

# 6

## PRINCIPLES FOR PROVIDING AND FINANCING HOMELAND SECURITY

Now that we have outlined a specific homeland security agenda, the next question to address is who should implement and pay for the proposed measures? The basic issue here is which measures should be the responsibility of the federal, state, and local governments, on one hand, and the private sector, on the other. We provide some broad principles in this regard but emphasize that specific policy responses depend on the sector and institutional setting (see chapters 2–5 for the policy steps relevant in each setting).

Assigning responsibility for homeland security, as in other areas, can be problematic because the desire to be fair may be inconsistent with the desire to provide sound incentives. For example, federal financing of private sector antiterrorism measures may strike some Americans as fair but could also lead policymakers to adopt unnecessarily expensive measures. At the same time, some forms of federal financing could strike Americans as unfair but could play a crucial role in encouraging appropriate levels of investment in security. Policymakers must therefore strike a balance between fairness and cost-effectiveness, and the balance will likely vary from sector to sector. Moreover, given the

uncertainties involved and the constantly changing nature of the potential threat, policymakers are best advised to experiment with alternative approaches and to learn incrementally from experience. Flexibility, especially as new risks manifest themselves and experience accumulates, is likely to be essential to an effective response to terrorism.

Nonetheless, the nation must start somewhere, and we suggest several principles for guiding the initial steps in the four general areas described in the preceding chapters: minimizing terrorist access to the country, tracking terrorists and limiting access to dangerous materials within the country, protecting key sites and activities within the United States, and reducing the toll from any attacks that do occur. As mentioned earlier in this volume, minimizing terrorist access to the country and reducing the costs of any attacks that do occur are primarily governmental functions, as is the tracking of potential terrorists domestically.<sup>1</sup> The principal questions with respect to these categories, therefore, are what level of government should undertake the measures and whether that same level of government should finance them.

Some of the thorniest issues, however, revolve around preventive activities and the protection of key sites within the United States. Inhibiting access to dangerous materials and protecting domestic sites, in particular, raise difficult questions. Why should the government be involved in protecting private property and activities within the United States against terrorist attacks, how should it be involved, and who should pay for the required security measures?

These are all complex issues, but we stress two points in this chapter: (1) some government action is necessary in order to provide appropriate protection against terrorist attacks on private property within the United States, and (2) the various users, providers, and owners of the property or activity should generally pay for the costs associated with the additional security. Furthermore, in most cases, the action should take the form of performance-oriented mandates on the private sector, perhaps coupled with insurance requirements or incentives, rather than direct subsidies or tax incentives. This approach, although imperfect, best balances the various trade-offs currently facing policymakers in designing cost-effective and equitable protection against terrorist threats in private sector settings. As explained later in the chapter, the purpose of the “stakeholder-pays”

approach is to discourage activity in the most dangerous settings, ensure that security measures are not gold-plated, discourage excessive rent seeking (that is, an intense pursuit of excess profits through government protection or other means), and promote innovation in antiterrorism security.

We also suggest how to implement and finance antiterrorism steps in public institutions, such as public hospitals or the local police force. In our opinion, the federal government should finance those steps that specifically and primarily address terrorist threats. But state and local governments should finance any such measures that carry substantial benefits within their own jurisdictions (in addition to affecting their ability to prevent or address terrorist attacks). The larger the local benefit of a specific measure in relation to the antiterrorism benefit, the larger the local and state share of the costs should be. Thus the federal government should finance specialized antiterrorism training and equipment for police and fire departments, but it should not finance the hiring of additional police or firefighters.

### **An Efficient Response to Terrorist Threats in the Private Sector**

This section examines antiterrorism measures in largely private sector settings, such as commercial buildings, athletic arenas, or commercial travel. Government policies toward such measures should reflect several offsetting considerations, including the “external” effects terrorist acts create beyond the impacts on their immediate targets, the need to avoid excessive costs in achieving any given level of protection against terrorism, the potential for innovation in providing security, and the fairness of different approaches.

#### *Externalities, Market Failures, and the Need for Government Intervention*

The first question that arises here is why government intervention is needed at all. Indeed, a top official at the Environmental Protection Agency recently argued that a federal counterterrorism security standard for chemical plants or refineries may be unnecessary because the “industry has a very powerful incentive to do the right thing. It ought to be their worst nightmare that their facility would be a target of a terrorist act because they did not meet their responsibility to their community.”<sup>22</sup> Individuals and corporations do

indeed have powerful incentives to protect themselves against terrorist attacks.<sup>3</sup> But why is that *private* motivation not sufficient to provide an optimal amount of protection for *society* as whole?

