Testimony of Howard Kunreuther

Cecilia Yen Koo Professor of Decision Sciences and Public Policy
and co-director of the Wharton Risk Management and Decision Processes Center
The Wharton School, University of Pennsylvania

before

The Subcommittee on Capital Markets, Insurance, and Government Sponsored Enterprises of the House Financial Services Committee
"Examining a Legislative Solution to Extend and Revise the Terrorism Risk Insurance Act"

June 21, 2007

Mr. Chairman Kanjorski, Ranking Member Pryce and Members of the Subcommittee, I appreciate your inviting me to testify on "Examining a Legislative Solution to Extend and Revise the Terrorism Risk Insurance Act." My name is Howard Kunreuther and I am the Cecilia Yen Koo Professor of Decision Sciences and Public Policy at the Wharton School, University of Pennsylvania and Co-Director of the Wharton Risk Management and Decision Processes Center. The Wharton Risk Center was founded in 1984 and its mission is to examine alternative strategies for dealing with low-probability high-consequence events (i.e. extreme events) based on an understanding of the decision processes of consumers, firms and public sector agencies.

Since the terrorist attacks of 9/11, the Wharton Risk Center has focused on the roles of the public and private sectors in providing adequate risk financing against terrorism threat here and abroad. The Center produced several studies and a large report on *TRIA and Beyond: Terrorism Risk Financing in the U.S.* in August 2005, which has been undertaken in consultation with key interested parties from the private and public sectors and other academic/research institutions. This report was discussed with Congressional staff during the fall of 2005 at the time the *Terrorism Risk Insurance Act of 2002* (TRIA1) was being evaluated to determine whether it should be extended in some form.

A National Bureau of Economic Research (NBER) working paper, "Looking Beyond TRIA: A Clinical Examination of Potential Terrorism Loss Sharing" that was written with my Wharton Risk Center colleague Erwann Michel-Kerjan appears as *Appendix A.* The NBER paper, written after TRIA1 was extended by Congress for two years in December 2005 when it passed the *Terrorism Risk Insurance Extension Act* (TRIA2), provides an extensive series of analyses as to who will incur the costs following different terrorist attacks scenarios.

My testimony today will focus on the following three questions that I feel should be considered as one determines the specifics of a terrorism insurance bill:

1. What are the key principles that should guide the analyses of the role of insurance and other risk transfer mechanisms for dealing with extreme events?

2. What are special features of terrorism that need to be considered in determining whether this risk is insurable through some type of private-public partnership?

3. How do these principles and special features of terrorism relate to the current design of the *Terrorism Risk Insurance Revisions and Extension Act of 2007* (TRIA3)?

1. Key General Principles

The following principles are ones that should guide the development of insurance and other risk transfer programs for providing financial protection

Risk-based Premiums*:* Insurance and reinsurance premiums should reflect the risk. The premiums will then signal to individuals and firms the hazards they face and encourage them to engage in cost-effective mitigation measures to reduce their vulnerability to catastrophes.

Equitability: Insurance and other risk transfer programs should be fair to insurers, reinsurers, policyholders, and the general taxpayer where there is federal participation.

Minimize Likelihood of Insolvency: Insurers and reinsurers should determine how much coverage and what premium to charge against the risk so that the chances of insolvency are below some predefined acceptable threshold level.

Sufficient Demand for Coverage: The demand by individuals and firms for insurance coverage with risk-based premiums should be sufficiently high so that insurers can cover the fixed costs of introducing a program for providing coverage and spread the risk broadly through their portfolios.

Minimize Gaming: There should be no economic incentive for some insurers or policyholders to take advantage of provisions in the insurance or risk transfer program by undertaking strategic behavior.

2. Special Features of Terrorism[1]

The above principles work well for some risks where there is considerable historical data and scientific information, such as automobile accidents, fire and life insurance and even natural hazards. The terrorism risk presents special challenges in this regard, which makes it difficult for private insurers to provide widespread protection to commercial enterprises against losses from a terrorist attack. The factors listed below increase the amount of capital that insurers must hold to provide terrorism risk insurance coverage. The associated cost of holding that capital means that insurers will have to charge higher premiums for the coverage to be profitable.

