REGULATORY STUDIES PROGRAM

MERCATUS POLICY SERIES

POLICY RESOURCE No. 3

A FRAMEWORK FOR EVALUATING COUNTERTERRORISM REGULATIONS

JERRY ELLIG
Senior Research Fellow, Regulatory Studies Program
Mercatus Center

AMOS GUIORA
Director, Institute for Global Security Law and Policy
Case Western Reserve University School of Law

KYLE MCKENZIE
Research Fellow, Regulatory Studies Program
Mercatus Center

SEPTEMBER 2006

MERCATUS CENTER
GEORGE MASON UNIVERSITY

About Jerry Ellig, co-author

Jerry Ellig is acting director of the Regulatory Studies Program at the Mercatus Center at George Mason University. He has been a Mercatus senior research fellow since 1996. Between August 2001 and August 2003, he served as deputy director and acting director of the Office of Policy Planning at the Federal Trade Commission while on a leave of absence from Mercatus. Dr. Ellig has also served as a senior economist for the Joint Economic Committee of the US Congress and as an assistant professor of economics at George Mason University. He has published numerous articles on government regulation and performance management in both scholarly and popular periodicals.

About Amos N. Guiora, co-author

Amos N. Guiora is a professor of law and director of the Institute for Global Security Law and Policy at the Case Western Reserve University School of Law. He teaches and develops courses and labs on the legal and policy aspects of counterterrorism, incorporating scenario-based instruction to explore national and international security issues. Professor Guiora authored the first casebook of its kind in the field, *Global Perspectives on Counterterrorism* (Aspen Publishers, forthcoming 2008). He has published on global perspectives on counterterrorism, torture, targeted killings, rule of law and terrorism, the security aspects of employment, judicial activism in armed conflict, and morality in armed conflict. For 19 years, Professor Guiora served in the Israel Defence Forces, retiring at the grade of Lieutenant Colonel.

About Kyle McKenzie, co-author

Kyle McKenzie is a research fellow at the Mercatus Center at George Mason University. His research covers outcome-based assessment of government agencies and economic analysis of the effects of regulation. He is coauthor, with Eileen Norcross, of *An Analysis of the Office of Management and Budget's Program Assessment Rating Tool for FY 2007*.

For more information about the Mercatus Center's Regulatory Studies Program, visit us online at www.mercatus.org/regulatorystudies or contact Erin Hymel at (703) 993-4930 or ehymel@gmu.edu.

MERCATUS CENTER
GEORGE MASON UNIVERSITY

A FRAMEWORK FOR EVALUATING COUNTERTERRORISM REGULATIONS

JERRY ELLIG, AMOS GUIORA, AND KYLE MCKENZIE

EXECUTIVE SUMMARY

Many analysts and decision makers have called on government to prioritize security initiatives based on risk assessment and cost effectiveness. Few, however, have explained why a comprehensive regulatory analysis framework is necessary to accomplish this. In this paper, we present a six-element regulatory analysis framework for such regulations.

1. IDENTIFY THE DESIRED OUTCOMES. If government does not specify the desired outcomes, then there are no concrete goals to guide action. Outcomes defined in terms of risk reduction and damage mitigation provide realistic benchmarks that measure the real benefits citizens receive from counterterrorism regulations.

2. ASSESS EVIDENCE OF MARKET FAILURE. Understanding the specific reasons that private action is insufficient and government action is necessary helps decision makers identify *why* people and assets are at risk. If we know why people and assets are at risk, we can better craft solutions that actually stand a chance of protecting them.

3. IDENTIFY THE UNIQUELY FEDERAL ROLE. Multiple levels of government, businesses, civil society, and individuals all have security responsibilities. To ensure that the most critical jobs get done, each should focus on what it is uniquely situated to do.

4. ASSESS EFFECTIVENESS OF ALTERNATIVE APPROACHES. Different regulations can accomplish the same or similar goals with vastly different levels of effectiveness. Regulators and legislators should seek the most effective means of accomplishing the goal.

5. IDENTIFY COSTS. Adopting a regulation directs government and private resources in one way instead of another. Decision makers should be conscious of the foregone benefits, or "opportunity costs," associated with each alternative.

6. COMPARE COSTS WITH OUTCOMES. Some security regulations will sacrifice other values identified with the American way of life. Government owes citizens a transparent accounting of how much the sacrifice of such values improves security and at what cost.

For more information about the Mercatus Center's Regulatory Studies Program, visit us online at www.mercatus.org/regulatorystudies or contact Erin Hymel at (703) 993-4930 or ehymel@gmu.edu.

A Framework for Evaluating Counterterrorism Regulations

INTRODUCTION

The terrorist attacks of September 11, 2001 left Americans feeling vulnerable as never before. For weeks thereafter, citizens on the streets of the nation's capital glanced nervously skyward in response to noises from above. Even in seemingly safe communities across the heartland, people thought twice before going out to shopping malls or restaurants. A year later, Americans were still on edge. Comments by the secretary of the Department of Homeland Security (DHS) created a run on duct tape and plastic sheeting, and Washington suburbanites brooded over whether the "Washington sniper" was the tip of al-Queda's latest plot. Arrests of shoe-bomber Richard Reid (2001), the Lackawanna Group (2002), terrorist cells in Toronto and Miami (June 2006), and the UK-based group plotting to blow up US-bound airplanes (August 2006) remind us that the threat to the US homeland has not gone away.

Everyone wants to be safe from terrorist attacks. Since protecting citizens' lives and property is a core function of government, it should be no surprise that the five years since 9/11 have seen a significant upswing in security-related initiatives. And since the vast majority of critical infrastructure and assets in the United States are privately owned, it should be no surprise that a significant number of these initiatives involve regulation of private activity.

Security-related regulations are quite diverse, ranging from data reporting on international visitors to reinforcement of airplane cockpit doors to tracking sources and destinations of food. As of March 2003, the Office of Management and Budget (OMB) identified 69 draft proposed and final regulations addressing homeland security. Of those, 49 were intended to reduce the risk of a future attack, and six were intended to mitigate the effects of a future attack. "The regulatory amendments made since then seek to address vulnerabilities at our borders, security threats through transportation, food, and chemicals, and provide law enforcement with the tools needed to interdict and apprehend potential terrorists," OMB notes.[1] Thus, the majority of homeland security

[1] OMB, Office of Information and Regulatory Affairs, *Informing Regulatory Decisions: 2003 Report to Congress on the Costs and Benefits of Federal Regulations and Unfunded Mandates on State, Local, and Tribal Entities* (2003):79, http://www.whitehouse.gov/omb /inforeg/2003_cost-ben_final _rpt.pdf . OMB has not included a similarly comprehensive review of security-related regulations in subsequent reports, but the reports have identified an additional 12 major security-related rules. See OMB, Office of Information and Regulatory Affairs, *Progress in Regulatory Reform: 2004 Report to Congress on the Costs and Benefits of Federal Regulations and Unfunded Mandates on State, Local, and Tribal Entities* (2004), http://www.whitehouse.gov/omb /inforeg/2004_cb_final.pdf , and OMB, Office of Information and Regulatory Affairs, *Draft 2006 Report to Congress on the Costs and Benefits of Federal Regulations and Unfunded Mandates on State, Local, and Tribal Entities*, http://www.whitehouse.gov/omb /inforeg/reports/2006_draft _cost_benefit_report.pdf .

regulations deal with counterterrorism, broadly defined, as they attempt to prevent, deter, or reduce the potential damage from terrorist attacks.

Risk-based analysis

Thoughtful scholars and policy makers recognize that effective security measures must be based on accurate assessment and prioritization of risks.[2] The 9/11 Commission's report repeatedly called on the government to implement security measures that reflect assessment of risks and cost-effectiveness.[3] The DHS *Strategic Plan* indicates the department's intention to use risk analysis when prioritizing resources.[4] The DHS *Interim National Infrastructure Protection Plan* notes, "[E]ven with all the resources of the United States, it is not possible to protect all assets against every possible type of terrorist attack."[5]

An almost infinite number of possible actions might serve to mitigate an almost infinite number of terrorist attacks. With limited public and private resources, we cannot invest in all of them, but rather must find a way to prioritize possible actions. Setting priorities for government action requires an understanding of the outcomes, consequences, and forgone benefits associated with different measures to mitigate terrorist risks.

This Policy Resource lays out a framework for ensuring that homeland security regulation is risk-based and cost-effective. The framework draws on two of the coauthors' experience in regulatory analysis and government performance management and one coauthor's experience in the legal and policy aspects of counterterrorism, including 19 years in the Israel Defense Forces Judge Advocate General's Corps. There are of course significant differences between America and Israel in terms of size, GDP, culture, and nature of the terrorist threat. In occasionally pointing out Israeli examples, we do not mean to advocate that America should simply copy what Israel does. But precisely because Israel has dealt with terrorism on a regular basis for decades, aspects of Israeli counterterrorism practice reveal a sophisticated and realistic attitude toward risk assessment that is informative in the context of the US debate.

Why examine security regulation?

We focus on regulation for several reasons. Federal security initiatives will inevitably involve a great

[2] See, for example, the secretary's opening letter in DHS, *Performance and Accountability Report, Fiscal Year 2005*: 1, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0430.xml (Hereafter referred to as "DHS PAR"); Henry H. Willis, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terror Risk* (Santa Monica, CA: Rand Center For Terrorism Risk Management Policy, 2005); DHS, *Interim National Infrastructure Protection Plan* (Feb. 2005): 1.

[3] See, for example, *The 9/11 Commission Report*: 364, 365, 391, 396, http://www.gpoaccess.gov/911/index.html.

[4] DHS, *Securing Our Homeland: US Department of Homeland Security Strategic Plan*: 11, http://www.dhs.gov/interweb/assetlibrary/DHS_StratPlan_FINAL_spread.pdf.

[5] DHS, *Interim National Infrastructure Protection Plan* (Feb. 2005): 1.

deal of regulation, and security-related regulation has seen significant growth.[6] But because the purpose of regulation is to modify the behavior of individuals and businesses, a full assessment of outcomes and effects is often more complicated and subtle than in the case of programs and services directly provided by the government. The threat of terrorism, however, means the stakes are quite high. To ensure that Americans are as safe as possible, we must carefully assess the likely effects of counterterrorism regulations.

The principles we outline are not new; indeed, most are articulated in the Office of Management and Budget's Circular A-4, which guides federal agencies' regulatory analyses. Others are implicit in initiatives to improve the management and performance of federal agencies, such as the Government Performance and Results Act and OMB's Program Assessment Rating Tool. Some can even be found in official DHS documents, such as its Strategic Plan. Thus, we largely extrapolate from the federal government's own stated policies and procedures for managing programs and regulations.

Our primary goal is to explain a framework. We draw upon many types of examples that illustrate various points in order to demonstrate the versatility of the framework. While we hope the information in the specific examples is useful to decision makers or analysts charged with assessing or deciding upon particular regulations, we do not claim to provide a comprehensive analysis of any of the regulations we discuss.

What an analytical framework can and cannot do

In policy debates, an analyst who points out beneficial aspects of a regulation often gets labeled "pro-regulatory." An analyst who points out undesirable consequences gets labeled "anti-regulatory." Those who glibly apply the labels fundamentally misunderstand the nature and purpose of regulatory analysis. The purpose of analysis is to provide decision makers with a realistic understanding of the consequences of alternative courses of action.

Effective decision making requires two things: knowledge of the consequences of alternative courses of action and value judgments that allow the decision maker to determine which consequences are most desirable. Regulatory analysis provides the first component, but not the second.

