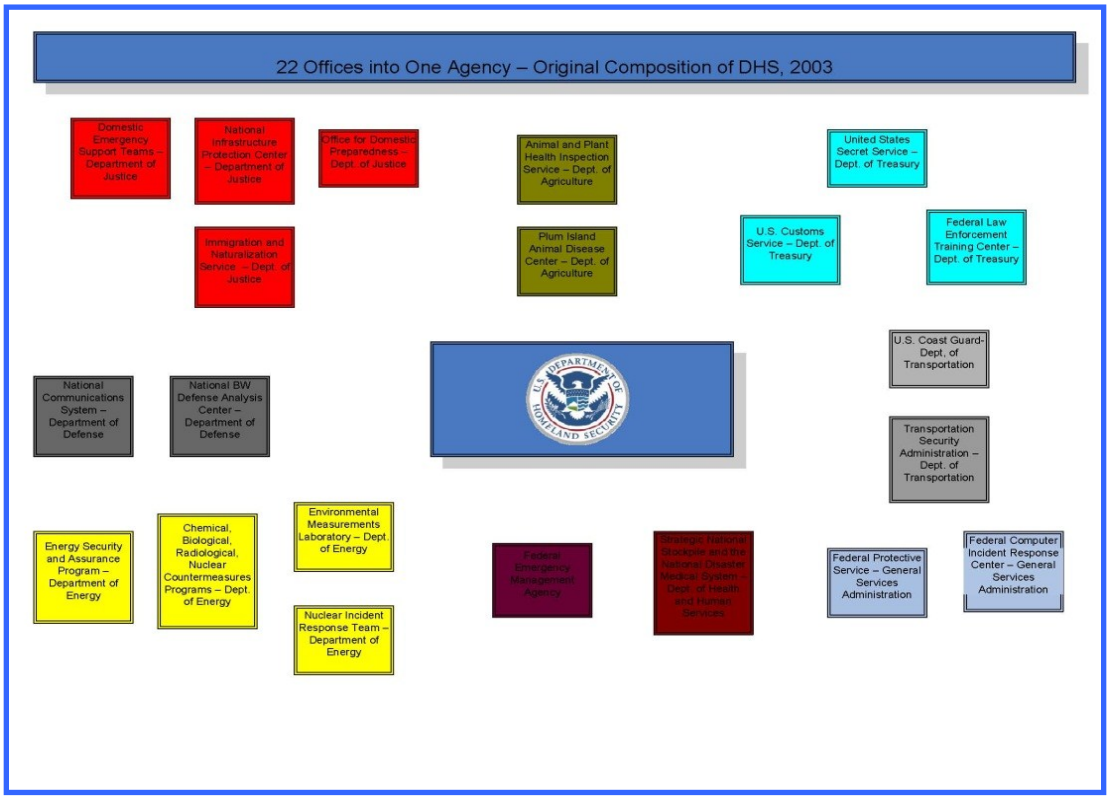
As DHS approaches its tenth anniversary, many of these inherent challenges persist. Various reasons are touted for why DHS has failed to mature and coalesce into a single unified coordinator for homeland security activities. One of the reasons cited is the department's inability to effectively manage its own resources, resulting in the department's inclusion on the Government Accountability Office's biennial "High-Risk" list since the department was created [8] [9] [10] [11]. Another reason cited is the department's lack of progress in integrating its legacy organizational cultures, resulting in a collection of agencies rather than an integrated department.[12] Yet another possible cause identified is the widely dispersed oversight by over 100 Congressional committees, which forces the department to spend an inordinate amount of resources compared to other agencies preparing and responding to Congressional inquiry[13] [14].

These points (Congressional oversight, internal barriers, lack of DHS managerial acumen) have been cited in legislative and policy circles as reasons for the department's failures, but there potentially lies a more fundamental capability in order to truly carry out its mission. The crucial decisions about what organizations would comprise the department and what authorities the department would be given were made in the nascent days of its creation, and have largely not been revisited since the DHS was created in 2003.

The thesis of this paper is that the department lacks key legal authorities and requires key organizational transfers, both to add and remove functions, that would create a more robust and comprehensive homeland security capability. In order for the

department to truly reach maturity, it must engage in another "rationalizing" set of activities, one that examines both legal and organizational barriers to success.

Figure 1 – Original Composition of DHS, January 2003



II. Paper Structure

DHS was created in order to coordinate the disparate efforts of the "homeland security enterprise," the various stakeholders that contribute to the collective security of the United States[15]. As an organization, DHS still lacks the necessary authorities to coordinate the various homeland security functions strewn throughout the federal government, the states, cities and the private sector. In addition, the department's own organizations lack key capabilities that are essential to fulfilling the five missions articulated in the Quadrennial Homeland Security Review[16], modeled after the Department of Defense's quadrennial review commenced after the Cold War[17]. In turn, the legislation that codified the DHS retained responsibility for numerous functions that have no homeland security nexus. The theory proposed is that the department can only evolve so far unless these fundamental issues are addressed. In essence, the department's ability to thrive is "stunted" by these institutional hindrances.

In order to better understand the challenges that DHS faces defining its role, a short history lesson is beneficial in order to examine the decision-making process that led to agencies and authorities' inclusion and exclusion. Examining the department's evolution from a White House Office of Homeland Security into a full federal department illustrates the decisions made within the context of the political and policymaking environment that now hinder the department's coordination of homeland security threats and allowed for the inheritance of many non-homeland security functions. This will also be conducted using some theoretical constructs about how the bureaucracy is developed, molded and altered.

The next step is to examine the Department's core missions as recently defined by its Quadrennial Homeland Security Review and examine specifically what authorities (and correspondingly, what authorities it lacks) it holds to conduct those missions. As mentioned previously, homeland security involves an enormous level of effort from state and local governments, the private sector and non-governmental organizations[18] In many cases, DHS must persuade or negotiate with those organizations to comply with its standards or recommendations, rather than possessing the power of regulatory authority or legislation to compel them.

Next, we will look at the department's current organizational structure, and contrast it with the dollars and organizations used for homeland security purposes. This can be done utilizing the Office of Management and Budget's *Organizing the Budget for Homeland Security,* published as part of the annual budget. For the budget year 2010, a total of $70 billion dollars was appropriated for homeland security activities across 32 agencies as diverse as the Department of Commerce and the Social Security Administration[19]. These appropriations will be examined in depth to review what homeland security functions reside within the department and what functions reside outside in other federal agencies. Lastly, based on these analyses, recommendations shall be offered in order to bolster the department's organizational structure and authorities. These recommendations shall include both additions and potential subtractions to the department in order to more properly align resources with their most appropriate organization, as well as potential changes in legal authorities.

It is acknowledged up front that these changes are fraught with political difficulties, and they cannot happen overnight. With that caveat in mind, included are specific thoughts for how some of these changes might be implemented.

II. Homeland Polity: DHS's Formulation

President George W. Bush announced the creation of a White House Office of Homeland Security 11 days after the attacks on the World Trade Center and the Pentagon[20]. Bush appointed Tom Ridge, then the Governor of Pennsylvania, as its Director. "Today, dozens of federal departments and agencies, as well as state and local governments, have responsibilities affecting homeland security. These efforts must be coordinated at the highest level," Bush said.[21] However, this simple declaration for the unified coordination of 40 different agencies with Homeland Security responsibilities belied the internal struggles, presidential recalcitrance and eventual dramatic turnaround that culminated with the creation of a Cabinet-level department in January, 2003.

An effort to establish a National Homeland Security Agency was first introduced before the 9/11 attacks by Rep. Mac Thornberry (R-TX)[22]. The agency Thornberry envisioned would have reported to the National Security Council and not been established as a Cabinet-level agency. Thornberry's also envisioned a significantly smaller organizational merger than the agency that was eventually founded in 2003. His bill only included the United States Coast Guard 9(then a part of the United States Department of Transportation, the Border Patrol (a part of the United States Treasury), the U.S. Customs Service (also a part of the Treasury), the Federal Emergency

Management Agency and several infrastructure security offices located in the Department of Commerce and the Federal Bureau of Investigation (FBI).

The National Homeland Security Agency's makeup was borne out of a report from a panel known as the Hart-Rudman Commission, which transmitted its findings to Congress in February of 2001. The work of the Commission originated in 1998 in response to the first bombing of the World Trade Center in 1993 and the 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City. In its research, the Commission concluded that over 40 entities contributed to homeland security at that time and that, first and foremost, the disparate functions required a "culture of coordinated strategic planning to permeate all U.S. national security institutions.[23] While the Commission did propose several structural changes in the national security bureaucracy, including the ones that Thornberry adopted in his bill, it left much of the apparatus alone.

The White House initially took a more conservative approach. Vice-President Dick Cheney, in response to the Commission's report, established a "National Preparedness Review" that focused on a terrorist attack utilizing a weapon of mass destruction.[24] The review did not begin until a few days before the 9/11 attacks occurred, and was quickly superseded by the White House's establishment of an Office of Homeland Security in October of 2001.[25] The office intended to develop a national strategy for homeland security but did not intend to move any agencies out of their existing organizational structures.[26] After the attacks, Bush appointed Tom Ridge, the governor of Pennsylvania, to the position of homeland security advisor and the head of the newly created office within the Executive Office of the President.

Almost concurrently, Senator Joseph Lieberman (I-CT, but then a Democrat) introduced a bill In October 2001 to create a Cabinet-level agency that included a set of organizations comparable to Thornberry's. Lieberman's bill was met with skepticism by the White House[27]; Bush spokesman Ari Fleischer stated that "Creating a cabinet post doesn't solve the problem"[28], and the White House continued to oppose the creation of a new department for several months after the 9/11 attacks.[29]

While Lieberman's bill sought to establish a Cabinet-level agency, Senator Bob Graham (D-Florida) introduced a bill to transfer the White House office of Homeland Security into a National Office for Combating Terrorism.[30] Graham's recommendation was based upon a study developed by the Gilmore Commission, chaired by former Virginia Governor James S. Gilmore. The Gilmore Commission produced five reports on an annual basis from 1999 until 2003. The commission recommended a White House Office with a coordinator that would be appointed by the Senate.

Despite the differences in the proposals, over the next several months a coalition formed in the Legislature to create a new Cabinet-level agency. Calculating that it would lose a battle with Congress over the creation of a new department,[31] the administration shifted gears and began to quietly formulate a proposal of its own to create a Cabinet-level Homeland Security agency.[32]

The department was formed by a small set of actors within the Bush administration.[33] One of the legislative requests the Bush White House made involved reasserting its ability to reorganize. Initially developed via a 1934 statute and altered via a Supreme Court decision involving the Immigration and Naturalization Service, the authority had expired in 1984.[34]

In summary level, President Bush's vision of a new department incorporated a series of directorates that organized the 22 agencies into a series of Directorates: Management, Science and Technology, Border and Transportation Security, Information Analysis and Infrastructure Protection and Emergency Preparedness and Response, each run by an Under Secretary. However, several organizations and offices would also report directly to the Secretary, including the United States Coast Guard and the United States Secret Service, which each retained status as a "distinct entity" within the organizational structure[35].

Bush introduced his plan for a Department of Homeland Security on June 18, 2002, and subsequently released his National Strategy for Homeland Security one month later.[36] Bush's proposal was sponsored by Rep. Dick Armey (R-Tex) and introduced to the House of Representatives on June 24, 2002[37]. The bill was quickly approved by the house and approved by the Senate in November, 2002. President Bush signed it into law on November, 25, 2002.

This history provides the factual elements of the department's formulation. In examining the history, a few observations emerge. First, the impetus to change homeland defense was undertaken at first via a slow bureaucratic process that was then dramatically interrupted by the introduction of a crisis. Second, once that crisis occurred, many competing interests, both individual and institutional, desired to change the structure of homeland security, with each individual or institution attempting to suit the bureaucratic realignment to their interests and authorities. This notion of "turf" was tantamount, and it manifested itself in a secretive and exclusionary alignment process that was essentially conducted by five individuals within the White House[38] Led by White House Chief of

Staff Andrew Card, those included Vice-president Richard Cheney, Ridge, national security adviser Condoleezza Rice, director of the office of Management and Budget Mitchell E. Daniels Jr. and Cheney Chief of Staff I. Lewis "Scooter" Libby.[39]

Within that process, many organizations were deemed politically infeasible for transfer, such as the Federal Bureau of Investigation and the National Guard[40]. Third, once the crisis occurred, the proceedings to create what was the largest government reorganization since the National Security Act of 1947 happened in dramatically quick fashion when compared to the usual pace of government change.

The next section provides a literature review of the theoretical foundations of bureaucratic change and applies those foundations to the specific mechanics of the formulation of DHS.

III. Theoretical Underpinnings

Only nine years old, analyses of DHS are somewhat limited, and have decreased in the last few years as attention has been pulled away in security think-tanks from homeland security back towards international security issues such as Afghanistan and the emergence of China as strategic adversary. Government think-tanks and oversight reports from entities such as the Government Accountability Office provide some perspective on the department's challenges, but primarily focus on the department's internal issues[41] [42]. However, Congressional dispersal of legislative authority in the context of newly created agencies and the reorganization of the government as a response to a policy crisis in not unusual; useful lessons can be gleaned from other government reorganizations and, more

generally, the perspectives of scholars who have studied policy formulation in the federal government.

Typically in the American bureaucracy, the formulation of government agencies has occurred for four different reasons: some were foundational agencies that constituted essential government functions (the Departments of State and Treasury); some were created in response to needs of growth (the Departments of Justice and Interior); others were created because of specific "clientele" (the Departments of Agriculture and Labor for farmers and industrial laborers, respectively); still others were created in response to specific national priorities (the Departments of Health and Human Services and Housing and Urban Development)[43] [44].

DHS was created in response to a national crisis rather than any one of the aforementioned reasons, specifically a terrorist attack. The notion of terrorism was certainly not new to the United States; the first real operational definition of terrorism in United States law was established in 1996; it established terrorism as "intimidation or coercion or to retaliate against government conduct"[45]. Terrorist attacks involving American citizen victims had previously been enacted a number of times, including foreign actors in international arenas (airplane hijackings and embassy bombings such as the near-simultaneous attacks on the American embassies in Nairobi, Kenya and Dar-Es-Salaam, Tanzania in 1998), foreign actors in domestic arenas (the 1993 World Trade Center bombing) or domestic actors in domestic arenas (the bombing of the Murrah Federal Building in Oklahoma City, OK, in 1995 by militia member Timothy McVeigh).

More specifically, Al-Qaeda, the terrorist organization led by Osama Bin Laden, had been identified in the mid-1980's as a nascent threat, even before the end of the Cold

War[46]. The recognition of Al Qaeda as a global threat, among other, initiated the series of commissions and reports described in the previous section.

None of these events or revelations, however, led to the widespread call for a reorganization of the government. Clearly the attacks on the World Trade Center, Pentagon, and the failed attack by a fourth plane that crash-landed in Shanksville, PA did promulgate that call. An event such as the 9/11 attacks is referred to a "policy disruption," a moment in time where a significant event presents a challenge and an opportunity to recalibrate the approach to a particular issue[47]. Scholars also refer to this type of disruption as a "punctuated equilibrium" theory of policymaking, where a pressing issue results in a period of instability. During these unstable windows, new institutional structures emerge that often remain in place for long periods of time[48]. The smaller events that preceded 9/11, however, were not sufficiently disruptive to puncture the existing homeland defense/ homeland security structure and promulgate legislative change[49]

Some of the more recent government agency formations have been instituted in order to provide a coordinating function after a period of instability occurred, though none was created with nearly as drastic a punctuated equilibrium as 9/11. The Department of Energy was formulated in 1977 as both a coordinating function as well as a response to a policy disruption, that being an energy crisis that produced an economic recession. The Energy department evolved from a White House Federal Energy office to a Federal Energy Administration and, finally, to a Cabinet-level agency.[50]

This period of instability can also be referred to as a "policy window;" policy windows emerge when a problem is identified, solutions are available, and institutional

inertia is surmountable.[51] In situations where the policy window is created by a crisis, typically the policy window has a short lifespan[52] [53]. The attacks of 9/11 proved the exception, not the rule, due to the seminal nature of the event and more importantly, the huge opportunity for potential change in authorities and structures that 9/11 afforded. As the history shows, despite Kingdon's and Downs' assertions that policy windows borne of crises happen in a short period, it took well over 18 months from 9/11 to a newly formed DHS, yet it was created.