There are at least six potential justifications for government intervention.

First, security against terrorism involves a negative externality. For example, loose security at a chemical facility can provide terrorists with the materials they need for an attack. Similarly, poor security at a biological laboratory can provide terrorists with access to dangerous pathogens. The costs that follow from allowing terrorists to obtain access to such materials and successfully carry out attacks are generally not borne by the facilities themselves. Such a negative externality provides a compelling rationale for government intervention to protect highly explosive materials, chemicals, and biological pathogens even if they are stored in private facilities.<sup>4</sup> More broadly, a negative externality can arise wherever the security of one firm is adversely affected by poor security at another firm. In the presence of such negative externalities, private markets will undertake less investment in security than would be socially desirable. Individuals or firms deciding how best to protect themselves against terrorism are unlikely to take the external costs of an attack fully into account and therefore will generally provide an inefficiently low level of security against terrorism on their own.<sup>5</sup> Without government involvement, private markets will thus typically underinvest in antiterrorism measures.<sup>6</sup>

Second, a significant terrorist attack not only causes material damage, but also undermines the nation's sovereignty by exposing our vulnerability. It may also embolden other terrorists or adversaries, and hinder our ability to carry out an intended agenda. In this case, the associated costs may be difficult to quantify, but are nonetheless real. In other words, the costs of a terrorist act extend well beyond the immediate areas and people affected to the entire nation.

Third, government intervention can be justified by the cost and difficulty of accurately evaluating security measures. One reason that governments promulgate building codes, for example, is that it would be too difficult for each individual to evaluate a building's structural soundness before deciding whether to enter it. Since it would also be difficult for the individual to evaluate how well the building's air intake system could filter out potential bioterrorist attacks, the same logic could suggest that the government

should set minimum antiterrorism standards for buildings if there were a nontrivial threat of a terrorist attack on the relevant type of building (so that the individual would have some interest in ensuring that the building was protected against biological attack). Similarly, it would be possible, but inefficient, for each individual to conduct extensive biological antiterrorism safety tests on the food that he or she was about to consume. The information costs associated with that type of system, however, make it much less attractive than a system of government regulation of food safety.

Fourth, corporate and individual financial exposure to the losses from a major terrorist attack are inherently limited by the bankruptcy laws. To illustrate, assume that there are two types of possible terrorist attacks on a specific firm: a very severe attack and a somewhat more modest one. Under either type of attack, the losses imposed would exceed the firm's net assets, the firm would declare bankruptcy, and therefore the extent of the losses beyond that which would bankrupt the firm would be irrelevant to the firm's owners. Since the outcome for the firm's owners would not depend on the severity of the attack, the firm would have little or no incentive to reduce the likelihood of the more severe version of the attack even if the required preventive steps were relatively inexpensive. From society's perspective, however, such security measures may be beneficial, and government intervention can therefore be justified to address catastrophic possibilities in the presence of the bankruptcy laws.

Fifth, the private sector may expect the government to bail it out should a terrorist attack occur. (The financial assistance to the airline industry provided by the government following the September 11 attacks provides just one example of such bailouts.) Such expectations create a moral hazard problem: they lead private firms to neglect undertaking as much security as they otherwise would.<sup>7</sup> If the government cannot credibly convince the private sector that no bailouts will occur after an attack, it may have to intervene before an attack to offset the adverse incentives created by the expectation of a bailout.

Sixth, government intervention may be necessary in the face of incomplete markets. The most relevant examples involve imperfections in capital and insurance markets. In the latter case, if insurance firms are unable to obtain reinsurance coverage for terrorism risks (that is, if primary insurers are not able to transfer some of the risk from terrorism costs to other insurance

firms in the reinsurance market), some government involvement may be warranted. In addition, certain types of activities may require large-scale coordination, which may be possible but difficult to achieve without governmental intervention.

The importance of these six factors varies from situation to situation. Furthermore, the benefits of government intervention must be weighed against the costs of government failure, where the government intervention may do more harm than good. Even if an omniscient government could theoretically improve homeland security in a manner that provides larger benefits than costs, it is not clear that real-world governments (suffering from political pressures, imperfect information, and skewed bureaucratic incentives) would do so. Furthermore, the potential for government failure depends on the characteristics of the government agency and the sector involved. For example, it seems plausible that government failure is a particular danger in innovative and rapidly evolving markets.<sup>8</sup>

Both the need for government intervention and the potential costs associated with it thus vary from sector to sector, as should the policy response. But in general, it seems that we cannot just “leave it up to the market” in protecting ourselves against terrorist threats. The market has an important role to play, but government intervention in some form and in some markets will be necessary to fashion the appropriate response to terrorism.

