Achieving Greater Homeland Security: Who Should Pay, and How?

Charlotte Kirschner, Alice Levy, Joseph J. Cordes, The George Washington University

Introduction

The terrorist attacks of September 11, 2001 in the United States have broadened the public sector's role in providing "protective goods and services" to include homeland security in addition to national security and public safety (e.g. police and fire protection). Although it is acknowledged that the federal government has a clear responsibility for taking the lead in shaping homeland security policies, the provision of greater homeland security involves significant participation by state and local governments, and the private sector, in addition to the national government.

This paper briefly summarizes why private markets are likely to under-invest in homeland security, leading to a need for public action. It provides an overview of both the range of budgetary and non-budgetary tools used by the United States (U.S.) federal government to "finance" the provision of homeland security, and the budgetary and non-budgetary cost of these federal actions. The paper also identifies and discusses some of the principle challenges faced in ensuring federal homeland security dollars are "well-spent." While the analysis focuses on the United States, the tools of government employed are applicable to all sovereign nations.

Why the Government Should Intervene

The classic "market failure paradigm" provides three broad rationales for public sector involvement in the provision of homeland security. First, increasing homeland security involves financing and providing public goods, whose consumption is non-rival, and also non-excludable. Some of these public goods, such as protection of borders are national in scope; others, such as protection of critical infrastructure, harbors, and "national icons" (such as the Statue of Liberty or the Golden Gate Bridge) provide some benefits that are national in scope, but also have benefits that are clearly concentrated locally and/or regionally.

In addition, 85 percent of the nation's critical infrastructures identified by the U.S. Department of Homeland Security (DHS) are owned by the private sector[1]. While owners of

Charlotte Kirschner is a Ph.D. candidate in the Trachtenberg School of Public Policy and Public Administration at The George Washington University. Ms. Kirschner's concentration is in national security policy and she has focused on homeland security and terrorism.

Alice Levy is a PhD candidate in the Trachtenberg School of Public Policy and Public Administration at The George Washington University. Her field is public budgeting and finance. Ms. Levy's research interests lie in performance budgeting.

Joseph J. Cordes is the director of the Trachtenberg School of Public Policy and Public Administration and Professor of Economics, Public Policy and Public Administration, and International Affairs at The George Washington University. Professor Cordes received his Ph.D. in Economics from the University of Wisconsin, Madison in 1977. From 1989–91 he was Deputy Assistant Director for Tax Analysis at the Congressional Budget Office. He is currently an Associate Scholar, at the Urban Institute. Professor Cordes has co-edited three books and authored or co-authored over sixty articles that have been published in scholarly journals or as chapters in books.

these structures have an incentive to protect their facilities, the cost of an attack to society exceeds the cost to the owner. In such cases, there are external benefits from protecting infrastructure, and private spending on homeland security may be less than socially optimal. There are also other cases, such as airline screening of baggage, where achieving a socially optimal amount of screening requires coordination/cooperation among multiple private parties, which may be more readily achievable with government guidance and intervention than without. In still other cases, private efforts at hardening infrastructure can actually impose negative externalities by shifting terrorist threats elsewhere in society. As in the case of the baggage screening example, such cases may call for public intervention to minimize the adverse effects of such threat-shifting. Thus, the rationale for government intervention in homeland security is premised on the existence of a number of classical economics market failures – public goods, high transaction costs, and externalities.

In addition to classical market failures, the attacks of September 11th have raised the specter of a new and potentially very costly business risk. As in the case of natural hazards, such as floods and hurricanes, private insurance markets face challenges in providing coverage against such risks, and as in the case of natural hazards, the government may have a role to play in either providing some measure of insurance, or in facilitating the emergence of private insurance markets.

The public sector has a range of policy tools at its disposal for attempting to respond to these market failures. Some of these tools are budgetary in nature, such as direct spending and grant programs, and possible tax incentives for private security-related investments. In addition, government has at its disposal non-budgetary tools, such as regulation, which in principle can be used to encourage private parties to make more socially efficient private investments in homeland security measures. Lastly, in the case of insurance market failures, governments can use "implicit budget mechanisms" such as promises to "back-up" private insurance reserves, as a means of supporting insurance markets. While the following paper looks at the tools employed by the U.S. government, homeland security is a public good in all nations and the authors anticipate that the findings of this paper will apply to other situations.

Budgetary Tools: Federal Spending on Homeland Security

We begin with an overview of total federal spending on increasing homeland security. A citizen might think that such outlays are concentrated in the U.S. DHS, which was created to consolidate resources from across the executive branch to transform and realign the efforts of the agencies that have input in securing the nation against terrorism. Even after the creation of the DHS, however, other U.S. Government departments and agencies have a critical role in this process with the result that spending programs are scattered throughout the federal budget in many different agencies. Hence, it is a challenge to provide an overview of how much money is being spent and on what at the federal level.

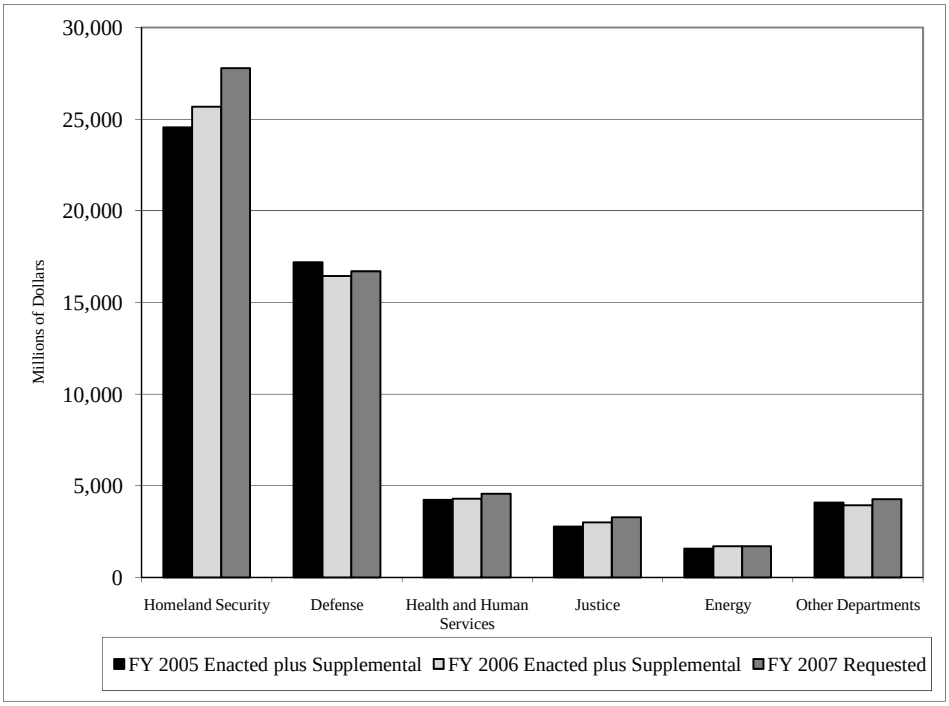
Figure 1 displays the U.S. federal budget appropriations for Fiscal Years 2005 and 2006, along with the President's budget request for Fiscal Year 2007, by the executive level departments that received the budget appropriations. Each year, the DHS has received the most

[1] U.S. Department of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: U.S. Department of Homeland Security, 2003).

funds, followed by the U.S. Department of Defense (DOD). However, it should be noted that the "Other Departments" category entails budget appropriations to 27 different departments, agencies or commissions. In Fiscal Year 2006, total federal appropriations for homeland security total roughly $55 billion.