Potential for Catastrophic Losses from Terrorism

Following the 9/11 events, insurers were concerned that catastrophic losses from future terrorist attacks would have a severe negative impact on their surplus and possibly lead to insolvency. Empirical evidence provided by experts on terrorism threats supports their concerns. Attacks using nuclear, biological, chemical and radiological (NBCR) weapons have the potential of inflicting very large insured losses, especially on workers' compensation and business interruption lines. The bombing of a chlorine tank in Washington, DC could kill and injure hundreds of thousands of people. Plausible scenarios elaborated by Risk Management Solutions, one of the three leading modeling firms examining catastrophe risks, indicate that large-scale anthrax attacks on New York City could cost between $30 and $90 billion in insured losses (Towers Perrin, 2004)[2].

A recent RAND study examined the impact of NBCR attacks on the losses to insurers and other interested parties from different scenarios.[3] The report presents the results of simulations for six attack scenarios: two conventional ones (1- and 10-ton truck bombs) and four NBCR scenarios such as a 5-kiloton nuclear bomb and an attack using a radiological device in the same metropolitan area. The report concludes that a 5-kiloton nuclear bomb would inflict losses of $630 billion dollars to commercial property and workers' compensation. The 2006 GAO report, written for the Chairman of the House Committee on Financial Services, concludes that "Given the challenges faced by insurers in providing coverage for, and pricing, NBCR risks, any purely market-driven expansion of coverage is highly unlikely in the foreseeable future."[4]

It is worth noting that other countries have included NBCR in coverage provided by their national terrorism (re)insurance program [e.g. United Kingdom (U.K.) and France]. But that inclusion comes at a cost. For example, when the protection of

---

[1] A more detailed discussion of these points appears in Wharton Risk Center (2005). *TRIA and Beyond: Terrorism Risk Financing in the U.S.,* p. 207 (Philadelphia: The Wharton School, University of Pennsylvania).

[2] Towers Perrin (2004), "Workers' Compensation Terrorism Reinsurance Pool Feasibility Study", March.

[3] Dixon, L. Lempert, R., LaTourrette, T., Reville, R. and Steinberg, P. (2007), *Trade-Offs Among Alternative Government Interventions in the Market for Terrorism Insurance* (Santa Monica, CA: RAND Center for Terrorism Risk Management Policy)

[4] U.S. Government Accountability Office (GAO) (2006), "Terrorism Insurance: Measuring and Predicting Losses from Unconventional Weapons is Difficult, but Some Industry Exposure Exists," GAO-06-1081, Washington, DC, September 2006..

companies operating in the U.K. under Pool Re was extended at the end of 2002 to "all risks," a category that now includes damage caused by chemical and biological as well as nuclear contamination, reinsurance prices charged by the pool against insurers doubled everywhere in the U.K.[5]

The 9/11 events, as well as the anthrax attacks in the month thereafter, also demonstrated a new kind of vulnerability: the use of networks as "weapons of mass disruption" (Michel-Kerjan, 2003)[6]. Terrorists can use the capacity of a country's critical networks to have a large-scale impact on the nation. In any given network (e.g. transportation) — every aircraft, every piece of mail, every marine container — can become a potential weapon. The impact of a supply chain disruption on the retail industry could be financially catastrophic should the federal government order a major port to be shut down in the wake of potential or actual threats from contaminated containers. As a point of reference, a 10-kiloton nuclear bomb planted in a shipping container that explodes in the port of Long Beach, California, could inflict total direct costs estimated to exceed $1 trillion, not to mention the ripple effects on trade and global supply chains that could even produce a global recession (Meade and Molander, 2006)[7].

Are these scenarios likely? According to experts in nuclear security and non-proliferation, they might very well be. A 2005 survey of 85 non-proliferation and national security experts led by Senator Richard Lugar put the likelihood of a nuclear attack somewhere in the world within the next ten years at 20% and the likelihood of a radiological attack at 40% (Lugar, 2005, p. 6).[8] It should be noted, however, that the report does not focus on the likelihood of attacks on any specific country.

Interdependent Security

The vulnerability of one organization, critical economic sector and/or country depends to some extent not only on its own choice of security investments, but also on the actions of other agents. This concept of *interdependent security* implies that failures of a weak link in a connected system could have devastating impacts on all parts of it, and that as a result there may be suboptimal investment in the individual components (Kunreuther and Heal, 2003; Heal and Kunreuther, 2006)[9]. The existence of such interdependencies provides another challenge in determining how much terrorism insurance to offer and what premium to charge.

---

[5] Michel-Kerjan, E. and B. Pedell. (2006), "How Does the Corporate World Cope with Mega-Terrorism? Puzzling Evidence from Terrorism Insurance Markets", *Journal of Applied Corporate Finance* (Morgan Stanley), 18 (4), December 2006.