### *Judging Measures to Reduce the Costs of Terrorism*

The need for some sort of government action to provide appropriate protection for private property and individuals against terrorism does not define how or in which situations the government should intervene. The various tools that the government could employ, furthermore, will likely determine how costly the intervention will be, as well as who will bear those costs. For example, to improve safety in commercial buildings, the government could

—*Impose direct regulation.* The federal government could require that certain antiterrorist features be included in any commercial or public building.<sup>9</sup>

—*Require insurance.* The federal government could require every commercial or public building to carry insurance against terrorism (much as state governments now typically require motorists to carry some form of

auto liability insurance).<sup>10</sup> The logic of such a requirement is that insurance companies would then provide incentives for buildings to be safer.

—*Provide a subsidy for antiterrorism activities.* The federal government could provide a subsidy—through direct government spending or through a tax incentive—for investing in antiterrorism building features or for other steps to protect buildings against attacks.

More broadly, each of the various approaches for minimizing the dangers and damages related to terrorism likely entails a different level of aggregate costs, and also a different distribution of those costs across sectors and individuals.<sup>11</sup> Cost-effectiveness is important because it reduces the economic burden of achieving any given level of security (see box 6-1).

The traditional approach to evaluating the various governmental approaches to improving homeland security would involve cost-benefit analysis, under which the costs and benefits of the various approaches would be compared and the one with the largest net benefits would be favored. In the terrorism context, however, the value of traditional cost-benefit analysis is not obvious. For example, given our current state of knowledge, it does not appear to be possible to determine with precision the quantitative benefits of any given tool, that is, to determine by precisely how much it reduces the risk of any potential terrorist attack (or the extent to which the action limits the damages any attack may cause).<sup>12</sup>

How then, should, policymakers decide which of these tools is more appropriate in any given situation? Realizing the difficulty of the task, we suggest that the applicability of any particular policy to any particular type of terrorist risk in private sector settings be judged according to at least the following (somewhat related) criteria. The criteria highlight the importance of incentives, which are central to fashioning cost-effective government intervention in the private sector, and fairness:

- To what degree would the tool affect private behavior?
- To what degree would the change in private behavior reduce the overall risk from terrorist activity, as opposed to merely shift it from one venue to another?
- How well will the government make decisions in this area, and how well will it avoid imposing unnecessary costs?
- How fair is the expected outcome? Will society accept the consequences in terms of income or wealth distribution?

**Box 6-1. *The Economic Impact of the Homeland Security Effort and Terrorist Attacks***

The measures we propose in previous chapters would involve federal costs of roughly \$45 billion a year and up to \$10 billion in private-sector costs.

These increased security efforts will reduce measured economic output, because they will displace both capital and labor from activities that would produce final goods and services. Improved security is not recorded in the national accounts, so spending \$1 on equipment that improves security rather than \$1 on equipment that makes goods will ultimately reduce measured economic activity. In other words, because we will be investing more in security, we will be investing less in other productive capital, while also diverting workers from activities that raise measured output and into security-related activities. (Note that insurance premiums should generally be counted as a cost of the homeland security effort only to the extent that they are not actuarially fair; actuarially fair premiums represent a transfer of resources, not an overall resource cost.)

The homeland security effort could reduce both the level of output and its growth rate over time. For example, delays in the transportation system associated with improved security and the initial diversion of both labor and capital into security activities could reduce real output levels by between 0.3 and 0.5 percentage points. But to the extent that providing a given level of security requires a growing share of inputs over time, the effort would also reduce productivity growth rates over time. Evidence from capital expenditures on pollution abatement equipment, which peaked at the equivalent of more than \$100 billion per year, suggests that the homeland security effort may reduce measured real growth rates by 0.1 percentage point or less per year.

Careful design of government regulations and scrutiny of the government's own spending on homeland security to ensure its cost-effectiveness can reduce the economic burden of achieving homeland security. Given the national income accounting system, government expenditures on homeland security will contribute to measured GDP. Nonetheless, such expenditures may still produce indirect economic costs and lower levels of productivity relative to what would have otherwise occurred (either by crowding out more productive government expenditures or by reducing national saving). That is precisely why the principles delineated in this chapter and the more detailed recommendations made in previous chapters are intended to produce a cost-effective approach to homeland security. (It is worth noting in this regard that the government does not currently track security spending by private firms. Given the increased importance associated with security measures, it is important to know how much is being spent on such activities. The Bureau of Economic Analysis, within the Department of Commerce, should create a supplemental account to the National Income and Product Accounts to track such spending.)