Regulatory analysis is a tool for understanding causation—what *is*, and what *would likely* happen as a result of various policy initiatives. To decide

[6] The post-9/11 budgets for the regulatory agencies now housed in DHS are $11 billion greater in fiscal 2006 than in fiscal 2000. For more information on trends in security-related regulation, see Susan Dudley and Melinda Warren, *Moderating Regulatory Growth: An Analysis of the US Budget for Fiscal Years 2006 and 2007* (Weidenbaum Center, Washington University in St. Louis and Mercatus Center, George Mason University, 2006), http://www.mercatus.org/Publications/pubID.2340,cfilter.5/pub_detail.asp.

what *should be done*, decision makers must combine the results of regulatory analysis with value judgments that reflect their assessment of what is worth doing. The analyst may be able to rank ten very different regulations intended to prevent terrorism in terms of their cost effectiveness in saving lives. But the analysis cannot, by itself, determine how many of those regulations are worth implementing. Similarly, comparing costs and benefits does not automate decisions, because the different decision makers may ascribe different values to the benefits. When benefits are expressed in monetary terms, the dollar amounts usually reflect the value of the benefits to the "average" or "typical" person. Cost-benefit analysis may mask significant diversity in the value that different people attach to the benefits. Two different decision makers, armed with the same information about cost effectiveness or the same cost-benefit comparisons, can still reasonably disagree about what to do based on their values.

Regulatory analysis is an indispensable tool for decision makers. It cannot, however, substitute for judgment when it comes time to make decisions. The analysis is not an algorithm that automatically produces a list of "correct" answers that can be read off of a graph or table.

But just as analysis is not a substitute for judgment, values are not a substitute for understanding reality. Without the firm grounding in reality provided by regulatory analysis, decision makers are flying blind, and we are less safe from terrorism as a result.

Key Steps in Regulatory Analysis

1. **Identify the desired outcomes**
2. **Assess evidence of market failure**
3. **Identify the uniquely federal role**
4. **Assess effectiveness of alternative approaches**
5. **Identify costs**
6. **Compare costs with outcomes**

1. Identify the Desired Outcomes

"If you don't know where you're going, any road will take you there."

—George Harrison

An outcome is the benefit to the public produced, or harm avoided, as a result of a government action.[7] Vague goals like "protecting the homeland" or "winning the war on terror" are

[7] We use the term "outcomes" rather than "benefits," because some policy results that are of great interest to decision makers may not fit the economist's definition of society-wide "benefits." A focus on outcomes, rather than a narrower focus on benefits, permits a much wider application of the regulatory analysis framework.

not useful for identifying specific outcomes. To constructively evaluate viable alternatives and their relative merits, it is essential to define what event/behavior/action the regulation is intended to promote, prevent, or mitigate.

1A. Victory or risk management?

Defining outcomes for homeland security requires understanding and acknowledging that acts of terrorism will occur. Accordingly, the question is how a liberal democratic society minimizes terrorism. If the public has realistic expectations, the government will likely develop better counterterrorism programs and institutions.

History has shown that terrorism cannot be defeated, especially in a one-time battle. Counterterrorism is similar to a war of attrition, requiring enormous resources wisely spent, great patience, and sophisticated policy. Decision makers do a great disservice to the public when guaranteeing victory over terrorism. Terrorism can be minimized, perhaps marginalized, but not completely eradicated—a characteristic shared with crime, political corruption, and other forms of evil in this world.

The 9/11 Commission recognized this fact when it noted,

> We do not believe it is possible to defeat all terrorist attacks against Americans, every time and everywhere. A president should tell the American people:
>
> - No president can promise that a catastrophic attack like that of 9/11 will not happen again. History has shown that even the most vigilant and expert agencies cannot always prevent detemined, suicidal attackers from reaching a target.
> - But the American people are entitled to expect their government to do its very best. They should expect that officials will have realistic objectives, clear guidance, and effective organization. They are entitled to see some standards for performance so they can judge, with the help of their elected representatives, whether the objectives are being met.[8]

This is a message the Israeli public is accustomed to hearing. Commenting on a recent terrorist attack in Israel, Prime Minister Ehud Olmert stated, "This is of course something we knew might happen, as the terror organizations are constantly looking for opportunities to carry out attacks in Israel. The security forces foil such attempts daily, and we have many specific warnings of more plans for attacks. The security forces are deployed all across the

[8] *9/11 Commission Report*, p. 365.

country, but we are aware that it is impossible to prevent every such incident."[9]

One can also find statements from past Israeli prime ministers that reflect this kind of realism. In his Nobel Peace Prize acceptance speech, former Prime Minister Yihtzak Rabin noted that even a society that values the sacredness of human life recognizes that lives will be lost despite enormous precautionary investments:

> To defend those lives, we call upon our citizens to enlist in the army. And to defend the lives of our citizens serving in the army, we invest huge sums in planes, and tanks, in armored plating and concrete fortifications. Yet despite it all, we fail to protect the lives of our citizens and soldiers. Military cemeteries in every corner of the world are silent testimony to the failure of national leaders to sanctify human life.[10]

Indeed, sometimes the defense of life itself requires that people place their lives in jeopardy:

> Almost all the regimes which did not place Man and the Sanctity of Life at the heart of their world view, all those regimes have collapsed and are no more. You can see it for yourselves in our own day.
>
> Yet this is not the whole picture. To preserve the Sanctity of Life, we must sometimes risk it. Sometimes there is no other way to defend our citizens than to fight for their lives, for their safety and sovereignty. This is the creed of every democratic state.[11]

Israeli business leaders offer similarly realistic sentiments. Opher Lincheveski, chief financial officer of Egged, Israel's largest bus line, noted sensible reasons that prevent his company from offering his passengers a 100 percent guarantee of safety:

> Well, we have shown the public we are trying our best to minimize the level of risk. But there's a marketing dilemma; we can't push security too hard. Let's say we run a commercial showing our guards checking the passengers. Okay, people watch the commercial and then confidently board an Egged bus, which is subsequently bombed. You see? There are matters of credibility, and there are legal matters that would arise . . . We won't say, "Egged is safe," because we don't see an elimination of attacks. Hopefully, what we've done will stop many.[12]

[9] Ilan Marciano, "Olmert: We'll Know How to Respond." *Ynetnews*, April 17, 2006, http://www.ynetnews.com/articles/1,7340,L-3240770,00.html.
[10] Yitzhak Rabin, Nobel Peace Prize Lecture, 1994, http://nobelprize.org/nobel_prizes/peace/laureates/1994/rabin-lecture.html
[11] Ibid.
[12] Dan Carrison, *Business Under Fire: How Israeli Companies Are Succeeding in the Face of Terror—and What We Can Learn From Them* (New York, NY: AMACOM, 2005), 53.

Sometimes counterterrorism "success" consists of mitigating the effects of attacks that cannot always be prevented. In the spring of 1996 (during the Jewish holiday of Purim), a Palestinian terrorist intended to carry out a suicide bombing inside a Tel Aviv shopping mall, Dizingoff Center.[13] When he approached the mall, he noticed the number of security guards at the entrance. As a result, the terrorist exploded himself at a street intersection. While the human tragedy was enormous, the damage was less than it would have been had the terrorist carried out the suicide bombing inside the mall. The only reason the terrorist changed his plans was the larger-than-normal number of guards at the entrance.[14]

British officials reiterated the risk reduction message when they announced the arrest of terrorists plotting to blow up US-bound planes in August 2006. John Reid, the British home secretary, noted, "[W]hile the security services would deliver 100 percent effort and dedication, they could not guarantee a 100 percent success rate in fighting terrorism."[15]

1B. Risk reduction and damage mitigation

The fact that a successful attack has not occurred on American soil since 9/11 should not be the primary measure of counterterrorism "success." Furthermore, if a terrorist attack occurred in the United States tomorrow, that would not inherently imply that all government policies had been abject failures. For this reason, goals and performance measures for homeland security need to be expressed in terms of reducing the risk and damage associated with terrorist attacks.

Consider, for example, regulations intended to prevent the recurrence of a major terrorist incident such as the 9/11 attacks. One measure of the effect of the attacks is the dollar value of damage done to the World Trade Center, New York City, and the national economy. Estimates of $50 billion—$200 billion are not uncommon, depending on the range of factors considered.[16] Given such figures, a regulation that significantly reduced the likelihood of a major terrorist attack would produce significant benefits. Even if the size of the risk reduction is not measurable, it would be useful to know how much a regulation is likely to reduce the size of a terrorist incident's effects.

1C. Risk vs. Uncertainty

Not every type of "risk" can be quantified. To understand the outcomes of counterterrorism regulations, one must distinguish between the idea

[13] Raine Marcus and Steve Rodan, "12 Die in TA as Hamas Terror Strikes Again," *The Jerusalem Post*, March 5, 1996, 1.
[14] Amos N. Guiora, "Counterterrorism and Employment: An Israeli Perspective" (August 2005). Case Legal Studies Research Paper No. 05-26, http://ssrn.com/abstract=785368.
[15] "UK Police Say Aircraft Bomb Plot Foiled," *Aljazerra.net*, August 10, 2006, http://english.aljazeera.net/NR/exeres/556C70AC-5DE4-41C3-A746-009274E8149F.htm.
[16] See, for example, US Government Accountability Office, "Impact of Terrorist Attacks on the World Trade Center," Report NO. GAO-02-700R.

of risk and the idea of uncertainty. The two concepts are often conflated into discussion of risk but they are distinct.

Risk is the probability that certain outcomes either will occur or will not occur. When all possible outcomes are known and their probabilities can be reasonably estimated, then it is possible to quantify a regulation's effect on security by estimating its effect on the likelihood and size of various outcomes. The probability of a terrorist event multiplied by the size of the consequences gives us the direct benefits of avoiding that event.

Uncertainty occurs when some probabilities or outcomes are genuinely unknown. It is impossible to make a risk profile and calculate a probability of an occurrence under genuine uncertainty. In short, risk is measurable, while uncertainty is unquantifiable.[17]

The Food and Drug Administration's (FDA's) analysis of recordkeeping regulations that allow the FDA to trace the source of food contamination illustrates the difference between risk and uncertainty.[18] Based on past data on the frequency and severity of food-borne illnesses, the FDA was able to estimate the probability of future accidental outbreaks, which helped it estimate the benefits of regulatory action. However, it was unable to estimate the probability of outbreaks intentionally caused by terrorists because there are few data on which to base such a probability.[19]

Defining outcomes of counterterrorism measures, therefore, requires identifying which types of terrorist attacks involve measurable risk and which ones involve genuine uncertainty. When risk can be measured or estimated, then one desirable outcome of counterterrorism regulation is a reduction in the measurable risk of attack. Another desirable outcome is a reduction in the likely damage the attack could do to lives and property. For terrorist attacks for which probabilities are unknown, it should still be possible to measure the effects of mitigation measures intended to reduce damage. If one cannot measure the likelihood of an attack, then the best one can hope for is a transparent policymaking process that lets citizens see, understand, and evaluate decision makers' "judgment calls."

[17] Mary R. Brooks and Kenneth J. Button, "Market Structures and Shipping Security," *Maritime Economics & Logistics* 8 (2006): 105-06. The classic distinctions are made in Frank H. Knight, *Risk, Uncertainty, and Profit* (Chicago: University of Chicago Press), 19-21, and Ludwig von Mises, *Human Action* (Chicago: Henry Regnery Company, 1949), 107-110.

[18] "Establishment and Maintenance of Records under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002," 69 *Federal Register* 71562, http://www.cfsan.fda.gov/~acrobat/fr04d09a.pdf.

[19] "Establishment and Maintenance of Records under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002," 69 *Federal Register* 71562, p. 71614, col. 3, http://www.cfsan.fda.gov/~acrobat/fr04d09a.pdf.

1D. Tradeoffs are inevitable

Resources are limited in comparison to the panoply of human wants and needs. Decision makers must necessarily choose which risks and uncertainties they will seek to mitigate, and to what extent. Limited resources mean zero risk is impossible. Government cannot put "a cop on every street corner" to prevent terrorism.