[6] Michel-Kerjan, E. (2003), "New Vulnerabilities in Critical Infrastructures: A U.S. Perspective", *Journal of Contingencies and Crisis Management*, vol. 11: 3, pp. 132-141.

[7] Meade, C. and Molander, R. (2006), "Considering the Effects of a Catastrophic Terrorist Attack," *Rand Corporation*, Santa Monica, CA, August 2006.

[8] Lugar, R. (2005), "The Lugar Survey on Proliferation Threats and Responses." U.S. Senate, Washington, DC.

[9] Kunreuther, H. and Heal, G. (2003), "Interdependent Security," *Journal of Risk and Uncertainty*. 26: 2/3, pp. 231-249; Heal, G. and Kunreuther, H. (2006), "You Can Only Die Once: Interdependent Security in an Uncertain World." in *The Economic Impacts of Terrorist Attacks*, edited by H.W. Richardson, P. Gordon, and J.E. Moore III, Northampton, MA: Edward Elgar Publishers.

Interdependencies do not require proximity. In the case of the 9/11 attacks, security failures at Boston's Logan airport led to crashes at the World Trade Center (WTC). The failure was embedded within the security protocols promulgated by the Federal Aviation Administration and not with the application of those protocols, i.e. checking for bombs in passengers' luggage but not profiling. There was nothing that the Port Authority of New York and New Jersey and firms located in the WTC could have done on their own to prevent these aircrafts from crashing into the Twin Towers. Any protective efforts they might have undertaken would have been rendered useless by the absence of action at a distant site.

Shifting Attention to Unprotected Targets

Terrorists may respond to security measures by shifting their attention to more vulnerable targets. Sandler (2003), Keohane and Zeckhauser (2003) and Bier, Oliveros and Samuelson (2007)[10] analyze the relationships between the actions of potential victims and the behavior of terrorists. Rather than investing in additional security measures, firms may prefer to move their operations from large cities to less populated areas to reduce the likelihood of an attack. Of course, terrorists may choose these less protected regions as targets if there is heightened security in the urban areas. Terrorists also may change the nature of their attacks if there are protective measures in place which would make the likelihood of success of the original option much lower than another course of action (e.g. switching from hijacking to bombing a plane).

Dynamic Uncertainty and Time Scale

Since terrorists are likely to design their strategy as a function of their own resources and their knowledge of the vulnerability of the entity they wish to attack, the nature of the risk is continuously evolving. The likelihood and consequences of a terrorist attack are determined by a mix of strategies and counterstrategies developed by a range of stakeholders that change over time. This *dynamic uncertainty* makes the likelihood of future terrorist events extremely difficult to predict (Michel-Kerjan, 2003)[11].

A factor that is associated with dynamic uncertainty is the *timing of an attack*. Given the eight years that separated the first World Trade Center bombing in 1993 and the large-scale terrorist attacks during the morning of September 11, 2001, one could conclude that terrorist groups plan their attacks far in advance and perpetrate them when the public's attention and concern with terrorism have receded.

---

[10] Sandler, T. (2003), "Collective Action and Transnational Terrorism", *The World Economy*. 26 (6), pp. 779–802; Keohane, N. and Zeckhauser, R. (2003), "The Ecology of Terror Defense", *Journal of Risk and Uncertainty*. 26: 2/3, pp. 201-229; Bier, V., Santiago O. and Samuelson, L.. (2007), "Choosing What to Protect" . Risk Analysis June. (in press)

[11] Michel-Kerjan, E. (2003), "Large-scale Terrorism: Risk Sharing and Public Policy." *Revue d'Economie Politique*. 113 (5), pp. 625-648.

Information Sharing

An important feature of terrorism is who manages knowledge of risk, and how the relevant data are obtained. The sharing of information on terrorism risk is clearly different than the sharing of information regarding other potentially catastrophic events. There are large historical databases and scientific studies in the public domain for natural hazards. Insurers, property owners, businesses and public sector agencies all have access to these findings. However, data on terrorist groups' activities and current threats are normally kept secret by federal agencies for national security reasons. For example, the public still has no idea who manufactured and disseminated anthrax in U.S. mailings during the fall of 2001. Without this information, it is difficult for modelers to make projections about the capability and opportunities of terrorists to undertake similar attacks or other disruptive actions in the future.