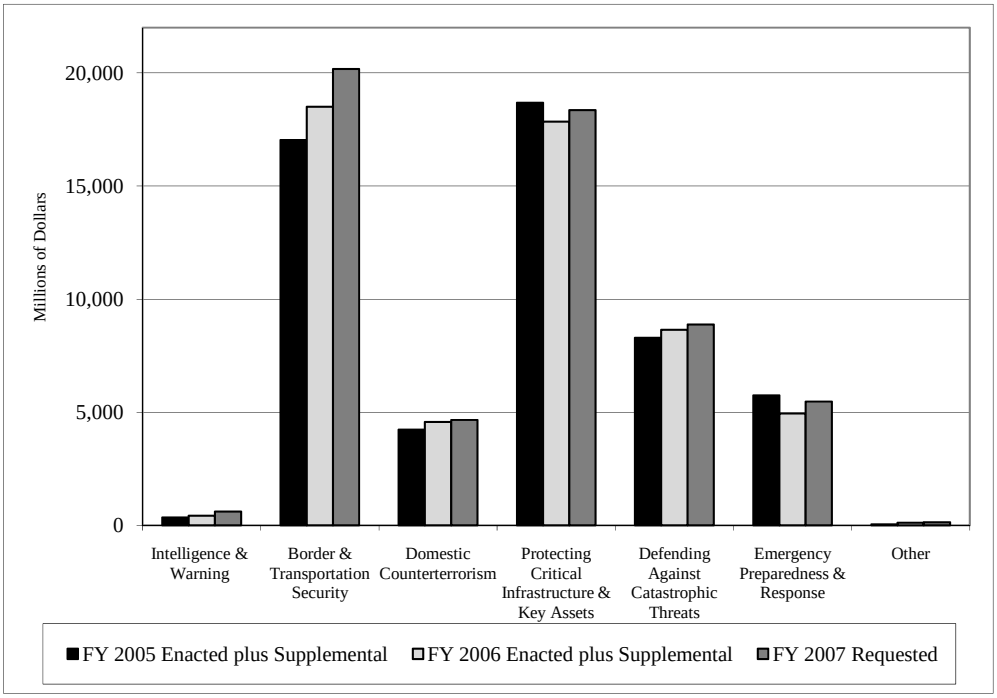
Less than a year after September 11th, the President of the United States released the *National Strategy for Homeland Security* which provides a framework for addressing the challenge of protecting the country while using limited resources efficiently and maintaining a free and open society. The *National Strategy* developed six major mission areas to direct homeland security activities. Figure 2 provides a breakdown of homeland security funding across these major mission areas. In the years since September 11th, the majority of homeland security funding has gone towards border and transportation security, which includes initiatives such as airport screening, security at the nation's ports, and screening of international visitors. Relatively less money has been spent on emergency preparedness and response efforts; however, a large percentage of this money is funneled to state and local governments in the form of grants.

Figure 1: U.S. Homeland Security Spending by Department[2]



[2] U.S. Office of Management and Budget, *Analytic Perspectives: Budget of the United States Government, Fiscal Year 2007* (Washington, DC: U.S. Government Printing Office, 2006).

Figure 2: U.S. Homeland Security Spending by Mission Area[3]



Direct Federal Provision of Homeland Security

In many cases the federal government has opted to manage the provision of security services itself, rather than collaborating with state and local governments. In some cases, the government finances and provides security services using its own agencies, while in others the government pays a third party to engage in the security-enhancing activities. There are also instances where the government provides the service, but finances some or all of it using private sector funds, as is the case with user fees.

Table 1 provides a list of the six homeland security mission areas and which agencies in the federal bureaucracy are participating in the provision of these services. The sections below detail two of the programs that the government has initiated or expanded to increase the United States' security and the costs involved in those programs.

Border and Transportation Security: U.S. VISIT

The United States Visitor and Immigration Status Indicator Technology (U.S. VISIT) is a program designed to enhance security for United States citizens and visitors to the U.S. while promoting legitimate travel across America's borders. U.S. VISIT applies to individuals holding non-immigrant visas traveling to and from the United States. The program involves the collection of biometric information (digital finger prints scans and a digital photograph) from visa applicants before the visa is processed by members of the Bureau of Consular Affairs within the Department of State (DOS). When the visa holder arrives in the U.S. an inkless digital finger

[3] Ibid.

Table 1: Provision of Homeland Security Services by the U.S. Government for Fiscal for FY 2007[4]

Mission Area	Mission	Federal Agencies Providing Services
Intelligence and Warning	Intelligence collection, analysis and distribution	Intelligence Community Office of Intelligence and Analysis Federal Bureau of Investigations National Counterterrorism Center
Border and Transportation Security	Protect border and transportation systems including ports of entry	Customs and Border Protection Transportation Security Administration U.S. Coast Guard Immigration and Customs Enforcement Bureau of Consular Affairs
Domestic Counterterrorism	Identify, thwart and prosecute terrorists in the United States	Federal Bureau of Investigations Immigration and Customs Enforcement
Protecting Critical Infrastructure and Key Assets	Secure nation's critical infrastructure and key assets	U.S. Military National Cyber Security Division Food and Drug Administration
Defending Against Catastrophic Threats	Detect and counter threat of chemical, biological, radiological, and nuclear weapons	National Institutes of Health Directorate of Science and Technology U.S. Northern Command Domestic Nuclear Detection Office
Emergency Preparedness and Response	Prepare for and minimize the damage from major incidents and disasters	Federal Emergency Management Agency Nuclear Emergency Support Team Department of Health and Human Services

scanner is used to capture scans of the individual's finger prints and another digital picture is taken. This information is verified with the individual's travel documents and checked against the Terrorism Watch List. Assuming verification of documents and satisfactory answers to biographic questions, the individual is allowed to enter the country. Originally, the U.S. VISIT program entry procedures collected digital scans from the visitor's two index fingers; however, beginning in November 2007, the DHS began collecting scans from all ten fingers at some U.S. airports[5].

Initially, exit procedures were tested at selected airports and required the visitor to use an exit kiosk, which scanned the visa, the individual's fingerprints and takes a digital photo. This information was verified and the individual was issued an exit receipt. While the intention of the program was that most foreign visitors would be required to check out before leaving the U.S., evidence from the pilot program revealed low traveler compliance. Therefore, on May 6, 2007,

[4] Ibid.
[5] U.S. Department of Homeland Security, "US-VISIT: How It Works," July 26, 2008, http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm.

the DHS suspended the exit kiosk pilot program and is now exploring integrating biometric exit procedures into the existing international visitor departure process[6].

While the U.S.VISIT program is intended to increase security and allow better monitoring of non-immigrants while they are traveling in the U.S., it also imposes a variety of costs. These costs include the costs of equipping all ports of entry with the necessary technology; creating a secure database; personnel costs; and the effects of fewer non-immigrants coming to the U.S., either as tourists or as students. In order for the U.S. VISIT program to function as intended each entry and exit port will need to be equipped with the appropriate numbers of digital cameras, fingerprint scanners, and other necessary supplies. Additionally, costs attributed to the design, development, and maintenance of a secure database that is capable of interacting with many government agencies will be included in the initial costs of the program. Finally, to ensure proper functioning of the program, the DOS and the U.S. Customs and Border Protection Agency within the DHS will need additional staff to review documentation during visa issuance, populate the database with necessary information, and to process individuals entering and exiting the United States. The Department of Homeland Security Appropriations Act of 2006 (P.L. 109-90) allocates $340 million for the development of the U.S. VISIT program[7].

The President's fiscal year 2007 budget request included $60 million for the DHS to increase the number of digital finger prints collected from two to ten and for improved interoperability with the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS); $71 million for the FBI to upgrade IAFIS and $10 million for the DOS to initiate the implementation of the new security measures[8].