During "policy windows," the differing federal branches (executive, legislative) each attempt to reformulate the existing structure(s) in such a way as to increase their sphere of control. Wise asserts that there are three distinct ways that this occurs: executive order coordination, a statutory coordinator and full Congressional control.[54]

Through executive order coordination, presidential leadership tends to try and centralize command and control of the institutions responsible for tackling the disruption. This is most often executed via the use of policy czars and other coordinating bodies.[55] [56]. This was President Bush's first approach when he established a White House office of Homeland Security with Gov. Ridge as its head. A vital necessity for executive order coordination is executive activism; the White House must be willing to vigilantly provide policy direction, enforce that direction via the threat of reducing resources and mitigate disputes between bureaucratic entities; otherwise, fragmentation will occur[57].

As previously discussed, the Gilmore commission had previously advocated for something in between a White House declared office and a full-fledged Cabinet agency. In this framework, referred to as a "statutory coordinator," Congress establishes by law a coordinating body within the White House, but because it is established by statute,

Congress retains significant oversight authority[58] Congress' motivation was one of control; if Homeland Security were housed within the White House, Congress would lack the ability to confirm a Departmental head via the Senate and experience a decreased ability to influence policymaking via the committee process.

The third option, Congressional control, would manifest itself in the creation of an entirely new agency where both the creation and continuation of programs (authorization) and the funding of programs (appropriation) would be controlled by the legislature. In this scenario, House and Senate committees retained their oversight over the individual functions of the proposed department.

This scenario, of course, eventually won the day. The obvious question is: why did it win? One definite reason was that the President recognized politically that Congress held the votes to establish a Cabinet-level agency and therefore relented.

However, the more structural reason is that a policy window had opened; a problem had been identified (terrorism on American soil) solutions were available (the concept of a DHS or something like it had already been circulated), and institutional inertia was surmountable. Government's tendency to offer a previously formulated solution with existing support to address a current problem[59] meant that the concept of a DHS, even though it was the President's, was quickly moved for approval by the Congress. Also, the uniquely traumatic occurrence of multiple attacks on American soil meant that by seizing the initiation of a DHS, the executive branch, while ceding the concept of Congressional control, could more effectively control the elements and the legislative edicts that comprised the new department.

The government now had a huge reorganization on its hands, a situation in which success depended on numerous factors, including degrees of organizational attention and the ways different players perceive the problems and opportunities[60]. The force with which a new bureaucratic institution alters or influences the existing system plays a major role in how effective the response is to a policy disruption. That force, however, is challenged by existing system dynamics. When those dynamics are disrupted by new problems or institutions, the tendency is for institutions to act resilient and resistant to significant changes[61] [62]. Existing organizations already possessed homeland security capabilities and, as the history shows, loathed to give that capability away to a new entity.

The merger of the Armed Forces offers a case study. After the end of the Second World War, the War Department submitted a plan to organize the Armed Forces under a single coordinating structure. The Army and the Navy voiced support and resistance, respectively, based upon the impacts a reorganization would have on their autonomy.[63] Autonomy is the notion that an organization enjoys relatively well-defined domains and can execute its mission in a space that allows an organization to develop effectively[64]. Within a government organization, high effectiveness tends to occur when agencies hold goals that are popular, engage in simple tasks, don't have a lot of bureaucratic rivals and possess minimal constraints. More informally, this is called "turf." Normally a pejorative term, "turf" can also be viewed as an appropriate assertion of authority over a subject matter to which an entity holds responsibility.

The Army believed that a unified command structure would benefit its autonomy because it feared that the emergence of nuclear deterrence as a military strategy would lessen the need for ground troops and infantry support, obviously its bellwethers. In turn,

the Navy opposed a unified command because its organizational structure provided it both an independent force of ground troops (The Marines) and, more importantly, its own air unit (naval aviation). Reorganization and the presumed examination of resource alignments would put the Navy's autonomy at risk, it believed.

Eventually a structure was formed that largely satisfied everyone's desires to maintain autonomy; it created a formally unified defense department structure but provided little authority to the Secretary of Defense; in fact, the bureaucracy increased via the introduction of a Department of the Air Force[65].What didn't happen was any type of systematic recalibration of resources based on the delineation of missions.

To synopsize these different theoretical lenses in the context of the formation of the Homeland Security department brings us to the following summary: the terrorist attacks of 9/11 represented a "punctuated equilibrium," or "policy disruption." This led to a "policy window," which was initially met with an organization (the White House office of Homeland Security) created under the tenet of "White House control." However, that 'policy window" remained open enough, due to the magnanimity of the event, that "Congressional Control," via the creation of a Cabinet-level agency, became the eventual reality. The White House, however, in a bit of political gamesmanship, introduced its own Homeland Security department prior to the passage of any legislation, and this concept became the choice of all parties, with its previously discussed inclusions and exclusions. This choice has led to consequences in the execution of the homeland security mission, intended or unintended. DHS lacks "turf," the hypothesis of this paper asserts based on the definition provided above. It cannot assert authority because it both lacks

the legislative mandates to do so and because it lacks control over many of the organizational assets needed to most effectively conduct its mission.

The next section of this paper will examine the results of this organizational transformation through two lenses; first, a series of key functional areas will be analyzed in terms of the current authorities granted to DHS and the agency's effectiveness within those functional areas. Second, we will examine federal expenditures of homeland security as a whole, to determine where the resources are allocated for the function across the federal government, and what that means for the effectiveness of the mission.

V. Authorities and Bureaucracies

DHS emerged via the Homeland Security Act of 2002, and was touted as the answer to America's need to prevent future terrorist attacks inside the United States. But as previously indicated, a number of choices were instituted in its formulation and early history that have impacted its ability to execute its Congressionally stated missions.

In examining the authorities granted to the DHS, an examination of the department's current missions, goals and objectives provides a useful lens. Congress chartered DHS to specifically prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the impact and recover from attacks that do occur[66]. However, the department inherited a host of agencies whose missions comprise broader edicts than simply preventing, protecting and responding to terrorist attacks. As part of a belated effort that was mandated in the Homeland Security Act, DHS completed its first Quadrennial Homeland Security Review (QHSR) in 2009. The

prevention of terrorism was but one element of securing the homeland defined in the QHSR; securing America's borders, enforcing immigration laws, responding to and recovering from natural, technological or hostile disasters and securing cyberspace have all emerged as distinct missions. The Department also compartmentalized the other functions that it inherited as part of the reorganization that created DHS into a sixth functional area.[67]

Table/Chart 1 – Missions and Goals of the Department of Homeland Security identified during the Quadrennial Homeland Security Review

Mission 1: Preventing Terrorism and Enhancing Security
• Goal 1.1: Prevent Terrorist Attacks • Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities • Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events
Mission 2: Securing and Managing Our Borders
• Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders • Goal 2.2: Safeguard Lawful Trade and Travel • Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations
Mission 3: Enforcing and Administering Our Immigration Laws
• Goal 3.1: Strengthen and Effectively Administer the Immigration System • Goal 3.2: Prevent Unlawful Immigration
Mission 4: Safeguarding and Securing Cyberspace

• Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment • Goal 4.2: Promote Cybersecurity Knowledge and Innovation
Mission 5: Ensuring Resilience to Disasters
• Goal 5.1: Mitigate Hazards • Goal 5.2: Enhance Preparedness • Goal 5.3: Ensure Effective Emergency Response • Goal 5.4: Rapidly Recover

Source: Department of Homeland Security Quadrennial Homeland Security Review

Table/Chart 2 – Additional Goals

Functional Area 6: Providing Essential Support to National and Economic Security
• Goal 6.1: Collect Customs Revenue and Enforce Import/Export Controls • Goal 6.2: Ensure Maritime Safety and Environmental Stewardship • Goal 6.3: Conduct and Support Other Law Enforcement Activities • Goal 6.4: Provide Specialized National Defense Capabilities

Source: Department of Homeland Security Quadrennial Homeland Security Review

Using this mission structure, we can examine a number of specific areas and examine whether the requisite authorities exist to effectively execute its stated goals.

Intelligence

In examining the mission structure at the objective level, we find that the very first objective of the department is to *Understand the Threat,* under the mission of

Preventing Terrorism and Enhancing Security. "Understand" in this context primarily relates to intelligence gathering and dissemination. Intelligence forms the basis of two other objectives within the mission structure, within Goals 1.2 (Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials) and Goal 4.1 (Create a Safe, Secure, and Resilient Cyber Environment)[68]

When the department was created, it initially formed a Directorate for Information Analysis and Infrastructure Protection (IAIP). The Information Analysis arm of that organization was pulled out and made into its own Office of Intelligence and Analysis in 2005 as part of the Department's Second Stage Review,[69] in an attempt to centralize the coordination and dissemination of intelligence products to state and local law enforcement. However, an examination of the authorities in the Homeland Security Act reveals inherent limitations

The Homeland Security Act specifically calls for the Information Analysis portion of the Directorate to "access, receive and analyze law enforcement information, intelligence information and other information from Agencies of the Federal Government," then aggregate and analyze these pieces of data for state and local issues[70]. At approximately the same time, a report released by a joint Congressional committee recommended that DHS establish an "all-source terrorism fusion center" that would amalgamate "raw" data, analyze it, package it, and disseminate it to state and local entities[71]. The law makes no mention of the department establishing its own intelligence gathering capability; instead, it renders the DHS specifically reliant on other agencies to furnish intelligence that it then can analyze and disseminate to state and local authorities. The Department primarily relies on open source data, and typically does not engage in

the more widely recognized actions related to international intelligence gathering, such as signals and imagery intelligence[72].

In addition to furnishing no organic intelligence capability within the DHS, the legislation also offers vague protocols for DHS obtaining "raw" information. On one hand, the Homeland Security Act indicates that the Secretary of DHS must specifically request information from other agencies, while a subsequent passage indicates that other agencies, despite a lack of a specific request, "shall promptly provide to the Secretary" all materials related to threats against the United States.

Furthermore, because no explicit authorities were established granting the department a central role in either the development of domestic intelligence or in the coordination and integration of existing agencies' domestic intelligence, other agencies filled the department's power vacuum. After 9/11, the FBI reacted swiftly to change its primary focus from law enforcement to counterterrorism[73]. At the same time Congress deliberated the formation of DHS, the Director of the Federal Bureau of Investigation, Robert Mueller, announced the creation of a Directorate of Intelligence as part of a significant reorganization to emphasize counterterrorism.[74] This Office of Intelligence would be created in order to assist in "pulling together bits and pieces of information that often comes from separate sources;" the Department of Justice dedicated millions of dollars to hiring and training more intelligence analysts[75].

The FBI, in fact, has acknowledged that since 9/11, it has shifted many of its resources and focus from law enforcement to terrorism, increasing its prosecutions for terrorism and national security cases by over 800 percent.[76]

There is no single domestic intelligence agency in the United States; unlike foreign intelligence, which relies on a few key players (the Central Intelligence Agency, the National Security Agency), domestic intelligence initiates at a variety of differing levels. Federal law enforcement agencies (most predominantly the FBI), as well as state and local law enforcement play key roles, as well as the owner/operators of private sector critical infrastructure. This coterie of law enforcement organizations and critical infrastructure owner/operators numbers in the thousands.[77] Therefore, much of the ability of the Department of Homeland Security to identify threats to the homeland depends on the intelligence-gathering and disseminating capabilities of other agencies, though the Office of I&A office does gather some intelligence from DHS operational components such as the Coast Guard, US Immigration and Customs Enforcement and US Customs and Border Protection.[78]

The department has attempted to integrate the intelligence and operational aspects of homeland security through a concept known as fusion centers. The stated goal of fusion centers is to 'blend relevant law enforcement and intelligence information analysis and Coordinate security measures to reduce threats in their communities[79]. Fusion centers began as an attempt to link federal, state and local resources in one environment in order to expand the traditional subjects of state and local intelligence (domestic and transnational crime including drugs, prostitution, and other organized criminal activity) and into acts of terrorism.

However, fusion centers have struggled to obtain federal resources from the interagency, despite support from DHS in the form of grants to the states (ibid), although information sharing appears to be trending in the right direction[80]. The I&A office still

lacks a permanent presence in many fusion centers, unlike the Department of Justice, which has located staff at all fusion centers since 2007[81]; in addition, DHS operational components often neglect to share information with the fusion centers, instead relying on local relationships established outside of this formal information sharing construct[82].

Even though the recommendations from the House Joint Committee on Intelligence recommended establishing an intelligence coordination center within the newly created department, President Bush instead chose to build a Terrorist Threat Integration Center within the Central Intelligence Agency in 2003[83]. A year later, primary coordination for domestic terrorism issues fell to the National Counterterrorism Center under the control of the Director for National Intelligence, which was created as an attempt to coordinate the efforts of all 16 agencies with intelligence capabilities, now known as the "Intelligence Community"[84] [85]. Although Intelligence and Analysis is a member of the intelligence community, DHS, again, must obtain information from other, more well-developed intelligence capabilities as opposed to generating its own[86].

The ability of the department to act on information is hindered by its ability to quickly gather that information for its progenitors. This challenge was clearly demonstrated in the bombing attempt on Christmas Day, 2009. Umar Farouk Abdulmattalab, a Nigerian national, boarded a plane in Yemen bound for Detroit. As the plane approached the Detroit airport, Abdulmattalab attempted to light a homemade incendiary device onboard the plane. His plan was thwarted by alert passengers.

An initial investigation by the White House revealed that the intelligence gathering had identified four differing streams of data – one from a United Nations advisor, one from the National Security Agency within the Department of Defense, one

within the NCTC within the Department of Justice and a fourth from the United States Embassy in Nigeria[87]. The fourth stream was the more commonly known attempt by Abdulmattalab's father to inform the embassy that his son was missing and "was likely under the influence of religious extremists based in Yemen."[88]

What appeared to work, at least in the initial analysis, was the sharing of information among the collectors. As was mentioned previously, there were a number of different threads of information related to Abdulmatallab from different sources. But what appeared to fail in this context was knowledge transfer from information collectors to actors; in this case, DHS organizations as United States Immigration and Customs Enforcement, which might have checked Abdulmattalab's name against a terrorist database and recommended to the State Department that Abdulmatallab's visa be denied, or US Customs and Border Protection, which through its Immigration Advisory Program, can make a recommendation to foreign authorities whether or not an individual should be allowed to board an aircraft bound for the United States. In this case, because Abdulmatallab's name did not appear on either the Terrorist Screening Database or the more restrictive No-Fly List, no recommendation was made to Dutch officials[89]. There appeared to be more of a focus on the potential of an attack on US interests in Yemen than on a direct attack on the United States[90]. Part of the lack of focus on securing the homeland still appears to be a cultural divide and an operational gap between the collectors of intelligence, who are primarily oriented in the international sphere, and the DHS operators, obviously focused on the domestic sphere[91] [92].

This captures only part of the problem. Because DHS lacks an inherent intelligence collection capability or an authoritative operational command to take in and

disseminate information, but instead relies on others who rarely orient their thinking towards a domestic threat, it remains stifled in its ability to rapidly deploy countermeasures that would have potentially interdicted a terrorist actor such as Abdulmatallab before he ever boarded a plane.

Another case of the failure to adequately share information occurred in the case of Nidal Hassan, a U.S. Army major serving as a psychiatrist. Hassan, of Palestinian descent, killed and wounded 42 persons on the campus of Ft. Hood, Texas. Although there are lingering debates about whether Hassan's attack was a manifestation or radical Islamic extremism or a case of radical workplace violence, there is no doubt that Hassan communicated with and proselytized about radical Islamic thinking. Hassan delivered a guest lecture in 2007 entitled, "Is the War on Terrorism a War on Islam? an Islamic Perspective," where he appeared to be justifying terrorism[93]. The military, in conducting an internal investigation, determined that Hassan was not a threat.[94]

This is indicative of a small but disturbing trend; an increase in threat diversification from overseas-based attacks to domestically-initiated attacks, plots and recruitment by terrorist organizations[95]. In each of those cases, it does not appear that intelligence or information sharing conducted or disseminated by DHS contributed in any significant way to intercepting or even identifying these incidents, despite their domestic orientation.

