Critical Infrastructure Protection and the Private Sector:
The Crucial Role of Incentives

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

Testimony before the Subcommittee on Cybersecurity, Science, and Research & Development
and the Subcommittee on Infrastructure and Border Security

House Select Committee on Homeland Security

September 4, 2003

The blackout of 2003 has underscored concerns about the vulnerability of our nation's critical infrastructure to both accidents and deliberate attack, providing an immediate connection to the nation's homeland security efforts. But the blackout may offer a deeper lesson beyond the vulnerability of the nation's electricity grid to terrorist attack. In particular, a common explanation for the problems facing the electricity system is that private firms have had inadequate incentives to invest in distribution lines.

The important point is that market incentives are extremely powerful. For that very reason, however, it is essential that they be structured properly. As Patrick Wood, chairman of the Federal Energy Regulatory Commission, has put it: "We cannot simply let markets work. We must make markets work."[2]

In homeland security, private markets do not automatically produce the best result. We must therefore alter the structure of incentives so that market forces are directed toward reducing the costs of providing a given level of security for the nation, instead of providing a lower level of security than is warranted. Given the significance of the private sector in homeland security settings, structuring incentives properly is critical.

To be sure, private firms currently 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 – and should therefore be supplemented with stronger market-based incentives in several sectors.

---

[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 for helpful comments. For related details, see *Protecting the American Homeland: One Year On* (Brookings Institution Press: 2003). Also see Howard Kunreuther, Geoffrey Heal, and Peter Orszag, "Interdependent Security: Implications for Homeland Security Policy and Other Areas," Policy Brief #108, Brookings Institution, October 2002, and Howard Kunreuther and Geoffrey Heal, "Interdependent Security," Journal of Risk and Uncertainty 26: 231-249 (March/May 2003).

[2] Quoted in David Wessel, "A Lesson from the Blackout: Free Markets Also Need Rules," *Wall Street Journal*, August 28, 2003.

My testimony argues that:

- Private markets, by themselves, do not provide adequate incentives to invest in homeland security, and

- 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.

Incentives for homeland security in private markets

Private markets by themselves do not generate sufficient incentives for homeland security for seven reasons:

- Most broadly, a significant terrorist attack undermines the nation's sovereignty, just as an invasion of the nation's territory by enemy armed forces would. The costs associated with a reduction in the nation's sovereignty or standing in the world may be difficult to quantify, but are nonetheless real. In other words, the costs of the terrorist attack extend well beyond the immediate areas and people affected; the attack imposes costs on the entire nation. In the terminology of economists, such an attack imposes a "negative externality." The presence of this negative externality means that 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.[3] Without government involvement, private markets will thus typically under-invest in anti-terrorism measures.[4]

- Second, a more specific negative externality exists with regard to *inputs* into terrorist activity. 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

[3] It is also possible, at least in theory, for private firms to invest *too much* in anti-terrorism security. In particular, visible security measures (such as more uniformed guards) undertaken by one firm may merely displace terrorist attacks onto other firms, without significantly affecting the overall probability of an attack. In such a scenario, the total security precautions undertaken can escalate beyond the socially desirable levels – and government intervention could theoretically improve matters by placing *limits* on how much security firms would undertake. Unobservable security precautions (which are difficult for potential terrorists to detect), on the other hand, do not displace vulnerabilities from one firm to another and can at least theoretically reduce the overall level of terrorism activity. For an interesting application of these ideas to the Lojack automobile security system, see Ian Ayres and Steven Levitt, "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack," *Quarterly Journal of Economics*, Vol. 108, no. 1 (February 1998). For further analysis of evaluating public policy in the presence of externalities, see Peter Orszag and Joseph Stiglitz, "Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities," Brookings Institution Working Paper, January 2002.

[4] The Coase theorem shows that under very restrictive conditions, the negative externality can be corrected by voluntary private actions even if the role of government is limited to enforcing property rights. But the Coase theorem requires that all affected parties are able to negotiate at sufficiently low cost with each other. Since virtually the entire nation could be affected indirectly by a terrorist attack, the costs of negotiation are prohibitive, making the Coase theorem essentially irrelevant in the terrorism context.

provide terrorists with access to dangerous pathogens. The costs of allowing terrorists to obtain access to such materials are generally not borne by the facilities themselves: the attacks that use the materials could occur elsewhere. Such a specific 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. In particular, preventing access to such materials is likely to reduce the overall risk of catastrophic terrorism, as opposed to merely displacing it from one venue to another.