Border and Transportation Security: Screening at U.S. Airports

In an effort to address the public fear of flying resulting from the September 11th attacks, just two months later, the U.S. Congress passed the Aviation and Transportation Security Act of 2001 (ATSA). This act created the Transportation and Security Administration (TSA) and federalized the workforce that conducts passenger and baggage screening in the nation's airports. However, section 108 of the ATSA also required the TSA to establish pilot programs at not more than five airports where private companies under federal oversight could conduct screening operations. Since November 19, 2004 all airports have been allowed to apply to the TSA to allow the airport to contract out for security services, but currently, only eleven airports are operating under contract, while the rest of the country has maintained the use of federal screeners[9].

Although not as common as some of the other tools, user fees have been assessed to help finance the costs of additional airline security. The Aviation and Transportation Security Act assesses passengers a fee of $2.50 - $5.00 per one-way ticket originating in the United States. This fee, known as the September 11th Security Fee requires airline passengers to share the cost of additional security without burdening citizens who refrain from air travel. Based on fee collections beginning on February 1, 2002 it is estimated that fees collected at the statutory

[6] U.S. Department of Homeland Security, "US-VISIT Moves Out of Biometric Exit Pilot Phase," July 26, 2008, http://www.dhs.gov/xnews/releases/pr_1178549052332.shtm.
[7] U.S. Department of Homeland Security Appropriations Act of 2006, Pub. L. No. 109-90. 119 STAT. 2066.
[8] U.S. Office of Management and Budget, *Analytic Perspectives: Budget of the United States Government, Fiscal Year 2007* (Washington, DC: U.S. Government Printing Office, 2006), p. 24.
[9] Transportation and Security Administration, "Screening Partnership Program: Frequently Asked Questions – Program," July 26, 2008, http://www.tsa.gov/what_we_do/optout/spp_faqs.shtm.

maximum would raise less than $1 billion in Fiscal Year 2002. The yield would be slightly larger in future fiscal years, but would still not cover all of TSA's costs for airport security screening[10]. These costs include, among other things: 1) the salary, benefits and overtime of screening personnel, managers, and federal law enforcement personnel stationed at airport screening locations; 2) the costs of training the above personnel and purchasing, operating and maintaining the equipment used by personnel; 3) the costs of the Federal Air Marshals program; and, 4) the costs of performing background investigations on personnel[11].

Recognizing that the September 11th Security Fee will not cover the TSA's screening costs, the Aviation and Transportation Security Act allows the TSA to impose a fee on domestic and foreign air carriers to cover the shortfall. According to the ATSA, the amount of the fee charged each year by the TSA may not exceed the aggregate amount that air carriers paid for screening passengers and their baggage in calendar year 2000. For the months up to and including September 2004, each air carrier must pay 8.333 percent of the total amount of their costs for screening passengers and property in calendar year 2000[12]. According to an April 2005 U.S. Government Accountability Office (GAO) report, these fees are not recouping enough of the TSA's costs of providing aviation security. The TSA's Fiscal Year 2004 appropriations for airport screening activities were $3.1 billion. However, the TSA only collected about $1.8 billion for passenger security fees and $319 million in airline security fees, resulting in the government funding nearly $1.6 billion out of general revenues. GAO has recommended that the TSA consider these estimates in their study in determining the limitation on the aggregate air carrier fees[13].

Issues and Challenges in Direct Provision of Homeland Security

Leman discusses some of the issues and challenges that can arise in the direct provision of government services[14]. He notes that historically direct government provision has tended to be inefficient when compared with alternative financing strategies, but that reforms undertaken during the 1990's have started to change this situation. Leman likens direct provision to "*The Sorcerer's Apprentice,"* noting that bureaucracies are very difficult to disband and that excessive devotion to the mission can cause "the tool [to] become an end in itself"[15]. Actions taken since September 11th have created a new bureaucracy, the Department of Homeland Security, which will likely create and retain its own constituency. While the need for increased security is currently high, if the Department retains its programs and funding during less secure times, Leman's concerns may prove highly perceptive regarding the direct provision of government services.

[10] "Aviation Security Infrastructure Fees and Assumption of Civil Aviation Security Functions and Responsibilities; Interim Final Rule and Notice," *Federal Register* 67:34 (February 20, 2002), p. 7927.
[11] Ibid, p. 7926-7927.
[12] "Notice of Resumption of the September 11th Security Fee and the Aviation Security Infrastructure Fee Following Temporary Suspension," *Federal Registrar* 68:188 (September 29, 2003), p. 55985.
[13] Government Accountability Office, *Aviation Fees: Review of Air Carriers' Year 2000 Passenger and Property Screening Costs* (Washington, DC: Government Accountability Office, 2005).
[14] Leman, Christopher, "Direct Government" In *The Tools of Government: A Guide to the New Governance*, edited by Lester M. Salamon, p. 48-79 (Oxford: Oxford University Press, 2002).
[15] Ibid, p. 74.

Grants to Secure the Nation's Homeland

Since September 11th, federal, state, and local governments have taken steps to prevent and prepare for the next terrorist attack. It is generally accepted that state and local public safety personnel - law enforcement, fire, Emergency Medical Services (EMS), and hospitals - will be the first to respond to a terrorist attack. These organizations, along with private security firms, are on the front lines for protecting America's homeland. Therefore, the federal government has provided funding to enhance the capabilities of these state, local, and private organizations through a variety of grant programs. The federal government is willing to subsidize expenditures for prevention and preparedness to encourage an integrated approach, bringing resources from all levels of government. As evident by the response to Hurricane Katrina, preparedness failures affect people across many jurisdictions creating a need for federal aid to compensate for this potential externality. However, the intent of the federal government is for these grants to be a short-term investment in capital and to build response capabilities[16]. Between 2001 and 2007, the DHS, the Department of Health and Human Services (HHS), and the Department of Justice (DOJ) have allocated $16 billion in grants to fund state and local preparedness efforts[17]. Table 2 provides funding information for many of the emergency preparedness grants offered from the DHS and other executive branch departments.

The Fiscal Year 2006 grant cycle is the first in which the Interim National Preparedness Goal has been in place to outline America's national priorities and to concentrate expenditures on enhancing capabilities. This common planning structure allows the nation to define targeted levels of performance and measure progress towards these goals[18]. The Interim National Preparedness Goal, along with the National Response Plan, published in December 2004, provided state and local grant recipients the guidance they have sought since the first round of homeland security grants were appropriated[19]. Prior to the release of these documents, there was no clear strategic guidance from the federal level about terrorism preparedness objectives, and many grant recipients report that they were unsure how to best spend the grant dollars they received which caused miscommunication between state and local governments about what capabilities needed to be funded[20].

Grants Offered through the Department of Homeland Security

The U.S. government provided financial assistance for terrorism preparedness prior to September 11th, in fact, the Office of Domestic Preparedness (ODP) was established in 1998 to help state and local officials enhance their ability to respond to chemical or biological terrorism. In Fiscal Year 1999, the ODP provided a total of $85.5 million in grant monies to all fifty states, and 157 of the nation's most populated cities and counties[21]. After September 11th, the amount of

[16] Gramlich, John, "Anti-Terror Funds to States are Shrinking", *Stateline.org*, July 19, 2007.
[17] U.S. Office of Management and Budget, *Analytic Perspectives: Budget of the United States Government, Fiscal Year 2008* (Washington, DC: U.S. Government Printing Office, 2007) p. 30.
[18] U.S. Department of Homeland Security, *Interim National Preparedness Goal Homeland Security Presidential Directive 8: National Preparedness* (Washington, DC: U.S. Department of Homeland Security, 2007) p. 1.
[19] In September 2007 the National Preparedness Goal was re-released and renamed the National Response Guidelines. Likewise, in January 2008 the DHS replaced the National Response Plan with the National Response Framework.
[20] "An Analysis of First Responder Grant Funding," (Washington, DC: House Select Committee on Homeland Security, 2004).
[21] U.S. Federal Emergency Management Agency, "Program Information," November 19, 2005, http://www.ojp.usdoj.gov/odp/grants_programs.htm.

money flowing to the states increased dramatically. In Fiscal Year 2004, over $3.7 billion was awarded across the many grant programs provided by the ODP[22].