What the Department of Homeland Security has, in fact, done is to substitute an entire information sharing network (fusion centers) because it lacks intelligence-gathering authority, despite having an inability to quantify the impact of the fusion centers or even be able to determine how much they cost.[96]

Critical Infrastructure Protection

Critical Infrastructure is defined as "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 national security, national economic security, national public health or safety, or any combination of those matters.[97]". As an executive mandate, the White House released Homeland Security Presidential Directive 7, which directed the Secretary of DHS to coordinate the national effort to protect Critical Infrastructure and Key Resources (CI/KR) from terrorist attacks[98].

The QHSR lumps three disparate elements into the mission goal concerning critical infrastructure, all under the mantra of protection: critical infrastructure/key resources, leadership and events.[99] For the purpose of this analysis, only the protection of critical infrastructure and key resources will be considered. The United States Secret Service, inserted whole into the DHS, has long owned the mission of protecting the President, Vice-President and other key officials and has long held the requisite authorities to do so.

Over 85 percent of the buildings, plants, pipelines, wiring and land classified as critical infrastructure is owned by the private sector. This includes over 5,800 hospitals, 120,000 miles of railroads, and 2,800 power generating stations across 18 different sectors.[100]

As mentioned in the previous section, the Department established a Directorate for Information Analysis and Infrastructure Protection pursuant to the direction provided within the Homeland Security Act. The Act establishes broad responsibilities for the department in the protection of critical infrastructure, including direction

> "To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems."[101]

Table/Chart 3 :National Infrastructure Protection Plan Sectors and Sector Leads

	Critical infrastructure and key resource sector
Departments of Agriculture[a] and Food and Drug Administration	Agriculture and Food
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security	
Office of Infrastructure Protection	Commercial Facilities Critical Manufacturing Emergency Services Nuclear Reactors, Materials, and Waste Dams Chemical Sectors
	Information Technology

Office of Cyber Security and Communications	Communications Sectors
Transportation Security Administration	Postal and Shipping
Transportation Security Administration and U. S. Coast Guard	Transportation Systems
Federal Protective Service	Government Facilities

Despite the breadth of responsibility, the language provided within the Act explicitly directs a new DHS to furnish the "voluntary" submission of critical infrastructure information and develop the appropriate standards and protocols for protecting said information. It also indicates that the President may designate authority to a federal critical infrastructure protection program to enter into "voluntary agreement(s) to promote critical infrastructure security."[102]

Under that auspices, the Department developed the National Infrastructure Protection Plan in 2006, which established a series of seventeen CI/KR sectors (an eighteenth was later added) to develop an overarching framework for protecting critical infrastructure.

Through the councils and resources provided by the department, a series of Seventeen sector-specific plans developed through consortia of lead federal agencies and a series of private-public coordinating councils to manage efforts in each sector. The only exceptions are the National Monuments and Icons and the Government Facilities sectors, where the stakeholders are only public agencies.

The results have been mixed. In 2007, an initial assessment of the sector-specific plans determined that while most of the plans that were reviewed contained some recommended elements, such as security goals, methodologies for prioritizing

infrastructure and developing programs to assess threats, risks, and vulnerabilities, many did not contain a key element identified for private-public cooperation, namely, incentives for private companies to implement protective security measures[103]. In response, DHS developed an Enhanced Critical Infrastructure Protection (ECIP) Security Survey in 2009, which provides an online, voluntary survey to assess vulnerabilities and protective measures taken by (CI/KR) owner-operators. An eighteenth sector, Critical Manufacturing, was also added. The Office of Infrastructure Protection, now an office under a DHS component called the National Protection and Programs Directorate, tracks the percent of CI/KR owner operators that implement recommended countermeasures. This recent approach received some praise for its increased use of a common risk assessment approach.[104]

In a June 2010 memorandum to the Assistant Secretary for NPPD, the Acting Director of Protective Security Coordination Division indicated that 234 (49 percent) of 437 sites where the ECIP security survey had been conducted implemented protective measures during the 180-day period following the conduct of the ECIP survey. The Acting Director reported that the 234 sites made a total of 497 improvements across the various categories covered by the ECIP security survey, including information sharing, security management, security force, physical security, and dependencies while 239 sites reported no improvements during the period[105]. Another GAO study found that while the department could better disseminate information about critical infrastructure protective measures to its private-sector partners, the voluntary nature of the relationship inherently makes the department cautious about purporting that countermeasures in its recommendations are interpreted as standards.[106]

The Department has attempted to utilize regulatory authority within one specific sector: chemical facilities. In 2007, an interim final rule was published effectively codifying the Chemical Facility Anti-Terrorism Standards[107], which established protective standards for a range of facilities that housed a list of 322 chemicals that were either referenced in other regulations, such as the Chemical Weapons Convention[108], or are considered critical to either a government mission or the national economy. However, it has taken DHS several years to fund, staff and develop a program to meet their obligations within the regulations; as a result, not a single facility has completed the CFATS process as of February 2011.[109]

Cybersecurity

The threat of physical terrorism has been with the United States for some time, but the emerging threat of terrorist or other malicious acts perpetrated through cyberspace also poses a daunting, emerging threat. An inability to prepare for and properly defend against cyber attacks is viewed as one of the "most serious economic and national security challenges we face as a nation"[110]. While cybersecurity is clearly a more nascent mission area than others within the DHS mission set, the initial actions underscore a lack of sufficient and comprehensive enough authority to properly secure cyberspace.

As part of its QHSR, DHS identified Safeguarding and Securing Cyberspace as one of its five core missions[111]. In addition, two of the sectors identified within the National Infrastructure Protection Plan are the Information Technology and Communications sectors. However, the emergence of cyber threats and actual incidents,

as well as our increasing reliance on cyberspace for a vast array of functions, led DHS to identify cybersecurity as a unique mission.

Overarching direction for network security of federal agencies was established in 2002 with the passage of the Federal Information Management Security Act (FISMA), passed as part of the E-Government Act of 2002. Standards for the FISMA are currently developed by the National Institute of Standards and Technology (NIST). Cybersecurity policy was first established in 2003 with the White House's National Strategy to Secure Cyberspace. Similar to the three tenets of the National Strategy for Homeland Security, the strategy identified foci of "Prevent(ing) cyber attacks against America's critical infrastructures; "Reduce(ing) national vulnerability to cyber attacks; and "Minimize(ing) damage and recovery time from cyber attacks that do occur."[112] The National Strategy was later augmented by Homeland Security Presidential Directive 23, which called for a National Cyber Security Initiative[113] (Executive Office of the President, 2008). While no unclassified version of the directive was originally released under the Bush administration, elements of the initiative were opened up under the Obama administration in 2010 (Executive Office of the President, 2010)[114]. Elements of the NCSI conducted by the National Security Agency remain classified.

Cybersecurity is problematic in two distinct senses. First, like the broader spectrum of critical infrastructure (information technology being but one sector), the vast majority of the hardware, software and support infrastructure that enables the cyber sphere is owned and operated by the private sector. Second, cybersecurity profoundly blurs the typical distinctions between the military's role and the civilian government's role. The military, through its Cyber Command and the NSA, is equipped with significant

technological resources and funding to both propagate cyber attacks as a military strategy and defend against them, while Homeland Security's role is strictly defensive in nature. Both agencies have reached out to the private sector to provide assistance in helping to secure private sector networks. Although Homeland Security has only recently identified cyber as a distinct mission; its front-line cyber capabilities are largely embedded as a sub-element of its National Protection and Programs Directorate, which also holds responsibility for the protection of all critical infrastructure, the security of federal executive branch buildings, the screening of visitors to the United States, and the National Communications System for first responders[115]. It has proposed ceding the function of screening visitors to a different component starting with the passage of a budget for FY2013[116].

The DOD and the DHS did sign a Memorandum of Agreement in the fall of 2010 that established parallel liaisons at each of the agencies' respective cyber operations centers.[117]. However, these are not agencies that stand on the same footing when it comes to resources: NSA's and the Cyber Command of DOD hold a combined budget of $3.5 billion, while the entire DHS budget related to cybersecurity, including protective capability, law enforcement capability, research and development and intelligence and analysis, is less than $1 billion.[118] [119].

In addition, unlike the prevention of terrorism against a physical asset such as a building or a ship, where the probability of an actual event is relatively unlikely, attacks in cyberspace are occurring frequently and with increasing consequences. An estimate by the Center for a New American Security indicates that the federal government's networks are attacked 1.8 billion times per month[120]. In the private sector, two significant

attacks occurred in 2011 that compromised extremely sensitive data belonging to two organizations. The data was housed at RSA Security, which creates digital authentication devices for the federal government and Fortune 500 companies, and the Comodo Group, which creates digital certificates that confirm that a website is legitimate[121] [122]. Within the federal government, a multi-pronged attack infiltrated numerous federal agencies in 2009, including DHS, the Department of Defense, the Federal Aviation Administration and others, causing several of their websites to be shut down[123].

Despite all of the various documents attempting to craft a cyber strategy, there is little or any distinct authority that emerges. The FISMA establishes standards for federal network security, which have been developed and refined by the National Institute for Standards and Technology within the Department of Commerce. Currently, the Office of Management and Budget, the President's arm for managing items such as real property and improper payments, is the organization responsible for overseeing FISMA.[124] However, there is no defined standard for cybersecurity outside of federal networks that the DHS, NSA or any other agency can even provide voluntary measures against, never mind regulations[125].

Additionally, the CNCI offers specific efforts as part of the initiative, but does not specifically identify DHS as having enforcement authority either within federal networks, state and local networks, or in the private sector. HSPD-23 established the creation of a National Cyber Security Center at DHS to coordinate and integrate information to secure information technology networks[126]. However, the function that the National Cyber Security Center (NCSC) was tasked with executing was largely already being conducted

within NPPD at DHS (The two were merged under the Obama administration) This fact, plus additional uncertainties and confusion about roles and responsibilities between the White House and executive agencies, led the first Director of the NCSC to resign abruptly.[127]

The lack of clear lines of authority and coordination within cybersecurity are well acknowledged. President Obama's cyberspace policy identified that "the federal government is not organized to address this growing problem effectively now or in the future.[128] It further states that existing authorities at the same time overlap and lack sufficient decision authority to enact a consistent approach to cybersecurity issues. President Obama, following one of the policy review's recommendations, did assign a cybersecurity "czar," or cyber coordinator for the federal government, but this again does little if anything to clarify the roles of specific organizations within the federal government. CSIS called the appointment of czars in general "a symptom of our industrial-age government organization.[129]

Pending legislation identifies a number of different initiatives to address these problems. The act would require companies to report when the private data of their customers has been compromised, which is viewed as a negative incentive for companies to increase their protective measures[130]. It would also establish DHS as a regulatory authority over critical infrastructure related to cybersecurity, although the exact nature and strength of that regulatory role is much in flux[131] [132].

In the absence of authority to enforce standards on critical infrastructure, DHS has allocated much of its resource in cybersecurity towards protection of the .gov environment, when in fact the vast majority of attacks (and the vast majority of the

economic activity) occurs in the private sector. Over 80 percent of the department's budget in its Fiscal Year 2013 submission to Congress addresses protection of the .gov domain. A pair of studies conducted by the protection firm McAfee and security consultant SAIC concluded that cyber attacks have advanced beyond simple identity theft of individuals and moved to the theft of corporate intellectual property, which has the potential for even greater economic impact than the $1 trillion in annual economic cost the first study reported.[133]

National Preparedness Grants

Since its inception, DHS has allocated nearly $35 billion dollars in grants to states and municipalities[134] although homeland security funding for states and localities has been allocated by Congress since 1996 through the passage of The Defense Against Weapons of Mass Destruction Act (also known as the Nunn-Lugar-Domenici Act)[135]. Created by the USA Patriot Act of 2001, the Homeland Security Grant Program was originally a series of seven grants, now consolidated to four – the State Homeland Security Program, the Urban Area Security Initiative, the Citizen Corps Program, and the Metropolitan Medical Response System. Under these four funding streams, multiple grant sub-programs include fire protection, emergency communications, public transit security and driver's license upgrades[136]. The Homeland Security Grant program was designed to provide needed capabilities to states and localities to be prepared for terrorist attacks. In addition, numerous other grant programs target more specific areas, but fall under the broader category of national preparedness, as seen in the table below.

Table/Chart 4. Homeland Security Preparedness Grant Programs
Homeland Security Grant Program
State Homeland Security Program
Urban Areas Security Initiative
Citizen Corps Program
Metropolitan Medical Response System
Assistance to Firefighters Grant Program
Buffer Zone Protection Program
Commercial Equipment Direct Assistance Program
Emergency Management Performance Grant Program
Emergency Operations Center Grant Program
Interoperable Emergency Communications Grant Program
Port Security Grant Program
Regional Catastrophic Preparedness Grant Program
Transit Security Grant Program

The scope of the programs listed here does not include grants that are aligned to other DHS mission areas, such as Operation Stonegarden, which provides funding for state and local law enforcement for states on the U.S. border with Mexico and grants for marine safety administered by the US Coast Guard.

The original formula for allocating Homeland Security grants came in two parts. According to the Act, each state was to receive a guaranteed minimum award equal to three-quarters of 1% (the "three-quarters rule") of the total funding, plus a discretionary amount of the total terrorism preparedness funds[137] (Congress of the United States, 2001). The rest of the funds were allocated on a "risk-based" formula that only took into account population as a meaningful variable. As a result, states such as Wyoming received $38 per person while the state of California, with a denser population, a land border, a maritime border and more critical infrastructure, received only $5 per capita.[138] (Matthews, Schneider, 2010).

Immediately, charges of political influence were raised, critics citing that rural, low population states obtained a much greater share of funding per capita than they

deserved (Randsell, 2004). In response, the Department developed a smaller program, the Urban Area Security Initiative, which allocated funds based upon a risk-based formula that includes threat, vulnerability and consequence.[139] However, funding for other grant programs such as the State Homeland Security Grant Program maintained population density as part of its overall framework, although it incorporated elements such as critical infrastructure[140].

Over $5 billion has been provided to cities since UASI began. A study shows that a positive correlation existed between risk factors and the allocation of monies via UASI[141]

Table/Chart 5. FY2002-FY2009 Appropriations for Homeland Security Assistance Programs

Amounts in millions

Program	02	03	04	05	06	07	08	09	10
SHSGP	316	1,870	1,700	1,100	550	525	950	950	950
UASI	3	800	725	885	765	770	820	838	887
LETPP			500	400	400	375			
CIPP		200							
PSP	198	170	125	150	175	210	400	550	300
TSP				150	150	175	400	550	300
BSP			10	10	10	12	12	12	12
TRSP			22	5	5	12	16	8	
EOC							15	35	60
BZPP					50	50	50	50	50
FIRE	390	750	750	715	655	662	750	985	810
EMPG	168	170	180	180	185	200	300	315	340
CCP	25	30	40	15	20	15	15	15	13
MMRS	25	30	40	15	20	15	15	15	13
TTAE&E	333	330	292	341	296	298	299	429	266
CEDAP					50	50	25	8	
PSIC							50	50	50
REAI ID							50	50	50
RCPG							35	35	35
TOTALS	1,428	4,370	4,394	3,981	3,341	3,387	4,228	4,921	4,164

Source: Congressional Research Service

However, even though grant monies are allocated based on risk, there is little ability for the Federal Emergency Management Agency (FEMA) to control how the money is spent. While FEMA provides grant guidance each year, it does not specify

items or even provide standards for items that are purchased by state and local partners – indeed, it does not have the legislative authority to do so. For example, FEMA's grant guidance for fiscal year 2011 indicated that "Maturation and Enhancement of State and Major Urban Area Fusion Centers," is one of the department's highest priorities. While states were "strongly recommended" to utilize their funding for this purpose.[142], there is no way to ensure that funding was used for fusion centers or FEMA's other priorities.

Even though DHS's authority is limited, the overall regulatory picture proves more complicated in the area of grants than in the other areas examined thus far. The original Patriot Act legislation, while providing baseline funding for every state, contains no provisions or mandates for states to report on its expenditures to DHS or provide quantifiable updates on progress. However, the Post-Katrina Emergency Management Reform Act (PKEMRA) of 2006 mandated that every state provide an annual preparedness report to Congress[143]. In 2007, as part of its response to the Act, FEMA released a set of National Preparedness Guidelines that included a process for establishing current levels of capability and measuring progress towards targeted capability. Part of the guidelines involved measuring a set of target capabilities established by FEMA that were standardized across jurisdictions[144] [145]. These guidelines were developed in order to assist states and localities with three primary objectives:

- to help (states and localities) address deficiencies
- to identify alternative sources of capabilities (e.g., from mutual aid or contracts with the private sector); and
- to identify which capabilities should be tested through exercises.