Suppose, for example, that there are three lines at an airport and one guard who can physically be stationed at only one of the lines. Perhaps the guard can rotate between all three, but at any given time, at least two of the three lines will be unprotected (and if he rotates between the three then at some time *all three* will be unprotected). The decision to post the guard in one location is also a decision not to post him in the other locations. It is a decision to accept some risks in order to reduce a more significant risk. Risk assessment is inherently necessary in proactive counterterrorism.

This lesson is well-understood in Israel. In the Israeli town of Sderot, which has been regularly bombarded with Palestinian missiles, children and adults face higher risk and are more likely to be traumatized as a result. However, the education minister decided in 2006 not to provide an "escape" summer camp for the kids of Sderot.[20] Protestors want additional security for the city under attack; however, the government has yet to comply with their demands. Presumably, part of this decision-making process involves comparing the effectiveness of alternative uses of resources.[21]

The government constantly redeploys security forces in Israel to the changing areas of greater threat, because it cannot simultaneously protect all locations. Therefore, it moves forces to the locations currently facing the greatest threat, such as public malls on school vacations and synagogues during religious holidays. The Israeli news media widely reports such redeployments.

- April 13, 2006: "In order to maintain the holiday atmosphere and make sure that all events go by peacefully, security forces have raised their alert level in the past few days. At this time, security authorities are contending with 78 warnings regarding plans to carry out terror attacks, including 16 concrete warnings."[22]

[20] Ariana Melamed, "Get the Kids Out of Sderot," *Ynetnews*, June 14, 2006, http://www.ynetnews.com/articles/0,7340,L-3262759,00.html.
[21] Shmulik Hadad, "Qassam Barrage Hits Sderot," *Ynetnews*, June 12, 2006, http://www.ynetnews.com/articles/0,7340,L-3261677,00.html.
[22] "Pesach: Israelis Head for Tourism Sites," *Ynetnews*, April 13, 2006, http://www.ynetnews.com/articles/0,7340,L-3239483,00.html.

- April 12, 2006: "While millions of Israelis will attend the Passover Seder Wednesday evening, thousands of soldiers will be deployed across the country for fear of terror attacks. Security will be boosted around synagogues as well, with at least one armed guard placed at every synagogue. Police officials also briefed hotel officials and requested that security be boosted for the holiday."[23]
- March 27, 2006: "Meanwhile, security at malls and entertainment venues will be significantly reinforced, as masses are expected to use the day off for shopping."[24]
- March 12, 2006: "The Israeli police completed its preparation measures for the Purim holiday this week. Thousands of additional police officers, Border Guard officers, volunteers, and IDF soldiers will spread out all over Israel, in town centers, vacation spots, parks, and entertainment centers. The high alert will last through Thursday."[25]
- December 31, 2005: "In addition to traffic control and law enforcement, the Israel Police has received 49 warnings of intensions by terror groups to carry out attacks this evening. Police said 10 of the warnings are based on pinpoint intelligence tips of plans to attack specific busy sites, where security checkpoints have been set up."[26]

Perhaps understandably, there are few public announcements identifying the facilities or assets that such redeployments leave less protected. But Gil Kleiman, a spokesperson for the Israeli National Police, noted in 2004, "There is no question that when (the intifada) began in September 2000 a lot of police manpower and resources were diverted to saving lives from terrorism. Detectives who would have been following up crime files were taken off to investigate the suicide bombings, which were happening almost daily."[27]

Thoughtful analysts in the United States have called for risk-based prioritization. A monograph by the RAND Center for Terrorism and Risk Management Policy suggests not only prioritiza-

[23] "Concrete Terror Warnings Up," *Ynetnews*, April 12, 2006, http://www.ynetnews.com/articles/0,7340,L-3239384,00.html.
[24] Efrat Weiss, "High Alert: 85 Terror Warnings," *Ynetnews*, March 27, 2006, http://www.ynetnews.com/articles/0,7340,L-3233027,00.html.
[25] "Police on High Alert for Purim Holiday," *Ynetnews*, March 12, 2006, http://www.ynetnews.com/articles/0,7340,L-3226530,00.html.
[26] "Israel Celebrates New Year," *Ynetnews*, December 31, 2005, http://www.ynetnews.com/articles/0,7340,L-3192892,00.html.
[27] "Israel Struggles to Keep Lid on Crime," *BBC News*, Monday, June 7, 2004, http://news.bbc.co.uk/2/hi/middle_east/3723895.stm.

tion based on risk, but also offers tips on sensible metrics. RAND finds that using a population-based approach to assess risk "fares little better than [a] random estimator."[28] A risk estimator that aggregates three types of risk, including some very specific event-based scenarios, does a much better job.

1E. Current goals and measures

How well do current counterterrorism goals and measures reflect outcomes associated with reducing the risk and mitigating the damage that terrorists could do? The federal government outlines the purpose of homeland security regulations in two principal sets of documents: the DHS *Strategic Plan* and *Performance and Accountability Report*, required by the Government Performance and Results Act, and the Office of Management and Budget's analysis of homeland security programs under the Program Assessment Rating Tool (PART).

1F. Strategic Plan and Performance and Accountability Report

DHS outlines seven strategic goals and multiple strategic objectives under each goal. The three strategic goals most likely to generate counterterrorism regulations—awareness, prevention, and protection—are also the most outcome-focused. This focus is most apparent in the areas of prevention and protection, where the emphasis is on safeguarding the American people from threats and reducing the potential harm from terrorist acts.

Some of the strategic objectives under the goals also qualify as outcomes. For example, most of the Protection objectives are pretty straightforward outcomes: "Protect the public from acts of terrorism and other illegal activities," "Reduce infrastructure vulnerability from acts of terrorism," "Secure the physical safety of the president, vice president, visiting world leaders and other protectees," and so forth.[29] The first objective under Prevention is "Secure our borders against terrorists, means of terrorism, illegal drugs, and violations of trade and immigration laws."[30] The results implied here relevant to terrorism are pretty clear: terrorists, means of terrorism, and illegal immigrants do not cross the border. These are intermediate outcomes that presumably contribute to the ultimate outcome of reduced likelihood of, or damage from, a terrorist attack.

Some objectives are written as activities but implicate outcomes. One objective under Awareness is "Provide timely, actionable, accurate, and relevant information based on intelligence analysis and vulnerability assessments to homeland security partners, including the

[28] Willis, Morral, Kelly, and Medby (2005), 47.
[29] DHS PAR, 38.
[30] DHS PAR, 38.

Department of Homeland Security Strategic Goals

Awareness: Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to our homeland security partners and the American public.

Prevention: Detect, deter, and mitigate threats to our homeland.

Protection: Safeguard our people and their freedoms, critical infrastructure, property, and the economy of our nation from acts of terrorism, natural disasters, or other emergencies.

Response: Lead, manage, and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.

Recovery: Lead national, state, local, and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.

Service: Serve the public effectively by facilitating lawful trade, travel, and immigration.

Organizational Excellence: Value our most important resource, our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability, and teamwork to achieve efficiencies, effectiveness, and operational synergies.

Source: Department of Homeland Security, Performance and Accountability Report, Fiscal Year 2005, 18.

public."[31] Although "providing information" is an activity, the rest of the objective suggests that the information must be useful to partners in accomplishing an outcome.

Unfortunately, other strategic goals focus more on activities than on outcomes. "Lead, manage, and coordinate" are clearly activities, not results. Similarly, the Organizational Excellence goal is really an internal management goal of building the capabilities necessary to achieve outcomes. The Service goal might be interpreted as the usual post-Tom Peters pledge to provide "excellent service," but the associated objectives reveal more substance than that. DHS uses the Service goal to enunciate other important values, such as the free flow of people and commerce—values that counterterrorism sometimes supports and sometimes restricts.

[31] DHS PAR, 33.

In similar fashion, many of the strategic objectives listed under the strategic goals are activities rather than outcomes. The first objective under Awareness is "Gather, fuse, and analyze all terrorism and threat related intelligence." This objective describes an important activity that DHS is supposed to do, but it is not an outcome. A number of objectives under Prevention are also activities, such as "Enforce trade and immigration laws" and "Coordinate national and international policy, law enforcement, and other actions to prevent terrorism."[32] The most obvious examples of activities occur under the Organizational Excellence goal. They include "Drive toward a single departmental culture" and "Continually improve our way of doing business."[33]

Ultimately, the agency must accompany outcome goals with outcome measures that indicate *how much* benefit the agency's actions produced or how much harm the agency's actions avoided. Relatively few of the DHS performance measures are outcome-oriented. Fewer than 20 of the 113 measures identify ultimate or intermediate outcomes. Many of the most outcome-oriented measures apply to the Coast Guard or the Secret Service. Some of the better ones include a maritime injury and fatality index (five-year moving average of maritime deaths and injuries), number of firefighter injuries and civilian deaths from fire, and percentage of Secret Service protectees who arrive and depart safely.[34] The Coast Guard has a Ports, Waterways, and Coastal Security Risk Index that appears to assess the contribution of the Coast Guard's actions in the fiscal year to the risk, vulnerability, and consequences of maritime terrorist attacks.[35]

The Federal Protective Service plans a Facility Security Index that is partly outcome-based because it involves testing the effectiveness of countermeasures implemented by the FPS. Other aspects of the index—which measure whether the FPS actually implemented countermeasures it planned to implement and how fast the FPS responds to incident calls—are more activity-focused.[36]

Some performance measures identify outcomes but could be improved. The Air Marshal Service tracks the number of criminal and terrorist attacks initiated from aircraft where at least one air marshal was present. (The target and the actual were both zero in fiscal 2004 and 2005.)[37]

[32] DHS PAR, 38.
[33] DHS PAR, 66.
[34] DHS PAR, 200, 212-13, 234, 236.
[35] DHS PAR, 232.
[36] DHS PAR, 233.
[37] DHS PAR, 195.

But if the goal of the program is deterrence, and part of its effect occurs because potential perpetrators do not know whether an air marshal is present or not, then a better outcome measure would include all flights, or perhaps some set of flights, where air marshals could be deployed.

Performance goals for airline baggage and passenger screening include an index that measures "effectiveness."[38] If "effectiveness" in keeping dangerous people or items off airplanes is indeed a leading indicator of safety, then this index may provide some indication of screening's contribution to passenger safety.

Numerous measures merely count activities, inputs, or outputs. Examples of these include:

- "number of information analysis products,"
- "number of information analysis community member organizations with which the Information Analysis and Infrastructure Protection (IAIP) Directorate is integrated,"
- "compliance rate for Customs Trade Partnership Against Terrorism (C-TPAT) members with the established C-TPAT security guidelines,"
- "percent of worldwide US destined containers processed through Container Security Initiative ports,"
- "percent of trucks and containers inspected using a specific technology, number of people trained, training programs accredited, and training programs conducted,"
- "development and support of a cyber security test bed,"
- "percent of assessed surface critical transportation assets or systems that have identified mitigation strategies,"
- "number of cyber security work products disseminated,"
- "percent of action items identified in After-Action Reports that were implemented,"
- "number of scholars supported," and
- a variety of compliance rates for cargo, vehicles, facilities, fishermen, and travelers.[39]

The problem with these activity-oriented objectives and measures is not that they are unimportant. Indeed, they may reflect critical tasks that the department must achieve or capabilities that it must develop. But achievement of activity-oriented objectives tells us nothing about whether the department and its regulations are successfully reducing the likelihood and potential damage from terrorist attacks. Only outcome-oriented objectives can do that.

[38] DHS PAR, 193-94.
[39] DHS PAR, 157, 158, 170, 171, 180-81, 182-83, 223, 187, 197, 210, 216, 173-76, 192, 230, 231.

1G. Program Assessment Rating Tool

For five years, OMB has sought to define and measure outcomes for each federal "program," which in some cases includes regulations. DHS and OMB have worked together to develop measures for many homeland security programs. We examined the PART reports on regulations related to domestic aviation. Some of the PART measures also appear as measures linked to strategic goals in the *Performance and Accountability Report*. Most of the measures are outputs or activities, not outcomes.

