

II. THE CORPORATION, RESPONSIBILITY, AND RISK MANAGEMENT

5. INTRODUCTION

A NEW APPROACH TO THE PRIVATE SECTOR AND HOMELAND SECURITY

Much attention has focused on the prospect of terrorists acquiring weapons of mass destruction, but in the near term they are much more likely to use our own infrastructure against us. On September 11, terrorists wielding knives and boxcutters turned four of our aircraft into guided missiles. Other relatively low-tech attacks could be even more devastating. Most of our infrastructural vulnerabilities are in the private sector. Following September 11, the administration recognized this and issued a National Strategy for the Physical Protection of Critical Infrastructures and Key Assets in February 2003. The strategy set out an approach to protecting these targets that relied largely on letting market forces dictate investment in security. The administration believed that Adam Smith’s “invisible hand” would lead executives to reduce vulnerabilities.

It hasn’t. In their August 2004 report, the 9/11 Commission concluded, “the private sector remains largely unprepared for a terrorist attack.” Despite glaring vulnerabilities in multiple sectors, most estimates place the post–September 11 rate of growth in security spending in the low single digits. In order to close this private sector gap in security, the federal government must act. In this part of the report, we sketch out a new approach to securing the private sector based on the lessons learned over the past four years. The elements of that new approach include:

- ♦ developing an approach to security that treats essential systems and high-impact targets as separate problems that require different solutions;
- ♦ creating an effective framework for partnering beyond the current arm’s-length approach;
- ♦ using smart regulation within a partnering framework; and

- ◆ providing an in-extremis federal backstop for companies that make sound investments to reduce risk and meet federal requirements.

Based on this approach, the Department of Homeland Security (DHS), together with Congress and the White House, could develop a new strategy that would secure the private sector in a way that is now impossible. Unlike previous DHS and White House “strategies,” this strategy would set tangible goals and specific timelines for achieving them. For each sector, the strategy would begin by identifying existing vulnerabilities, the measures needed to reach an adequate level of security, and the mechanisms that would best promote that level of security. In this chapter, we expand on the elements of the approach outlined above. In the following chapters, we apply these principles to the financial, chemical, energy, and cyber sectors of the economy.

ESSENTIAL SYSTEMS VS. HIGH-IMPACT TARGETS

In its National Strategy for Homeland Security, released in 2002, the administration identified thirteen sectors of the economy as “critical infrastructure.” That number has since expanded to seventeen. Four years later, the Department of Homeland Security has yet to determine what assets and operations within these sectors are, in fact, critical. When DHS compiled a list of critical assets supplied by the fifty states, it ran to several thousand facilities. But if everything is critical, nothing is. Widespread application of this term has made it impossible to focus on the private sector operations that are at greatest risk of being attacked, either because they could generate large numbers of casualties, or because an attack would have a cascading effect on the rest of the economy.

Before we can develop a workable strategy to protect critical infrastructure, we need to more narrowly define what we mean by the term. We propose dividing critical infrastructure into two categories: essential systems and high-impact targets.

ASSURING CONTINUITY OF ESSENTIAL SYSTEMS (ACES)

For an asset to be considered an essential system its interruption must have a widespread, cascading effect that would make the sector incapable of providing minimum essential service for a long enough period of time to significantly affect the economy, public health, or national defense. For essential systems, our concern is with key nodes and assets whose failure would prompt this type of outcome.

Revealing the influence of the military on homeland security policy, the administration continues to call upon infrastructure owners and operators to increase their level of protection through the “hardening” of facilities and systems. But other risk management options, such as creating redundancies, relocating assets, and developing rapid response and recovery capabilities, should be seriously considered as alternatives to protective measures. If other nodes or assets have additional capacity to replace what is lost in an attack, additional protective measures may be unnecessary. The ability of the entire system to perform minimum essential functions is the important thing. In some cases, physical protection may be the best, or the only, defense. In others, building resilient systems, focusing on response and recovery, or encouraging the markets to respond quickly may be a better way to manage risk.