Using the targeted capabilities list as its starting point, FEMA attempted to specifically quantify national preparedness through what it called its "Cost to Capabilities" Initiative, which it designed to help prioritize grant funding based on what capabilities were lacking on a jurisdictional basis. However, FEMA never was able to develop specific, quantifiable metrics that could assess national capabilities; it chose to scrap the cost to capabilities program in 2009[146]. Subsequently, FEMA planned on conducting a nationwide, multi-year gap analysis program, starting in 2009, "to provide emergency management agencies at all levels of government with greater situational awareness of response resources and capabilities,"(FEMA, 2009). However, FEMA discontinued this effort in late 2010 due to states' inability to provide information about their own capabilities[147].

Arguably, if FEMA has stronger authorities to withhold grant funds, jurisdictions would be more inclined to effectively report progress. On the other hand, FEMA has not produced a well thought-out plan to systematically collect, measure and manage against a set of targeted capabilities; it has rightly been criticized by numerous sources for its inability to measure achievements made via grant funding[148] [149]. With the introduction of Presidential Planning Directive 8 in March of 2011, the current set of targeted capabilities has been scrapped and will be replaced in 2012[150]. The implication is that for the time being, there is no definitive path towards understanding national preparedness; the current plan, released in August of 2011, plans for a National Preparedness Report to be produced by March 2012[151]. At this time there is no definitive methodology established for how "national preparedness" will be quantified.

VI. The Homeland Security Enterprise: Still Disjointed

An examination of particular authorities in the Department of Homeland Security reveals some potential hurdles to maturation. However, when considering the Department's challenges from a legislative standpoint, it is impossible not to consider organizational barriers as well, both internal to DHS and outside of DHS. The main reason internal organizational challenges must be considered is that, among its many other directions to DHS, the PKEMRA rescinded the Department's authority to internally reorganize, due to what it saw as negatively impactful prior shuffling[152].

Organizational Constructs

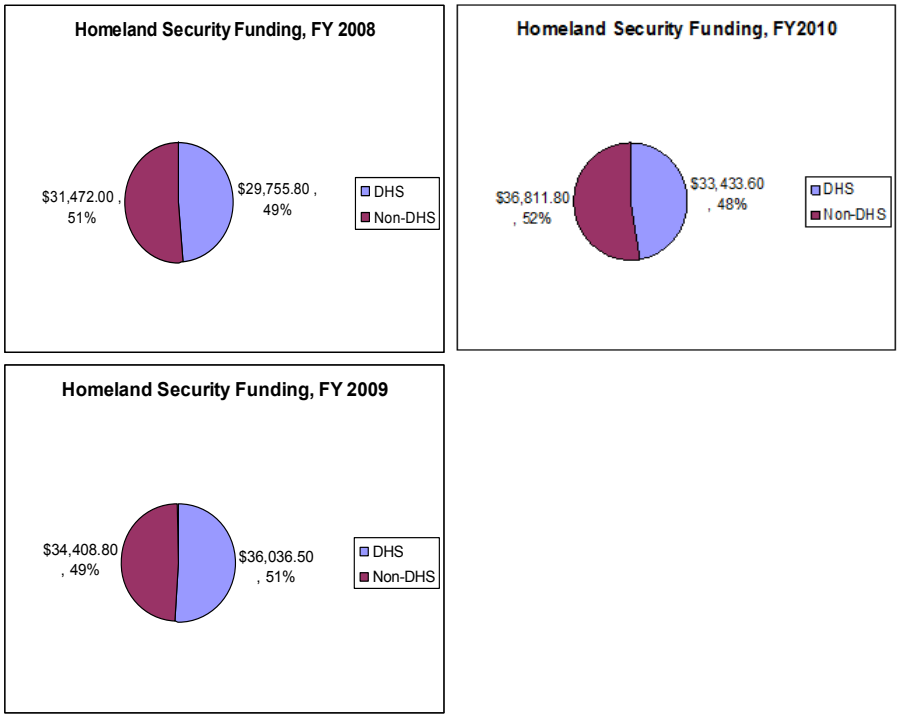
When Congress established DHS in 2003, it never intended to consolidate all homeland security activities under one organizational banner. Indeed, the merger of 22 agencies, despite being the largest government re-organization since the Department of Defense in 1947, left enormous swaths of personnel, money and functions categorized as homeland security in other organizations.

In examining the history of the department's formation, it was shown that significant political motivations influenced which organizations were incorporated and which were left out of the new DHS. By consequence, this left a significant number of organizations with homeland security functions outside of the DHS. As a method for examining which agencies may be useful candidates to move into or out of DHS to help facilitate the department's maturation, it is useful to examine where the money for homeland security is spent in the federal government currently.

As an analytical tool for determining what organizations may be candidates for transfer, the Office of Management and Budget's (OMB) annual tabulation of resources dedicated to homeland security functions, published in the President's Budget to Congress, proves a useful tool. For the budget year 2008, a total of $61.2 billion dollars was appropriated for homeland security activities across 32 federal agencies as diverse as the Department of Commerce and the Social Security Administration[153]. This increased in FY 2009 to 70.5 billion. and slightly decreased in FY 2010 to 70.2 billion.

In FY 2008, 29.7 billion, or 49 percent, was comprised of the Department of Homeland Security expenditures in FY 2008. In FY 2009 36 billion, or 51 percent, of the total homeland security funding was expended within the department. Finally, in FY 2010, 32.8 million, or 47 percent, of the total homeland security expenditures were spent within DHS. Because a budget was never passed for FY 2011, the funding allocations for these years remain at FY 2010 levels with minor modifications.

Table/Chart 6 - DHS spending versus total Homeland Security Spending (in billions of dollars)



Admittedly, analyzing homeland security expenditures is somewhat crude if it only ascribes to the top-line budget, so a more detailed examination is necessary. OMB's annual document reveals that of the $70 billion is allocated for homeland security activities, 52.4 percent ($36.8 billion) is contained within 29 other Cabinet-level agencies and smaller organizations. By comparison, in 2003, the first year DHS operated as a Cabinet-level agency, OMB estimated that 54 percent, or 23 billion, of the total homeland security funding was contained within DHS[154]. In the intervening years, there is some slight vacillation due to supplemental funding requests for response to events, but these data reveal that generally between 50 and 55 percent of all homeland security funding is contained within DHS.

The Analytical Perspectives documentation provided by the Office of Management and Budget presents some limitations in its data. For one, OMB does not consider funds expended for natural disasters as part of the scope of homeland security, despite the historical roots of homeland security residing in civil defense[155]. In addition, the current set of DHS missions incorporates a mission that provides resilience to disasters for all hazards, regardless of whether they originate via natural, man-made or hostile means[156].

In order to develop a list where there might be efficiency and effectiveness gained by the transfer of functions, the principles of scale and political feasibility where applied. Utilizing scale, a cutoff line of a minimum of $50 million in funds must have been allocated as homeland security funding. Political feasibility is examined on a case-by-case basis within the context of the recommendations made later in this paper.

In addition, a few operating assumptions were made. First, OMB categorizes funds that are used to pay for security at federal buildings as part of the protecting critical infrastructure and key assets, pursuant to the National Infrastructure Protection Plan[157]. The NIPP lists federal buildings as one of the 18 key sectors. Because agencies would likely spend this money regardless of whether OMB and the NIPP categorized it as critical or not, these funds were excluded from the set taken under consideration, with the exception of the Defense Department, which retains its own security for military bases separate from other federal buildings at a cost of $12.3 billion. Also, every federal agency utilizes funding to pay for its Continuity of Operations (COOP) programs and activities. Although FEMA is the lead government agency for Continuity of Operations among executive agencies, each agency must bear some expense for determining its own

unique plan to address how it maintains critical operations in the event of an emergency. Therefore, these funds are excluded from the analysis as well.

This renders a set of 42 programs that warrant inspection, listed below in descending order by their FY 2012 appropriation:

Table/Chart 7: Non-DHS federal funds requested for homeland security (FY 2012)

Agency	Appropriation	Alignment	Amount (in Millions)
Health and Human Services	Dep. Mgmt./ Public Health and Social Services Emergency Fund	Defending Against Catastrophic Threats	$2,729.10
Justice	FBI/ Salaries and Expenses	Domestic Counterterrorism	$2,282.00
Health and Human Services	NIH	Defending Against Catastrophic Threats	$1,794.00
State	Admin. of Foreign Affairs/Diplomatic and Consular Programs	Border and Transportation Security	$1,709.70
Energy	Natl. Nuclear Security Administration/Weapons	Protecting Critical Infrastructure and Key Assets	$1,126.50
Defense	RDT&E/Defense	Defending Against Catastrophic Threats	$817.70
Defense	Operation and Maintenance/ Navy	Defending Against Catastrophic Threats	$728.70
Defense	Operation and Maintenance/ Army	Defending Against Catastrophic Threats	$611.10
Justice	ATF/Salaries and Expenses	Domestic Counterterrorism	$450.50
NSF	Research and Related Activities	Protecting Critical Infrastructure and Key Assets	$355.30
Justice	FBI/ Salaries and Expenses	Protecting Critical Infrastructure and Key Assets	$309.30
Energy	Env. and other Defense Activities/Defense Environmental Cleanup	Protecting Critical Infrastructure and Key Assets	$276.50
Justice	General Administration/Tactical Law Enforcement Wireless Communications	Protecting Critical Infrastructure and Key Assets	$230.00

Agriculture	Animal and Plant Health Inspection Service	Border and Transportation Security	$228.20
Health and Human Services	FDA/ Salaries and Expenses	Defending Against Catastrophic Threats	$217.50
Justice	FBI/ Salaries and Expenses	Intelligence and Warning	$198.20
SSA	Social Security Administration/Limitation on Administrative Expenses	Protecting Critical Infrastructure and Key Assets	$189.10
Veterans' Affairs	Departmental Administration, IT Systems	Protecting Critical Infrastructure and Key Assets	$184.50
Agriculture	Animal and Plant Health Inspection Service	Defending Against Catastrophic Threats	$183.10
NASA	Cross-Agency Support	Protecting Critical Infrastructure and Key Assets	$180.10
Energy	Env. and other Defense Activities/Other Defense Activities	Protecting Critical Infrastructure and Key Assets	$158.20
Energy	Natl. Nuclear Security Administration/Weapons	Emergency Preparedness and Response	$155.20
Defense	Operation and Maintenance/ Air Force	Defending Against Catastrophic Threats	$152.80
GSA	Real Property Activities/Federal Buildings Fund	Border and Transportation Security	$151.00
Agriculture	US Forest Service	Protecting Critical Infrastructure and Key Assets	$135.00
Transportation	FAA/Operations	Protecting Critical Infrastructure and Key Assets	$133.20
Energy	Natl. Nuclear Security Administration/Defense Nuclear Nonproliferation	Defending Against Catastrophic Threats	$103.10
Veterans' Affairs	Veterans' Health Admin./Medical Support and Compliance	Emergency Preparedness and Response	$102.30
Justice	Legal Activities and US Marshalls/Salaries and Expenses, US Marshalls Service	Protecting Critical Infrastructure and Key Assets	$92.60
Defense	Procurement/Other, Navy	Defending Against Catastrophic Threats	$89.70
Justice	National Security Division/Salaries and Expenses	Intelligence and Warning	$87.90

Defense	Operation and Maintenance/ Army	Emergency Preparedness and Response	$86.90
Commerce	Bureau of Industry and Security/operations and Admin.	Defending Against Catastrophic Threats	$85.80
Energy	Energy Programs/Science	Protecting Critical Infrastructure and Key Assets	$83.00
Defense	Operation and Maintenance/ Air Force	Emergency Preparedness and Response	$80.20
Health and Human Services	NIH	Protecting Critical Infrastructure and Key Assets	$74.20
Health and Human Services	FDA/ Salaries and Expenses	Emergency Preparedness and Response	$72.00
Justice	DEA/Salaries and Expenses	Domestic Counterterrorism	$64.20
State	Admin. of Foreign Affairs/Diplomatic and Consular Programs	Intelligence and Warning	$56.50
Health and Human Services	CDC	Protecting Critical Infrastructure and Key Assets	$55.70
EPA	Hazardous Substance Superfund	Emergency Preparedness and Response	$54.80
Defense	Procurement/Defense-Wide	Defending Against Catastrophic Threats	$53.80
Justice	Legal Activities and US Marshalls/Salaries and Expenses, US Attorneys	Domestic Counterterrorism	$52.00
EPA	Science and Technology	Protecting Critical Infrastructure and Key Assets	$50.20

In examining each funding stream in depth, we will look to each organization's Congressional Justification to Congress for details about the explicit activities it conducts, as well as other supportive documents as needed

Health and Human Services *(Public Health and Social Services Emergency Fund, National Institutes of Health, Food and Drug Administration, Center for Disease Control and Prevention,* ***$4.94 billion****)* – The Public Health and Social Services Emergency Fund contains a myriad of programs in its role as the lead agency for Emergency Support Function #8, which involves the public health response for disasters developed under the National Response Framework[158]. These include the National Disaster Medical System, which provides emergency medical services to states and localities whose resources are overwhelmed, as well as preparedness activities associated with deploying those assets. Another major program is Project Bioshield, a program that deploys medical countermeasures in the form of vaccines and medicines should there be a biological, chemical or radioloigical attack. In addition, the funding includes grants for hospital preparedness, which provide funding for hospital around the country to develop evacuation protocols and other emergency procedures.[159]

Authorities are somewhat convoluted within the context of health emergency response. While the PKEMRA established a Chief Medical Officer (CMO) within DHS, the legislation explicitly stated that the CMO was responsible for coordinating response and recovery for medical issues natural disasters, acts of terrorism and other man-made disasters within DHS, but overall coordination for federal efforts related issues rests with the Secretary of HHS, pursuant to the Pandemic and All-Hazards Preparedness Act[160].

HHS is certainly in the best position to acquire, test and deploy vaccines and other medications through Project Bioshield and the Center for Disease Control and Prevention, as well as deploy medical professionals through the NDMS. However, when it comes to hospital preparedness, many of the emergency preparedness functions

articulated as objectives within this program are very similar to actions taken by state and local governments that receive Homeland Security Grants.

In addition, there is a notable omission in what OMB includes within the Emergency Preparedness and Response arena. HHS requests $643 million in its 2012 budget for a Public Health and Emergency Preparedness grant program it administers to states and localities[161]. DHS administers $3.8 billion in grants designed for a variety of purposes centered around emergency preparedness and security and requests about the same amount in 2012[162].

In terms of the National Institutes of Health, the Homeland Security Act specifically laid out a research and development program that authorized HHS as the primary agency to research and develop countermeasures for civilian human health (biological, biomedical and infectious disease).

DHS performs research and development in a host of other areas via its Science and Technology Directorate, but is forbidden from conducting research in human health[163]. The Food and Drug Administration's homeland security funding is principally geared towards the testing and approval process for these medical countermeasures[164]. The Center for Disease Control and Prevention is the agency responsible for maintaining and deploying if necessary, medical countermeasures in the case of a medical emergency[165].

Besides the activities listed previously, DHS's resources allocated to health issues are relatively small. The DHS Office of Health Affairs' (OHA) budget request for 2012 claims that it serves as the principal medical advisor to DHS leadership, leads DHS

biodefense, chemical defense, and food, veterinary and agricultural defense, provides health guidance and policy, coordinates health security activities and improves the health and safety of the DHS workforce. Yet the budget reveals that over $122 million of a $160 million budget are requested for biodefense programs, while only $2 million is requested for chemical defense and $6 million for planning and coordination[166]. No specific money is requested for food, veterinary and agriculture programs.

The dominant program within DHS's health expenditures is BioWatch, a grid of sensors designed to detect biological threats of high concern. The current concept of operations involves collecting samples from sensors once a day and sending them to a laboratory for analysis; if the analysis verifies a known pathogen, then local public health officials are informed to develop and coordinate a response[167]. The next version of Biowatch, known as Generation-3, will incorporate analysis of the sample directly within the detection unit, reducing the time it takes to make a positive detection of a pathogen[168].