The accompanying table shows that 98 percent of federal spending on airline security regulation is for programs that received a "results not demonstrated" rating as of fiscal 2005. "Results not demonstrated" does not mean the regulation is ineffective. Rather, it indicates that the federal government lacks sufficient measures or data to determine whether it is accomplishing the intended results. None of these regulatory programs received a results score above 34 out of 100.[40]

The first section of PART asks questions about the purpose and design of the program. The program will be most effective if its stated purpose reflects outcomes, rather than inputs and outputs. Therefore, a counterterrorism program's purpose should include language that depicts public benefits produced or harms avoided. The Air Cargo Security program of DHS has a program purpose that points towards outcomes. The purpose stated in the PART assessment reads, "The Air Cargo program develops and deploys advanced programs and systems to ensure the safe and secure transport of passengers and property in air transportation."[41] The desired outcomes—safe and secure transport—appear in the second half of the sentence. The program purpose is good but would be more precise if it mentioned the reduction of risk instead of "ensure the safe and secure transport." Similarly, the Flight Crew Training program purpose stated in the PART evaluation reads: "The purpose of the Flight Crew Training program is to provide training to volunteer crewmembers to prevent acts directed against commercial aviation that could result in mass violence and death, destruction of property, and damage to the national economy."[42] Although the second half of the sentence hints at outcomes, it seems to imply that the program has achieved its purpose as long as it "provides training."

[40] The actual "results" factors in PART—the measures and performance data—count for 50 percent of the program's PART score. A program can receive an "adequate" rating in spite of a low results score if it receives a high score on factors like program design, clarity of purpose, etc.

[41] Detailed Information on the Transportation Security Administration: Air Cargo Security Programs Assessment, Question 1.1, January 13, 2006, http://www.whitehouse.gov/omb/expectmore/detail.10003602.2005.html.

[42] Detailed Information on the Transportation Security Administration: Flight Crew Training Assessment, Question 1.1, January 13, 2006, http://www.whitehouse.gov/omb/expectmore/detail.10003616.2005.html.

Table 1

PART Scores and Funding Levels for Regulations Related to Aviation

Regulation	PART score	PART Results Section Score (Out of 100)	2005 Funding Level Estimate (millions)
Baggage Screening Technology	Results Not Demonstrated	28	$645
Passenger Screening Technology	Results Not Demonstrated	34	$103
Screener Training	Adequate	13	$89
Screener Workforce	Results Not Demonstrated	20	$2,522
Air Cargo Security Programs	Results Not Demonstrated	22	$45
Aviation Regulation and Enforcement	Results Not Demonstrated	13	$226
Flight Crew Training	Results Not Demonstrated	0	$27
Federal Air Marshal Service	Results Not Demonstrated	0	$663
Total 2005 Funding			**$4,320**
Percent of funding rated "Results Not Demonstrated"			**97.9**

Source: Information taken from the respective PART reports at http://www.expectmore.gov.

The "details" section of each PART report lists the measures that each program uses and labels them as either "outcome" measures, "output" measures, or "efficiency" measures.[43] Many outcome measures and even some of the output measures would be better classified as intermediate outcomes. They do not provide a measure of the public benefit produced or harm avoided, but they might be leading indicators of the outcome.

True outcome measures are few and far between in PART analysis of air transport security. The Screener Workforce Program has one outcome-oriented measure that is not directly related to safety. It is a measure of "Level of the Customer Satisfaction Index (CSI-A) for Aviation Operations." If one goal of the Screener Workforce is to provide customer satisfaction, then this might be a good outcome measure—though not a measure of security outcomes. The only other PART measure that could be classified as an outcome under a program's PART evaluation is a measure for the Federal Air Marshal program that is also included in the DHS Performance and Accountability Report: "Number of successful terrorist and other criminal attacks initiated from commercial passenger aircraft cabins with FAM coverage." As noted above, this measure could be improved.

The vast majority of the other PART measures classified as outcomes are actually intermediate outcome measures. One example is the "Percentage compliance with leading security indicators" for both airlines and airports for the Aviation Regulation and Enforcement program. Level of baggage and passenger screening covert test results (which are classified) would also qualify as an intermediate outcome for the Screener Workforce program if more effective screening at airports reduces the likelihood of terrorist takeover of airplanes. Finally, for the Screener Training program, the "Level of screeners scoring 85% or greater on annual performance recertification on the first attempt" could be a good indicator of the level at which the trainers would protect passengers in the future.

Many measures of program performance are accurately labeled as output or efficiency measures. These types of measures range from the cost per passenger and bag screened to number of inspections to the number of days the air marshals are actually flying on airplanes.

Some output measures are clearly activities that tell us little about the effectiveness of a program. The Aviation Regulation and Enforcement program lists the "Number of Inspections conducted domestically by TSA." This measure really has no

[43] Some outcome and output measures are labeled inaccurately or are labeled in a contradictory fashion. For example, the "level of machine efficiency" is labeled as an outcome for the Passenger Screening Technology program but as an efficiency measure for the Baggage Screening Technology program. Clearly the same measure for two similar programs should not be labeled as an outcome for one and an output or efficiency measure for another.

bearing on the effectiveness of the regulatory program as it fails to tell us anything about how much safer passengers are as a result of DHS' activity.

2. Assess Evidence of Market Failure

"First, do no harm."

—Hippocratic Oath

Protecting lives and property is clearly one of the most basic duties that citizens expect government to perform well. Yet even security involves decisions about the relevant government and private roles. Governments provide police, but citizens pay for locks on their doors.

In a free economy like that of the United States, what is the core government role in providing security against terrorist attacks? Individuals must make decisions about their personal safety all the time. The people who run business enterprises, nonprofit organizations, neighborhood associations, and countless other organizations similarly make decisions that affect the safety of customers, clients, employees, and others who interact with their organizations. At what point do these decisions become public decisions?

Regulatory economists generally accept that government should intervene in the case of a clear "market failure" that cannot be adequately addressed by other means. This is because voluntary action by individuals and organizations is very effective at allocating scarce resources to the uses that citizens value most highly. As Nobel laureate economist Friedrich Hayek showed, decentralized processes are superior to centralized regulatory solutions because decentralized markets focus dispersed information—information that no one individual (not even a regulator) can obtain—and convey it effectively to market participants.[44] Decentralized markets also permit trial-and-error experimentation in order to discover things that would not otherwise be discovered.[45] Evidence abounds that individuals with diverse, localized knowledge can make choices, generate ideas, and solve problems far better than small groups of experts, no matter how well intentioned, knowledgeable, or intelligent.[46]

Concentrating government effort on market failure does not mean that the government should sit back and wait for a terrorist attack to reveal where the private sector has provided inadequate security. Rather, government and independent analysts need to identify situations in which private individuals, businesses, or other organizations

[44] Friedrich A. Hayek, "The Use of Knowledge in Society," *American Economic Review* 35, no. 4 (1945): 519-30.
[45] Friedrich A. Hayek, "Competition as a Discovery Procedure," in Hayek, *New Studies in Philosophy, Politics, and Economics* (Chicago: University of Chicago Press, 1978),179-90.
[46] James Surowiecki, *The Wisdom of Crowds: Why the Many are Smarter than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations* (New York: Anchor Books, 2004).

may lack incentives to provide security. Regulatory actions that do not explicitly recognize the market failure or identify some other systemic problem underlying the need for action are bound to be less effective than those that identify and correct the fundamental problem.

The term "market failure" is perhaps an unfortunate piece of economics jargon, because to most people the term "market" implies some form of commercial, for-profit business activity. Market failure then presumably refers to any situation in which commercial activity fails to solve a perceived problem. For many economists, however, the term "market" often has a much broader meaning, referring to any type of voluntary interaction in which people mutually coordinate their activities, rather than taking directions from a higher (governmental) authority. We use the term in this broader sense. A "market failure" occurs when voluntary activity fails to direct resources to the uses that people value most. When that occurs, some services (such as security) may be under-provided.

2A. Public Goods

One form of market failure involves "public goods." Public goods are common resources for which it is very costly to exclude users. National defense is a classic example, and homeland security is closely related. Community members cannot be excluded from the benefits of homeland security activities, even when they do not contribute to the cost of providing the defense. This is known as the "free rider problem": because no one can be excluded from receiving the benefits of homeland security once it is provided, no individual has the incentive to contribute voluntarily to its provision. As a result, if left to voluntary activity, homeland security would likely be under-provided.

Furthermore, public goods have the characteristic of "nonrivalrous consumption": consumption by one party does not diminish the value to another. Thus, even if one could exclude others from a public good, it would not be efficient to do so.

The public good concept generally justifies government provision of national defense or homeland security. But that does not mean that every form of "security" is necessarily a government responsibility. The appropriateness of a government role depends in part on whether the particular application involves nonexcludability and nonrival consumption.

In Israel, for example, citizens rely on government protection against terrorist attacks. However, individuals and businesses are also responsible for preventive measures. Israeli transportation security depends on four levels of security, one of which is public vigilance. The public takes on the responsibility for noticing unclaimed packages and suspicious travelers.[47] Businesses also hire guards

[47] Rafi Melzer and Sigal Kaplan, "Personal Security Using Public Transport: The Israeli Experience," *UITP Case Study, Public Transportation International* (May 2004).

and employ security measures. One business leader noted, "[O]ur well-being cannot be based on peace. Our companies have to be successful under any conditions; otherwise, other people have the ability to influence our way of life. We have to live our lives the way we want, whether there is peace or not."[48]

Business leaders assume responsibility for the protection of their assets and customers; one cannot walk into a coffee house in Israel without having a guard from a private guard service check one's bags. Similarly, the Egged bus company, target of most suicide bombings (presumably because it is the largest carrier) has 500 security guards on its buses.[49] It shoulders other substantial security-related costs as well:

> Our drivers get therapy sessions, personally and in groups, from clinical psychologists we have hired. We also give a lot of training to the drivers so that they can deal with a terrorist attack. This amounts to thousands of hours of both therapy and training. The overall effect is our drivers feel as if Egged is doing its best to deal with the problem and to take care of its people.[50]

Far from being merely "eyes and ears," private security guards play an active role that one might normally assume would be reserved to police officers. Guards have regularly placed themselves in peril when preventing suicide bombers from entering coffee houses.[51] In Netanya on December 5, 2005, security guards prevented a bomber from entering a shopping mall. Press reports note,

> The suicide bomber blew himself up meters from the entrance to the shopping center. He carried his explosives device in a bag. According to witnesses, a female police officer and civilians passing by identified the terrorist as a suicide bomber, and managed to shout out warnings to others. The guard to the shopping center prevented the terrorist from entering the building, but could not prevent him from blowing himself up. He was killed as he prevented the suicide bomber from entering the mall.
>
> Einav Tzabari, who stood by the nearby courthouse, witnessed the attack. "We saw the mall's guard approach a man carrying a bag. The guard pulled the terrorist towards

[48] Carrison (2005), 181.
[49] Carrison (2005), 52.
[50] Unexpectedly, one of the costs not found is an increased salary for drivers, even those on particularly dangerous routes. Lincheveski notes, "Some of the busses, which now look like tanks, have to go into dangerous areas. Even these drivers do not resign. Some even volunteer for these routes. We ask, 'Who wants to go?' and the hands go up. There is no increase in pay." See Carrison (2005), 54.
[51] Joel Leyden, "Israel: Syria, Iran Terrorism Behind Tel Aviv Bombing," *Israel News Agency,* February 26, 2005, http://www.israelnewsagency.com/terrorismisraelsyriapalestinians6870226.html.

> the direction of the sidewalk, placing distance between the bomber and the entrance to the mall. We heard shouts. Two police officers arrived at the scene and stood with their back towards the bomber and the terrorist, and then the explosion happened. We saw things flying in the air; we immediately understood this was a terror attack."[52]

Why do private citizens and businesses take responsibility for providing "security," which many people regard as a government responsibility? Security is a public good for those people who choose to enter the restaurant, bus, or other business; once in, the guard protects them. But this form of security is not a public good for society as a whole. The guard protects only those individuals who enter the business establishment. Realistically, the guard can only protect those individuals effectively—not all of society. Consumption is nonrivalrous, and it is possible to exclude nonpayers. Consumers demand security by patronizing better protected establishments. Businesses are thus driven to provide basic security, such as guards, to attract customers.