The Homeland Security Grant Program (HSPG) consolidates five grant programs from previous years and is perhaps the single largest grant program available for emergency preparedness activities. It provides funding for organization, planning, training, exercises, equipment, and management and administration to prevent, protect against, respond to, and recover from hazards including terrorist attacks and major disasters[23]. The Fiscal Year 2006 grant program is the first real push to begin allocating federal money to the states based on risk and need in an effort to create a high return on investment[24]. Base allocations are still available to states under the State Homeland Security Program and the Law Enforcement Terrorism Prevention Program, with the remainder of those funds allocated based on risk. However, the Urban Area Security Initiative grants are awarded based solely on risk and need. The Metropolitan Medical Response System and the Citizen Corps Program remain allocated based on the Fiscal Year 2005 formula[25]. Other grant programs managed by the DHS focus on securing critical infrastructure like transit systems and ports. Some of these programs allocate funds based on a formula, and others are allocated based on risk or need.

The HSGP, along with many other grants managed by the DHS require the State Administrative Agency to apply for and coordinate the grant monies provided by the federal government. States must then obligate or pass through 80% of the funds they receive under formula grants for use by localities. Although Fiscal Year 2006 is the first year that the federal government has allocated grants based on risk and need, some states report having incorporated some threat, risk, or vulnerability factors into their funding formulas for their Fiscal Year 2003 allocations[26]. According to a report completed by the Staff of the House Select Committee on Homeland Security, 22 states allocated grant money to their local governments based on some consideration of risk or threat, and 25 states made allocations based on some consideration of achieving capabilities or fulfilling needs[27].

Grants Offered Outside of the Department of Homeland Security

Management of some aspects of preparedness remains outside of the DHS, since the grants are better administered in the department most familiar with the specific area of expertise. The HHS makes grants available from/to hospitals and healthcare systems to provide care to victims of terrorism or other public health emergencies. These tasks include increasing surge capacity, decontamination capacity and isolation capacity. Additional grants provide support to health care educational facilities to prepare a workforce of healthcare professionals to address emergency preparedness and response issues[28]. In an effort to coordinate the management of these funding streams with those offered by the DHS, a Federal Preparedness Grant Program

---

[22] Ibid.
[23] U.S. Department of Homeland Security, "FY 2006 Homeland Security Grant Program: Program Guidelines and Application Kit" (Washington, DC: U.S. Department of Homeland Security, 2005) p. ii.
[24] Ibid, p. 1.
[25] Ibid, p. 52.
[26] "An Analysis of First Responder Grant Funding," (Washington, DC: House Select Committee on Homeland Security, 2004).
[27] Ibid.
[28] U.S. Department of Homeland Security, *FY 2006 Homeland Security Grant Program: Program Guidelines and Application Kit* (Washington, DC: U.S. Department of Homeland Security, 2005) 17-18.

Table 2: Funds Obligated by the U.S. Government to Preparedness Grant Programs[29] (in millions of dollars)

Program	FY2006	FY 2005	FY 2004
Urban Area Security Initiative	734.6	854.7	671.1[1]
Law Enforcement Terrorism Prevention Program	400.0[2]	386.3	497.1
State Homeland Security Program	544.0	1,062.3	1,669.4
Citizen Corps Program	19.8	13.5	39.8
Metropolitan Medical Response System Program	29.7	22.3	50.0
Emergency Management Performance Grant Program	170.0	178.9	178.3
Assistance to Firefighters Grant Program	524.4	633.5	684.3[3]
Buffer Zone Protection Program	50.0	92.0	0.0[4]
Transit Security Grant Program/Intercity Passenger Rail Security Grant Program	148.5	150.0	49.0[1]
Port Security Grant Program	173.0	150.0	179.0
Intercity Bus Security Grant Program	10.0	10.0	10.0
National Bioterrorism Hospital Preparedness Program	458.0	466.0	497.0
Bioterrorism Training and Curriculum Development Program	26.0	26.0	26.6
Public Health Emergency Preparedness Cooperative Agreement	n/a	862.8[5]	849.6[5]
FEMA Pre-disaster Mitigation Grants	n/a	282.6	212.0
FEMA Flood Mitigation Grants	28.0	20.0	n/a
FEMA Hazard Mitigation Grants	n/a	184.5	n/a
Edward Byrne Memorial Justice Assistance Grant Program	416.5[6]	634.0[6]	474.9
Homeland Security Agricultural Grant	28.8	8.6	7.6
Hazardous Materials Emergency Preparedness Grant Program	n/a	n/a	12.8[7]

[1] The CFDA does not provide FY 2004 data for these two programs. According to the Department of Homeland Security's Office of Grants and Training, the FY 2004 Urban Areas Security Imitative funds included $671 million to enhance the security of key urban areas and $49 million to protect critical mass transit systems with heavy rail and commuter rail components.

[2] The CFDA estimate for the FY 2006 obligation for the Law Enforcement Terrorism Prevention Program was not yet available. The Department of Homeland Security Appropriations Act, 2006 (P.L. 109 - 90) appropriated $400.0 million to this grant program.

[3] CFDA does not provide FY 2004 data for this program. However, the Assistance to Firefighters Grant Program's website reports that $684.3 million was allocated in FY 2004.

[4] The Buffer Zone Protection Program was initiated in FY 2005.

[5] The CFDA does not provide information regarding the current Public Health Emergency Preparedness Cooperative Agreement. The Center for Disease Control's website reports that $849.6 and $862.8 million were allocated to this program in FY 2004 and FY 2005 respectively.

[6] The CFDA estimate for the FY 2005 and FY 2006 obligation for the Edward Byrne Memorial Justice Assistance Grant Program were not yet available. The Consolidated Appropriations Act of 2005 (P.L. 108-447) and the Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006 (P.L. 109 - 108) appropriated $634.0 and $416.5 million, respectively to this grant program.

[7] Information regarding the Hazardous Materials Emergency Preparedness Grant Program was not located within the CFDA database. However, the grant program's website reported that $12.8 million was allocated in FY 2004.

[29] Data compiled using the Catalogue of Federal Domestic Assistance (CFDA) website. Retrieved April 18, 2006, from http://12.46.245.173/cfda/cfda.html.

Steering Committee was formed by DHS and HHS to strengthen each agencies respective grant programs while maintaining the focus of each program[30]. Preparedness grants are also offered through the DOJ, the Department of Agriculture (DOA), and the Department of Transportation (DOT). Most of these grants are allocated based on formulas; however, the Fiscal Year 2005 program guidance for both the National Bioterrorism Hospital Preparedness Program and the Public Health Emergency Preparedness Cooperative Agreement report that they envision the Fiscal Year 2006 allocations to be based on risk[31,32].

Structure of Grants to Secure the Nation's Homeland

Overall, the form of and requirements for these federal grants vary considerably. Table 3 provides detailed information on this variety for each of the analyzed grant programs during Fiscal Years 2005 and 2006. Most of the grants are block grants allowing states flexibility in the types of programs it supports. However, the grants are often categorical and have narrowly defined purposes. In the Program Guidance for the HSGP, the DHS specifies a set of allowable costs for many of the grant programs including some administered outside of the DHS. Matching requirements also vary by grant program. In the majority of cases, matching is not required; however, some grant programs like the Emergency Management Performance Grant Program and the Assistance to Firefighters Grant Program require the grantee to match the funds provided by the federal government. Almost all of the grant programs examined mandate that federal funds only supplement existing funds rather than replace them. Some programs require a certification to this extent a few like the Assistance to Firefighters Grant Program and the Hazardous Materials Emergency Preparedness Grant Program require that grantees maintain spending levels at a rate at least equal to an average of the prior two years spending.