Such costs must be weighed against the costs of the terrorist attacks they

help to prevent. The September 11 attack, for example, imposed economic costs of perhaps \$100 billion or so. Other attacks could prove even more costly if they involved larger losses of life or more prolonged interruptions to economic activity.

Examining the costs of September 11 in more detail may be illuminating as a guide to the benefits of an effective homeland security strategy. The costs from the terrorist attacks have two main components: the direct loss of physical and human capital as a result of the attack, and the macroeconomic costs caused by the interruption to normal business activities. (Note that a small component of the macroeconomic loss reflects the loss in physical and human capital from the attack, so that there is a small element of double counting in this approach.)

Current estimates suggest that insured losses from the attacks—which provide a proxy for the direct loss of physical and human capital—may amount to between \$36 billion and \$54 billion. The macroeconomic cost from interrupting business activities following the attacks is more difficult to measure, since many factors influence the behavior of the macroeconomy and since some of the reduction in activity in September caused by the attacks may merely have been shifted into later months. It is possible to put a plausible upper bound on the potential effect, however.

In particular, on September 10, 2001, the Blue Chip consensus estimate for real GDP growth in the third quarter of 2001 was 1.6 percent (on a seasonally adjusted, annualized basis). The consensus estimate for real GDP growth in the fourth quarter was 2.6 percent. In the aftermath of the attack, which occurred in the final month of the third quarter, the real GDP growth figures turned out to be -1.3 percent in the third quarter and 1.7 percent in the fourth quarter. Even if the entire difference between the Blue Chip estimate and the actual outcome is attributed to the September 11 attacks, and even if we assume that none of the reduction in activity at the end of 2001 is subsequently offset by increased activity in 2002, the cost of the lost production amounts to about \$100 billion.

A more reasonable but still generous figure assumes that, say, half of the reduction in economic activity during the third and fourth quarters is either unrelated to the attacks or will be offset by increased activity in the future. In that case, the loss from reduced economic activity amounts to about \$50 billion, and the direct loss to physical and human capital also amounts to about \$50 billion. The total loss is then about \$100 billion. Even this figure is likely to exaggerate the cost of the September 11 attacks, because it is unlikely that as much as half the reduction in economic activity during the third and fourth quarters was due to the attacks and would not be offset by higher activity later.

### Effectiveness of Instruments of Government Intervention

With these criteria in mind, we now review briefly each of the instruments of government action described earlier and attempt, at least in a broad way (since some points have already been raised in previous chapters), to judge how effective they are likely to be.

#### *Regulation*

The principal benefit of a regulatory approach is that the regulatory standard provides a minimum guarantee regarding antiterrorism protection (assuming the regulations are enforced).<sup>13</sup> It also can discourage the most dangerous activities. If skyscrapers are natural targets for terrorists, requiring security measures in new skyscrapers discourages their construction (and also raises the cost of living in them, even if they are built), which may be an appropriate means of diminishing the nation's exposure to catastrophic attack, given the buildings' assumed attractiveness to terrorists.

But there are also downsides to regulation. First, the minimum regulatory threshold may be set at an inappropriate level.<sup>14</sup> Second, a regulatory approach, especially one that consists of "commands and controls" rather than market-like incentives, can be an unnecessarily expensive mechanism for achieving a given level of security.<sup>15</sup> Third, this approach does not generally provide incentives for innovation. Firms would be motivated to meet the minimum regulatory standard, but not necessarily exceed it. Indeed, depending on how they are written, rules may impede innovation in finding new (and less costly) approaches to improving protection against terrorism, especially if they are of the "command-and-control" variety.

These costs can be reduced, although not eliminated, through careful attention to the design of the regulations. In particular, the more that they focus on processes and performance, rather than specific inputs, the better. For example, a regulation affecting an indoor athletic arena could state that the arena's air ventilation system must be able to contain a given type of bioterrorist attack within a specific amount of time, rather than that the system must include specific devices. Compliance with the performance-based regulation could then be tested regularly by government inspectors. Such a system gives firms at least some incentive to design and implement less expensive mechanisms for achieving any given level of security.<sup>16</sup>

A final issue here is fairness. Regulation imposes its costs on the users and providers of a particular service. Such a “stakeholder-pays” approach may strike some Americans as unfair, especially since many of the stakeholders would have made physical and human capital investments before the threat of terrorism manifested itself in a significant manner.<sup>17</sup> But it may strike other Americans as eminently fair: from this perspective, those who engage in the most dangerous activities (in terms of their exposure to terrorist attacks) should pay for the costs associated with those risks. Furthermore, since higher earners likely represent a disproportionate share of the stakeholders in many of the most vulnerable services (such as air travel) and buildings (such as skyscrapers), the stakeholder-pays approach may also strike many Americans as equitable from an income inequality perspective.