This example demonstrates a key economic principle about public goods. The extent to which something is a public good depends on the particular context, the size of the market, and particular institutional arrangements.[53] All "homeland security" is not inherently a public good; it depends on the nature of the particular threat, the particular counter-measures, and myriad other contextual factors. To determine whether government intervention is necessary to provide security in particular cases, one must analyze the specifics, rather than make broad philosophical statements about the presumed nature of "security" in the abstract.

In the US, airline security might seem to present a similar situation. Security is excludable, and the users pay. Even under government provision of passenger and baggage screening, airline passengers pay for security—partly in the price of the airline ticket and partly in the "9/11" fee added onto the price of the ticket. Airports and airlines both have a strong interest in ensuring that air travel is actually safe and perceived as such.

The public goods rationale for airline security becomes stronger if a principal purpose is to prevent terrorists from using airplanes as weapons, as occurred on 9/11. The vast majority of individuals killed on that day were working in the World Trade Center, not flying on airplanes. Protection of non-passengers who happened to be in buildings targeted for terrorist attack via air is

[52] Raanan Ben-Zur, "5 Killed in Netanya Bombing," *Ynetnews*, December 5, 2005, http://www.ynetnews.com/articles/0,7340,L-3179585,00.html.
[53] Tyler Cowen, "Public Goods Definitions and Their Institutional Context: A Critique of Public Goods Theory," *Review of Social Economy* 43:1 (April 1985): 53-63.

much more likely to be characterized by nonexcludability and nonrival consumption.[54]

The police and intelligence work involved in uncovering terrorist plots is another likely example of nonexcludability. When government investigates, monitors, and infiltrates terrorist organizations, it is protecting the public from a variety of threats that may not be known at the time the investigation was initiated. Only after a particular plan is discovered is it clear which citizens or businesses were at risk. Police in the UK, for example, thwarted the August 2006 plot to blow up multiple airplanes bound for America through investigations and arrests. It is doubtful that airlines would employ private investigators or mercenaries to root out terrorist cells just in case some of them might be planning to attack airplanes.

2B. Externalities

A somewhat related, but conceptually distinct, market failure involves externalities. Broadly speaking, an externality occurs when one party does something that affects another party's welfare but does not take those effects into account. Classic examples of negative externalities include air pollution and ugly neckties. Classic examples of positive externalities include safe streets and well-kept lawns.

As the examples suggest, not every form of externality implies that a policy response is necessary. Economic theory suggests that government intervention may improve welfare when (1) one party's action creates external benefits or costs for another, (2) a change in the level of the first party's action would change the amount of external benefit or cost, and (3) the value of this change to the second party exceeds the costs of changing the first party's behavior.[55]

Some forms of counterterrorism arguably involve significant externalities. The decision of one person, business, or organization to engage in counterterrorist measures could well make everyone else safer by deterring a terrorist attack on someone else. The fact that an office building is well-guarded, for example, may lessen the likelihood of terrorist attacks in the surrounding neighborhood. When people, things, or information flow through networks—such as airline, financial market, or computer networks—one network member's decision to adopt security measures can create costs or benefits for others.[56] If the party engaging in counterterrorism does not

[54] Cletus C. Coughlin, Jeffrey P. Cohen, and Sarosh R. Khan, "Aviation Security and Terrorism: A Review of the Economic Issues," *Federal Reserve Bank of St. Louis Working Paper,* 2002-009A: 7.
[55] James M. Buchanan and W. Craig Stubblebine, "Externality," *Economica* 29 (1962): 371-384.
[56] See, e.g., Coughlin, Cohen, and Khan (2002): 15-17, and D. Bruce Johnsen and Supriya Sarnikar, "Cybersecurity and the National Market System," in Alexander R. Woodcock and Christine Pommerining (eds.), *Critical Infrastructure Protection Program: Workshop II Working Papers* (Fairfax, VA: George Mason University Press, 2004): 49-61.

take these "spillover" benefits into account, then it may under-invest in counterterrorism. "Underinvestment" occurs *only if* additional counterterrorist measures would create additional positive spillover benefits and the value of these additional benefits exceeds the additional cost of producing them. Government can correct this problem by undertaking, requiring, or facilitating additional counterterrorist measures, up to the point where the additional benefits equal the additional costs.

Another plausible externality rationale applies in cases where terrorism causes widespread demoralization, in addition to its direct effects on the people or assets that get attacked.[57] Asset owners might not take these society-wide effects of terrorism into account when making their own decisions about security. If additional efforts could reduce these external effects by a large amount, then government could play a positive role.[58]

2C. Government Failure

Other forms of "market failure" may arise as a result of poor incentives or other constraints on private parties created by previously-existing policies. While such policy-driven problems are not technically "market" failures, such problems are likely to persist in the absence of some additional government action. The fundamental solution would be to correct the original policy. In some cases, however, decision makers will likely find that they must mitigate the effects of some policy that is unlikely to change in the foreseeable future.

Terrorism—especially large-scale terrorist events such as 9/11—provides some good examples of this kind of quandary. By paying $5 billion in compensation to airlines and $7 billion[59] to the victims after 9/11, the federal government effectively served as "insurer of last resort."[60] By creating a $10 billion loan stabilization fund for airlines, the government effectively served as a "lender of last resort."[61] While motivated by compassion (as well as a desire to let all concerned avoid endless litigation), such practices do somewhat diminish the incentives of airlines and the insurance industry to take precautions against terrorism. These specific policies were not in place prior to 9/11, but the federal government has a long tradition of providing disaster recovery assistance and bailing out

[57] Brooks and Button (2006): 103-04.
[58] Since the psychological costs of terrorism can be quite speculative, however, they need to be proven rather than just asserted.
[59] David Hechler, "Lawyer Who Made 9/11 Fund Work Looks Back," *Miami Daily Business Review,* December 27, 2004.
[60] Air Transportation Safety and System Stabilization Act, Public Law 107–42
[61] Air Transportation Safety and System Stabilization Act, Public Law 107–42.

businesses that "cannot" be allowed to fail. It was not unreasonable, therefore, for private parties to expect some kind of federal help.

The Transportation Security Administration's (TSA) provision of passenger and baggage screening has similarly diminished the incentives of airlines, airports, and the insurance industry to reduce terrorism risks, because the federal takeover shields these parties from liability for terrorist acts.[62] Ex post, the Air Transportation Security Act limited airlines' liability for 9/11.[63] If these kinds of policy-induced distortions are significant, then private parties may under-provide security. And if the government cannot credibly commit to changing these policies in the future, then some level of government will have to take some other action to counteract private parties' incentives to under-provide security.

Government efforts intended to remedy a market failure can also open the door to government failure. Public officials are neither benevolent nor omniscient; they can pursue their own self-interest just as individuals in the private sector. The incentives and information flows created by government institutions may prevent government officials from promoting the public interest. Regulation can solve problems, but it also creates winners and losers by distributing costs and benefits. Interest groups offer political support to government officials who will minimize group costs and maximize group benefits. Interest groups who are better organized and have more at stake are likely to be more effective at bending regulation to their liking. Regulation is likely to benefit small interest groups, with strongly-felt preferences, at the expense of the general public.[64] This occurs even when the stated goal of regulation is to promote some public interest goal, such as reducing terrorism. Indeed, sometimes interest groups may even ally themselves with vocal public interest advocates who are more concerned about the broad intentions of the regulation than the details of its implementation. Under cover of the broad public interest goal, the private interests get benefits that may actually harm the public interest, such as subsidies, restrictions on competition, or differential regulatory burdens.[65]

In proposing regulation to correct market failures, therefore, policy makers must take care to avoid creating even worse government failures. This does not mean that government regulation cannot have positive net effects, only that careful analysis is

[62] Aviation and Transportation Security Act, Public Law 107-71.
[63] Aviation and Transportation Security Act, Public Law 107-71.
[64] George J. Stigler, "The Theory of Economic Regulation," *The Bell Journal of Economics and Management Science* 2, No. 1 (1971): 3-21.
[65] Bruce Yandle, "Bootleggers and Baptists: The Education of a Regulatory Economist," *Regulation* (May/June 1983):12-16.

necessary to avoid creating solutions that are worse than the problems they are intended to address.

3. Identify the Uniquely Federal Role

"If this was easy it wouldn't be so hard."

—Yogi Berra

All levels of government, as well as individuals and communities, play important roles in protecting homeland security. Depending on the threat and the possible mitigation efforts to address it, responsibility for action may lie most appropriately with federal, state, and local governments, communities, individuals, or some combination of these. As the International Union of Public Transport recently noted,

> Recent terrorist attacks in Moscow metro and Madrid suburban rail show that public transport systems are vulnerable and potential targets for terrorists. It is clear that preventing and discouraging terrorist activities as such is the prime responsibility of national security agencies and similar bodies. Yet, the responsibility for the passengers requires public transport stakeholders to acknowledge the threat and to ensure the best possible level of prevention and preparedness.[66]

Broadly speaking, there are strong reasons for a federal role in homeland security. Federal regulation may be appropriate if state or local regulations would burden interstate commerce or compromise the rights of national citizenship. Travel among the 50 states is commonplace, so the costs individual states would incur to protect against terrorist entry would have benefits to citizens of other states. The public good characteristics of nonexcludability and nonrivalrous consumption apply to the entire country and do not end at state borders. Individual states and localities would arguably invest too little in counterterror measures if they bear the full costs, but the benefits accrued to the whole nation (or continent).

That's not to say that the federal government must provide, direct, or regulate all homeland security measures. Where both the costs and benefits are largely confined to a single state, then it is appropriate for that state to provide the funding and make the decisions. Federal authority should be involved when there are significant spillovers across state lines.

What kinds of activities are more appropriate for state or local governments? One example might be dissemination of preparedness information about potential threats and emergency plans. The state of California currently has a law pending

[66] Mohamed Mezghani and Andrea Soehnchen, "Public Transport and Anti-terrorism Security," International Union of Public Transport, Knowledge and Membership Services Department (November 15, 2005), http://www.uitp.com/mediaroom/2005/06/security-en.cfm.

that would "[require] the State Department of Education to electronically distribute disaster preparedness educational materials and lesson plans that are currently available to local education agencies. [The law would also require] the department to ensure that the materials are available in at least the three most dominant primary languages spoken by English learners in the state."[67] A great deal of dissemination of emergency information is best handled on a local rather than national level because of local knowledge that can be much more accurate. For example, the local level is much better at handling where to go in the case of an emergency, evacuation plans, or suggestions for provisions in case of an emergency. The spillover of these kinds of location-specific information does not necessarily help people in other states.

It is clear that the federal government's desire to fund most homeland security efforts in the US has decreased the incentive for states to provide the funding for their own homeland security. For example, Florida's 2003–2004 domestic security plan included as one of its guiding principles, "Maximize the use of federal funds." Federal programs were to fund almost all of the state's many homeland security efforts, except for the proposed agricultural safety programs.[68] Federal officials should take care to avoid crowding out state and local initiative.

4. Assess effectiveness of alternative approaches

"Steer, don't row."

—David Osborne and Ted Gaebler

The fact that market failure justifies *some* federal role does not mean that *any conceivable* federal role will do. Government has a wide variety of options to influence security outcomes. These include direct federal provision of security services, partnerships with the states, public-private partnerships, performance-based regulation, command-and-control regulation, information disclosure regulations, and ex post liability rules.

Government can often accomplish more when it chooses to "steer, not row,"[69] and counterterrorism is no exception. Experience shows that effective counterterrorism requires flexibility and deftness on numerous levels. That is not to suggest

[67] Assembly Bill No. 103, California Legislature 2005–06 Regular sessions, *Legislative Counsel's Digest*, last amended May 22, 2006, http://www.homeland.ca.gov/legislative.html.