One issue that has been raised about the federal homeland security grants is whether funds are allocated on the basis of terrorism risk. In a study done by the RAND Center for Terrorism Risk Management Policy, Willis, Morral, Kelly, and Medby estimate the risk factors associated with the urban areas that received Urban Area Security Initiative funding in Fiscal Year 2004 and compared the shares of funding with the shares of risk each city faced. The authors find that risk shares vary much more widely than funding shares, suggesting that if risk is to be the basis for grant allocation, some urban areas are under-funded, while others may be over-funded[33]. Although it is possible that these results reflect the fact that aggregated estimates of risk-shares have a wider variance than shares based on both population or density-weighted population, the authors note that these results suggest that even the small portion of grants that are said to be allocated on the basis of risk in 2004, may be only marginally so, and that considerations other than risk determined funding allocations. Since the U.S. is a democracy funding patterns that correspond to electoral advantage as opposed to risk may be inevitable, but this finding suggests a need to account for political structure when evaluating homeland security funding.

---

[30] Ibid, p. 21.

[31] U.S. Health Resources and Service Administration, *National Bioterrorism Hospital Preparedness Program: Fiscal Year 2005 Continuation Guidance* (Washington DC: U.S. Health Resources and Services Administration, 2005).

[32] Centers for Disease Control and Prevention, *Cooperative Agreement Guidance for Public Health Emergency Preparedness: Program Announcement AA154* (Washington, DC: Centers for Disease Control and Prevention, 2005).

[33] Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Meadby. *Estimating Terrorism Risk* (Santa Monica, CA: RAND Corporation 2005) p. 62.

Table 3: Grant Structures of Emergency Preparedness Grants during Fiscal Years 2005 and 2006[34]

Program	Eligibility	Funds Awarded	Matching Requirements	Maintenance of Effort
Urban Area Security Initiative	Designated urban areas	Risk and need	No match	Non-supplanting certification
Law Enforcement Terrorism Prevention Program	States, DC and territories	Base allocation, then risk and need	No match	Non-supplanting certification
State Homeland Security Program	States, DC and territories	Base allocation, then risk and need	No match	Non-supplanting certification
Citizen Corps Program	States, DC and territories	Formula	No match	Non-supplanting certification
Metropolitan Medical Response System Program (MMRSP)	Designated MMRSP jurisdictions	Formula	No match	Non-supplanting certification
Emergency Management Performance Grant Program	States, DC and territories	Formula	Matching = 50%	Non-supplanting certification
Assistance to Firefighters Grant Program	Fire Departments & non-affiliated EMS working in states and territories	Competitive with demographic restrictions	Matching = percentage based on population served	Maintain operating expenditures at level equal to average over last two years
Buffer Zone Protection Program	Designated critical infrastructure/key resource sites (State must apply)	Base allocation, then risk and need	No match	Non-supplanting certification
Transit Security Grant Program	Designated transit systems (States must apply)	Formula - risk assessment required in grant application	No match	Non-supplanting certification
Port Security Grant Program	Eligible ports	Risk	Matching = 50% for private sector only	Non-supplanting certification
Intercity Bus Security Grant Program	Owners/operators of fixed route, intercity bus services	Competitive	No match	Non-supplanting certification
Intercity Passenger Rail Security Grant Program	Amtrak is the only eligible grantee for FY 2005	Funding directly to Amtrak	No match	Non-supplanting certification
National Bioterrorism Hospital Preparedness Program	States, DC and territories along with three largest municipalities	Formula, but beginning in FY 06 program envisioned to include risk	No match	Not specified
Bioterrorism Training and Curriculum Development Program	Nonprofit accredited health professions schools and other educational entities	Competitive	No match	Not specified
Public Health Emergency Preparedness Cooperative Agreement	States, DC and territories	Formula, but beginning in FY 06 program envisioned to include risk	No match	Non-supplanting statement in guidance, no certification required
FEMA Mitigation Grants	States, DC and territories	Competitive	Matching = 25%	Not specified
Edward Byrne Memorial Justice Assistance Grant Program	States, DC and territories	Formula	Matching = 25%	Non-supplanting statement in guidance, no certification required
Homeland Security Agricultural Grant Program	Any entity that may further research or educational in food and agricultural sciences	Competitive	No match	Not specified
Hazardous Materials Emergency Preparedness Grant Program	States, DC and territories	Formula	Matching = 20%	Maintain operating expenditures at level equal to average over last two years

[34] The data on the structure of the grants was compiled from program guidance and application kits, the Catalogue of Federal Domestic Assistance and documentation from the program's website.

Despite RAND's findings, according to the U.S. Office of Management and Budget (OMB), since Fiscal Year 2006, over half of the homeland security grant funding is based on risk and need[35]. The DHS determined a formula for the FY 2006 HSGP grants that contains two complementary risk calculations. Asset-based risk focuses on the assets within a jurisdiction that might be susceptible to a terrorist attack. For example, nuclear power plants, theme parks, mass transit systems, and national monuments and icons are some of the assets that increase a jurisdiction's risk of terrorist attack. Geographically-based risk ascribes risk to jurisdictions based on unique characteristics that are not attributable to a specific asset. Jurisdictions with military bases or high population density are examples of places with high geographically-based risk. Likewise, need is determined based on a state's Program and Capability Enhancement Plan and its' Investment Justifications which are required parts of the grant application process[36].

Another issue is the classic public finance question of whether intergovernmental grants actually stimulate greater spending on the designated activity by the recipient. There is limited evidence regarding the effectiveness of these grant programs and their impact on state and local spending on preparedness. In 2004 the National Association of Counties released survey results that indicated that as a result of intergovernmental funding and planning, 75 percent of surveyed counties felt they were better prepared to respond to the terrorist threat. While the survey found that 40 percent of the counties had appropriated their own funds to assist with homeland security, it also showed that 54 percent of the counties had not used any of their own funds to increase homeland security[37]. Because shared fiscal responsibility is an important condition of successful federalism, research should look into whether federal funds have stimulated or displaced state and local level efforts at securing the United States.

Issues and Challenges in Using Intergovernmental Grants

Beam and Conlan note that grants in general are prone to "goal displacement," duplication of efforts, and "leakages of funds"[38]. Because grants require recipients to execute the policy, the goals of the donor government must, to some extent, be supplanted by recipient governments. In addition, because recipient governments have multiple funding sources, it is possible for them to use the grant moneys to displace current spending and use their previous funding sources for purposes other than those for which the grants were originally intended. When multiple grants are aimed at achieving the same objective, such displacement may be easier and will also result in decreased efficiency with respect to achieving social objectives. In the case of grants for homeland security, Table 2 indicates the number of different programs aimed at achieving the similar objectives, while Table 3 shows that most grant programs have relatively few controls to ensure that granted moneys are used to augment and not replace state and local spending. Thus, the current grant structures may be achieving relatively small increases in funding for homeland security at a relatively high price.

---

[35] U.S. Office of Management and Budget, "*Budget of the United States Government, Fiscal Year 2007: Department of Homeland Security*" March 2, 2006, http://www.whitehouse.gov/omb/budget/fy2007/dhs.html.

[36] U.S. Department of Homeland Security, "FY 2006 Homeland Security Grant Program: Program Guidelines and Application Kit" (Washington, DC: U.S. Department of Homeland Security, 2005) p. 53.

[37] U.S. Office of Management and Budget, *Analytic Perspectives: Budget of the United States Government, Fiscal Year 2008* (Washington, DC: U.S. Government Printing Office, 2007) p. 30.

[38] Beam, David R., and Timothy J. Conlan. "Grants" In *The Tools of Government: A Guide to the New Governance*, edited by Lester M. Salamon, p. 340-380. (Oxford: Oxford University Press, 2002) p. 371-372.