- Third, a related type of externality involves "contamination effects." Contamination effects arise when a catastrophic risk faced by one firm is determined in part by the behavior of others, and the behavior of these others affects the incentives of the first firm to reduce its exposure to the risk. Such interdependent security problems can arise, for example, in network settings. The problem in these settings is that the risk to any member of a network depends not only on its own security precautions but also on those taken by others. Poor security at one establishment can affect security at others. The result can often be weakened incentives for security precautions.[5] For example, once a hacker or virus reaches one computer on a network, the remaining computers can more easily be contaminated. This possibility reduces the incentive for any individual computer operator to protect against outside hackers. Even stringent cyber-security may not be particularly helpful if a hacker has already entered the network through a "weak link."

- A fourth potential motivation for government intervention involves information – in particular, the cost and difficulty of accurately evaluating security measures. For example, one reason that governments promulgate building codes is that it would be too difficult for each individual entering a building to evaluate its structural soundness. Since it would also be difficult for the individual to evaluate how well the building's air intake system could filter out potential bio-terrorist attacks, the same logic would suggest that the government should set minimum anti-terrorism standards for buildings if there were some reasonable threat of a terrorist attack on the relevant type of buildings (so that the individual would have some interest in ensuring that the building were protected against biological attack). Similarly, it would be possible, but inefficient, for each individual to conduct extensive biological anti-terrorism 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.

- The fifth justification for government intervention is that corporate and individual financial exposures to the losses from a major terrorist attack are inherently limited by the bankruptcy laws. For example, 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, and the firm would declare bankruptcy – and therefore the extent of the losses beyond that which

[5] See Howard Kunreuther and Geoffrey Heal, "Interdependent Security," Journal of Risk and Uncertainty 26: 231-249 (March/May 2003), and Howard Kunreuther, Geoffrey Heal, and Peter Orszag, "Interdependent Security: Implications for Homeland Security Policy and Other Areas," Policy Brief #108, Brookings Institution, October 2002.

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.

- The sixth justification for government intervention is that 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 11th attacks provides just one example of such bailouts. Such expectations create a "moral hazard" problem: private firms, expecting the government to bail them out should an attack occur, do not undertake as much security as they otherwise would. 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.

- The final justification for government intervention involves incomplete markets. The most relevant examples involve imperfections in capital and insurance markets. For example, 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 relative strength of these potential justifications for government intervention varies from case to case. Furthermore, the benefits of any government intervention must be weighed against the costs of ineffective or excessively costly interventions -- that is, that 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. The potential for government failure depends on the characteristics of the particular government agency and the sector involved. For example, it seems plausible that government failure is a particular danger in innovative and rapidly evolving markets.[6]

Both the need for government intervention and the potential costs associated with it thus vary from sector to sector, as should the policy response. Government intervention will generally only be warranted in situations in which a terrorist attack could have catastrophic consequences. Nonetheless, the general conclusion is that we can't just "leave it up to the market" in protecting ourselves against terrorist attacks. The market has an important role to

[6] As the great British economist Alfred Marshall emphasized, "A Government could print a good edition of Shakespeare's works, but it could not get them written…Every new extension of Governmental work in branches of production which need ceaseless creation and initiative is to be regarded as prima facie anti-social, because it retards the growth of that knowledge and those ideas which are incomparably the most important form of collective wealth." Alfred Marshall, "The Social Possibilities of Economic Chivalry," *Economic Journal*, 1907, pages 7-29.

play, but government intervention in some form and in some markets will be necessary to fashion the appropriate response to the threat of terrorism.

Modifying incentives for the private sector to invest in homeland security

The need for some sort of government intervention to protect private property and activities against terrorism does not determine 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 anti-terrorist features be included in any commercial or public building.[7]

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

- Provide a subsidy for anti-terrorism measures: The Federal government could provide a subsidy -- through direct government spending or through a tax incentive -- for investing in anti-terrorism building features or for other steps to protect buildings against attacks.

More broadly, each of the various approaches for minimizing the dangers and potential damages related to terrorism likely entails a different level of aggregate costs, and also a different distribution of those costs across sectors and individuals.[9]

[7] 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 pre-emption 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.

[8] 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.

[9] 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.

Direct regulation

The principal benefit of a direct regulatory approach is that the regulatory standard provides a minimum guarantee regarding anti-terrorism protection, assuming the regulations are enforced.[10] For example, if skyscrapers are natural targets for terrorists, requiring security measures in such buildings accomplishes two goals:

- First, it ensures that the buildings are better protected against attack.