#### *Insurance Requirement*

An insurance requirement is an alternative to direct government regulation.<sup>18</sup> At first glance, such a requirement may seem counterproductive. Firms and individuals who have insurance against terrorism would appear to lack incentives to take appropriate precautions against an attack. Where such insurance is available, however, it typically comes with provisions (such as deductibles, coinsurance, and coverage limits) to ensure that the insured bear at least some of the cost of an attack and thus have at least some economic incentive to avoid such attacks or minimize their consequences. Furthermore, the insurance companies themselves have an incentive to encourage risk-reducing activities.<sup>19</sup> Insurance firms could provide incentives for measures that reduce the exposure of buildings to terrorist attack (such as protecting or moving the air intake), or that reduce the likelihood of a successful cyberattack on a computer system or Intranet (such as improved firewalls and more advanced encryption).

Universal insurance is clearly not a panacea, however.<sup>20</sup> A particular concern is that the insurance premium market may not work that well in discriminating among terrorism risks. Indeed, the fairness of allowing differential premiums to discriminate among different exposures to terrorism is unclear. Consider the higher risks for such “iconic” structures as the World Trade Center, the Empire State Building, and other tall structures elsewhere in the country. If insurers are not restricted by government policy from charging appropriately risk-related premiums, insurance markets will

discourage the construction of such potential terrorist targets in the future. Such an outcome may be efficient in the sense of reducing potential exposure to terrorist attacks, but socially undesirable in another if the buildings have substantial symbolic value.

Furthermore, allowing substantial variations in insurance premiums would impose costs on the owners of tall buildings. In evaluating the effects of such costs, a distinction should be drawn between existing buildings and new construction. The owners of existing buildings likely did not anticipate the terrorist threat when the buildings were constructed. Any additional costs on such existing buildings would reduce their market values, imposing capital losses on their owners. Some may not view this outcome as fair: it effectively imposes much higher costs on the owners (or occupants) of an existing building to address a threat that was largely unexpected when the buildings were constructed. Others may view the outcome as eminently fair, since the alternative would be to have the population as a whole effectively provide a subsidy to the owners of prominent buildings. Furthermore, failing to allow insurance firms to discriminate across risks in pricing policies could induce “cherry picking” of the lowest risks by the insurance firms and make it difficult for the higher risks to obtain the insurance from any firm. (In the United Kingdom, a government-sponsored mutual insurance organization, Pool Re, provides antiterrorism insurance. The rates vary by location, with the highest in Central London and the lowest in rural parts of Scotland and Wales.)<sup>21</sup> For new construction, the case for differentiated insurance premiums is stronger, since the prospective owners are now aware of the threat of attack and since differentiated premiums could play an important role in encouraging safer designs of prominent buildings.

In any event, even without government prohibition of risk-related premiums, if government regulators find it difficult to undertake comparative benefit analysis in fighting terrorism, private insurers would be highly likely to face similar challenges. The absence of solid actuarial information on the risks involved reflects the nation’s good fortune thus far in not being exposed to a large number of terrorist attacks but makes it much more difficult for private insurers to price the risks associated with terrorism. So too does the fact that terrorists can shift their targets and respond to security measures in a manner that does not arise with regard to natural risks. Nonetheless, as the Congressional Budget Office has noted, “Not every new

risk has proved to be uninsurable. For example, the changing legal environment for product liability, which makes predicting losses difficult, has affected how insurers manage such risks, but it has not resulted in insurers' dropping all product liability coverage. Rather it has produced a combination of more restricted coverage, shared responsibility, and modifications in producers' behavior." CBO also notes that private insurers in Israel provide some antiterrorism coverage (involving indirect losses such as the costs of business interruptions from terrorist attacks).<sup>22</sup>

Perhaps most fundamentally, an insurance system will not work if insurers do not offer the insurance (or offer it only at extremely high prices in relation to some underlying actuarial model). A particular concern involves reinsurance: the transfer of risk from the primary insurance company to another entity. Rather than maintaining high reserves to meet the potential costs of extreme events, primary insurance firms buy reinsurance from other firms. The reinsurance covers at least part of a severe loss, attenuating the risks faced by the primary insurers. Reinsurance firms, however, have generally stopped offering reinsurance on terrorism risks. In response, many primary insurance companies have eliminated terrorism coverage from their policies (when allowed by state commissioners to do so).<sup>23</sup>

Thus far, lenders appear to be providing credit to commercial borrowers who lack terrorism insurance.<sup>24</sup> But it is unclear how sustainable—or desirable—such an outcome is. Even in the absence of an insurance mandate, policymakers should therefore explore a variety of options to facilitate the provision of terrorism insurance.