Regulation and Homeland Security

In addition to the budgetary tools described in the previous sections, the federal government can also make use of its regulatory powers to require actors in the private sector to take certain actions that are designed to enhance security. Table 4 lists the critical infrastructures (as defined in the "National Strategy for the Physical Protection of Critical Infrastructure and Key Assets") and the organizations that are responsible for regulation. This table illustrates the myriad of actors involved in regulating private behaviors in the U.S.

Estimating the cost of mandating increased homeland security by means of government regulation is difficult because much of the nation's critical infrastructure has been regulated since long before September 11th. Thus, the cost of using government regulation to increase homeland security is the *added* regulatory cost associated with tightening and/or augmenting existing regulations in the aftermath of the terrorist attacks.

Table 4 indicates the breadth of areas of homeland security governed by regulations and the large number of public and private regulatory bodies involved in the regulatory process, all of which create a highly complex system. Because it is difficult to obtain information about the effects and costs of all the regulations summarized in Table 4, the case of nuclear power is examined as an example.

Nuclear Power Plant Regulation: What and How Much?

The Nuclear Regulatory Commission (NRC) was established in 1974 and has primary jurisdiction over the regulation of nuclear power plants. Even prior to September 11th the potential costs resulting from a nuclear accident were seen to be sufficiently large to warrant government regulation. Although the risk of such an accident is quite small, the costs to society are high enough that reliance on the market alone may generate insufficient levels of security, especially due to the high negative externalities associated with a nuclear meltdown. According to a 1982 report prepared by Sandia National Laboratories for the NRC, the probability of a severe accidental release may be in the range of 1 in 10,000 to 1 in 100,000 but could result in the deaths of over 100,000 people, injuries to over 100,000 people, and costs exceeding $100 - 300 billion[39]. After September 11th, the probability of such a nuclear event occurring has increased due to the possibility of terrorist attacks.

Nuclear regulations are extremely complex and numerous. The following paragraphs describe some of the major types of nuclear power plant regulations enforced by the NRC. For each type of reactor, the NRC publishes Standard Technical Specifications (STS) that plants are required to comply with, such as concrete structures to protect reactor cores. Specifications are continuously being updated and plants are encouraged to upgrade their technology accordingly[40]. In addition to the STS's, plants are required to be equipped with several safety systems such as emergency core cooling systems[41] and the NRC regulates the power level at which each plant can operate[42].

[39] Sandia. *Technical Guidance for Siting Criteria Development.* (Albuquerque, New Mexico: Sandia National Laboratories, 1982).
[40] NRC. *Technical Specifications*. (Washington, DC: U.S. Nuclear Regulatory Commission, 2006).
[41] NRC. *PWR Sump Performance*. (Washington, DC: U.S. Nuclear Regulatory Commission, 2006).
[42] NRC. *Power Updates*. (Washington, DC: U.S. Nuclear Regulatory Commission, 2006).

Table 4: Critical Infrastructures and Regulatory Bodies[43]

Infrastructure	Regulatory Bodies
Agriculture and Food	DHS, HHS Food and Drug Administration (FDA), U.S. Department of Agriculture (USDA)
Water	DHS, Environmental Protection Agency (EPA), state and local governments, water ISAC*
Public Health	DHS, HHS, state and local governments, private health facilities
Emergency Services	DHS, DOJ, state and local governments
Defense Industrial Base	DHS, DOD
Telecommunications	DHS, U.S. Department of Energy (DOE), President's National Security Advisory Committee and Critical Infrastructure Protection Board, Government Network Security Information Exchanges, telecommunications ISAC
Energy	DHS, DOE, North American Electric Reliability Council, Federal Energy Regulatory Commission, Nuclear Regulatory Commission, state and local governments, electricity ISAC
Transportation	DHS, DOT, state and local governments, surface transportation ISAC, port authorities, Coast Guard, Customs, local transit authorities
Banking and Finance	DHS, Treasury, Federal Reserve, Securities and Exchange Commission, Federal Banking Information Infrastructure Committee, state governments, financial services ISAC
Chemical Industry and Hazardous Materials	DHS, EPA, state and local governments, private sector trade associations
Postal and Shipping	DHS, U.S Postal Service (USPS)

*ISAC's are Information Sharing and Analysis Centers, associations of organizations in the private sector

Licensees (the owners of nuclear power plants) are required to monitor their maintenance efforts to ensure that safety components are functioning, non-safety related activities will not impede safety procedures, and failures resulting in the need to engage in safety-related activities are minimized[44]. In addition to licensee activity, the NRC has its own Reactor Oversight Process that measures plant performance in the areas of reactor safety, radiation safety, and security. The NRC's seven cornerstones for safety include initiating events, mitigating systems, barrier integrity, emergency preparedness, occupational radiation safety, public radiation safety, and physical protection[45]. Finally, the NRC establishes regulations for emergency plans and the types of threats operators must protect against and requires background checks of all operators[46]. Regulations are enforced through an oversight and licensing process. In addition to the regulation

[43] U.S. Department of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: U.S. Department of Homeland Security, 2003).
[44] NRC. *Operating Reactor Maintenance Efforts*. (Washington, DC: U.S. Nuclear Regulatory Commission, 2006).
[45] NRC. *Multiple/ Repetitive Degraded Cornerstone Column*. (Washington, DC: U.S. Nuclear Regulatory Commission, 2006).
[46] CBO, *Homeland Security and the Private Sector*. (Washington, DC: Congressional Budget Office, 2004).

of nuclear power plants, other regulations exist in the nuclear sector to address the long-term storage of spent fuel and the potential consequences of accidents, but those regulations are outside the scope of this discussion.

As is well-known from the case of other government regulations, although there are budgetary costs of adopting regulatory standards – overseeing private actors, and enforcing regulatory policies – these costs generally represent only a small portion of the total costs of regulation. The lion's share of the costs generally falls on private individuals and firms who must bear the costs of complying with the regulations.

In the case of nuclear power plant regulation, the most obvious costs of these regulations are the costs of the NRC, which totaled $670 million in 2005. Of these, 10 percent or $67 million was funded through the budget, while the remaining $603 million was financed through fees and fines assessed to license holders and applicants. While these costs are initially born by the plant operators and investors, they are then passed on to electricity consumers through the rate base. Thus, the consumers of the power finance 90 percent of the costs of the NRC[47].

In addition to the costs of the NRC, nuclear power regulations impose compliance costs on the private sector. One of the difficulties in measuring these costs is that in the case of nuclear power plants, distinguishing between an operating or maintenance cost and a safety-related cost is practically impossible. James Joosten at the Energy Information Administration (EIA) suggests using two-thirds of the operating and maintenance costs as a rough estimate of the costs of compliance[48]. Because this represents a very rough estimate, the following numbers should be interpreted with some caution.

The Nuclear Energy Institute (NEI) estimates that the average yearly operating and maintenance costs for 2004 were 1.26 cents/kWh and applying the two-thirds rule, this gives us 0.84 cents/kWh for compliance with nuclear safety regulations[49]. In 2004, the NEI estimates that the U.S. produced 788.6 million MWh of nuclear energy[50] which means the costs of security related-activities were approximately $6.62 billion, almost 10 times higher than the costs of the NRC, and almost 100 times higher than the costs born by taxpayers. As is the case with licensing and application fees, nuclear plants then pass this cost on to ratepayers in their electrical service areas. What is significant about these costs is that they illustrate that regulatory costs are like an iceberg. The budgetary costs are like the exposed part of the iceberg, and represent only a tiny fraction of the true costs of the regulation; estimating the much larger hidden costs is almost impossible to do by examining the costs from the surface. Budgeting for regulation is thus, much more difficult than budgeting for direct expenditures or grants due to the environment of uncertainty.

Incremental Cost of Regulatory Changes Enacted in Response to 9/11

[47] J. Joosten, Energy Information Administration, personal communication, January 27, 2005.

