Homeland Security:
The Problems with Providing Tax Incentives to Private Firms

Peter R. Orszag[1]
Joseph A. Pechman Senior Fellow in Economic Studies

Testimony before the House Committee on Small Business
Subcommittee on Rural Enterprise, Agriculture and Technology

July 21, 2004

Thank you for inviting me to testify this morning.

In homeland security, private markets do not automatically produce the best result. To be sure, private firms have some incentive to avoid the direct financial losses associated with a terrorist attack on their facilities or operations. In general, however, that incentive is not compelling enough to encourage the appropriate level of security.

Providing a tax subsidy to private firms for homeland security costs would represent one way of changing the incentives facing firms. This approach, however, does not represent sound policy, especially in light of the nation's massive long-term fiscal gap. A mixed system of minimum regulatory standards, insurance, and third-party inspections would better harness the power of private markets to invest in homeland security in a cost-effective manner.

Modifying incentives for the private sector to invest in homeland security

In other testimony and in a co-authored Brookings volume, I have presented the reasons that private firms have inadequate incentives to invest in homeland security.[2] The need for some sort of government intervention to alter the incentives facing private firms does not, however, determine how or in which situations the government should intervene. For example, to bolster safety in commercial buildings, the government could:

---

[1] The views expressed here do not necessarily represent those of the staff, officers, or board of the Brookings Institution. I thank Michael O'Hanlon, Ivo Daalder, I.M. Destler, David Gunter, Robert Litan, and Jim Steinberg for the joint work upon which this testimony draws, Emil Apostolov for excellent research assistance, and Howard Kunreuther, Janusz Ordover, and Bobby Willig for helpful discussions. For related details, see *Protecting the American Homeland: One Year On* (Brookings Institution Press: 2003).

[2] See *Protecting the American Homeland: One Year On* (Brookings Institution Press: 2003), Peter R. Orszag, "Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives," Testimony before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security, September 4, 2003; and Peter R. Orszag, "Homeland Security and the Private Sector," Testimony before the National Commission on Terrorist Attacks Upon the United States, November 19, 2003.

- Impose direct regulation: The Federal government could require that certain anti-terrorist features be included in any commercial or public building.[3]

- 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.[4] The logic of such a requirement is that insurance companies would then provide incentives for buildings to be safer.

- Provide a tax credit for anti-terrorism measures: The Federal government could provide a tax credit for investing in anti-terrorism building features or for other steps to protect buildings against attacks. This is basically the approach undertaken in legislation proposed by Representative Shuster.

- Create a new program on the outlay side of the budget: The Federal government could directly purchase specific types of equipment for private-sector buildings.

Each of these approaches typically entails a different level of aggregate costs, and also a different distribution of those costs across sectors and individuals.[5]

Tax credits

Representative Shuster's legislation (H.R. 3562) would provide a business tax credit for various security expenditures by private firms, including for:

- An electronic access control device or system.
- Biometric identification or verification device or system.
- Closed-circuit television or other surveillance and security cameras and equipment

[3] Although building codes traditionally fall within the jurisdiction of local governments, the Americans with Disabilities Act (ADA) mandated changes in buildings. A precedent therefore exists for Federal preemption of local building codes. It should be noted that the ADA does not directly affect existing building codes. But the legislation requires changes in building access and permits the Attorney General to certify that a State law, local building code, or similar ordinance "meets or exceeds the minimum accessibility requirements" for public accommodations and commercial facilities under the ADA. Such certification is considered "rebuttable evidence" that the state law or local ordinance meets or exceeds the minimum requirements of the ADA.

[4] The McCarren-Ferguson Act delegates insurance regulation to the states. The Federal government could nonetheless effectively impose an insurance mandate either by providing strong incentives to the states to adopt such a mandate, or perhaps by mandating that all commercial loans from a federally related financial institution require the borrower to hold such insurance.

[5] In theory, the different approaches to implementing a security measure could be separated from how the costs of the measure were financed – for example, firms adhering to regulatory standards could be reimbursed by the Federal budget for their costs. In practice, however, the method of implementation often implies a method of financing: the cost of regulations will be borne by the producers and users of a service, and the cost of a general subsidy will be borne by taxpayers as a whole. In evaluating different implementation strategies, financing implications must therefore be taken into account.

- Locks for doors and windows, including tumbler, key, and numerical or other coded devices
- Computers and software used to combat cyberterrorism
- Electronic alarm systems to provide detection notification and off-premises transmission of an unauthorized entry, attack, or fire
- An electronic device capable of tracking or verifying the presence of assets
- High efficiency air filtering systems
- Mechanical and non-mechanical vehicle arresting barricades
- Metal detectors
- Signal repeating devices for emergency response personnel wireless communication systems
- Components, wiring, system displays, terminals, auxiliary power supplies, computer systems, software, networking infrastructure and other equipment necessary or incidental to the operation of any item described in any of the preceding subparagraphs.