- Second, it raises the costs of living in skyscrapers and therefore discourages people from living there – which may be appropriate as a means of diminishing the nation's exposure to catastrophic attack, given the buildings' assumed attractiveness to terrorists.

There are, however, also downsides to direct regulation:

- First, the minimum regulatory threshold may be set at an inappropriate level.[11]

- Second, a regulatory approach, especially one that reflects a "command and control" system rather than market-like incentives, can be an unnecessarily expensive mechanism for achieving a given level of security.[12] Such an approach may be particularly inefficient because of the substantial resources required to enforce the regulations.

- Third, the regulatory approach does not generally provide incentives for innovation. Firms would have an incentive to meet the minimum regulatory standard, but little incentive to exceed it. Indeed, depending on how it is written, regulation may impede innovation in finding new (and less costly) approaches to improving protection against terrorism, especially if the rules are of the standard "command and control" variety.

These costs of regulation can be reduced, although not eliminated, through careful attention to the design of the regulations. In particular, the more regulations focus on outcomes 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 bio-terrorist attack within a specific amount of time, rather than that the system

[10] Fines could be adopted as part of the regulatory system to ensure compliance with minimum standards for preventative measures.

[11] In other words, an anti-terrorism standard for, say, athletic arenas could impose an excessively tight standard (which would involve unnecessary costs) or an excessively loose standard (which would involve insufficient protection against terrorist threats).

[12] For example, in the environmental context, placing the same limit on emissions of harmful substances by all firms or individuals ignores the differences in costs of preventing pollution. That is why economists have long advocated market-based approaches to emission reductions, such as a permit trading system (which is currently in place for sulfur dioxide emissions) or a tax on emissions. Either market-based approach to regulation can achieve the same level of environmental protection at lower overall cost than a regulatory approach because it encourages those who can most cheaply control pollution do so (to avoid paying for the permit or the tax). A key requirement for a permit trading system or a tax, however, is some system for measuring "outcomes," such as the monitoring of pollution emitted by parties subject to the tax or participating in the system. In the context of anti-terrorism measures, the appropriate metric would be related to the expected loss from a terrorist attack. Yet it is difficult to see how such expected losses could be quantified and thus provide the basis for a permit trading system or a tax.

must include specific devices. Compliance with the performance-based regulation can then be tested regularly by government inspectors or third-party auditors. Such a performance-oriented set of regulations provides at least some incentive for firms to design and implement less expensive mechanisms for achieving any given level of security.

Insurance requirement

An insurance requirement is a possible alternative to direct government regulation.[13] At first glance, an insurance requirement may seem counterproductive: Firms and individuals who have insurance against terrorism would appear to lack incentives to take appropriate precautions against an attack. However, where such insurance is available, it typically comes with provisions (such as a deductible) to ensure that the insured bear at least some of the cost of an attack, and thus have an economic incentive to avoid such attacks or minimize their consequences. Furthermore, and perhaps more importantly, the insurance companies themselves have an incentive to encourage risk-reducing activities.[14] 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 cyber-attack on a computer system or intranet (such as improved firewalls and more advanced encryption).

An insurance requirement is clearly not a panacea, however. One issue is the degree to which the insurance market would discriminate among terrorism risks (or would be allowed to do so by regulators). For example, 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 it may have other social costs.

In evaluating the effects of variation in insurance premiums, 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 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.[15] For new construction, the case for differentiated insurance

[13] The insurance requirement would complement the use of the liability system to encourage protective measures: Insurance coverage would be relatively more important in the context of large liability exposures.

[14] By similar reasoning, insurers should not be able to use genetic information to discriminate in rates charged for health coverage since individuals cannot control their genetic makeup.

[15] Failing to allow insurance firms to discriminate across risks in pricing policies could also 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. It is worth noting that in the United Kingdom, a government-sponsored mutual insurance organization, Pool Re, provides anti-terrorism insurance. The rates vary by location, with the highest in Central London and the lowest in rural parts of Scotland and Wales. See Howard Kunreuther, "The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage" *Business Economics* April 2002 For further analysis of the Pool Re

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.