[68] Florida Domestic Security Oversight Board, *Domestic Security Funding Recommendations Fiscal Year 2003–2004*, December 1, 2002, http://www.fdle.state.fl.us/osi/DomesticSecurity/Documents/FY0304fundingrecspackage.pdf.

[69] The phrase, popularized by David Osborne and Ted Gaebler, precisely captures the idea that government's main role is to articulate outcomes and find the most effective way of accomplishing them, rather than treating any particular means as sacrosanct. See David Osborne and Ted Gaebler, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector* (Boston: Addison-Wesley, 1992).

methods that are illegal or in violation of statutes and regulations; rather, we merely note that over-regulation by government agencies seeking to prevent terrorism may unwittingly provide an advantage to those seeking to attack our society. The question of how much and what kind of regulation takes on added significance in the case of counterterrorism since lives may be at stake. Private sector initiative is important in counter-terrorism, and the wrong kind of regulation, however well-intentioned, could smother this initiative. Responsible decisions, therefore, require consideration of alternative means to accomplish the same end.

In some cases, the effectiveness of different approaches is relatively easy to compare. The Government Accountability Office (GAO), for example, monitored the effectiveness of aviation security screening both before and after 9/11. This permits a comparison of the effectiveness of three different arrangements: private contractors paid by the airlines prior to 9/11, TSA screeners after 9/11, and private contractors employed by several airports under a pilot program permitted after 9/11. One investigation involved undercover audits by DHS. According to the DHS inspector general, federal airport security screeners after 9/11 performed no better in their ability to stop prohibited items from entering the "sterile" areas of airports than screeners before 9/11.[70] GAO examined two studies to assess the post-9/11 pilot program that allowed five airports in the US to use non-federal screeners. The GAO itself performed one investigation, and BearingPoint, under contract to the TSA, performed the other. Both studies found no evidence to conclude that privately hired screeners performed worse than federal screeners.[71] In fact, the BearingPoint study cited one airport, Kansas City, in which the private screeners performed better than the federal screeners.[72] The GAO and TSA investigations both suggest that private screeners under federal regulatory guidance provide screening at least as effectively as TSA employees.

A frequently-cited example of highly effective airline security is the Israeli airline, El Al. A traveler seeking to leave Israel's Ben Gurion airport must go through the following "checks" before boarding a plane: 1) Upon arrival at the outer perimeter of the airport, whether by private or public transportation, the individual will

[70] Richard L. Skinner, Acting Inspector General, US Department of Homeland Security, Senate Committee on Homeland Security and Government Affairs, January 26, 2005.
[71] Norman J. Rabkin, Managing Director, Homeland Security and Justice. House Subcommittee on Aviation, Committee on Transportation and Infrastructure, *Aviation Security: Private Screening Contractors Have Little Flexibility to Implement Innovative Approaches*, Thursday April 22, 2004. See GAO Report GAO-04-505T.
[72] Sara Kehaulani Goo, "Airport Screeners Do Poorly, Panel Told," *Washington Post*, April 23, 2004, http://www.secure-skies.org/Airport_Screeners.php.

be screened; if need be the car and the individual will be pulled aside for additional questioning and possible searching of the car, the passengers, and their belongings. 2) Upon arrival at the outer gate of the terminal, those seeking to enter will be observed by highly trained security personnel; the process includes both screening manifestly clear to the individual as well as unobtrusive behavior observation. 3) Upon entering the terminal, the individual will be similarly observed. 4) Prior to reaching the gate, the passenger will be asked a series of questions; the responses are scrutinized both by the individual asking and others who are observing the process. 5) After receiving a boarding pass from the gate agent, the passenger is asked to show both boarding pass and passport prior to approaching the carry-on and person scanner (similar to procedures at US airports), which completes the checking process. After being scanned, the passenger may proceed towards the gate. At all times, security personnel are observing the behavior of the passengers, whether noticed or not.

Though El Al operates in a dangerous area of the world and is an attractive symbolic target for terrorists, the airline has not had a hijacking since it instituted these security measures.[73] On August 10, 2006, when hundreds of flights to and from Heathrow airport were delayed due to the terrorist bomb plot, El Al's security procedures ensured that it had no trouble receiving permission to take off and land at Heathrow. The flight from Israel to London departed two minutes late at the height of the incident, and the flight from London to Israel departed on time.

As the Israeli and US examples demonstrate, there are many alternative ways to handle airline security with different levels of effectiveness (and, presumably, costs).

Sometimes agencies lack discretion to consider meaningful alternatives. For example, one DHS airline regulation requires that passenger and crew manifests be electronically delivered to the Bureau of Customs and Border Protection before the passengers land in the US. In this case, however, "[e]xploration of regulatory alternatives [was] limited during the rulemaking process" because legislation mandated the regulation.[74] In other words, Congress prohibited the agency from considering alternative means of accomplishing the goal. If legislators refuse to give the agency discretion, then Congress has a responsibility to examine the effectiveness of alternatives itself.

[73] El Al's only hijacking was in 1968 before current security measures were in place. See Vivienne Walt, "Unfriendly Skies are No Match for El Al," *USA Today*, Oct. 1, 2001.

[74] Bureau of Customs and Border Protection, "Electronic Transmission of Passenger and Crew Manifests for Vessels and Aircraft," *Federal Register* 70, No. 66 (April 7, 2005) p. 17846, http://web.nbaa.org/public/ops/intl/apis/apisfinalrule040705.pdf.

5. Identify Costs

"Our goal is to optimize our security, but not security at any price. Our security strategy must promote Americans' freedom, privacy, prosperity, and mobility."

—DHS Secretary Michael Chertoff[75]

Costs are not necessarily money. A decision to use resources in one way is a decision not to use them in some other way. The benefits that could have been achieved by using the resources in some other way are the "opportunity cost" of the decision.

The accurate measure of the cost of any regulation is its opportunity cost: what did we as a society give up in order to devote resources to enacting and complying with the regulation? Government and private expenditures only partially measure the opportunity cost. Sound regulatory analysis also identifies hidden and indirect costs that are less obvious than direct expenditures.

5A. Direct costs

The most obvious direct costs associated with homeland security are the funds spent by federal agencies responsible for security. The DHS budget for administering regulations is $19 billion in 2006.[76] This figure includes only those regulatory activities that are actually housed in DHS; the total would be higher if it included regulations from other agencies that may have an effect on terrorism or security.

Another direct resource cost is the money spent by various non-federal parties to comply with the regulations. A regulatory impact analysis performed by the Bureau of Customs and Border Protection gives one example of the estimated private costs due to counterterrorism regulation. The analysis covered four versions of a 2003-2004 regulation that requires advance electronic presentation of cargo information on any shipment arriving or departing the US by air, truck, rail, or sea. The analysis monetized five costs to private air cargo carriers: the implementation of a computer database system, costs due to delays, data entry costs, service degradation, and loss of revenue on passenger carrying operations. The estimated direct resource costs due to the computer database system and data entry costs add up to more than $2.5 billion.[77] The four versions of the regulation are all fairly similar—simply changing the severity of the regulation, not the means by which the government tries to prevent harm.

[75] DHS PAR 2005, 1.

[76] Dudley and Warren (2006), Appendix Table A-1.

[77] Bureau of Customs and Border Protection, Department of Homeland Security, "Regulatory Impact Analysis: Advanced Electronic Filing Rule," November 13, 2003, http://www.cbp.gov/linkhandler/cgov/import/communications_to_trade/advance_info/ria_electronic_filing.ctt/ria_electronic_filing.pdf.

Different versions vary the size of cargo that must be reported and the time at which the information must be reported. The costs of these different alternatives ranged from $269 million to $4.66 billion annually.[78]

El Al Airline's security measures are highly effective, but they also entail significant outlays. The airline spends approximately $100 million annually on security, of which the government reimburses approximately half. With 270 flights per week, that works out to about $7100 per flight. If airlines and the US government spent a similar amount per flight, airline security would cost approximately $79 billion annually—far more than this country currently spends.[79]

Clearly, counterterrorism regulation generates significant federal expenditures and non-federal compliance costs. But these direct, visible dollar outlays are not the only costs.

5B. Hidden/indirect costs

Government programs and regulations both contain hidden, indirect costs that economic analysis can help identify.

5C-1. Price distortions

When federal agencies and private firms spend money to enforce and comply with regulations, the money has to come from somewhere. Government, of course, gets money from taxes. Businesses and other entities, such as airports, ultimately have to get the money by charging customers. In both cases, the costs of regulation ultimately affect the prices that consumers pay for the things they buy.

When prices or taxes increase due to regulation, consumers pay more. In addition to these direct costs are the indirect costs that arise when consumers respond to the price increases by purchasing less of the products or services whose prices have increased. The value that this lost output would have created for consumers and producers is called the "deadweight loss" or "excess burden" associated with the tax or regulation.

Scholarly research finds that the deadweight loss associated with general taxation ranges from 25-40 cents per dollar raised.[80] An OMB "rule of thumb" assumes that the deadweight loss associated with federal taxation equals 25 percent of revenues.[81] Thus, the deadweight loss associated

[78] Bureau of Customs and Border Protection, Department of Homeland Security, "Regulatory Impact Analysis: Advanced Electronic Filing Rule," November 13, 2003, http://www.cbp.gov/linkhandler/cgov/import/communications_to_trade/advance_info/ria_electronic_filing.ctt/ria_electronic_filing.pdf.

[79] US airlines had approximately 11 million departures in 2004. See Air Transport Association, *Annual Report 2005*, 9, http://www.airlines.org/files/2005AnnualReport.pdf.

[80] Jerry Hausman, "Efficiency Effects on the US Economy from Wireless Taxation," *National Tax Journal* 53 (September 2000): 733-42.

[81] Office of Management and Budget, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, Circular No. A-94 Revised, Transmittal Memo No. 64, October 29, 1992, http://www.whitehouse.gov/omb/circulars/a094/a094.html.

with homeland security funding likely equals at least 25 percent of the expenditure, about $5 billion in 2006.

The deadweight loss associated with some security-related regulations, such as those affecting air travel, is likely much higher than the above calculation would imply, for two reasons. First, specific taxes on airline tickets fund some federal expenditures on airline security. Second, passengers ultimately pay the private expenditures on security in the form of higher ticket prices. Since much air travel is price-sensitive, a small increase in the price can create a big drop in ticket sales. Passengers forego the value that this air travel would have provided, and the aviation industry forgoes the contribution to fixed costs that these passengers would have made if they had purchased tickets.

Of the two fees that fund the TSA, the most well-known is often called the "9/11 fee." This is a $2.50 per enplanement fee with a maximum of $5.00 on a one-way trip ($10.00 roundtrip), and it shows up directly on customers' tickets. The less well-known fee, the Aviation Security Infrastructure Fee (ASIF), also funds the TSA. Each airline was surveyed after 9/11 to find out what its screening costs were before 9/11. The government then required that each airline pay this amount to fund the TSA's newly implemented screening. This fee does not show up as an add-on, but rather is incorporated into the price the passenger pays for the ticket. The amount paid by each airline is different and is confidential.[82]

The two fees collected from passengers and airlines totaled $1.9 billion in 2005.[83] That equates to approximately $2.75 per enplanement.[84] Since the average airline revenue per enplanement (minus the ASIF) equaled $122.50 in 2005, the security fees represent a 2.2 percent price increase. Ticket sales are quite sensitive to price; economic studies find that a 1 percent increase in ticket price leads to a 1 percent or larger reduction in ticket sales.[85] Therefore, the security fees reduced enplanements

[82] Air Transport Association Economics Section, "Special Taxes and Fees Levied on Commercial Aviation," February 1, 2006, http://www.airlines.org/econ/d.aspx?nid=4919.