The biosurveillance system is a complex mix of federal agencies, capabilities, and responsibilities, of which Biowatch only plays a part. Strong concerns about the costs and benefits of automated detection have been raised by numerous entities, as well as the need for DHS to better coordinate with state and local public health officials, who will play the leading role in developing the response to the release of a toxic agent [169] [170]. Both entities also articulated the need for a national strategy for biosurveillance and a declared coordinating entity for all biosurveillance efforts[171] [172].

Dept. Of Justice *(Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), General Administration*, *Drug Enforcement*

Administration (DEA), U.S. Marshalls' Service, National Security Division, $3.76 billion) – The FBI, as the principal law enforcement investigative agency in the United States, assumes a primary role in gathering intelligence about terrorists and their potential activity within the United States. It also administers a series of Joint Terrorism Task Forces in 104 cities nationwide that provide security for special events, respond to incidents and gather intelligence[173]. The FBI also operates the Terrorism Screening Center, the principal repository for screening individuals for terrorism activity and providing that information to appropriate federal and state law enforcement. DHS is often the recipient of this information, and utilizes it for programs such as Secure Flight that cross-reference airline passengers against the terrorism watchlist.

The FBI maintains a Weapons of Mass Destruction Directorate that investigates the potential hostile use of biological, chemical, and radiological/nuclear weapons, while DHS provides the defensive posture against these weapons with programs such as Biowatch, which monitors cities nationwide for biological exposures, and Advanced Spectroscopic Portals (ASP), which screen cargo for nuclear and radiological material at entry points to the United States[174].

The ATF's principal capabilities related to homeland security reside in the forensic analysis unit it shares with the FBI to investigate bombings, including the analysis of Improvised Explosive Devices (IEDs) from Afghanistan and Iraq (Bureau of Alcohol, Tobacco, Firearms and Explosives, 2011). It also operates a National Center for Explosives Training and Research, which trains federal, state and local law enforcement and the US military[175].

Law Enforcement Wireless Communications' budget request primarily seeks to consolidate and modernize the four major legacy wireless communications networks of the FBI, DEA, ATF and the US Marshall Service, and expand the program to other law enforcement partners, including DHS. The Departments of Justice, Treasury and Homeland Security signed a joint memorandum in 2004 to develop a joint wireless system, but modified that agreement in 2008 to "deploy shared systems where their respective interests and mission priorities overlap.[176]".

Courthouse security is conducted by the US Marshall Service[177] (ibid). The US Marshall Service also provides protective details for federal judges and prosecutors, a function similar to the role the United States Secret Service plays in protecting the President, Vice-President, and visiting heads of state[178].

The entirety of the Department of Justice's National Security Division's Budget is categorized under homeland security funding. However, the vast majority of the National Security Division's programs are purely legal in nature, including its programs that ensure intelligence operations conform to the rule of law[179] and those that represent federal agencies in court seeking to conduct surveillance or searches under the Foreign Intelligence Surveillance Act.[180]

Finally, the Drug Enforcement Agency's primarily responsibility involves breaking traditional criminal enterprises that traffic drugs, but the agency has also investigated and successfully interdicted incidences of narco-terrorism. It has also conducted operations in Afghanistan to assist the military with the elimination of the poppy industry to prevent Afghanistan from assuming a role as a major heroin importer to the United States[181].

In examining DHS's budget and programs, it provides little capability in examining explosives. In fact, it explicitly omitted explosives from its strategic goal dealing with Chemical, Biological, Radiological and Nuclear (CBRN) threats in the QHSR[182]. However, the department does maintain a large Federal Law Enforcement Training Center (FLETC) in many operational techniques of law enforcement.[183] One limited program exists within the Department's National Protection and Programs Directorate (NPPD); an Office of Bombing Prevention, which primarily serves as a "go-between" among federal partners and state and local governments[184].

NPPD's Federal Protective Service operates a program of providing security at federal executive agency buildings, a function very similar to the role of the U.S. Marshall's Service at courthouses (ibid). NPPD also operates the Office of Emergency Communications, which is responsible for the National Communications System, which allows the government to prioritize its communications over differing communication channels (landline, classified landline, wireless, and radio) in the event of an emergency and also has developed the National Strategy for Interoperability between Federal, State and local national security and emergency management officials[185].

Finally, this paper has already paid significant attention to the challenges faced between the DHS Office of Intelligence and Analysis's authorities and responsibilities and those of the FBI. To synopsize, the FBI has significant capabilities in intelligence gathering that the DHS I&A is not allowed to possess per the Homeland Security Act, yet it must rely on the FBI for this very type of data in order to identify patterns and communicate information to state and local officials.

Department of Energy (National Nuclear Security Administration, Environmental and Other Defense Activities, Energy Programs (Science), $1.9 billion – The Department of Energy's homeland security activities represent a broad cross-section of activity, spanning a range of operational and research activities. Approximately $155 million is budgeted in FY 2012 for emergency response coordination in the result a nuclear incident, including a Nuclear Emergency Support Team[186] (Department of Energy, 2011).It also provides technical expertise in the form of a nuclear forensics lab and technical expertise related to stolen, modified or improvised nuclear devices possibly intended for hostile use (ibid). While FEMA coordinates all federal agency response capabilities in the event of a disaster, it relies on specific expertise from a variety of different agencies, including DOE, within the National Response Framework's Emergency Support Functions[187].

Another major element of DOE's homeland security budget includes the protection of various nuclear facilities, including physical security, security systems, and screening processes ($722 million), which is categorized under the protection of critical infrastructure and key assets. Although there are some specialized elements to the protection of facilities that contain nuclear material, many of the core screening processes are similar to work conducted by the Federal Protective Service at DHS, which provides the same screening capabilities to over 1,400 federal facilities[188]. Thirty-five million is also requested by DOE for the removal of radiological materials from various sites, while DOE requests $51 million for the protection of nuclear materials at civilian facilities via security enhancements[189].

Finally, $125 million is allocated towards protecting critical infrastructure and key assets in the form of cyber security, specifically as it relates to facilities that house nuclear materials. As previously discussed in the cybersecurity section of this paper, DHS may potentially assume authority over cybersecurity as it relates to critical infrastructure and key resources[190] [191]. Other aspects of the Department of Energy's budget allocated as homeland security funding include a very small portion, percentage-wise, of the cleanup of nuclear material from various National Laboratory sites ($276 million, or 4.4 percent), as well as a small amount of DOE's scientific research program related to nuclear isotopes[192].

By comparison, most DHS capabilities relating to radiological and nuclear threats reside within the department's Domestic Nuclear Detection Office (DNDO), which largely came into being as part of Homeland Security Presidential Directive 14[193]. The DNDO is largely staffed via scientists and engineers from other federal agencies, including Energy. The Bush administration chartered DNDO and ordered it to develop a Global Nuclear Detection Architecture (GNDA), which is the framework for how nuclear material shall be detected when it presents a threat to the United States, both before and after it reaches U.S borders[194] (Executive Office of the President, 2005). DNDO led the effort to design a series of Advanced Spectroscopic Portals (ASPs), which were meant to examine cargo at land and sea ports to detect nuclear material. However, the department recently cancelled the ASP program, citing repeated issues with operational speed and effectiveness that had occurred throughout the life of the program[195] [196]. It is not certain at this point what the replacement will entail.

DNDO also provides a limited amount of grant funding to assist cities with developing specific detection architectures, known as *Securing The Cities* but so far has only initiated this effort for one location (New York City) since the program began[197]. The department also operates a Radiological Emergency Preparedness program via FEMA, which helps state and local governments to develop emergency preparedness plans if a nuclear power plant resides within their jurisdiction[198].

Department of State *(Administration of Foreign Affairs, Diplomatic and Consular Programs, $1.765 billion)* – OMB's budget perspective allocates a total of $1.76 billion of State's $12.7 billion budget to homeland security, of which $1.7 billion is dedicated towards border and transportation security.[199] The State department's primary function is to screen immigrant and non-immigrant visa requests and the supportive technology and processes that facilitate screening.[200] Other funds are allocated towards information sharing conducted between consular posts and US law enforcement, including DHS. In reviewing these elements, there is little potential conflict in the functions that the State Department conducts versus the systems and processes that DHS supports.

Department of Defense (Operations and Maintenance, Research, Development, Test and Evaluation, $2.59 billion) – The Department of Defense's (DOD) detailed breakout of homeland security dollars is not easily discerned. Unlike other agencies, DOD does not provide detailed congressional justifications for each of its subprograms or activities. A small amount of funding is targeted towards anti-terrorism technologies[201] .

This is discerned by separating the amount in the homeland security budget dedicated towards Research, Development Test and Evaluation identified in DOD's appropriation ($817 million). Also included is funding to maintain a constant state of readiness and execute air patrols at 18 locations throughout the United States, which are executed predominantly through the Northern Command, or NORTHCOM[202].

Although this study categorically excluded funding for federal agency-specific physical security, it should be noted that the $12 billion previously excluded for internal security represents another significant and separate physical security program, distinct from the ones already identified at DHS, DOJ and DOE.

National Science Foundation (Research and Related Activities - $355.3 million) – While diversified across numerous directorates and homeland security categories, the largest amount of resources NSF dedicates to homeland security functions is in the area of cybersecurity and critical infrastructure resilience[203]. Most of this funding is dedicated towards applied research, with $40 million allocated towards implementing elements of the Comprehensive Cyber Security Initiative (CNCI), a cyber-focused strategic plan authored by the Bush administration[204]. NSF's contributions to CNCI are composed of three elements: Moving Target Defense, which consists of developing flexible systems that can thwart potential cyber attacks; Tailored Trustworthy Spaces, which provide adaptable technologies for developing trusted internet connections that can help prevent damage propagated by cyber attacks; and Cyber Economic Initiatives, which strive to enhance network security through the development and adoption of market-based incentives. NSF's infrastructure resilience program primarily funds research with the

objective of mitigating damage done to buildings are other infrastructure by earthquakes and other natural disasters[205].

Through its Science and Technology Directorate, DHS funds a very similar program to the NSF Economic Initiatives program mentioned above. It also funds research for "studying trustworthy computing in scaled environments." It also identifies a "Moving Target Defense" initiative that will "move and shift over time to increase and complexity and cost for attackers"[206].

Department of Agriculture (Animal and Plant Health Inspection Service (APHIS); US Forest Service, $556 million) – Most of the personnel and screening technology to actually prevent hostile plants and animals from entering the Unites States was transferred to US Customs and Border Protection via the Homeland Security Act. The vast majority of the remaining APHIS budget is dedicated towards research and operations in order to eliminate hostile species[207].

The US Forest Service's contribution to homeland security involve specific law enforcement operations on forest service lands to counter violations against natural resources; The Forest Service, does, however, operate an investigative division that examines the growing and trafficking of illegal drugs on forest service lands[208].

Although the Forest Service does conduct law enforcement operations, they are primarily geared towards natural resources, an area in which the Forest Service obviously holds more expertise. However, the investigative capacity of drug growing and trafficking appears to overlap Immigration and Customs Enforcement's Homeland Security Investigations (HIS) division, which holds wide authority for investigating

illegal immigration, drug trafficking, human trafficking, weapons smuggling and other illegal activity within the United States interior[209].

Social Security Administration (Limitation on Administrative Expenses, $189.1 million) – However awkwardly named, the Limitation on Administrative Expenses appropriation administers the social security and supplemental security income programs[210]. An extremely small slice (1.4 percent) of the 12.9 billion allocated for administering social security assists DHS in administering E-Verify, a nationwide program that allows employer to determine, through social security and criminal checks, if a prospective employee is legally authorized to work in the United States. E-Verify utilizes a Social Security Administration developed and maintained database as one verification element[211]. As the generator of social security numbers for the nation, the SSA clearly owns this capability and provides an essential verification element for DHS's Citizenship and Immigration Services to provide a tool for US employer to hire legal labor.

Veterans' Affairs (Departmental Administration; Medical Support and Compliance, $286.8 million) – Veterans' Affairs resources are allocated towards information and system security within the departmental administration funding block; the VA has a $3 billion-plus information technology architecture that includes the vast VA medical system. Medical Support and Compliance funds provide preparedness capabilities for Veterans' Hospitals in order to help them respond effectively to an emergency. This program bears similarity to the Health and Human services' program

that assists civilian public and private hospitals prepare for emergencies[212] [213], which we have previously mentioned bear similarity to the FEMA programs that deal with all-hazards preparedness for a variety of different entities and structures[214]

NASA (Cross-Agency Support, $180.1 million) – Information in NASA's budget as it relates to homeland security is extremely limited; however, funding appears to be allocated towards implementation of information technology security and providing identification cards that use fingerprints for access to buildings and computer systems, commensurate with Homeland Security Presidential Directive 12[215].

General Services Administration (Real Property Activity, Federal Buildings Fund, $151 million) – GSA owns and maintains a significant number of border checkpoints on both the Canadian and Mexican borders[216] (General Services Administration, 2011). The Office of Management and Budget has proposed a transfer of these facilities and their budgets to US Customs and Border Protection starting in fiscal year 2013 [217].

Department of Transportation (Federal Aviation Administration Operations, $133.2 million) – Federal Aviation Administration operations contribute to homeland security via the ability to screen and train airline pilots, as well as providing radar and computer technology to monitor and inform DHS operations about threats or incursions to United States airspace[218] (Federal Aviation Administration, 2011a). DHS is involved as partner with the FAA in developing the next generation of air traffic control technology, which will migrate from a radar-based platform to a satellite-based system[219].

The FAA clearly operates these capabilities primarily for the purpose of managing US airspace for commercial and civil aviation, and provides the added benefit of providing domain awareness to DHS.

Department of Commerce (Bureau of Industry and Security, $85.8 million) – The primary function of Commerce's Bureau of Industry and Security is to control exports of goods, processes and technologies that may pose a security hazard if obtained by United States adversaries. There would appear to be some potential opportunity for comingling with US Customs and Border Protection, which operates a Container Security Initiative (CSI) program. CSI operates in several foreign ports to inspect cargo bound for the United States[220] [221] . In addition, Commerce inspects outgoing cargo for violations of United States boycotts for political reasons. Although not classified as a homeland security mission, Customs and Border Protection's Office of Field Operations inspects inbound cargo for intellectual property violations above and beyond inspecting for threats[222].

Environmental Protection Agency (Science and Technology; Hazardous Materials Superfund, $105 million) - the EPA serves as the agency responsible for the protection of the nation's water supply and wastewater treatment facilities. These functions represent one of the critical infrastructure sectors under the National Infrastructure Protection Plan[223]. It also provides capability to help states and localities prepare for, respond to and recover from chemical, biological and radiological or nuclear attacks, including large-scale efforts dedicated towards decontamination methods and

strategies if an attack occurs. While more general, FEMA's National Preparedness Directorate performs many of the same functions for state and local entities, whether the threat is from an accidental release or hostile use[224].

In addition, EPA's budget references that "testing and evaluation of commercially available technologies will continue to support those in need of purchasing reliable equipment to detect and decontaminate CBR contaminants resulting from terrorist attacks on buildings and outdoor areas"[225]. This is also in conflict with DHS Science and Technology's Test and Evaluation group, which is currently developing the National Biodefense Analysis and Countermeasures Center (NBACC), as well as a Chemical Security Analysis Center, a BioAgent detection program and several other programs related to CBRN threats[226].

VII. Observations and Recommendations

In examining both key authorities and agency responsibilities related to homeland security across the government, it is clear that limitations in authority exist that appear to hinder the operational effectiveness of the department. Intelligence in particular stands out as an area where specific incidents, such as the case of Abdulmutallab, highlight an inability for DHS to take information and translate it into action, in part because of the limitations set by the Homeland Security Act.

Even with the dollar thresholds and categorical eliminations set forth in this analysis, the capabilities budgeted under the homeland security federal umbrella are enormously spread out across many agencies. This analysis is not simply, hwever, about

throwing more organizations and money at DHS; some of the observations about the allocation of federal capabilities demonstrate a potential for removing some activities currently residing in DHS. Before recommendations are attempted, however a few key observations must be established:

Due to the political environment in which the Department was created, it has been hindered by an inability to hold others accountable for success: In examining the political history of the department's formulation, there was a lack of specific coordinating authorities granted to the department; subsequently, other agencies, sensing the coming influx of money that would come with the reaction to 9/11, established their own programs dedicated to fighting terrorism. The FBI, in particular, reordered its priorities from traditional criminal investigations to those of terrorism. Also, because of the tendency to avoid federal regulations espoused by the Bush administration, there were no specific requirements set upon states and localities, the entities responsible for implementing many of the protective and preparatory activities that will help prevent an attack.