Government Influencing the Risk

Finally, there are also more fundamental aspects of the threat of terrorism. International terrorism has always been viewed as a matter of national security as well as foreign policy. It is obvious that the government can influence the level of risk of future attacks through appropriate counter-terrorism policies and international cooperation as well as through adequate crisis management to limit consequences should an attack occur. Some decisions made by a government as part of its foreign policy can also affect the will of terrorist groups to attack this country or its interests abroad (Lapan and Sandler, 1988; Lee, 1988; Pillar, 2001)[12]. Government success or failure to adequately address a large-scale crisis such as one that would emerge in the aftermath of a large terrorist attack would have a direct impact on many individuals, commercial enterprises and their insurers.

3. Designing a Bill for Terrorism Insurance

The above principles and special features of terrorism have important implications for designing a Congressional bill for extending TRIA2. The Wharton *TRIA and Beyond* report concludes that there is a role and responsibility for government in collaboration with the private sector to provide protection against terrorism losses. There are several reasons for this public-private partnership:

- Federal government policy and actions significantly influence the risk of terrorism.
- The creation of a pure government program would exclude the insurers' expertise as well as its financial and operational capacity to provide coverage, assess losses when they occur, and process claims in an expeditious fashion.
- Although insurers' equity capital has increased recently, the private market has limited capacity to provide coverage for extreme losses from terrorism. This is, in

[12] Lapan, H. and Sandler, T. (1988), "To Bargain or Not to Bargain: That is The Question," *American Economic Review*, 78 (2), pp. 16-20; Lee, D. (1988), "Free Riding and Paid Riding in the Fight Against Terrorism," *American Economic Review*, 78 (2), pp. 22-26; Pillar, P. (2001), *Terrorism and U.S. Foreign Policy*. Brookings Institution Press. Washington, DC.

part, due to federal tax policy, which significantly increases insurers' and reinsurers' costs of accumulating the large amounts of capital necessary to back the sale of terrorism and other catastrophe insurance.

- The mandatory coverage of terrorism losses for workers' compensation policies in all states and for any losses from fires that occur following a terrorist attack in approximately 11 major industrial states leaves insurers exposed to possible large losses that could lead to insolvencies for some of them.
- The expectation that the federal government will provide considerable assistance to uninsured victims of a terrorist attack could distort consumer and firm incentives for buying insurance and investing in loss reduction measures.
- Federal disaster assistance following a major attack will likely be significantly greater with a commensurately higher cost to taxpayers if there is no predefined public sector role in a terrorism insurance program.

I now discuss each of the principles that should guide the analyses of the role of insurance and other risk transfer mechanisms for dealing with the terrorism risk as they relate to the *Terrorism Risk Insurance Revisions and Extension Act of 2007* (TRIA3).

Risk-based Premiums

It should be clear from the above discussion that there are limited data for estimating the likelihood of a terrorist attack and the resulting consequences should such an event occur. Experts utilize a *scenario-based approach* to estimate direct consequences (e.g. physical damage, lives lost) as well as indirect impacts (e.g. losses due to business interruption) from a range of terrorism-related events. However, while the majority of modeling companies and insurers use estimates of recurrence times and probabilities with natural hazards, scenarios do not generate a sufficiently rich set of outcomes to represent the full range of possible terrorism threats. There is an opportunity for insurers to improve their estimates of the likelihood of a terrorist attack to the extent that available information from agencies such as the Department of Homeland Security, the State Department and the Department of Defense can be shared without violating privacy and security considerations.

Even though it may be difficult to achieve risk-based premiums for terrorism, state insurance regulators should not restrict rates unduly to the extent that insurers will not want to provide coverage. Currently, some states limit the premiums that insurers can charge for terrorism coverage. These restrictions may lead insurers **not** to offer property insurance to certain firms if they feel that such coverage will be unprofitable in the long-run.

Equitability

TRIA3 maintains a similar loss-sharing arrangement between the federal government and insurers for an event that is certified by the Secretary of the Treasury as an "act of terrorism" as in the current Act. Today an "act of terrorism" is defined as one

"committed by an individual or individuals acting on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian population of the U.S. or to influence the policy or to affect the conduct of the U.S. Government by coercion," and one in which aggregate insured losses are at least $100 million. The proposed legislation removes the foreign person or interest restriction and reduces the total insured loss trigger to $50 million.

The rationale for a decrease in the loss trigger is that small insurers could suffer severe losses from a terrorist attack, losses that might severely deplete their surpluses or that might lead to insolvency if the current $100 million trigger level were maintained. This proposed reduction to $50 million in total insured losses would thus satisfy the principle of equitability by keeping small firms in business assuming that they would have difficulty obtaining affordable reinsurance premiums to protect themselves from losses between $50 million and $100 million.