[48] The rationale behind the two-thirds measure is that about 50% of plant components are related to the nuclear island, but the number needs to be adjusted upwards to reflect the fact that nuclear plant parts cost 3 to 10 times more money when used in a safety-related application (J. Joosten, Energy Information Administration, personal communication, January 27, 2005).

[49] NEI, "*U.S. nuclear non-fuel operating and maintenance costs 1981 – 2004"* March 5, 2006, http://www.nei.org/documents/U.S._Nuclear_Industry_Non-Fuel_OM_Costs.pdf.

[50] NEI. "*Top ten nuclear generating countries 2004"* March 5, 2006, http://www.nei.org/documents/top_10_nuclear_generating_countries.pdf.

Although the NRC has been continuously updating regulations for some time, the NEI suggests that both public and private security measures have increased since September 11th. Among the changes are: an increase in the number of security personnel and the training they are required to have; a strengthening of plant perimeters, such as new protections against vehicle bombs; and additional surveillance equipment. The NEI estimates that these changes have cost $1.2 billion[51], representing an increase in the costs of approximately 10 percent.

Issues and Challenges in Government Regulation as a Policy Tool

Governments often find regulation to be an attractive policy instrument, and a Congressional Budget Office (CBO)[52] report notes that there are a number of ways in which existing federal regulations could be modified to improve the security of the nation's private infrastructure. Nonetheless, as May[53] notes challenges abound in both the design and implementation of regulations, particularly when attempting to determine the socially optimal levels of risk and enforcement severity. May concludes that "regulations that address first-order, visible, and concentrated harms" are the easiest to manage, while indirect and diffuse harms are more difficult. In the case of nuclear regulation, the threat is highly diffuse and the uncertainty great, suggesting that identifying the socially optimal level of risk may not be possible. This difficulty is compounded in a world in which the threat of a terrorist attack is an additional risk factor; especially since unlike natural and physical hazards, threats involving human behavior can react in response to changes in regulatory policies aimed at lowering threats of attack.

Providing Insurance

Unlike some of the other policies discussed above, facilitating the provision of insurance does not protect homeland security by preventing an attack or mitigating the risks associated with one. Rather, it serves to prevent negative consequences arising from the fear of an attack by spreading the potential financial costs. Providing insurance to private parties enhances economic well-being by allowing private actors to mitigate the potentially devastating economic effects of individual catastrophic terrorist incidents. The ability to insure against the consequences of terrorist attacks is useful *ex-ante* because it helps individuals and business plan for the future, and *ex-post* because it spreads large concentrated losses among a broader population. A potential issue, however, is that, if insurance premiums are set lower than would be warranted based on true actuarial risks, by subsidizing risk, the government may move business activity into sectors and regions that have higher than average risks, and encourage more risk-taking than is socially desirable. Since the relationship between risk and business activity is highly endogenous (terrorists preferring more populated, thriving areas all else equal) assessing the extent of this second consequence is methodologically challenging. The most prominent use of insurance in response to the September 11th terrorist attacks is the Terrorism Risk Insurance Act of 2002 (TRIA).

[51] NEI, *Post-Sept. 11 Security Enhancements: More Personnel, Patrols, Equipment, Barriers*. (Nuclear Energy Institute, 2006).
[52] CBO, *Homeland Security and the Private Sector*. (Washington, DC: Congressional Budget Office, 2004).
[53] May, Peter, "Social Regulation" In *The Tools of Government: A Guide to the New Governance*, edited by Lester M. Salamon, p.156 - 186 (Oxford: Oxford University Press, 2002).

TRIA: What and Why?

Insurance against terrorist attacks was provided in the private sector prior to September 11th, and as a result of the attacks privately insured losses were $30 - $35 billion. Insurers total underwriting losses for 2001 reached $52.6 billion. Investment income proved inadequate to cover these losses, leading to a decrease in industry net worth of $27.8 billion[54]. These drastic losses resulted in a reluctance to continue to offer insurance in the private sector. The collapse of a private market for terrorism insurance provoked concerns about further economic consequences, such as excess risk to property owners, reduced economic activity, and a decline in commercial construction[55]. The concerns about commercial construction were particularly important because commercial mortgage-backed securities generally require terrorism insurance as a prerequisite for the loan or and in other cases may set the bond rating, in part on whether the entity has insurance[56]. Without terrorism insurance, loans become either unavailable or more expensive due to the increased interest rates that occur resulting from a lower bond rating, investment in commercial construction could be significantly reduced in the absence of a market for terrorism insurance.

As a response to these concerns, Congress enacted TRIA in 2002, which requires all commercial property and casualty insurers to offer terrorism coverage and established the federal government as the reinsurer. In the event of an attack, insurers would be required to pay a deductible, which in 2005 equaled 15 percent of its revenues from premiums for the previous year. Under TRIA, the deductibles rose annually, reaching 20 percent in 2007. After the deductible has been met, the federal government would pay 90 percent of additional losses up to $100 billion per year and the insurer would pay the remaining 10 percent, with the government's contribution dropping to 85 percent in 2007[57]. It is not clear what would happen if industry losses exceeded $100 billion, but the insurance companies would not be responsible for such losses. Currently, the government exacts no payments for its reinsurance, but in the event of an attack, it is required to recoup some of its money from annual surcharges assessed on insurers and policy holders. The amount they are required to recoup (known as the aggregate industry retention level) was $15 billion in 2005, but it increases annually, rising to $25 billion in 2006 and $27.5 billion in 2007. Surcharges would be limited to 3 percent of each insurers' aggregate premiums on property and casualty or group life insurance, but can be charged for as long as is necessary to recover the necessary retention level. The CBO estimates that the surcharges will total $1.6 billion, but that not all of these revenues will be collected during the 2006 -2015 time period[58].

The TRIA legislation was intended to foster the development of a private insurance market, not to make the government the final reinsurer. The purpose of requiring all insurers to offer coverage and the increasing deductibles and industry retention levels is to pass more of the risk onto the private market, hoping that this will foster its development independent of the

[54] CBO, *Federal Terrorism and Reinsurance Act: An Update*. (Washington, DC: Congressional Budget Office, 2005), p. 3.
[55] CBO, *Terrorism Risk Insurance Extension Act of 2005*. (Washington, DC: Congressional Budget Office, 2005).
[56] Ibid, p. 10.
[57] CBO, *Cost Estimate for S. 476: Terrorism Risk Insurance Act of 2005*. (Washington, DC: Congressional Budget Office, 2006), p.2.
[58] Ibid.

federal government's involvement[59]. Because the goal was to revive the previously existing insurance market and not to expand coverage, several types of terrorism are excluded from TRIA coverage. Acts of war and domestic terrorism are not covered, and most insurers do not cover losses from nuclear, biological, chemical and radiological attacks. TRIA expired on December 31, 2005 and the U.S. Congress passed the Terrorism Risk Insurance Extension Act of 2005, extending TRIA until 2007. The extension of TRIA, S. 467 sets a minimum amount of damages necessary to qualify of $50 million in 2006 and $100 million in 2007[60]. In December 2007, TRIA received a further renewal through calendar year 2014 and requiring insurers to cover domestic terrorism attacks[61].

The Costs of TRIA: Who Pays and How Much?

Estimating the costs of TRIA is very difficult because the probability, expected magnitude, and timing of an attack are all unknowns. Because there were no terrorist attacks under the original TRIA, the only budgetary costs are administrative expenses. For the 2005 extension, the president's budget only included the administrative costs, which were $4 million in 2005 and $6 million in 2006[62]. The CBO's estimates that between 2006 and 2010 the extension of TRIA will increase spending by $1.4 billion and revenues by $150 million; and over the next 10 years will increase spending by $1.5 billion and revenues by $720 million[63]. The 2007 extension is expected to increase direct spending by $6.6 billion from 2008 until 2017, but to receive offsetting revenues of $6.6 billion, making it revenue neutral. The increase in projected costs arises from the inclusion of domestic terrorism under TRIA, while increasing revenues reflect the higher assessments imposed on insurers[64] TRIA also includes some intergovernmental mandates, which are expected to cost a total of $62 million and private-sector mandates, which are expected to cost $123 million. Costs to the state governments include the adoption of guidelines for reserves and premium costs. TRIA also preempts certain state laws that regulate insurance. Costs to the private sector result from the requirement to offer coverage, the associated deductible, along with, any future assessments and surcharges[65].