Homeland security never was meant to be and never will be a federal responsibility contained exclusively inside DHS. In almost all of the areas examined, the efforts of states, localities, the private sector, academia and others are tantamount to achieving success. The federal government, by nature of the federalist political system designed in the United States, will never have the absolute ability to execute the homeland security mission itself, a mixture of prevention protection, mitigation, preparedness, response and recovery. The enormity of the homeland security mission is too broad for only one agency to handle alone, and the necessary reorganization of the

government in order to effective channel homeland security into one agency was predicted to take enormous planning over several years' time[227] [228] [229](Newmann, 1998; CSIS, 2004; Donley, Pollard, 2002).

DHS rightly emphasized this very point when it created the notion of a "Homeland Security Enterprise" strategy during the inaugural QHSR. DHS defined the enterprise as "the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners." Because of this principle, any improvement to the Department of Homeland Security's effectiveness must take into account how the department will work with these diverse entities, who will most often be the first to respond in the event of a terrorist attack or natural disaster.

DHS is primarily an operational agency and should coalesce resources around operational capabilities – Through the capabilities of its major components, such as the Coast Guard, ICEE and NPPD (although a directorate, it holds many operational capabilities including federal building security and cyber incident response), DHS's core capabilities lie in the functions of screening people, identity and cargo; vetting persons and their identity, detection of hostile threats via technology and processes, and preparing, mitigating, responding to and recovering from incidents when they do occur. These are the core elements the original Homeland Security strategy laid out for DHS, and they are still applicable today.

The department does retain capability in other areas such as investigatory functions, which include ICE, but this is not the department's niche. In looking at opportunities to better define authorities and agency functions that appropriately belong

in DHS, authorities and agency functions that promulgate success in these functional areas are ones that will be considered.

Research and Development in homeland security is especially spread out – A host of agencies contribute large amounts of money to the development of homeland security technology research and development. An area where this dissemination is particularly egregious is in the CBRNE (Chemical, Biological, Radiological, Nuclear and Explosive) domain. No fewer than six agencies (Homeland Security, Defense, the National Science Foundation, Health and Human Services, Energy and the Environmental Protection Agency) all spend money on research and development. There are definite opportunities to rationalize the overall research footprint.

Poor management is also a problem - The Department has not helped its cause through weak management, ineffective attempts at measurement and a general lack of risk-based analysis in its decision-making. Although the department's own management failings and difficulties are not within the scope of this paper, they have to be briefly acknowledged. As mentioned previously, the department's transformation from 22 components into a single agency has appeared on the GAO "High-Risk list" ever since DHS was formed in 2003. The department has been primarily responsible for spectacular failures in both operations (Hurricane Katrina) and in capabilities development (the Secure Border Initiative technology program) due to poor leadership, management, relationships with contractors and other internal factors. The ability of the department to effectively utilize risk in its decision-making, for example, has been so poor that Congress dissolved the Department's Office of Risk Management and Analysis due to its lack of effectiveness[230] (United States House of Representatives, 2011).

A risk-based approach to resource allocation is vital not just for operational reasons, but now, for fiscal ones as well. Like almost all agencies, Congress never enacted a budget for DHS in Fiscal Year 2011, meaning its funding was essentially flatlined. The budget passed for DHS in fiscal year 2012 is actually smaller than Fiscal Year 2011's by over $2 billion dollars, not including funding in the case of disasters (ibid). This restrictive fiscal environment, enforced by the Budget Control Act of 2011[231] (United States House of Representatives, 2011), will likely continue for a number of years. Risk-based approaches to resource allocation loom more important as resources grow scarcer.

IV. Recommendations

DHS was envisioned, much like prior government reorganizations such as the Department of Transportation, as "holding companies" for amalgamations of preexisting entities[232]. But in the case of Transportation, for example, the coordinating function had an arguably less urgent objective - the efficiency and effectiveness of the intermodal transportation system, as opposed to protecting the United States from terrorist attacks. An important distinction between the four agencies that Meier characterizes as responses to a national priority (HHS, HUD, and the Departments of Energy and Transportation) is that none of these were formulated as singular responses to a seminal event, and therefore there was a significantly less compelling desire to quickly organize these departments. The closest case may be Energy, which was created in part due to the oil crises of the 1970's, but these were a pair of lengthy events, as opposed to the immediate upheaval 9/11 created. In other words, these agencies were not organized because of a "policy

disruption."

Since DHS was organized by a policy disruption (an incredibly disruptive one, at that), there was an immediate outcry for the creation of a new bureaucracy, one of the alternatives identified as typical reactions to a policy window[233]. Unfortunately, there was an incredible amount of political calculation made in its formulation, and as a result the department's formulation, and the formulation of the government for Homeland Security overall, proved significantly less than optimal.

In its Management Challenges report for 2009, GAO takes note of the department's attempt to integrate its "non Homeland Security missions"[234] into its strategic plan. If we use Wilson's concept of autonomy as a theoretical basis, this is an incorrect approach. There are opportunities for DHS to request realignment of some programs that are superfluous to its core mission and request authorities and agencies that can grant it better autonomy. The problem here is not one of reshuffling the office chairs, in the sense that the DHS needs to assume the FBI or that FEMA needs to leave the department The problem to solve is what agency is best organized and resourced to most effectively perform different homeland security functions?. The White House should re-examine the National Strategy for Homeland Security and determine if the current configuration of agencies is most appropriately aligned to secure the nation.

Unfortunately, there is a perception among some scholars that the time for re-organization has ended[235]; however, this stands in contrast to other formulations of government agencies that were formulated and recalibrated over time, most notably the Department of Defense. The military apparatus underwent numerous, major structural realignments before the five fighting forces (Army, Navy, Air Force, Marines, Coast

Guard) were organized under the Joint Chiefs of Staff and Unified Combatant Commands that comprise the Department of Defense's structure today.

In order to better rationalize the Department of Homeland Security's ability to carry out its mission, the following measures are recommended. These are not taken lightly, as they will require significant political will to carry out. It is suggested that these recommendations could take form under the rubric of a national homeland security strategy review. A justification of a homeland security review could take two forms, applied separately or in unison: the elimination of Osama Bin Laden and the need to better organize the government for efficiency due to budgetary pressures. The killing of Bin Laden can be considered a strategic opportunity to reassess the various threats to the homeland. The president can also propose a strategic review as a means of potential cost savings to the government in these tight fiscal times.

While some of the following recommendations are oriented in reorganizations of existing entities, others are intended to close legislative gaps that currently expose vulnerabilities in DHS's ability to apply risk-based approach to homeland security across the nation.

Reestablish the national strategy for homeland security as a follow-on to the next QHSR; pursuant to it, conduct a full-suite capabilities and requirements review of all federal government homeland security activity that is led by DHS; allocate resources to all homeland security activity holders based on this process:

While there are opportunities for reorganization and better codification that will be examined in proceeding recommendations, the greatest unifying element to improve the mission of homeland security will be to coordinate budgets across all homeland

security entities based on a risk-driven strategy. DHS plans a national risk assessment as part of its second QHSR, slated to begin in January. It should pursue executive authority to conduct a government-wide review of homeland security capabilities pursuant to its missions, goals and objectives based on this risk assessment. This would potentially help the department coordinate an effective response to addressing gaps identified in its risk assessment and help to ensure that the 48 percent of federal dollars spent outside of DHS on homeland security are coordinated.

Create a new Import-Export Security division of DHS that would consolidate the functions of Customs and Border Protection inspection of imports for security and safety and the regulation of exports for national security and other considerations by the Department of Commerce's Bureau of Industry and Security – Combining these organizations into one entity would mean administering very similar functions under one umbrella; there would also be an opportunity for efficiencies if inspectors can be used for both import and export purposes.

Pass pending cyber legislation that consolidates DHS authorities to monitor and enforce compliance with federal cybersecurity standards and create standards for the private sector, especially in the critical infrastructure sectors; also create an independent a National Cybersecurity Agency (NCA) within DHS that centralizes protective capabilities and cyber law enforcement – Cyber attacks are, by many accounts, an underappreciated threat. The Internet security company Symantec, in response to the increasing volume and sophistication of cyber attacks, identified over 300 million attempted cyber attacks in 2011[236]. In the constantly adapting world of cyber threats, the current federal regulations related to information and technology security are

considered weak for the federal government and virtually nonexistent for the private sector, a troubling fact when it one considers that three-quarters of the critical information infrastructure is owned by private entities[237]. While CSIS criticized DHS for its failure to satisfy it key responsibilities for protecting critical infrastructure, it also cited uncertainty about its own authority as a factor in the department's inaction (ibid).

Pending cybersecurity legislation would provide the protocols for information sharing about cyber threats and attacks between the government and the private sector, while limiting the amount of liability companies would undertake by releasing the data[238]. The one weakness of the bill as currently written is that it provides little enforcement authority for the Department to compel agencies to comply with standards, but frankly, this is less of a concern in the cyber arena than in physical terrorism or other criminal acts because the threat has already been recognized by the private sector. Generally speaking, companies have been calling for more sharing of information between the government and the private sector [239].

However, in examining the current structure of capabilities in cybersecurity, DHS does not possess sufficient organizational resources to counter the rapidly expanding cyber threat theater. It is not, however, sufficient to grow parallel structures in DHS to those that already exist. The government has an opportunity to learn the lessons from previous failures and get the cybersecurity mission of the federal government closer to right, and it must do so under the guise of increasing restraints upon resources. Therefore, several significant organizational transfers should occur.

First, the Infraguard program from the FBI, which establishes private-public partnership programs with state and local governments and the private sector for

infrastructure protection, should be transferred to DHS. In addition, the government should also transfer the Computer Crime and Intellectual Property Section of the FBI to DHS. Third, the National Cyber-Forensics and Training Alliance, should be transferred to DHS as well, and this should be combined with the Electronic Crimes Task Forces of the Secret Service and US Immigration and Customs Enforcement's Cyber Crimes Center to create a national cyber forensics center. The bureau's programs focus on financial crimes and intellectual property; the Secret Service also focuses on financial crimes, while ICE's forensics scope a wide variety of crimes but focus on child pornography and sex trafficking and tourism.[240]

The combined forensic capabilities of these three organizations would represent a significant combination of forensic staff and technology, while also representing an all-source investigative center for cyber crimes.

Second, the Information Assurance Division of the National Security Agency, which holds responsibility for protection of national security data and information, should also be transferred to DHS. This would allow a cleaner delineation between the signals intelligence and offensive cyber capabilities of NSA (appropriate for a military agency) and the defensive elements of the Information Security Division (appropriate for a domestic security agency).

In order to provide this organization sufficient authority, a National Cybersecurity Agency should be established that brings together all of these activities under a Director who is a direct report to the Secretary of Homeland Security. This organization would have three principal divisions - a cyber defense organization, a cyber investigations division, and a cyber mission support division, which would be responsible for public

awareness, transformational research and development, international outreach, cyber policy and other support functions.

Transfer the operation and maintenance of the terrorism watchlist from the Terrorist Screening Center to the DHS Office of Intelligence and Analysis – In terms of intelligence, it is unnecessary and potentially counterproductive to create another intelligence bureaucracy in the United States. The consideration of a domestic intelligence agency, separate and distinct from the Central Intelligence Agency and the NSA, has been considered by policy think-tanks and scholars alike.[241] [242] However, the ability to absorb of the FBI's domestic intelligence capabilities into DHS would be such a bureaucratic challenge that from a risk-based proposition, it would be unwise to pursue. In fact, this is not the problem at hand. As the previous examination showed, the current problem lies less with the government's ability to collect intelligence but rather to get the intelligence quickly into the Hands of front-line operators who can protect actually do something to protect against a catastrophic attack, as illustrated by the Abdumutallab.

Because DHS owns the responsibility for preventing acts of terrorism in the United States, it utilizes the terrorism watchlist for a wide variety of purposes: screening flight manifests on domestic flight through TSA's Secure Flight program, advising international airlines on allowing American-bound passengers to board flights (Customs and Border Protection's Immigration Advisory Program), and screening criminals in the United States for inclusion on the watchlist (Immigration and Customs Enforcement's Secure Communities Program), among others.

Because of these operational capabilities, DHS represents the best location for information to be quickly integrated into operational protocols. It also owns the

mechanisms for communicating with state and local law enforcement, which obviously can deploy resources the quickest if a threat is already within the United States. Obviously, DHS is not the only recipient of terrorism screening information (the FBI and the State Dept. uses it for visa requests as well). In the case of State, however, DHS already is a checkpoint in the visa application process through its Visa Security program[243] (Government Accountability Office, 2010a).

The FBI does communicate with state and local law enforcement, but this responsibility can be easily assumed by DHS within its existing work.

Examine consolidation government-wide of federal resources dedicated to the protection of physical infrastructure to an expanded Federal Protective Service – Federal agencies dedicate enormous resources to physical security; those agencies identified include DHS, DOD, Energy, the U.S. Forest Service in the Department of Agriculture and the US Marshalls Service in the Department of Justice. Because this type of physical security is a DHS core capability, it makes a great deal of sense for these various programs to be potentially consolidated into the Federal Protective Service inside of DHS. Many of these security officers are contractors; in fact, within DHS, the vast majority of the Federal Protective Service's security guards are contractors[244]

In addition, various branches of the military utilize contract security guards currently to augment security forces deployed overseas[245] [246]. There are potential efficiencies garnered just by consolidating these contracts, as well as establishing core training and vetting (background checks, etc.) for contract security personnel. Agencies' inability to detect criminal histories on the part of security contractors has been cited in

numerous reports [247] [248] [249](GAO, 2010; GAO, 2006, Department of Defense Office of the Inspector General, 2009). A more unified process could help correct these flaws.

The Department of Homeland Security should have broader statutory authority to establish risk-based standards for critical infrastructure: Because of the size of the task and the inherently federalized nature of our government, DHS cannot control the security operations for the security of every nuclear power plant, bridge and skyscraper. But what the department can do and do effectively is enforce a unified set of standards for securing these aspects of our critical infrastructure. Currently, the department still relies on a fair measure of voluntary compliance from the private sector. DHS should possess the ability, based on risk analysis, to determine what threats are most probable (both natural and man-made). It should also be given the authority to enforce and systematically measure those standards.

The Department's Protective Security Advisors program, currently a cadre of civil servants, would require additional resources to monitor compliance with regulations. As of December 2010, only 93 staff was responsible for 74 districts within the 50 states and Puerto Rico.[250]

The federal government should consolidate its national preparedness grant programs such as port security, transit security and HHS-based hospital preparedness into a DHS-led grants program that focuses on critical infrastructure vulnerabilities to all hazards. The department should lead and conduct a real national preparedness assessment that takes into account the particular risk factors of a given locality, then establish capability standards to mitigate those risks. Then, only allocate grant funds that aim to address gaps or maintain standards.

Recommendation three has close linkages with recommendation two. As previously noted, over $40 billion in grant monies have been distributed by DHS or its predecessor agencies since 2001, much of which has been uniformly allocated to states and municipalities without accountability. In addition, other agencies such as Health and Human Services administer grants for hospital preparedness. If risk-based standards can be established for the 18 critical infrastructure sectors, then preparedness grant monies should be allocated towards the preparedness of these specific sectors.

Under this framework, grant allocations should be done with a zero-based budget mindset; in other words, funding is exclusively contingent upon risk, rather than any formula that guarantees a percentage of funding to states. The assessments should determine the level of risk, and develop a plan established to mitigate the risk and then maintain, as necessary, the level of resilience against the risk. While no one is completely certain of the overall level of preparedness of each of these sectors, a systematic effort would at least help to ensure that future dollars are spent more wisely. This would also ensure that there is a sufficient pool of resources associated with the creation of regulations governing critical infrastructure, so that the private sector is not financially burdened by these regulations.