By providing financial protection to those who suffer losses from any terrorist attack, whether by a foreigner or someone from this country, the insurance program is more equitable. Under TRIA2, an attack like the Oklahoma City bombing of 1995 that killed 168 people and was the most damaging attack on domestic soil prior to 9/11, would not be a certified event because it would be considered domestic terrorism. It makes good sense to include all "acts of terrorism" as certified events as proposed in TRIA3. In fact, the distinction between what would be a "certified" event covered by TRIA2 and a so-called "domestic" terrorist event may be difficult to establish. For example, are attacks on the U.S. soil similar to the ones perpetrated in London on July 7, 2005 considered domestic or international? We know today that some of the terrorists were British citizens who were trained to kill in Pakistan. The frontier between domestic and international is likely to be a gray area in many cases.

A third area of equitability relates to who should pay for the losses following a terrorist attack. Both TRIA2 and TRIA3 hold that if the insurance industry suffers terrorism losses that require the government to cover a portion of their claims, then these outlays shall be fully or partially recouped *ex post* by levying a surcharge on all commercially insured policyholders, not just the policyholders who had purchased terrorism coverage. This implies that if losses are sufficiently high, the responsibility for recouping these payments rests with all firms who have purchased insurance in any of the TRIA-covered lines.

Using data collected on the top 451 insurers operating in the United States, Kunreuther and Michel-Kerjan[13] examined the impact of the 2006 TRIA2 design on loss sharing between the key stakeholders: victims, insurers and their policyholders, and the taxpayers. By simulating the explosion of a 5-ton truck bomb in major cities in the United States, we conclude that under the current program, taxpayers are not likely to pay anything for losses below $25 billion. For a $40 billion loss, insurers and policyholders

[13] Kunreuther, H. and Michel-Kerjan, E. (2006), "Looking Beyond TRIA A Clinical Examination of Potential Terrorism Loss Sharing," Working Paper No. 12069 (Cambridge, Mass.: National Bureau of Economic Research, February).

would handle between 75% and 95% of the loss depending on the proportion of policyholders who purchased some type of terrorism insurance (i.e. the property take-up rate). In one scenario, all commercial policyholders would end up paying $6.3 billion as the result of the mandatory recoupment, whether or not they had purchased terrorism insurance. Only for terrorist attacks where insured losses were $100 billion or more would taxpayers have to pay 50% of the claims.

Minimize Likelihood of Insolvency

Due to the uncertainty in the likelihood of terrorism losses, insurers use a survival constraint to determine the extent of coverage that they are willing to offer. The essence of the survival constraint is to write coverage so that an insurer's aggregate exposure (*E*) under an assumed scenario will not exceed a certain percentage of its policyholders' surplus (*S*). One can determine how much any particular insurer will have to pay for claims by calculating its deductible *D* under TRIA2 (in 2007 it is 20% of the direct-earned premiums collected for TRIA2-lines in 2006; it was only 7% in 2003 under TRIA1) and then calculating its deductible/surplus (*D/S*) ratio. Those insurers with large deductibles (D) relative to their surplus (S) are the ones most at risk if they are providing terrorism coverage to most of their policyholders. In 2003, 36 out of the 451 largest insurers had a *D/S* ratio above 20%; there were 80 such insurers in 2004 and 162 in 2005 (including 8 of the 30 largest insurers). Such ratios would likely be viewed as extremely high by rating agencies.

In states such as California and New York, where only a few companies insure the largest portion of the workers compensation market, these insurers are likely to bear the largest portion of the losses as well. Should a large-scale terrorist attack occur and inflict mass casualties, their losses could then greatly exceed their TRIA2 deductible. Under TRIA2, 85% of the losses above their deductibles would initially be covered by the federal government and eventually be paid by all policyholders and taxpayers. Since workers' compensation providers are not able to exclude terrorism from their policies, if TRIA2 is not renewed some of these insurers are likely to become insolvent after a large terrorist attack unless they were to be able to obtain protection against catastrophic losses from the private sector and/or reduce their exposure to such losses by downsizing their portfolios.

Sufficient Demand for Coverage

By requiring insurance companies to offer terrorism coverage to their commercial policyholders, TRIA1 and TRIA2 have made terrorism insurance largely available. Data from one of the largest insurance brokers (Marsh Inc.) provides a sense of the evolution over time of the proportion of their clients who have purchased some type of terrorism insurance (i.e. the take-up rate).