[83] *Budget of The United States Government, Fiscal Year 2007*—Appendix, p. 484.

[84] An "enplanement" occurs whenever a passenger boards a plane. Thus, a passenger with a direct flight has two enplanements (one for each direction), while a passenger with a connecting flight has four enplanements (two for each direction). We use enplanements as our measure of output and revenue per enplanement as our measure of price, because both figures are readily available from the Air Transport Association's annual reports and the 9/11 fee is a charge per enplanement. Enplanements and passenger revenues are from Air Transport Association, *Annual Report 2005*, http://www.airlines.org/econ/d.aspx?nid=9052.

[85] For a list of elasticities of demand for air travel, see Table B-1 in Kenneth J. Button and Henry Vega, "The Taxation of Air Transportation," Center for Transportation Policy, Operations and Logistics (April 2005).

by approximately 16 million. A very rough calculation suggests that this created a deadweight loss of approximately $1.75 billion, nearly equal to the revenue raised.[86]

The budget of the Transportation Security Administration in 2005 was $4.3 billion. General revenues covered the $2.4 billion discrepancy. Using OMB's 25 percent rule of thumb, a deadweight loss of $600 million accompanied these revenues. Therefore, the total deadweight loss associated with TSA expenditures on air security regulation is about $2.35 billion.

5C-2. Service degradation

Indirect costs may also consist of effects on quality rather than price. It is well understood by anyone who travels that more time spent standing in lines and longer time at the airport decreases the quality of the trip. Numerous studies estimate the effect of security measures on the time passengers have to spend in airports.

Harumi Ito at Brown University and Darin Lee from the economic consulting firm LECG performed an analysis of the impact of the 9/11 terrorist attacks on air travel. They examined the percentage change in passenger volume on trips of different distances between the year ending June 2001 and the year ending June 2003. If weak demand for air travel following 9/11 were solely due to a weak economy, then passenger volumes should have fallen pretty uniformly, regardless of distance. In fact, the following table from their study shows that volumes declined much more dramatically on short-haul flights. The hassle to fly after 9/11 increased dramatically. It was easier for people to substitute other modes of transportation for short-haul flights than for long ones. Such a decline in short-haul traffic is unprecedented; the declines associated with the Gulf War recession were largely uniform across distance traveled.[87]

A White House Commission under President Clinton suggested numerous improvements for the air transport system in response to the crash of TWA Flight 800 in 1996. Although the crash was never determined to have been due to terrorism, the commission directed many of the

[86] Assuming a linear demand curve and constant elasticity of demand, the deadweight loss to consumers is approximately equal to .5ΔpΔq, and the change in producer welfare is approximately equal to Δq(p-m), where m is the marginal cost of one additional enplanement. The elasticity of demand is defined as (Δq/q)/(Δp/p). If one has an estimate of the elasticity and also the values of p, Δp, and q, then one can solve for Δq and use it to calculate the deadweight losses of consumers and producers. In our calculation, Δp=$2.75, q (enplanements)=698 million, p=$122.75 (passenger revenues/enplanements), and the elasticity of demand=1, yielding a Δq=15.7 million enplanements. We assume marginal cost equals 10 percent of revenues. A spreadsheet with more extensive details on calculations is available upon request from the authors.

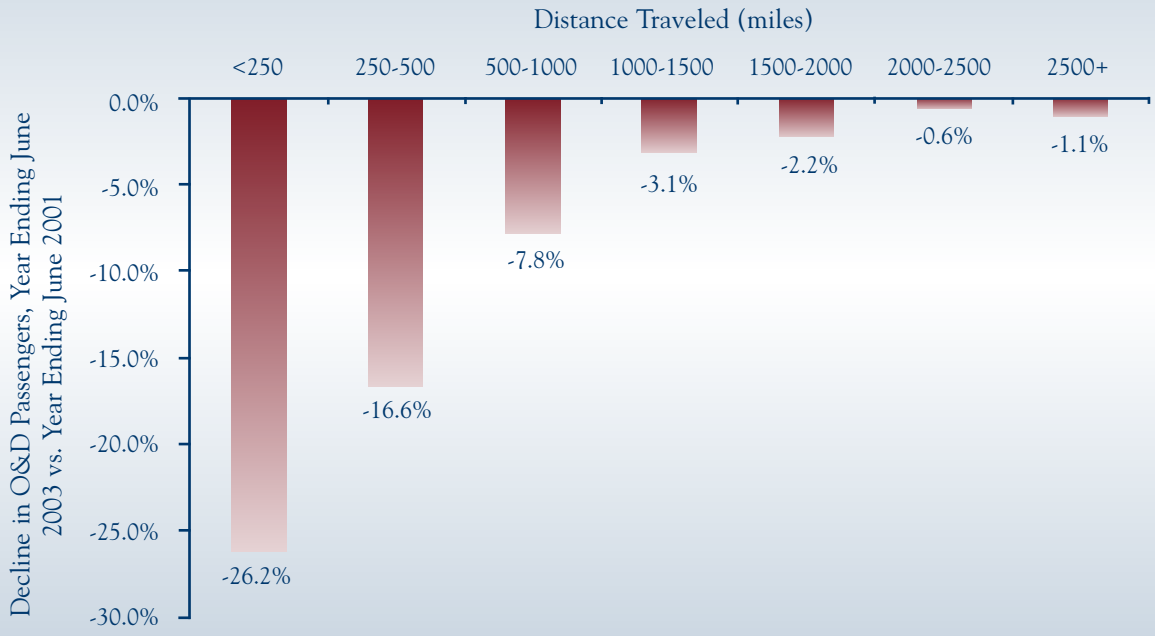
[87] Harumi Ito and Darin Lee, "Assessing the Impact of the September 11 Terrorist Attacks on US Airline Demand," *Journal of Economics and Business* 57:1 (2005): 75-95.

57 suggestions at improving air transport security. A 1997 analysis by Robert Hahn found that the additional 30 minutes of wait time recommended by the Federal Aviation Administration to implement additional security measures cost airline passengers $8-10 billion per year due to additional time spent at the airport. This cost estimate is for additional wait time due to the security measures put in place in 1996, well in advance of 9/11.[88]

TSA assumes that post-9/11 security measures at airports lead to 10 additional minutes of travel time on average. The Department of Transportation assumes passengers flying on

FIGURE 1

VOLUME ON SHORT TRIPS DECLINED MORE



Source: Harumi Ito and Darin Lee, "Assessing the Impact of the September 11 Terrorist Attacks on US Airline Demand," *Journal of Economics and Business* 57:1 (2005): 75-95.

[88] Robert W. Hahn, "The Economics of Airline Safety and Security: An Analysis of the White House Commission's Recommendations." *Harvard Journal of Law and Public Policy* 20:3 (Summer 1997): 791.

business value their time at $40 per hour and passengers flying for personal reasons value their time at $33 per hour.[89] Assuming the equivalent of 453.93 million one-way trips[90] taken on domestic flights, a back-of-the-envelope calculation would yield a total extra travel time cost of $2.76 billion in 2005.[91]

These costs seem small compared to the time cost associated with El Al's pervasive screening. Passengers typically need to arrive at the airport three hours before the flight—compared to the usual two hours for international flights on other airlines and one hour for domestic US flights. In the US, an additional hour of time per passenger would entail a cost of $16.6 billion, assuming 454 million trips.

Some of the US security numbers may, however, be significant underestimates. Government averages of additional time needed for the security measures often ignore the fact that wait times are highly variable, depending on the airport and time of day.[92] Therefore, people often come to airports much earlier than sometimes necessary to make sure they have time to board their flight. Employing TSA data from 2004-05, *USA Today* calculated that average wait times at the 15 busiest airports were seldom more than five minutes long. However, the maximum wait could be as long as 133 minutes (Los Angeles), 120 minutes (Atlanta), or 100 minutes (Ft. Lauderdale).[93] The variability in waiting time can lead to a longer time at airports for passengers, thus generating a higher cost estimate.

Quality distortions were also a major cost considered in the Bureau of Customs and Border Protection's analysis of its regulation requiring advance electronic presentation of cargo information. A major degradation of service to scheduled cargo carriers occurs due to the need to delay flights or hold them on the ground. Shippers then need to hold larger inventories due to the volatility in transport times. The cost estimate to "perishables ranges from $46 per ton for a 30-minute delay to $181.14 per ton for a two-hour delay; the cost of non-perishables is estimated to range from $6.90 per ton to $27.70 per ton."[94]

[89] In year 2000 dollars. See US Department of Transportation, Office of the Secretary of Transportation, "Revised Departmental Guidance, Valuation of Travel Time in Economic Analysis," February 11, 2003.

[90] An enplanement occurs when a passenger boards an aircraft—originating or connecting. It is necessary to adjust the 635.5 million domestic enplanements because 40 percent of one-way trips contain two or more enplanements. The passengers would not go through security more than once.

[91] Calculation was performed using an average value of passenger time of $36.50 per hour.

[92] Robert Poole, "Airport Security: Time for a New Model," *Reason Policy Study* 340 (2006).

[93] Thomas Frank, "Checkpoint or Chokepoint?" *USA Today*, July 14, 2005.

[94] Bureau of Customs and Border Protection, Department of Homeland Security, "Regulatory Impact Analysis: Advanced Electronic Filing Rule," November 13, 2003, http://www.cbp.gov/linkhandler/cgov/import/communications_to_trade/advance_info/ria_electronic_filing.ctt/ria_electronic_filing.pdf.

Customs' regulatory analysis calculates these costs assuming known delays; volatile and uncertain delays are much more costly.

5C-3. Increased risks

Regulation also involves tradeoffs between different types of risks. One cost of reducing terrorism risk could well be an increase in some other type of risk that threatens life and safety.

Airline security provides a notable case in point. Federal passenger and baggage screening have increased both the monetary cost of air travel, due to higher ticket prices, and the nonmonetary costs, due to longer delays and waiting times at airports. Travelers have responded by substituting automobile travel for air travel—particularly on shorter routes. Statistically, auto travel is much more dangerous than air travel; per mile, the risk of fatality is 8.9 times greater.[95] A study by University of Maryland economists Adriana Rossiter and Martin Dresner estimates that the 10-minute increase in wait time assumed by the TSA and a security fee of $2.50 per flight segment will lead to an additional 66.2 additional highway deaths per year.[96]

Another study by Garrick Blalock, Vrinda Kadiyali, and Daniel Simon from Cornell University estimates the decreased demand for air travel due to the costs of airport baggage screening. They find that a decrease of one million enplanements results in 15 more driving fatalities. They combine this figure with their estimate of how many people substituted driving for flying due to the inconvenience of baggage screening, finding that "in the 4th quarter of 2002 approximately 116 individuals died in automobile accidents which resulted from travelers substituting driving for flying."[97]

Robert Hahn, in his 1997 paper, also estimates the number of highway deaths attributable to more costly security measures. He estimates that a 30 minute delay increase at airports would

[95] Using average yearly data from 1992-2001 from the National Transportation Statistics (US Bureau of Transportation Statistics, 1992-2001) and the Aviation Accident Statistics cited in Adriana Rossiter and Martin Dresner, "The Impact of the September 11th Security Fee and Passenger Wait Time on Traffic Diversion and Highway Fatalities," *Journal of Air Transport Management* 10 (2004): 227-232. Some research finds that air passengers who diverted to automobile travel are probably safer than average drivers; the diverted air passenger is only 76 percent as likely to be involved in a fatal accident as the average driver. See L. Evans, M.C. Frick, and R.C. Schwing, "Is it Safer to Fly or Drive?" *Risk Analysis* 10 (1990): 239-246.

[96] Rossiter and Dresner (2004): 227-232. If the assumptions and parameters of their equation are varied, the number of additional deaths due to automobile travel can range from 1.0 to 99.3.