While grants themselves would be consolidated and administered under DHS, the department should empanel interagency review of grant proposals that involve federal agencies with subject-matter expertise, such as HHS, the Department of the Interior (for national monuments), the Department of the Treasury (for the banking and financial sectors) and the DOD (for the defense industrial sector).

Establish a WMD Directorate within DHS that consolidates the programs focused on CBRN protections; any programs focused on lower-impact explosives, such as the NPPD Office of Bombing Prevention, should be eliminated and capabilities transferred to the Department of Justice's Bureau of Alcohol, Tobacco, Firearms and Explosives – Several small programs exist in DHS in the CBRN arena that all operate with their own management and business processes, as well as others in the Departments of Energy, Justice and Health and Human Services. These capabilities focused on the prevention and protection against catastrophic threats should be consolidated into a single directorate. Specifically, this would bring together from DHS the following components: the Office of Health Affairs, the Domestic Nuclear Detection Office and the Chemical Facility Anti-Terrorism Standards (CFATS) program from the National Protection and Programs Directorate. It would also bring together the Department of Energy's Nuclear Incident Support Teams and its security funding for protecting nuclear power plants, as well as the EPA's Decontamination programs. Because the Department of Justice's Weapons of Mass Destruction Directorate is primarily investigatory in nature, it shall remain housed there. Other capabilities in CBRNE that are research-and-development focused shall also be consolidated within DHS, but within a different organizational structure, defined below.

In addition to the elements that would authority or consolidate organizations into DHS, there are opportunities for streamlining DHS operations by removing certain programs.

Remove the BioWatch biological pathogen detection program from DHS and place it within the Department of Health and Human Services' Center for Disease

Control and Prevention – DHS once managed the program (Project BioShield) that maintained the critical vaccines for dangerous pathogens such as anthrax, but lobbied and eventually received permission from Congress to turn the operation and maintenance of the program to the CDC, because it felt that HHS could better manage the vaccine stockpile. A similar logic follows with biodetection; HHS has better established relationships with state and local health officials and can utilize those relationships to make swift, informed decisions to move from a positive detection of a pathogen to the deployment of a vaccine or other countermeasure.

Consolidate basic research for homeland security functions into the National Science Foundation, and applied research into DHS Science and Technology - Because the National Science Foundation has the scientific breadth of a wide variety of disciplines, such as biology, chemistry, engineering, computer science, and others, it represents an ideal location to target homeland security basic research that can lead to technological breakthroughs. The NSF already breaks out its basic research into a homeland security category when it submits its budget in order to allow the OMB to develop its homeland security budgetary exhibit; the NSF could develop a Homeland Security Center of Excellence for which it solicits proposals. Medical research, because of statute, would still reside in the National Institutes of Health. The significant resources and infrastructure of the NIH provide arguably the best environment for this type of research. In contrast, DHS Science and Technology should focus on applied research that gathers specific requirements from the operational components of the DHS, with the exception of cybersecurity, where the practitioners of cyber defense are often those who

are also best equipped to identify innovation. The newly created National Cybersecurity Agency would house cyber R&D.

The specific research DOD and DOE conduct in anti-terrorism technologies would be transferred to DHS, as well as the three programs identified by NSF as targeted cyber research areas (Moving Target Defense; Tailored Trustworthy Spaces and Cyber Economic Initiatives). Basic research dollars expended by S&T would be made available to the NSF for competitive grants.

X. Conclusion

In the challenging economic environment we now face, other national priorities may loom greater in the political and policy environment we currently occupy than homeland security, such as job creation and entitlement reform. It may seem like an inopportune moment to address the problems of homeland security, but very few events have the ability to impact the political and policy environments the way a terrorist attack on American soil can. While not all of the recommendations provided herein are geared towards the prevention of terrorism, many of them are and all of them represent distinct threats to American security. One only is reminded of the need to tap the Strategic Petroleum Reserve before Hurricane Katrina's landfall to identify the interconnections between natural disasters and the U.S security environment. The policy window for this type of effort will prove challenging, but it can be done within the context of a broader effort towards a more efficient government and a need to review our approach in the wake of another seminal event (the killing of Bin Laden). On the budgetary side, the

Obama administration began an initiative last spring to look at an optimization of the government; only in early 2012 has it requested to reinstate authority to actually consolidate agencies [251](Landler, Lowrey, 2012). The challenge would be finding the proper "policy window" in which to structure such a diverse set of changes as proposed; organizational changes can certainly be entertained as part of a general restructuring of government if they can be seen as providing cost savings.

Changing governmental authorities is another issue entirely; finding the political capital to institute a change, such as broader authority over regulations to critical infrastructure that could result in more governmental power, is daunting at best. Short of another catastrophic event acting as a catalyst (something no one hopes for), infrastructure improvements for security could be incentivized as part of a modernization effort to bring deficient physical infrastructure up to date - the concept of an "infrastructure bank" has been a policy proposal often touted by the Obama administration and members of Congress as a means of economic stimulus[252] (Plumer, 2011).

Regardless of the tactical considerations that would effectuate such changes, the need to adjust the DHS should be viewed as a priority. The agency, as currently designed, requires some additional "nourishment" in the form of authorities and other organizations' capabilities to achieve optimization. In addition, some "addition by subtraction" can occur if the department sheds some of the functions where its knowledge and capabilities are limited. If the department is allowed to remain in its current state, there is a real chance that it will be permanently ensconced in a kind of stymied

adolescence – mature beyond the initial chaos of its infancy but unable to make the necessary leaps to adulthood.

REFERENCES

[1] Department of Homeland Security, FY 2008 Citizens Report, Feb. 2007. p. 6

[2] ibid

[3] Department of Homeland Security, FY 2010 Budget-In-Brief (totals were summed from each DHS component's personnel (Full Time Equivalent (FTE) counts provided within their budget summaries), Feb. 2009

[4] 107th Congress, Public Law 107-296 (Homeland Security Act of 2002), Sec. 412, Sec. 821 Sec. 888

[5] Cooper, Christopher and Robert Block, *Disaster: Hurricane Katrina and the Failure of Homeland Security*, Times Books, 2006, pp. 67-94

[6] 109th Congress, Committee on Homeland Security and Governmental Affairs, *Hurricane Katrina; A Nation Still Unprepared,* pp. 203- 232

[7] Heyman, David, James Jay Carafano, "Homeland Security 3.0: Building a National Enterprise To Keep America Free, Safe, and Prosperous, Center for Strategic and International Studies and The Heritage Foundation, Sep. 2008 p. 3

[8] United States Government Accountability Office, "GAO High-Risk Series: An Update," Jan. 2003 pp. 18-20

[9] United States Government Accountability Office, "GAO High-Risk Series: An Update," Jan. 2005, pp. 48-49

[10] United States Government Accountability Office, "GAO High-Risk Series: An Update," Jan. 2007, pp.48-49

[11] United States Government Accountability Office, "GAO High-Risk Series: An Update," Jan. 2009, p.49

[12] Roberts, Patrick S. and Paul N. Stockton, "Findings from the Forum on Homeland Security After the Bush Administration; Next Steps in Building Unity of Effort," Center for International security and Cooperation, Stanford University, p.1

[13] Kingsbury, Alex, "Janet Napolitano's Tough Job at Homeland Security," US News and World Report, July, 24, 2009, viewed at: http://www.usnews.com/articles/news/national/2009/07/24/janet-napolitanos-tough-job-at-homeland-security.html

[14] Strohm, Chris, "DHS: Following Up On The Fifth Anniversary," National Journal, Feb. 18, 2008, viewed at http://www3.nationaljournal.com/pubs/congressdaily/report/tech/features/issues/issu080218.htm

[15] Department of Homeland Security, Quadrennial Homeland Security Report, January 2010, pp. 12-13

[16] Ibid

[17] Brake, Jeffrey D. "Quadrennial Defense Review (QDR): Background, Process, and Issues". Library of Congress Congressional Research Service. June 21, 2001

[18] Roberts, Stockton, p.2

[19] United States Office of Management and Budget, "Fiscal Year 2012 Analytical perspectives of the U.S. Government," pp.403-410

[20] Department of Homeland Security, "Brief Documentary History of the Department of Homeland Security," p.4

[21] Archives of President George W. Bush, "Address to a Joint Session of Congress and the American People," available at http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html

[22] 107th Congress, 1st Session, "HR 1158: To Establish the National Homeland Security Agency," March 21, 2001, available at http://www.gpo.gov/fdsys/pkg/BILLS-107hr1158ih/pdf/BILLS-107hr1158ih.pdf

[23] The United States Commission on National Security, "Road map for National Security; Imperative for Change," Feb. 15, 2001, p. viii

[24] Glasser, Susan, Michael Grunwald, "Department's Mission was Undermined from the Start," Washington Post, Dec. 22, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/12/21/AR2005122102327.html

[25] Executive Office of the President, "Establishing the Office of Homeland Security and The Homeland Security Council," Federal Register, Vol. 66. Num. 196, October 8, 2001

[26] Cuellar, Mariano-Florentino, Dara Cohen, Barry R. Weingast "Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates," Stanford Law Review, pp. 687-688

[27] Glasser, Grunwald, ibid

[28] ibid

[29] Cushman Jr. , Charles C, *An Introduction to the U.S. Congress,* pp.163-166

[30] Cuellar, Cohen, Weingast, pp. 687-688

[31] Cuellar, Cohen, Weingast, pp. 690-691

[32] Glasser, Grunwald, ibid

[33] ibid

[34] Moe, Ronald C., The President's Reorganization Authority: Review and Analysis, "Congressional Research Service, March 2001, p.1, available at http://congressionalresearch.com/RL30876/document.php?study=THE+PRESIDENTS+REORGANIZATION+AUTHORITY+REVIEW+AND+ANALYSIS

[35] 107th Congress, Public Law 107-296 (Homeland Security Act of 2002, Sec.888

[36] Department of Homeland Security, "Brief Documentary History of the Department of Homeland Security," p.6

[37] ibid

[38] Glasser, Grunwald, ibid

[39] ibid

[40] ibid

[41] United States Government Accountability Office, "GAO High-Risk Series: An Update," Jan. 2009, p.49

[42] Heyman, David, James Jay Carafano, "DHS 2.0: Rethinking the Department of Homeland Security, joint project of the Center for Strategic and International Studies and the Heritage Foundation, Sep. 18, 2008, pp. 11-14

[43] Parsons, Wayne, "Public Policy: An Introduction to the Theory and Practice of Policy Analysis," pp. 203-207

[44] Meier, Kenneth, *Politics and the Bureaucracy: Policymaking in the Fourth Branch of Government," pp. 8-10*

[45] Noftsinger, John B. Kenneth F. Newbold and Jack K. Wheele, Understanding Homeland Security: Policy, Perspectives, and Paradoxes, pp. 2-4

[46] Perrow, Charles, "The Disaster after 9/11: The Department of Homeland Security and the Intelligence Reorganization," Homeland Security Affairs, Vol. II, No.1, April 2006,

[47] May, Peter J., Joshua Sapotichne, Samuel Workman, "Widespread Policy Disruption and Interest Mobilization," Policy Studies Journal, pp. 793-81

[48] Baumgartner, F.R. and B.D. Jones, "Agenda Dynamics and Policy Subsystems," Journal of Politics, Vol. 53, pp.1044-1074

[49] Noftsinger, et al, pp. 31-32

[50] Fehner, Terence, Jack M Holl, "Department of Energy Summary History," Department of Energy Executive Secretariat, November 1994, pp.27-30

[51] Kingdon, John W., "Agendas, Alternatives, and Public Policies," pp. 165-195

[52] Kingdon, ibid

[53]Downs, Anthony, "Up and Down with Ecology; the "Issue-Attention Cycle," The Public Interest 28, Summer 1972, pp. 38-50

[54] Wise, Charles, "Organizing for Homeland Security," Public Administration Review, Vol. 62, No.2 (Mar.-Apr. 2002), pp. 131-144

[55] May, et al, ibid

[56] Wise, ibid

[57] Perrow, ibid

[58] Wise, ibid

59 Jackson, et al, "The Challenge of Domestic Intelligence in a Free Society; A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency," The Rand Corporation, January 2009

[60] March, James G., Johan P. Olson, Organizing Political Life: What Administrative Reorganization Tells Us about Government, The American Political Science Review, pp. 281-296

[61] Jeff Worsham, Marc Eisner, and Evan Ringquist. 1997. "Assessing the Assumptions: A Critical Analysis of Agency Theory**."** *Administration and Society*. 28(February)4: 419-440

[62] Jeff Worsham, Evan Rinquist and Marc Eisner. 1998. "A Theory of Political Influence of the Bureaucracy." in Jay D White, ed. *Research in Public Administration*. Stamford, CT: JAI Press.

63 Wilson James Q, "Bureaucracy: What Government Agencies Do And Why They Do It."

[64] Wilson, ibid

[65] ibid

[66] Homeland Security Council, "National Strategy for Homeland Security," p.3

[67] Department of Homeland Security, Quadrennial Homeland Security Report, January 2010, pp. 12-15

[68] ibid

[69] Department of Homeland Security, *Homeland Security Secretary Michael Chertoff announces six-point agenda for Department of Homeland Security*, Press Release, July 13, 2005, www.dhs.gov/xnews/releases/press_release_0703.shtm

[70] 107th Congress, Public Law 107-296 (Homeland Security Act of 2002), Sec. 201-202

[71] ibid

[72] Randol, Mark A., "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress" Congressional Research Service, May 27, 2009

[73] Bowers, Faye, "How FBI is remaking intelligence functions," The Christian Science Monitor, May 19, 2004, available at http://www.csmonitor.com/2004/0519/p02s02-usju.html

74 Mueller, Robert, Statement Before the House Permanent Select Committee on Intelligence, October 6, 2011, available at http://www.fbi.gov/news/testimony/the-state-of-intelligence-reform-10-years-after-911

[75] Bowers, ibid

76 Dan Eggen and John Solomon, FBI Audit Prompts Calls for Reform, The Washington Post, March 10, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/03/09/AR2007030902356.html

[77] Jackson, Brian, et al, "Considering the creation of a domestic intelligence agency in the United States : lessons from the experiences of Australia, Canada, France, Germany, and the United Kingdom." Rand Corporation, furnished for the Department of Homeland Security, 2009

[78] Randol, ibid

79 Monahan, Torin and Neal A. Palmer, "The Emerging Politics of DHS Fusion Centers," Security Dialogue vol. 40, no. 6, December 2009, pp. 617-636

[80] Department of Homeland Security Office of the Inspector General, "Information Sharing With Fusion Centers Has Improved, but Information System Challenges Remain," October, 2010

[81] Randol, ibid

[82] Department of Homeland Security Office of the Inspector General, ibid

[83] Congressional Research Service, National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns, Jan.7, 2011

[84] Lipton, Eric, Eric Schmitt, Mark Mazetti, "Review of Jet Bomb Plot Shows More Missed Clues," The New York Times, Jan. 17, 2010, available at http://www.nytimes.com/2010/01/18/us/18intel.html?pagewanted=all&_r=0

[85] Congressional Research Service, ibid

86 Walker, David "9/11 Commission Report; Reorganization, Transformation, and Information Sharing," Testimony Before the Committee on Government Reform, House of Representatives, August 3, 2004

87 The White House, Office of the Press Secretary, : "White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack," available at http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack

[88] Lipton, Schmitt, Mazetti, ibid

89 Department of Homeland Security, "Testimony of Secretary Napolitano before the Senate Committee on the Homeland Security and Governmental Affairs, "Intelligence Reform: The Lessons and Implications of the Christmas Day Attack" available at http://www.dhs.gov/news/2010/01/20/secretary-napolitanos-testimony-intelligence-reform-lessons-and-implications

90 111th Congress, 2nd session, Report of the Senate Select Committee on Intelligence, "Attempted terrorist Attack on Northwest Airlines Flight 253," United States Senate, available at http://intelligence.senate.gov/pdfs/111199.pdf

[91] Jackson, ibid

[92] CRS, ibid

93 Bender, Bryan, "Ft. Hood suspect was Army dilemma," The Boston Globe, Feb. 22, 2010, available at http://www.boston.com/news/nation/articles/2010/02/22/ft_hood_suspect_was_army_dilemma/