One possibility is a federal reinsurance program. In late 2001, both the House and Senate considered legislation that would provide catastrophic terrorism reinsurance assistance to the insurance industry, although the approaches differed somewhat and the Senate did not hold a vote on its legislation.<sup>25</sup> If federal reinsurance is provided, it is important that the insurance companies themselves face some liability in the case of a terrorist attack, so that they have an incentive to encourage efficient behavior among those they insure.<sup>26</sup> Such incentives could be provided, as under the House and Senate legislation, through deductibles that apply before the government reinsurance is available.<sup>27</sup> But a substantial flaw in both bills is that neither would impose a fee for the federal reinsurance effort. A better approach would have the government share the risk, but also the premiums,

from primary terrorism insurance.<sup>28</sup> Finally, any such federal reinsurance program should be temporary. Over time, as new approaches to spreading the financial risks associated with antiterrorism insurance develop, the need for any government reinsurance program could be reduced.<sup>29</sup>

Any move toward a broader system of antiterrorism insurance thus faces substantial obstacles. Some economists and market observers have raised important questions about whether capital market imperfections impede the ability of insurers to provide coverage against catastrophic risks, such as those involved in terrorist activities.<sup>30</sup> Despite these potential problems, it is plausible that a broader system of antiterrorism insurance could develop over the medium to long term and thereby play a crucial role in providing incentives to private sector firms to undertake additional security measures when such steps are warranted given the risk of a terrorist attack (at least as viewed by the insurance firm).

#### *Subsidies for Antiterrorism Measures*

Government action can also take the form of subsidies for antiterrorism measures undertaken by private actors.<sup>31</sup> Subsidies could affect firm behavior and (if appropriately designed) provide some protection against terrorist threats. Subsidies carry four dangers, however. First, they can encourage unnecessarily expensive investments in security measures (or “gold plating”).<sup>32</sup> Second, they would likely prompt firms to engage in intensive lobbying to capture the subsidies, which would not only dissipate resources that could have been used more productively elsewhere, but may skew the definition of what qualifies for the subsidy toward inappropriate items.<sup>33</sup> Third, subsidies could provide benefits to firms that would have undertaken the activities even in the absence of the subsidy, raising the budget cost without providing any additional security measures. And fourth, subsidies financed from general revenue are in effect paid for by the entire population. As discussed earlier, the fairness and feasibility of that approach is debatable, especially in face of the dramatic deterioration in the outlook of the federal budget since the September attacks and the recognition that other pressing needs in the war on terrorism will put increased pressure on the budget even without subsidizing private sector protective measures.<sup>34</sup>

### Toward a Mixed System: Minimum Regulatory Standards and Insurance

Though all government interventions have their shortcomings, which vary in importance from sector to sector, one longer-term approach appears to be the least undesirable and most cost-effective: a combination of regulatory standards and antiterrorism insurance. Such a mixed system should only be applied when government intervention is warranted; as emphasized earlier, a key question in evaluating that threshold is the degree to which the government action will reduce overall exposure to the risk of major terrorism (rather than merely shift it from one target to another with a comparable level of damage).

A mixed regulatory/insurance system is employed in many other circumstances, such as owning a home or driving a car. Local building codes specify minimum standards that homes must meet. But mortgages generally require that homes also carry home insurance, and insurance companies provide incentives for improvements beyond the building code level, for example, by offering a reduction in the premiums they charge if the homeowner installs a security system. Similarly, governments specify minimum standards that drivers must meet in order to operate a motor vehicle. But they also require drivers to carry liability insurance for accidents arising out of the operation of their vehicles. Meanwhile, insurance companies provide incentives for safer driving by charging higher premiums to those with poorer driving records.