At a national level, the Marsh survey indicates a significant and fairly continuous increase of the take-up rate over the four years that the broker has been tracking the purchase of terrorism insurance by its clients that are mainly large companies. According

to its latest report on demand for terrorism insurance,[14] the overall terrorism insurance marketplace remained the same over the past two years with 59% of companies purchasing coverage in 2006, up slightly from 58% in 2005. These data suggests that most of the surveyed companies which wanted such coverage have now purchased it. The remaining companies are self-insured, except for terrorist losses that would be covered by workers' compensation or by fire insurance in the states that cover losses from fire due to terrorism.

Minimize Gaming

TRIA3's requirement that the program be reviewed on a regular basis reduces the likelihood that insurers will engage in gaming behavior. To illustrate, certain very large insurers with low deductible/surplus ratios could strategize by significantly increasing their terrorism underwriting, then collecting large amounts of premiums for terrorism insurance but would be financially responsible for only a small portion of the claims[15]. Commercial policyholders (whether or not they are covered against terrorism) and the federal government would absorb the residual insured losses. How significant this strategy might be depends on several factors, including market share and the loss-sharing design under the program.

There are several reasons why insurers might *not* be willing to assume the large aggregate exposure implied by such a strategy. First, a larger amount of terrorism exposure increases the likelihood that an insurer will experience medium to large losses below its TRIA deductible in high-risk areas. In this case, insurers may decide to limit their aggregate exposure by estimating the likelihoods of different terrorist attack scenarios and reduce their aggregate exposure by utilizing their survival constraint in a manner similar to the processes they follow for other catastrophic risks.

Second, when an insurer provides coverage against terrorism, it also provides insurance against all other events that could cause damage or losses to their property and/or claims from their workers' compensation coverage. An insurer's decision on whether to write more terrorism coverage thus depends upon its aggregate exposure from a much broader set of risks (e.g. fire, theft, job injury).

Insurers may also be concerned that Congress will amend TRIA3 if legislators observe the type of strategizing described above. Suppose insurers who expanded their coverage were to be held responsible for 50% of their losses above their TRIA3 deductible. These insurers will very likely want to cancel some of their commercial policies for fear of incurring large claim costs after a terrorist attack. One reason why these insurers have not followed such a strategy today is their knowledge that TRIA2 is a

[14] Marsh (2007), *Marketwatch: Terrorism Insurance—2006 Market Conditions and Analysis* (New York: Marsh Inc.)

[15] Kunreuther, H. and Michel-Kerjan, E. (2006), "Looking Beyond TRIA A Clinical Examination of Potential Terrorism Loss Sharing," Working Paper No. 12069 (Cambridge, Mass.: National Bureau of Economic Research, February).

2-year program. This is one reason for having a provision in TRIA3 that the program will be reviewed on a regular basis to determine whether it is fulfilling its intended purpose.

4. Summary and Conclusions

The extension of TRIA2 is an important and necessary solution to providing insurance protection to commercial firms. TRIA3 should address the five key principles for providing financial protection against extreme events: ***Risk-based Premiums, Equitability, Minimize Likelihood of Insolvency, Sufficient Demand for Coverage*** and ***Minimize Gaming.*** At the same time the provisions of the bill needs to reflect the special challenges that the terrorism risk presents for insurers who are required by law to offer coverage to commercial enterprises.

TRIA3 modifies the current program by addressing some of the above principles such as equitability, minimizing the likelihood of insolvency and creating sufficient demand for coverage. One also needs to be cognizant of the possibility of gaming when the legislation is reviewed on a regular basis. The bill also creates a Commission on Terrorism Risk Insurance to propose long-term solutions for covering terrorism risks by the private insurance industry. Such a commission in consultation with the Presidential Working Group on Financial Markets could explore the objectives of a terrorism risk financing program and how to achieve them through alternative risk sharing and risk-reducing mechanisms such as more effectively deploying the capital of reinsurers, facilitating the use of terrorism insurance-linked securities, mutual insurance pools and developing incentive programs for encouraging mitigation and investment in security.

The commission could also examine how other countries cope with the terrorism risk to determine whether these approaches merit consideration for the United States. The insurance infrastructure would undoubtedly play a key role in such a program, but it should be viewed as part of a broader strategy for dealing with terrorism. For example, the public and private sectors could provide economic incentives in the form of lower taxes, subsidies or lower insurance premiums to encourage those at risk to adopt higher security and loss reduction measures. It also is likely that there will be a need for well-enforced regulations and standards that complement these incentive programs.