This type of approach could help to strengthen firm's incentives to protect themselves against attack, but tax credits also carry several dangers:

- First, they can encourage unnecessarily expensive investments in security measures (or "gold plating"). The problem is particularly severe in the case of investments that provide protection against terrorist attack but also have substantial other benefits to firms. Consider, for example, the mundane case of door locks. Such systems can provide some protection against terrorist attack, but that is not likely to be their primary function. Yet even if the homeland security protection provided is relatively modest, though, the firm may find it worthwhile to purchase an expensive door security system if offered a 20 or 30 percent tax credit for that expenditure, since so much of the cost is borne by others. The door locks may provide significant other benefits to the firm (such as reduced theft and vandalism).

- Second, tax credits could provide benefits to firms that would have undertaken the investments even in the absence of the tax subsidy – raising the budget cost without providing any additional security. In other words, the proposed tax credits "buy out the base" of what firms are already doing to protect themselves against terrorist attack. A tax credit focused on marginal investments, albeit difficult to design and implement, would be better targeted.

- Third, tax credits do a poor job of differentiating between high-risk and lower-risk sectors, yet 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 endanger remote areas in the nation to nearly the same degree 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. Yet the tax credits would provide the same benefit to shopping malls as chemical plants.

- Fourth, these types of tax credits unduly complicate the tax code, which is already excessively complex. Defining and implementing the specific expenditures that would qualify for the proposed tax credit is administratively complex. For example, how exactly should the IRS differentiate a computer "used to combat cyberterrorism" from any other computer?

- Fifth, tax credits would further worsen an already bleak fiscal outlook. The nation's long-term fiscal gap amounts to between 7 and 10 percent of GDP.[6] New tax credits that are not offset by other policy changes would exacerbate this gap.

- Finally, tax credits spread the cost of homeland security spending in a particular sector across the entire population, rather than the stakeholders (the owners of businesses, the workers, and consumers of the product) in that sector itself. If particular sectors are more dangerous than others, we as a society may want to discourage activity in that sector – which would be better accomplished by having stakeholders in that sector bear the full cost of protection. This cost-sharing issue is explored in the next section.

Who bears the cost?

A fundamental question in evaluating different approaches to homeland security costs in the private sector is how those costs should be shared. Tax credits at least partially spread those costs across the public as a whole; other approaches do not spread the cost in this way.

As one example, consider the higher risks of terrorism for "iconic" structures. Any additional costs of protection -- say, installing a finer filter on the air intake system to protect against bio-attack -- would either reduce the market values of such buildings or be passed along in higher rents to occupants.[7] From one perspective, this outcome seems unfair: it effectively imposes higher costs on the owners or occupants of a specific building to address a threat related to the nation's security. A tax credit for homeland security investments could instead distribute the burden across the broader tax-paying public. A tax-credit approach, however, would mean the population as a whole was effectively providing a subsidy to the owners of prominent buildings – an outcome that itself may seem unfair.

Rather than wading into this philosophical debate over fairness, I'd like to emphasize instead the role of incentives. Imposing the cost on the stakeholders rather than the general public could raise the costs of occupying the skyscrapers and therefore discourage people from living and working there. Given the buildings' assumed attractiveness to terrorists, this may be an appropriate response to diminish the nation's exposure to catastrophic attack. Basically, such

[6] Alan J. Auerbach, William G. Gale, and Peter R. Orszag, "Sources of the Long-Term Fiscal Gap," *Tax Notes*, May 24, 2004.

[7] For *existing* buildings, the cost is more likely to be borne by the owners of the building. For *new* buildings, the cost is more likely to be shifted forward to occupants.

a "stakeholder pays" approach ensures that those who engage in the most dangerous activities (in terms of their exposure to terrorist attacks) pay for the costs associated with those risks.

In other words, from an incentive perspective, spreading the cost of protection across the entire population would seem less desirable than concentrating the cost on the users or producers of a specific service. This perspective only augments the other shortcomings associated with tax credits identified above, leading to my view that such tax credits do not represent sound policy.

Toward a mixed system

If tax credits are not the answer, what is? All of the various approaches to government intervention have shortcomings, and the relative importance of these drawbacks is likely to vary from sector to sector. Nonetheless, in many cases that require government intervention, one longer-term approach appears to be the least undesirable and most cost-effective: a combination of regulatory standards, insurance requirements, and third-party inspections.

A mixed regulatory-insurance system is already applied in many other areas, 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 providing 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.[8]

A mixed system of minimum standards coupled with an insurance mandate not only can encourage actors to act safely, but also can provide incentives for innovation to reduce the costs of achieving any given level of safety.[9] The presence of minimum regulatory standards also helps to attenuate the moral hazard effect from insurance, and can provide guidance to courts in determining negligence under the liability laws.[10]

---

[8] To be sure, crucial differences exist between the terrorist case and these other examples. For example, 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. See, for example, Moody's Investors Service, "Moody's Approach to Terrorism Insurance for U.S. Commercial Real Estate," March 1, 2002.