[97] Garrick Blalock, Vrinda Kadiyali, and Daniel H. Simon, "The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel," (February 23, 2005), http://ssrn.com/abstract=677563.

generate between 30 and 140 more fatalities per year.[98]

Michael Sivak and Michael Flannagan from the University of Michigan Transportation Research Institute argue that, after 9/11, there wasn't simply a shift from flying to driving, but a shift from long distance travel to more local travel. Their main finding was that there were 1018 more traffic fatalities in October-December 2001 than would normally be expected—an 8.8 percent increase over the expected frequency. However, rural interstates contributed only 1 percent of the increase in fatalities. If people were simply substituting flying for driving to the same destinations, there would be more deaths on interstate rural highways. There was also a marked increase in pedestrian and bicyclist fatalities, pointing towards the authors' argument that 9/11 resulted in not just a simple modal transfer from flying to driving on interstates, but a shift from flying to other alternatives such as local travel.[99]

Terrorists kill, but so can safety precautions. Zero risk is unattainable. Even in a wealthy country like the United States, not every policy that reduces the risk of terrorism makes society safer overall. Sound counterterrorism decisions require careful analysis of all risks, not just the risk the regulation is intended to reduce.

6. Compare Costs with Outcomes

"Everyone is entitled to his own opinion, but not his own facts."

—Sen. Daniel Patrick Moynihan

Cost information cannot be considered in isolation. A costly regulation may nevertheless create significant positive outcomes that are valuable to policy makers and citizens. Airline security, for example, costs billions of dollars per year, but the 9/11 attacks may well have cost America $100 billion or more. Cost-effective airline security is likely a bargain.

Information on outcomes and costs can be combined in a variety of ways to aid decision making. Three key examples are cost effectiveness analysis, cost-benefit analysis, and breakeven analysis

6A. Cost effectiveness analysis

Cost effectiveness analysis facilitates choice among alternative ways of achieving the same outcome. Decision makers will likely find a wide variety of initiatives that seek to accomplish the same outcome employing widely different means. Improving governmental effectiveness requires analysts to express outcomes in comparable units (such as lives saved or injuries avoided) and rank different programs and regulations according to

[98] Hahn (1997): 806.

[99] Michael Sivak and Michael J. Flannagan, "Consequences for Road Traffic Fatalities of the Reduction in Flying Following September 11, 2001," *Transportation Research Part F* (2004): 301-305.

their cost effectiveness. Activities judged less effective should either be reformed or discontinued, so that resources can be reallocated to the programs and regulations that are more effective. Activities that are actually counterproductive should be discontinued as soon as possible—both to save resources for effective activities and to prevent further damage.

The FDA's analysis of alternative versions of a recordkeeping rule intended to prevent foodborne illnesses provides a good example of cost effectiveness analysis.[100] The FDA considered the costs and outcomes (number of avoided illnesses) under multiple alternative versions of the regulation. Three instructive ones are exemption of very small entities, exemption of small entities

Table 2

Projected Results of Alternative Food Recordkeeping Rules

Option	Annualized cost	Annual Illnesses averted	Average cost per averted illness	Incremental cost per illness averted
Exempt very small entities	$30,610,378	1067	$28,688	$28,688
Exempt very small grocers (Final Rule)	$132,750,092	1204	$110,258	$745,545
No small entity exemption	$244,134,086	1282	$190,432	$1,428,000

Source: Food and Drug Administration, Human Health & Services, Final Rule "Establishment and Maintenance of Records Under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002," December 9, 2004, 69 *Federal Register* 71562-71655. Option H, Final Rule, and Adjusted Comprehensive Figures taken from Table 18, 71645.

[100] Food and Drug Administration, Human Health & Services, Final Rule "Establishment and Maintenance of Records under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002," December 9, 2004, 69 *Federal Register* 71562-71655.

only in the grocery sector, and no exemption for small entities.[101] All three options are projected to be effective; that is, all three would avoid rather than cause illnesses. But their cost effectiveness—indicated by the average and incremental cost per illness avoided—differs significantly.

The difference is especially noteworthy when one considers that the FDA examined multiple variations on the same basic recordkeeping regulation. Legislators generally have much wider discretion than administrative agencies to consider alternative ways of accomplishing the same outcome. As a result, analysis of different regulations issued by different agencies pursuant to different legislation will likely exhibit even wider variations in cost effectiveness. When this occurs, policy makers have significant opportunities to improve the overall effectiveness of regulation by focusing resources on the most cost effective measures.

6B. Cost-benefit analysis

Cost-benefit analysis translates the costs and outcomes into a common metric (usually money) to aid comparison. This requires attaching a monetary value to various outcomes that may be difficult to monetize, such as lives saved or injuries avoided. The practice generates a great deal of controversy, and sometimes even moral outrage, directed at the idea that human life or the quality of life could ever be translated into a monetary value. In reality, people frequently behave as if they place a monetary value on their lives when they decide to engage in various risky activities. The soundest form of cost-benefit analysis assumes that the monetary value of benefits is the monetary value implied by decisions that real people actually make.[102]

6C. Breakeven analysis

In some cases, analysis may generate a reasonably reliable estimate of costs, but significant likely benefits cannot be quantified. Instead of ignoring the unquantified benefits, analysts can use "breakeven analysis" to calculate how large the unquantified benefits would need to be in order to justify the costs.[103]

The FDA food recordkeeping rule again provides an illustrative example. The FDA did not calculate the net benefits of its rule and the alternatives, but did provide sufficient data for us to do so. Using the higher benefit values FDA

[101] The legislation itself exempts restaurants and farms—two notable provisions that seem to undermine the effectiveness of any regulation intended to safeguard the food supply.

[102] Office of Management and Budget, *Regulatory Analysis*, Circular No. A-4, September 17, 2003, 2, http://www.whitehouse.gov/OMB/circulars/a004/a-4.pdf. The document also notes that if "revealed preferences" methods (based on actual human decisions) are not available, stated preference or benefit-transfer methods can be used.

[103] OMB Circular No. A-4, p.2.

Table 3

Projected Net Benefits of Alternative Food Recordkeeping Rules

Option	Annualized cost	Net Benefit (low)	Net Benefit (medium)	Net Benefit (high)
Exempt very small entities	$30,610,378	(23,344,108)	(15,797,217)	(8,251,393)
Exempt very small grocers (Final Rule)	$132,750,092	(124,550,852)	(116,034,960)	(107,520,272)
No small entity exemption	$244,134,086	(235,403,666)	(226,336,080)	(217,269,776)

Source: Authors' calculations.

presents, we calculated the following net benefits.[104] As the table indicates, all the scenarios FDA considered result in quantified costs that exceed quantified benefits.

These estimates understate the expected benefits of the rule because FDA only quantified and assigned monetary values to accidental outbreaks, what it refers to as "food safety benefits," but not intentional contamination, or "food security benefits."

Given the information FDA has provided, it is possible to calculate what the value of the food security benefit would have to be in order for the rule to be cost-effective. This break-even analysis suggests that for FDA's final rule to be cost-effective, the value of avoided

[104] FDA derives cost of illness estimates based on a value of a statistical life of $5 million and $6.5 million, and we use $6.5 million in this table. See FDA, Final Rule, p. 71622.

bioterrorist attacks on the nation's food supply would have to be between $108 million and $125 million each year. To justify the less costly alternative to the rule, which would have excluded all small entities from the recordkeeping requirements, the value of avoided bioterrorist attacks would have to be between $8 million and $23 million.

6D. What if information is incomplete?

Sound regulatory analysis should produce information that lets decision makers compare regulatory alternatives along various dimensions, including effectiveness, cost effectiveness, and overall net benefits. Where such information is incomplete, the analysis can still be informative.

For example, a careful assessment of the evidence of market failure can help identify the root causes of problems and identify solutions that are most likely to be effective even if information on costs and benefits is scant. Even partial information about benefits and costs may suggest that a regulation is highly likely to benefit citizens on net—or not. Breakeven analysis can suggest how large the unquantifiable benefits of a regulation would need to be in order to outweigh the costs. Careful examination of unintended consequences may reveal that some regulations are unlikely to accomplish their intended goals and others are more likely to be effective. Explicit articulation of desired outcomes and performance measures provides a benchmark that can be used to evaluate whether a regulation does indeed accomplish the intended goals.

CONCLUSION

Many analysts and decision makers have called on government to prioritize security initiatives based on risk assessment and cost effectiveness. Few, however, have explained why a comprehensive regulatory analysis framework is necessary to accomplish this. We believe a thorough focus on risk assessment and cost effectiveness requires all six elements of the regulatory analysis framework, for the following reasons:

1. Identify the desired outcomes. If government does not specify the desired outcomes, then there are no concrete goals to guide action. Outcomes defined in terms of risk reduction and damage mitigation provide realistic benchmarks that measure the real benefits citizens receive from counterterrorism regulations.

2. Assess evidence of market failure. Understanding the specific reasons that private action is insufficient and government action is necessary helps decision makers identify *why* people and assets are at risk. If we know why people and assets are at risk, we can better craft solutions that actually stand a chance of protecting them.

3. Identify the uniquely federal role. Multiple levels of government, businesses, civil society, and individuals all have security responsibilities. To ensure that the most critical jobs get done, each should focus on what it is uniquely situated to do.

4. Assess effectiveness of alternative approaches. Experience shows that different regulations can accomplish the same or similar goals with vastly different levels of effectiveness. The relevant decision makers—regulators or legislators—should seek the most effective means of accomplishing the goal.

5. Identify costs. A decision to adopt a regulation is a decision to use government and private resources in one way instead of another. To ensure that resources are used most effectively, decision makers should be conscious of the foregone benefits, or "opportunity costs," associated with each alternative.

6. Compare costs with outcomes. Some security regulations will necessarily involve the sacrifice of other values identified with the American way of life. Citizens may have to forego some money, time, privacy, or freedom in order to prevent or mitigate the damage from terrorist attacks. When calling for such sacrifices, government owes citizens a transparent accounting of how much the sacrifice improves security and at what cost.

About Frederic Sautet, editor

Frederic Sautet is a senior research fellow at the Mercatus Center at George Mason University. Prior to joining Mercatus, Frederic was a senior economist at the New Zealand Commerce Commission and a senior analyst at the New Zealand Treasury where he focused on economic transformation, entrepreneurship, utility development, and tax policy. Frederic holds a doctorate in economics from the Université de Paris Dauphine and did the course work for his doctorate at the Institut des Etudes Politiques in Paris. He also studied at New York University as a post-doc. Frederic's current work focuses on entrepreneurship, institutions, and social change.

About the Mercatus Center

The Mercatus Center at George Mason University is a research, education, and outreach organization that works with scholars, policy experts, and government officials to connect academic learning and real world practice.

The mission of Mercatus is to promote sound interdisciplinary research and application in the humane sciences that integrates theory and practice to produce solutions that advance in a sustainable way a free, prosperous, and civil society. Mercatus's research and outreach programs, Capitol Hill Campus, Government Accountability Project, Regulatory Studies Program, Social Change Project, and Global Prosperity Initiative, support this mission.

The Mercatus Center is a 501(c)(3) tax-exempt organization. The ideas presented in this series do not represent an official position of George Mason University.

About the Mercatus Policy Series

The objective of the Mercatus Policy Series is to help policy makers, scholars, and others involved in the policy process make more effective decisions by incorporating insights from sound interdisciplinary research. The Series aims to bridge the gap between advances in scholarship and the practical requirements of policy through four types of studies:

- **Policy Primers** present an accessible explanation of fundamental economic ideas necessary to the practice of sound policy.
- **Policy Resources** present a more in depth, yet still accessible introduction to the basic elements of government processes or specific policy areas.
- **Policy Comments** present an analysis of a specific policy situation that Mercatus scholars have explored and provide advice on potential policy changes.
- **Country Briefs** present an institutional perspective of critical issues facing countries in which Mercatus scholars have worked and provide direction for policy improvements.

Mercatus Center
George Mason University

3301 North Fairfax Drive
Arlington, Virginia 22201
Tel: (703) 993-4930
Fax: (703) 993-4935