To be sure, crucial differences exist between the terrorist case and these other examples. For one thing, stable actuarial data exist for home and auto accidents, but not for terrorist attacks. Nonetheless, it may be possible for insurers to distinguish risks of loss based on differences in damage exposures, given a terrorist incident. Some financial firms are already trying to devise basic frameworks for evaluating such risks.<sup>35</sup>

In short, a mixed system of minimum standards coupled with an insurance mandate can encourage actors not only to act safely, but also to seek innovative ways to reduce the costs of achieving any given level of safety.<sup>36</sup> (In some cases, a formal insurance requirement may not be necessary because lenders already require terrorism insurance to be carried before extending a loan, and a government mandate is thus superfluous.) The presence of

minimum regulatory standards also helps to attenuate the moral hazard effect from insurance and can offer courts some guidance in determining negligence under the liability laws (see appendix A for further discussion of legal liability issues).<sup>37</sup>

A mixed system also has the advantage of being flexible, a key virtue in an arena where new threats seem to be “discovered” repeatedly. In situations in which insurance firms are particularly unlikely to provide proper incentives to the private sector for efficient risk reduction (for example, because insurers lack experience in these areas), regulation can play a larger role. But when insurance firms are able to devise incentives for innovative and cost-effective security measures, regulation could play a smaller role.

The mixed system of regulatory standards and antiterrorism insurance seems well suited for three kinds of risks, beginning with security at chemical and biological plants. Such plants contain materials that could be used as part of a catastrophic terrorist attack and should therefore be subjected to more stringent security requirements than other commercial facilities. But the regulatory standards could be supplemented by insurance coverage, which would then allow insurance firms to provide incentives for more innovative security measures.

Second, the mixed approach is appropriate for buildings that house thousands of people. The federal government could supplement existing building codes for large commercial buildings with minimum performance-based antiterrorism standards. These in turn could be supplemented by requiring the owners of buildings to obtain antiterrorism insurance covering some multiple of the value of their property. Even if the regulators decided that basic antiterrorism insurance premiums should not vary by type of building (for the reasons mentioned), they could still allow the basic premium to be adjusted for building improvements that reduce the probability or severity of an attack (such as protecting the air intake system or reinforcing the building structure).

Third, some regulatory measures may be warranted for critical telecommunications and cyber infrastructure, at least temporarily. For example, performance-oriented regulatory steps could perhaps require critical systems to be able to withstand mock cyberattacks (with the nature of the cyberattack varying from firm to firm). Given the ease with which mock

attacks and tests could be conducted (which could provide a basis for pricing the insurance), an insurance requirement may also be feasible and beneficial; insurance firms today already employ experts to advise insured firms on how to reduce their exposure to cyberattacks. To be consistent with our thresholds for government action, government intervention should occur only in cases of infrastructure components that are critical to human safety or whose disruption would cause systemic economic harm.

Our case for a mixed system of minimum standards and insurance, it should be emphasized, is a “rebuttable” one. In other words, it is a first choice over the longer term, but it can and should be supplemented or replaced when there is evidence that other approaches would be more efficient or when there are significant externalities associated with a given type of terrorism.

Furthermore, as noted earlier in the chapter, the capacity of the insurance industry to play the role envisioned for it in this mixed system is somewhat unclear and may depend in part on whether the federal government provides some kind of reinsurance in the short run. It will also take time for the industry to develop appropriate ways of pricing policies covering potentially catastrophic attacks.

Finally, the degree of government intervention should clearly vary by circumstance. For example, consider the difference between security at a mall and security at a chemical facility. Poor security at a mall does not pose the same scale of harm as poor security at a chemical facility. The products of chemical plants could be used as *inputs* in a terrorist attack, and therefore the facilities warrant more aggressive government intervention than shopping malls. Thus security regulations for chemical plants may make sense, even if they do not for shopping malls.

A critical challenge is deciding how extensive government regulation should be. It is one thing to set standards for commercial facilities such as chemical and biological plants. But should the government attempt to provide antiterrorism regulations for *all* commercial buildings? For hospitals? For universities? Where does the regulatory process stop? As we have argued throughout this analysis, the focus should be on reducing the risk of terrorist attacks with large-scale human or economic impact. Hence policymakers should proceed carefully in extending regulations beyond the areas delineated in the preceding chapters.

### *Coordinating Government Intervention*

Who should set the standards? Because terrorism almost by definition involves potentially significant externalities for the nation as a whole, we believe there is a presumptive case favoring minimum federal standards, which states and municipalities could strengthen if they so desire. But simply saying that the responsibility belongs to the federal government does not fully answer the question. As we highlight in chapter 7, numerous federal agencies have jurisdiction over different parts of the U.S. economy.