[9] Moreover, an insurance *requirement* (as opposed to an insurance option) avoids the adverse selection problem that can occur in voluntary insurance settings. In particular, if anti-terrorism insurance were not mandatory, firms with the most severe terrorism exposure would be the most likely to demand insurance against terrorist acts. The insurance companies, which may have less information about the exposure to terrorism than the firms themselves, may therefore be hesitant to offer insurance against terrorist attacks, since the worst risks would disproportionately want such insurance. The outcome could be either that the insurance companies do not offer the insurance, or that they charge such a high price for it that many firms (with lower exposure to terrorism but nonetheless some need to purchase insurance against it) find it unattractive. This preference for mandatory insurance assumes no constraints or imperfections on the supply side of the insurance market.

A mixed system also has the advantage of being flexible, a key virtue in an arena where new threats will be "discovered" on an ongoing basis. 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.

Third-party inspections can be coupled with insurance protection to encourage companies to reduce the risk of accidents and disasters. Under such schemes, insurance corporations would hire third-party inspectors to evaluate the safety and security of plants seeking insurance cover. Passing the inspection would indicate to the community and government that a firm complies with safety and security regulations. The firm would also benefit from reduced insurance premiums, since the insurer would have more confidence in the safety and security of the firm.

This system takes advantage of two potent market mechanisms to make firms safer, while freeing government resources to focus on the largest risks. Insurance firms have a strong incentive to make sure that the inspections are rigorous and that the inspected firms are safe, since they bear the costs of an accident or terrorist attack. Private sector inspections also reduce the number of audits the regulatory agency itself must undertake, allowing the government to focus its resources more effectively on those companies that it perceives to pose the highest risks. The more firms decide to take advantage of private third-party inspections, the greater the chances that high-risk firms will be audited by the regulatory agency.

Studies have shown how such a program could be implemented in practice. In Delaware and Pennsylvania, the State Departments of Environmental Protection have worked closely with the insurance industry and chemical plants to test this approach for chemical facility safety.[11]

Applying the mixed system

Three examples of homeland security issues seem relatively well-suited to a mixed system of regulatory standards, anti-terrorism insurance, and third-party inspections:

- 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. The regulatory standards could be supplemented by an insurance requirement, which would then allow insurance firms to provide incentives for more innovative security measures.

[10] For a discussion of the potential benefits of a mixed system of building code regulations and mandatory catastrophic risk insurance in the context of natural disasters, see Peter Diamond, "Comment on Catastrophic Risk Management," in Kenneth Froot, ed., *The Financing of Catastrophe Risk* (University of Chicago Press: Chicago, 1999), pages 85-88.

[11] For further information, see Howard Kunreuther, Patrick McNulty, and Yong Kang, "Improving Environmental Safety Through Third Party Inspection," *Risk Analysis.* 22: 309-18, 2002.

- Building security for large buildings or arenas. The Federal government could supplement existing building codes for large commercial buildings with minimum performance-based anti-terrorism standards. Those regulations could then be supplemented by requiring the owners of buildings to obtain anti-terrorism insurance covering some multiple of the value of their property. Adjustments to the basic premium could encourage building improvements that reduce the probability or severity of an attack (such as protecting the air intake system or reinforcing the building structure).

- Cyber-security. Since the steps involved in protecting a computer system against terrorist attack are similar to those involved in protecting it against more conventional hacking, the case for Federal financing is relatively weak. Federal subsidies of anti-terrorism cyber-security measures at private firms would likely induce excessive "investment," since the firms would not bear the full costs but would capture many of the benefits (through improved security against hacking attempts). Nonetheless, a successful terrorist cyber-attack could cripple the nation's infrastructure, at least temporarily. Some performance-oriented regulatory steps may therefore be warranted. For example, the government could require critical computer systems to be able to withstand mock cyber-attacks, with the nature of the cyber-attack 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 be feasible and beneficial. One could even imagine insurance firms hiring cyber-experts to advise insured firms on how to reduce their exposure to cyber-attacks. To be consistent with reasonable thresholds for government intervention, any regulatory or insurance requirements could be imposed only on larger firms or those that have direct access to critical computer infrastructure components.

Conclusion

I am pleased that policy-makers are considering various ways of changing the incentives facing private firms to invest in homeland security protections. One of the most significant policy-making failures over the past several years has been inadequate attention to this problem.

Unfortunately, though, tax credits are not the right approach to altering private incentives. In addition to encouraging gold-plating, tax credits spread the cost of protecting private firms across the population as a whole. In my view, the costs should instead be imposed on the users and providers of a particular service, which ensures that those who engage in the most dangerous activities (in terms of homeland security risks) pay for the costs associated with those risks. Furthermore, tax credits would worsen an already bleak fiscal outlook.

Instead of providing tax credits, a mixed system of minimum standards, insurance, and third-party inspections could better harness market forces to provide homeland security at minimum cost. This approach 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. For example, in some cases, the insurance requirement may not be necessary because lenders already require terrorism insurance to be carried before extending loans – and a government mandate is thus effectively superfluous.

Furthermore, it will undoubtedly take time for the insurance industry to develop appropriate ways of pricing policies covering potentially catastrophic attacks.

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 anti-terrorism regulations for *all* commercial buildings? For hospitals? For universities? Where does the regulatory process stop? One answer to this question is provided in *Protecting the American Homeland*, which focuses on reducing the risk of large-scale terrorist attacks.