[94] ibid

95 Bergen, Peter and Bruce Hoffman, "Assessing the Terrorist Threat," Bipartisan Policy Center, pp. 4-13

[96] United States Senate, Permanent SubCommittee on Investigations, Committee on Homeland Security and Government Affairs, "Federal Support and Involvement in State and local Fusion Centers," October 2, 2012

[97] 107th Congress, 1st Session, HR 3162 "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act)," Sec. 701, available at http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

98 Executive Office of the President, Homeland Security Presidential Directive 7-Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2004, available at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

[99] Department of Homeland Security, Quadrennial Homeland Security Report, January 2010, pp. 21-24

100 Department of Homeland Security, National Infrastructure Protection Plan, p. 19

[101] 107th Congress, Public Law 107-296 (Homeland Security Act of 2002), Sec. 211-215

[102] ibid

[103] Homeland Security and Justice Branch, "Multiple Efforts to Secure Control Systems Are Under

Way, but Challenges Remain," Government Accountability Office September 2007

[104] Homeland Security and Justice Branch, "Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience," Government Accountability Office March 2010

[105]Homeland Security and Justice Branch, "Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve," Government Accountability Office July 10, 2007

[106] Homeland Security and Justice Branch, "Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened," Government Accountability Office September 2010

107 Federal Register, "Chemical Facility Anti-Terrorism Standards; Final Rule," April 9, 2007

[108] Organisation for the Prohibition of Chemical Weapons, *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction,* available at http://www.opcw.org/chemical-weapons-convention

[109] National Protection and Programs Directorate, Internal Memorandum from Infrastructure Security Compliance Division to the Undersecretary on the Success of the CFATS program, November, 2011

[110] Office of the President of the United States, "Comprehensive National Cybersecurity Initiative," Cyberspace Policy Review pursuant to the appointment of President Obama May, 2009

[111] Department of Homeland Security, Quadrennial Homeland Security Report, January 2010, pp.54-58

[112] Executive Office of the President, "The National Strategy to Secure Cyberspace," February 2003

[113] Executive Office of the President, "Homeland Security Presidential Directive 23 - Comprehensive National Cybersecurity Initiative," January 2008

[114] Office of the President of the United States, "Comprehensive National Cybersecurity Initiative," Cyberspace Policy Review pursuant to the appointment of President Obama May, 2009

[115] Department of Homeland Security, Description of the National Protection and Programs Directorate, available at http://www.dhs.gov/about-national-protection-and-programs-directorate

[116] Department of Homeland Security, "Budget in Brief: Fiscal Year 2013," February, 2012

[117] Department of Homeland Security, Department of Defense, "Memorandum of Agreement between The Department of Homeland Security and the Department of Defense regarding Cybersecurity," Oct. 13, 2010

[118] Department of Homeland Security, "Budget in Brief: Fiscal Year 2013," February, 2012

[119] Corrin, Amber, "DOD budget and Industry; Prepare For Change," Federal Computer Week, "Feb. 15, 2012, available at http://fcw.com/articles/2012/02/15/defense-budget-cybersecurity-industry.aspx?sc_lang=en

120 Lord, Kristin and Travis Sharp, "America's Cyber Future: Security and Prosperity in the Information Age

[121] Nakashima, Ellen "U.S. Agencies Respond to Cyberattack on InformationSecurity Firm," *The Washington Post*, March 23, 2011, available at http://www.washingtonpost.com/world/us-agencies-respond-to-cyberattack-on-information-security-firm/2011/03/23/ABDhjoKB_story.html

[122] Richmond, Riva, "An Attack Sheds Light on Internet Security Holes," The New York Times, April 6, 2011, available at http://www.nytimes.com/2011/04/07/technology/07hack.html

[123] Center for a New American Security, ibid

[124] Lord, Sharp, ibid

[125] Congress of the United States, "H.R. 2458 – 48, Federal Information Security Management Act of 2002," December 2002, available at http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[126] Office of the President of the United States, ibid

[127] Gorman, Siobhan," Cybersecurity Chief Resigns," Wall Street Journal, March 7, 2009, available at http://online.wsj.com/article/SB123638468860758145.html

[128] Office of the President of the United States, "Comprehensive National Cybersecurity Initiative," Cyberspace Policy Review pursuant to the appointment of President Obama May, 2009

[129] CSIS Commission on Cyberspace for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, December, 2008

[130] Etzioni, Amatai, "Cybersecurity in the Private Sector," *Issues in Science and Technology,* October 2011 pp.58-62

[131] ibid

[132] Johnson, Nicole Blake, "Senators to Introduce Long-Awaited Cybersecurity Bill Next Week," Federal Times, Feb.9, 2012, available at http://www.federaltimes.com/article/20120209/IT01/202090309/

133 McAfee Corporation , "Unsecured Economies: Protecting Vital Information," January, 2009

[134] Center for Investigative Reporting, *States Spend Billions on Local Homeland Security*, Dec.21, 2011, available at http://projects.cironline.org/police-grants

135 Reese, Shawn, "Department of Homeland Security Assistance to States and Localities: A Summary and Issues for the 111th Congress," Congressional Research Service, December, 2009

[136] Center For Investigative Reporting, ibid

[137] Reese, ibid

138 Gilliard-Matthews, Stacia and Anne Schneider, "Politics or Risks? An Analysis of Homeland

Security Grant Allocations to the States Journal of Emergency Management, Volume 7, Issue 1, December, 2010

[139] Reese, ibid

140 Statement of William O. Jenkins, "DHS Improved its Risk-Based Grant Programs' Allocation and Management Methods, But Measuring Programs' Impact on National Capabilities Remains a Challenge," Government Accountability Officer, March, 2008

[141] Gilliard-Matthews, Schneider, ibid

[142] Federal Emergency Management Agency, Non_Disaster Grant Guidance for FY 2011, previously available (accessed March 12, 2011) at http://www.fema.gov/preparedness-non-disaster-grants

[143] 109th Congress, Public Law 109-295, "Post Katrina Emergency Management Reform Act," Section 501 of the 2007 DHS Appropriations Bill, Oct. 6, 2006

144 US Department of Homeland Security, "Target Capabilities List: A companion to the National Preparedness Guidelines," September, 2007

145 Bea, Keith, Elaine Halchin, Henry Hogue, Frederick Kaiser, Natalie Love, Francis X. McCarthy, Shawn Reese, Barbara Schwemle, "Federal Emergency Management Policy Changes After Hurricane Katrina: A Summary of Statutory Provisions, Congressional Research Service, 2006

[146] Reese, ibid

147 Homeland Security and Justice Division, "FEMA Has Made Limited Progress in Efforts to Develop and Implement a System to Assess National Preparedness Capabilities," Government Accountability Office, October, 2010

[148] Statement of William O. Jenkins, ibid

[149] Gilliard-Matthews, Schneider, ibid

[150] The White House, "Presidential Policy Directive 8 – National Preparedness," March 30, 2011

[151] Brown, Jared T., "Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress," Congressional Research Service, October, 2011

[152] 109th Congress, Public Law 109-295, ibid

[153] Office of Management and Budget, *Analytical Perspectives: Appendix A; Homeland Security Mission Funding by Agency and Budget Account*, FY 2012 Budget to Congress, pp. 1-24

[154] Government Accountability Office, *Combating Terrorism: Determining and Reporting Federal Funding Data,* January 2006

[155] Kettl, Donald, Homeland Security and American Politics, 2nd Edition, pp.37-60

[156] Department of Homeland Security, Quadrennial Homeland Security Review Report, pp.59-63

157 Department of Homeland Security, "National Infrastructure Protection Plan; Partnering to enhance protection and Resiliency," 2009

[158] Department of Homeland Security, "National Response Framework," January 2008

[159] Department of Health and Human Services, FY 2012 Budget to Congress, February 2011

[160] Congress of the United States, Public Law 109-417, "S. 3678:Pandemic and All-Hazards Preparedness Act," 109th Congress, Dec. 2006

[161] Department of Health and Human Services, ibid

[162] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[163] 107th Congress, Public Law 107-296, "H.R. 5005: Homeland Security Act of 2002," Sec. 304

[164] Department of Health and Human Services, FY 2012 Budget to Congress, February 2011

[165] ibid

[166] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

167 O'Toole, Tara, "Biosurveillance," Testimony of Tara O'Toole Before the House Subcommittee on Homeland Security Appropriations, on Biosurveillance, April 16, 2010

[168] Lister, Sarah, "Public Health and Medical Emergency Management: Issues in the 112th Congress," Congressional Research Service, February, 2011, available at http://www.fas.org/sgp/crs/misc/R41646.pdf

[169] Goldstein, et al, "BioWatch and Public Health Surveillance: Evaluating Systems for the Early Detection of Biological Threats," Board on Health Sciences Policy, Board on Chemical Sciences and Technology, Board on Life Sciences, National Academy of Sciences, January, 2011

170 Homeland Security and Justice Division, "Biosurveillance: Efforts to Develop a National Biosurveillance Capability Need a National Strategy and a Designated Leader," Government Accountability Office June, 2010

[171] Goldstein, et al, ibid

[172] Homeland Security and Justice Division, ibid

[173] Joint Terrorism Task Force website, accessed Feb. 12, 2012 at http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs

[174] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[175] Department of Justice, FY 2012 Budget to Congress, February 2011

[176] Department of Justice, Law Enforcement Wireless Communications, Wireless Communications Implementation Plan, FY 2012 Budget to Congress, February 2012

[177] Department of Justice, FY 2012 Budget to Congress, February 2011

[178] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[179] Department of Justice, FY 2012 Budget to Congress, February 2011

[180] ibid

[181] Drug Enforcement Agency, FY 2012 Budget to Congress, February 2011

[182] Department of Homeland Security, Quadrennial Homeland Security Review Report, pp.59-63

[183] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[184] ibid

[185] Department of Homeland Security, National Emergency Communications Plan, July 2008

[186] Department of Homeland Security, Quadrennial Homeland Security Review Report, pp. 40-41

[187] Federal Emergency Management Agency, Emergency Support Function Annexes: Introduction," January 2008

[188] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[189] Department of Energy, FY 2012 Budget to Congress, February 2011

[190] Etzioni, ibid

[191] Johnson, ibid

[192] Department of Energy, FY 2012 Budget to Congress, February 2011

193 Executive Office of the President, Homeland Security Presidential Directive 14 – Domestic Nuclear Detection (National Security Presidential Directive 43), April 15, 2005, obtained from www.fas.org/irp/offdocs/nspd/nspd-43.html

194 ibid

195 McCarter, Mickey, "DHS Cancels Next Generation Radiation Portal For Cargo Screening, Homeland Security Today, July 27, 2011, available at http://www.hstoday.us/briefings/daily-news-briefings/single-article/dhs-cancels-next-generation-radiation-portal-for-cargo-screening/f816bd0387d0a22e030953bf84e99caf.html

196 Homeland Security and Justice Division,"Combating Nuclear Smuggling Inadequate Communication and Oversight Hampered DHS Efforts to Develop an Advanced Radiography System to Detect Nuclear Materials," , Government Accountability Office, Sep.2010

[197] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[198] ibid

[199] Office of Management and Budget, ibid

[200] Department of State, FY 2012 Budget to Congress, February 2011

[201] Schmitt, Matthew, Gerald Trimarco, Melissa Murrell, "Federal Funding for Homeland Security," Congressional Budget Office, April 30, 2004

[202] Homeland Security and Justice Division, "Homeland Defense: Continued Actions Needed to Improve Management of Air Sovereignty Alert Operations," Jan. 2012,

Government Accountability Office accessed at http://www.gao.gov/products/GAO-12-311

[203] National Science Foundation, FY 2012 Budget to Congress, February 2011

[204] Office of the President of the United States, Comprehensive National Cybersecurity Initiative, ibid

[205] National Science Foundation, FY 2012 Budget to Congress, February 2011

[206] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[207] Department of Agriculture, FY 2012 Budget to Congress, February 2011

[208] ibid

[209]Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[210] Social Security Administration, FY 2012 Budget to Congress, February 2011

[211] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[212] Department of Veterans' Affairs, FY 2012 Budget to Congress, February 2011

[213] Department of Health and Human Services, FY 2012 Budget to Congress, February 2011

[214] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[215] National Aeronautics and Space Administration, FY 2012 Budget to Congress, February 2011

[216] General Services Administration, FY 2012 Budget to Congress, February 2011

[217] Office of Management and Budget, FY 2013 Passback to the Department of Homeland Security, November 2011

[218] Federal Aviation Administration, FY 2012 Budget to Congress, February 2011

[219] Federal Aviation Administration, Next Gen Implementation Plan, February 2012

[220] Department of Commerce, FY 2012 Budget to Congress, February 2011

[221] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[222] ibid

[223] Environmental Protection Agency, FY 2012 Budget to Congress, February 2011

[224] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[225] Environmental Protection Agency, FY 2012 Budget to Congress, February 2011

[226] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[227] Newmann, William W., "Reorganizing for National Security and Homeland Security," *Public Administration Review* 62, Special Issue (September 2002), pp. 126-137

[228] Heyman, David, James Jay Carafano, "DHS 2.0: Rethinking the Department of Homeland Security, joint project of the Center for Strategic and International Studies and the Heritage Foundation, Sep. 18, 2008, pp. 11-14

[229] Donley M.B.; Pollard N.A, "Homeland Security: The Difference between a Vision and a Wish," *Public Administration Review* 62, Special Issue (September 2002), pp. 138-144

[230] 112th Congress, "HR 2017:2012 Consolidated Appropriations Act of 2012," Jan.5, 2011

[231] 112th Congress, "S 365: Budget Control Act," Jan.5, 2011

232 Barsness, Richard W., "The Department of Transportation: Concept and Structure.' The Western Political Quarterly, Vol. 23, No. 3 (Sep., 1970), pp. 500-515

[233] Kingdon, Chapter 8

[234] Government Accountability Office, "High-Risk Series; An Update," January 2009

[235] Heyman, David, James Jay Carafano, "DHS 3.0: Building a National Enterprise to keep America free, safe and prosperous," joint project of the Center for Strategic and International Studies and the Heritage Foundation, Sep. 8, 2008

236 Worthen, Ben, "Watching and Waiting", The Wall Street Journal, April 2, 2012

237 "Securing Cyberspace for the 44th Presidency: Report of the CSIS Commission on Cybersecurity," CSIS, December 2008

[238] 112th Congress, 2nd session, S. 2105"To enhance the security and resiliency of the cyber and communications

infrastructure of the United States," introduced Feb. 14, 2011 (not passed into law)

239 Montalbano, Elizabeth, "DHS to Gain Autonomy under Obama Cybersecurity Plan," Information Week, May 24, 2011, available at http://www.informationweek.com/news/government/state-local/229625515, accessed Jan.8, 2012

[240] Department of Homeland Security, FY 2012 Budget to Congress, February 2011

[241] Jackson, et al, ibid

[242] Burch, James, "A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and their Implications for Homeland Security," Homeland Security Affairs, Volume II, No. 2 (June 2007)

[243] Government Accountability Office, "Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security," Jan. 2010

244 Goldstein, Mark, " Federal Protective Service; Preliminary Results on Efforts to Assess Facility Risks and Oversee Contract Guards," Government Accountability Office, July 24, 2012

245 Government Accountability Office, Combating Terrorism: Determining and Reporting Federal Funding Data, January 2006, available at www.gao.gov/new.items/d06161.pdf

[246] Department Of Defense, Office of the Inspector General, "Security Guard Services Contract at
Naval Weapons Station Earle," January, 2009

[247] Goldstein, ibid

248 Government Accountability Office, "Combating Terrorism: Determining and Reporting Federal Funding Data," January 2006

[249] Department of Defense, Office of Inspector General, ibid

[250] Department of Homeland Security, information on Protective Security Advisors, available at http://www.dhs.gov/protective-security-advisors

251 Lander, Mark, Annie Lowery, "Obama Bid to Cut the Government Tests Congress," The New York Times, Jan. 13, 2012, accessed on Jan. 16, 2012 at http://www.nytimes.com/2012/01/14/us/politics/obama-to-ask-congress-for-power-to-merge-agencies.html

252 Plumer, Brad, "How Obama's Plan for Infrastructure Bank Would Work," The Washington Post, Sep.19, 2011, accessed on January 16, 2012 at http://www.washingtonpost.com/business/economy/how-obamas-plan-for-infrastructure-bank-would-work/2011/09/19/gIQAfDgUgK_story.html