To prevent a regulatory turf war, as well as to ensure a coordinated federal response, the new Office of Homeland Security should provide a regulatory road map, with assignments to specific agencies to deal with specific threats. The office should coordinate its activities with the Office of Information and Regulatory Affairs (OIRA) of the Office of Management and Budget (OMB). OIRA is the division responsible for overseeing the regulatory activities of executive branch agencies. In late 2001, OIRA developed a “prompt letter” through which it plans to suggest to agencies new rules that should be adopted or changes in existing rules that may be warranted. We can think of no better use of the prompt letter than to suggest regulations, developed and coordinated through the Office of Homeland Security, that agencies might introduce or tighten to deal cost-effectively with the terrorist threat.

### **An Efficient Response to Terrorist Threats in the Public Sector**

Since the government will have primary responsibility for minimizing terrorist access to the United States and mitigating the costs of any attacks that do occur, another important policy question is how to allocate the implementation and cost of homeland security measures within the *public sector*. For example, many state and local governments will need to expand their hazardous materials response teams, increase police forces, and undertake other steps in response to the threats underscored by the September 11 attacks. How should such costs be financed?

Traditional models of fiscal federalism suggest that the federal government should finance those activities that have significant spatial externalities (that is, in which the costs or benefits of the activity spill over to other

geographic areas), and that state and local governments should finance those activities with limited or no spatial externalities.<sup>38</sup> Thus national defense lies in the federal domain, whereas local police activities are the responsibility of lower levels of government.

Many antiterrorism measures within the public sector, however, appear difficult to classify. Are they national defense (and therefore a federal expense) or traditional policing (and therefore a state and local concern)? For example, expanding the number of local police may help to identify and prevent terrorist activities, but it can also reduce local crime. So who should pay for the expansion? As with private sector activities, several criteria may help to determine the nature of the intervention within the public sector:

—To what degree will state and local governments undertake insufficient antiterrorism efforts in the absence of a federal mandate or subsidy?

—To what degree does the measure provide collateral benefits to the local geographical area?

—To what degree will incompatible state and local regulations or approaches impose additional costs on individuals and firms (including any costs related to displacing terrorist activity from one area to another), and to what extent will they allow valuable experimentation with various antiterrorism measures?

—How fair is the expected outcome? Will society accept the consequences of the action on the distribution of income or wealth?

Although the appropriate response will vary from issue to issue, the general principle we adopt for public sector activities is that the federal government should be responsible for measures that are clearly, primarily, and specifically linked to reducing the threat or severity of terrorist attacks. Measures that primarily provide collateral benefits to the local area should generally be financed by local or state governments, even if they provide some antiterrorism benefits.

One of the crucial factors to evaluate is the degree to which a spatial externality is involved: the larger the spatial externality, the more likely it is that federal financing is justified. Thus public health activities should be financed at least in part by the federal government, given the communicability of disease and therefore the significant spatial externality involved. Similarly, basic research—for example, on vaccines and innovative antiterrorism devices—would have significant benefits for people across the entire

nation and therefore should be financed by the federal government. Security measures at the nation's ports should be financed at least in part by the federal government, since the ports are a gateway to the nation as a whole and inadequate security could allow terrorist materials to gain entry and be dispersed to remote geographical areas. But expanded police patrols should be financed by state and local governments, since the patrols largely if not entirely guard against attacks that would be confined to the immediate area.

In summary, the federal government should undertake those antiterrorism measures that have clear national benefits, but it should not finance state and local government activities with substantial local benefits (such as hiring additional police or firefighters). The larger the collateral local benefit in relation to the antiterrorism benefit, the smaller the federal share should be. Such an approach avoids excessive federal subsidization of activities that have significant local benefits.

## Conclusions

Policymakers concerned with homeland security must carefully balance the gains from deterring the number and severity of future terrorist attacks against the costs of the security measures. To prevent attacks that would involve the loss of thousands of lives, or widespread economic harm, government action is warranted. Over the longer term, a promising approach for such action is a mixed regulatory and insurance system. This approach ensures that costs are borne by the users and producers of a service, rather than by the population as a whole, and thus avoids "gold plating" the antiterrorism activities. It also seeks to provide some benefit—for example, in terms of reduced insurance premiums—from undertaking additional security measures.

Public sector homeland security activities should be financed by the federal government when they involve a specific antiterrorism measure or address significant spatial externalities, but state and local governments should finance antiterrorism activities that provide substantial collateral local benefits (in addition to reducing the probability or severity of a terrorist attack). These guidelines will need to evolve over time as more experience accumulates.

They underscore two of the three general themes of this book regarding how to achieve homeland security at reasonable economic cost: security measures should provide some benefit (for example, reduced waiting times or insurance premiums) to induce additional security precautions, and stakeholders should pay for most such measures. As earlier chapters make plain, the third theme is that information technologies will play an important role in promoting security at reasonable cost.