As in the case of regulation, however, it is important to note that budgetary outlays are likely to understate the true cost of a program such as TRIA because the budgetary estimates presented above do not include any charge for the risk and uncertainty borne by taxpayers. Thus, the budgetary estimates are less than the economic cost of such reinsurance. As noted by the CBO, the consequences of extending TRIA would be to expose taxpayers to tens of billions of potential liabilities (which might or might not materialize) for an additional two years.

Because of the uncertainty of the actual costs of an attack (or even the probability of an attack) the preceding numbers must be taken as very rough estimates at best. However, it is possible to identify some of the effects of TRIA in shifting financial responsibility between sectors. First, by requiring insurance to be offered, TRIA shifts risk from property owners to the insurers and then, the reinsurance policy further shifts risks onto taxpayers. Even if the aggregate

[59] CBO, *Federal Terrorism Reinsurance*, p. 2.
[60] CBO, *Cost Estimate for S. 476*.
[61] CBO, *Cost Estimate for H.R. 2761: Terrorism Risk Insurance Program Reauthorization Act*. (Washington, DC: Congressional Budget Office, 2008).
[62] OMB, *FY 2006 Budget*, p. 919.
[63] CBO, *Cost Estimate for S. 476*.
[64] CBO, *Cost Estimate for H.R. 2761*.
[65] CBO, *Federal Terrorism Reinsurance*.

industry retention rate is high enough for the government to recoup all of their costs, TRIA represents an inter-temporal transfer from the private sector to the public sector. This shifting of risk in effect subsidizes the insurance costs to property owners and may impose costs on society as a whole in deterring risk retention efforts.

In addition to imposing social costs in the form of deferred risk abatement, Kunreuther and Michel-Kerjan argue that the permanent extension of TRIA could induce insurers to increase their TRIA coverage, which would shift risk to all commercial insurance owners in the event of an attack. More specifically, because the costs of an attack are currently born by tax payers and then recouped from all insurers (regardless of whether they experience an attack), TRIA highly subsidizes the costs of an attack while insurers still keep the premium revenue, providing an incentive for excess provision of insurance[66]. Due to the structure of the deductible/ risk sharing policy, insurers also have the incentive to insure geographically concentrated buildings in high risk areas, since they realize that a terrorist attack is likely to damage not only a single building, but also those surrounding them[67]. The combined result of excess insurance provided in geographically concentrated areas would be a shifting of financial responsibility from the private to the public sector and a continued absence of adequate risk abatement in the private sector. While TRIA was not intended to become permanent, if it ends up being extended indefinitely, it is likely to exacerbate current market distortions.

Issues and Challenges in Providing Government Sponsored Insurance

Feldman notes that insurance in general is likely to exacerbate moral hazard problems by removing financial responsibility from the private sector[68]and that it generally only achieves cost savings when it supplants, rather than supplements, disaster relief[69]. Both of these concerns are relevant in the case of TRIA. As noted earlier, risk deterrence is reduced by the presence of insurance and instead of locating in safer areas companies may continue to concentrate themselves geographically, creating attractive targets for terrorists. While insurers are required to offer insurance, companies and individuals are not required to purchase it, suggesting that in the event of an attack, the government would probably be spending money for reinsurance and disaster relief simultaneously. In addition, if the attack were particularly severe, disaster relief efforts may be required to address damages exceeding the $100 billion limit under TRIA, further suggesting that TRIA imposes both accounting and efficiency costs on society.

Summary and Conclusion

The public sector has always assumed responsibility for providing homeland security in addition to national defense and police protection, which are inherently governmental functions. However, in the wake of the September 11th terrorist attacks, the public sector role has expanded considerably in the United States. This paper has discussed three broad areas of federal response: budgetary outlays for direct federal spending and for government grants to state and local

[66] Krunther & Kerjan, *Looking Beyond TRIA: A Clinical Examination of Potential Terrorism Loss Sharing*. (Washington, DC: National Bureau of Economic Research, 2006), p. 28.
[67] Ibid, p. 23.
[68] Feldman, Ron. "Government Insurance" In *The Tools of Government: A Guide to the New Governance*, edited by Lester M. Salamon, p. 186-216 (Oxford: Oxford University Press, 2002) p. 207.
[69] Ibid, p. 212.

governments; modifications of existing federal regulatory programs; and, subsidization of anti-terrorism insurance. While this paper has focused on the use of these tools in the U.S. approach to homeland security, spending money, regulation, and insurance are policy tools available to all governments in a variety of policy areas. Understanding their economic effects and costs is important to both government officials and academics alike.

From a public economics standpoint, an overarching policy objective should be to ensure that scarce public funds and resources generally are well-spent. However, as we have noted, homeland security is no different from any other government policy in that issues and challenges arise in their use and implementation.

As a concluding note, we point to three challenges which we believe to be of special importance. One is to develop means of evaluating the performance both of budgetary and non-budgetary tools in the area of homeland security. On one hand, as a new and emerging policy area, the evaluation of government spending and regulatory policies intended to increase homeland security is able to draw upon an extensive body of prior work on performance evaluation, and regulatory impact and cost-benefit analysis in the federal government. On the other hand, evaluating whether dollars on homeland security programs are well-spent requires addressing new and complex issues of risk analysis. Dealing with terrorism risk, unlike dealing with risks from natural hazards, or toxic chemicals, involves playing games against human actors, whose behavior can change in response to government policies, thereby changing threat probabilities. For example, businesses and people are attracted to thriving urban areas, which then make these areas a greater target for terrorists. Providing insurance can prevent the economic losses that occur with urban decline and population sprawl if the threat of terrorism is an impediment to economic development. However, in removing the market incentives that risk creates, government may be promoting a concentration of economic activity in risky locations, raising overall costs to society.

An additional area for future research involves the effectiveness of federal grants to state and local governments. By its very nature, the provision of homeland security must involve close collaboration between the national and state and local governments, and intergovernmental grants have long been used as a mechanism for financing public goods that are both national and local in character. As we have documented, the federal government provides multiple grants in aid to state and/or local governments to encourage greater spending at the local level for homeland security. As has been the case in other grant programs, the jury is still out as to whether these grant programs, which are largely structured as non-matching grants, will actually increase spending for homeland security at the state and local levels, or whether despite "maintenance of effort provisions" such grants will, over time, substitute for resources that state and local governments would have spent anyway. The issue of assessing program performance in the area of federal-state and local programs is also a salient one since, at least according to accounts in the popular press, there is some evidence that grants for homeland security have been viewed in the legislative process as a new form of "pork" to be brought home by members of the U.S. Congress.

Finally, this paper highlights the need for a greater understanding of the actions of state and local governments and private actors in response to increased security needs post-September 11th. As the example of nuclear power illustrates, many of the costs of protecting our homeland may be largely invisible to the public sector, but crucial to homeland security. A greater understanding of these costs and their effectiveness is important in evaluating governmental

actions that affect private-sector behaviors, such as regulations and the provision of insurance. Evaluating the effectiveness and costs of homeland security policies without consideration to these additional actors' behavior will only portray an incomplete picture of a nation's efforts to secure the homeland.

This paper was presented May 18th 2006 University of Kentucky's "The Buck Starts Where: Public Finance Symposium" Lexington, KY.