Another potential problem with an insurance approach involves the capacity of insurers to price the insurance and provide incentives for specific anti-terrorism steps. If government regulators find it difficult to undertake comparative benefit analysis in fighting terrorism, it is likely that private insurers would face similar challenges – especially in the face of network effects. The problem is exacerbated by the absence of solid actuarial information on the risks involved, which in turn reflects the nation's good fortune thus far in not being exposed to a large number of terrorist attacks. 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."[16]

Perhaps most fundamentally, an insurance system won't work if insurers won't offer the insurance or offer it only at extremely high prices relative to their underlying actuarial models, or if firms are not required to purchase the insurance and don't see a need for it. 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.[17] 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. To ensure that primary insurers continue to cover terrorism risks, the Federal government has provided terrorism reinsurance. A temporary Federal program makes sense; over time, as new approaches to spreading the financial risks associated with anti-terrorism insurance develop, the need for any government reinsurance program could be reduced.[18] A substantial flaw with the current reinsurance program, though, is that no fee is imposed. A better approach to federal reinsurance would have the government share the risk, but also the premiums, from primary terrorism insurance.[19]

---

and other programs abroad, see General Accounting Office, "Terrorism Insurance: Alternative Programs for Protecting Insurance Consumers," GAO-02-199T, October 24, 2001, and Congressional Budget Office, "Federal Reinsurance for Terrorism Risks," October 2001.

[16] CBO also notes that private insurers in Israel provide some anti-terrorism coverage (involving indirect losses such as the costs of business interruptions from terrorist attacks). Congressional Budget Office, "Federal Reinsurance for Terrorism Risks," October 2001.

[17] See, for example, Kenneth Froot, "The Market for Catastrophic Risk: A Clinical Examination," NBER Working Paper 8110, February 2001.

[18] For alternatives to a federal reinsurance program, see J. Robert Hunter, "How the Lack of Federal Back Up for Terrorism Insurance Affected Insurers and Consumers: An Analysis of Market Conditions and Policy Implications," Consumer Federation of America, January 23, 2002.

[19] See, for example, David Moss, Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, October 30, 2001.

Despite these potential problems, it is plausible that a broader system of anti-terrorism 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 anti-terrorism measures

A third form of government intervention would take the form of subsidies for anti-terrorism measures undertaken by private actors. Subsidies could affect firm behavior, and (if appropriately designed) provide some protection against terrorist threats. Subsidies, however, carry four dangers:

- First, they can encourage unnecessarily expensive investments in security measures (or "gold plating").[20]

- Second, a subsidy approach would likely spark intensive lobbying efforts by firms to capture the subsidies – which not only dissipates resources that could have been used more productively elsewhere, but may skew the definition of what qualifies for the subsidy toward inappropriate items.[21]

- 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.

- Finally, subsidies financed from general revenue are effectively paid for by the entire population. The fairness and feasibility of that approach is debatable, especially in face of the dramatic deterioration in the Federal budget outlook over the past several years and the recognition that other pressing needs will put increased pressure on the budget even without subsidizing private-sector protective measures.

Toward a mixed system: Minimum regulatory standards, insurance, and third-party inspections

As the discussion above has highlighted, all of the various approaches to government intervention have shortcomings, and the relative importance of these drawbacks is likely to vary

[20] Consider, for example, a tax credit equal to 50 percent of the cost of building improvements that protect against terrorism. Such a high subsidy rate may encourage firms to undertake too much investment in security against terrorism – in the sense that the costs of the investment are not fully justified by the protections they provide against terrorism. For example, reinforced windows may provide protection against shattering in the event of a terrorist attack. Even if the protection provided is minimal, the firm may find it worthwhile to undertake the investment since so much of the cost is borne by others, and since the reinforced windows may provide other benefits (such as reduced heating and cooling costs because of the added insulation). Relatedly, a subsidy provides a strong incentive for firms to classify changes that would have otherwise been undertaken as "anti-terrorism" measures in order to qualify for the subsidy.

[21] Lobbying would undoubtedly occur in the context of a regulatory approach, but since regulations are made on the basis of some kind of evidentiary record and are subject to judicial review, the room for lobbying is restricted. In contrast, subsidies are expenditures of the government and handed out by Congress, which is inherently much more amenable to lobbying.

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.[22]

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.[23] 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.[24]

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.

---

[22] 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.

[23] 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.

[24] 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.

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.[25]

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.

- Building security for buildings that house thousands of people. 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

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

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

This testimony argues that a mixed system of minimum standards, insurance, and third-party inspections could 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.

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. Thus security regulations for chemical plants may make sense, even if they don't 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 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.

A final issue is who should pay for improved security in the private sector. My general answer is that the costs should be imposed on the users and providers of a particular service. Such 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.