SECURING HIGH-IMPACT TARGETS (HITS)

We call private sector entities whose operations can be exploited by terrorists to kill large numbers of people high-impact targets. HITS include chemical plants, natural gas facilities, and nuclear power stations—operations where poor security can endanger thousands of lives. HITS provide terrorists the opportunity to use a conventional attack to generate disproportionately damaging effects. Securing HITS may not be possible through purely voluntary private sector measures. Unlike essential systems, an individual HIT might not be critical to the economy. Owners of HITS are more likely to conclude that terrorism poses little financial risk to their operations and that spending on security is not a

necessary investment. This is when partnering between government and the private sector enters the picture. Within the meaning of the term, the government might mandate security measures in coordination with the private sector, provide financial incentives, or do both in order to maximize security.

MAKING PARTNERING WORK

The owners and operators of critical infrastructure are currently without a competent government partner. There is a growing consensus among experts and policymakers that the prevailing partnership model is not only flawed, but is a major factor in the currently poor state of critical infrastructure protection. Traditional government regulation of security is offered as the only alternative to the partnership model now on the table. This is a false choice. We believe that partnering with the private sector instead of establishing an adversarial relationship is in fact the most effective means of securing infrastructure vulnerabilities. We also believe, however, that smart regulation is consistent with effective partnering, and that it may be needed in certain instances and certain sectors to correct the market's failure to deliver appropriate levels of security. The problem of securing our critical infrastructure is not with public-private partnerships, but with the administration's approach to establishing such partnerships.

POOR EXECUTION VS. FLAWED DESIGN

The Bush administration has correctly identified public-private partnering as a cornerstone of U.S. homeland security policy. The administration has repeatedly stated in its national strategies, plans, and presidential directives that partnership between private industry and government is essential to securing the nation's key resources and critical infrastructure. What it has failed to do is create a structure in which partnering can in fact be an effective mechanism for protecting the homeland. There are no joint processes for developing, implementing,

or reviewing partnership plans. There is no agreement between the government and private sector on the end-state to be reached, the basis for determining when it is reached, or the requirements to sustain it once it is reached. The National Infrastructure Protection Plan (NIPP) is currently in its third draft. We have yet to agree on the process for cataloging critical infrastructure, let alone securing it. The NIPP remains too cumbersome and centralized, and fails to recognize that the sectors are not single players that can easily interface with one small office in Washington.

The result of the Bush administration's approach to homeland security and the private sector is a relationship characterized by a series of arm's-length transactions rather than by close collaboration. The approach creates a division of labor whereby government provides general guidelines of what it would like the private sector to do, and the private sector is expected to carry out in detail what it thinks the government wishes. But matters of security are rarely self-evident, let alone self-executing, in the marketplace. Unsurprisingly, government is frustrated and unhappy with the lack of industry progress in securing itself, but cannot describe the results it wants. Without establishing conditions for effective partnering, defining appropriate levels of security, and recognizing that partnerships and regulation are not mutually exclusive, partnership will remain an ever-receding goal.

ELEMENTS OF PARTNERSHIP

As a first step, the nature of an effective partnership in the context of homeland security must be defined. Partnerships are collaborative enterprises established between parties having defined roles and responsibilities for the purpose of achieving a common goal or outcome. Parties usually enter into such relationships because they cannot achieve their goals through independent efforts, or because independent efforts, even if feasible, would not be cost effective. In the context of critical infrastructure security, public-private partnerships are essential for the purpose of attaining levels of security appropriate to the risks posed by known and evolving threats. These risks must be managed; they cannot be eliminated. Threats must be identified, vulnerabilities assessed, consequences

estimated, and resources allocated *in a collaborative process* to reach an optimal, cost-effective security posture.

As with any collaborative enterprise, public-private partnerships can succeed only to the extent there is agreement on:

- ◆ the outcome to be achieved and the basis for determining when it has been reached;
- ◆ the respective roles and responsibilities of the parties;
- ◆ the processes and procedures by which strategies and plans are to be jointly developed and implemented; and
- ◆ how senior executive participation and commitment will be obtained, and how progress will be assessed, problems identified, course corrections taken, and performance evaluated.

None of these conditions apply in the federal government's current approach to partnering with the private sector on homeland security.

ROLES, RESPONSIBILITIES, AND PROCESSES

To effectively secure critical infrastructure, we must move from the Bush administration's process-driven approach to one geared toward outcomes and results. With no shared strategic vision or end-state, sector partnerships serve today mainly as devices for fostering political inclusion, conduits for exchanging generic information, channels for communicating government policy, and bully pulpits for exhorting industry to make greater strides in security.

As stated above, the desired outcome is to assure the provision of essential services and prevent high-impact targets from being used by terrorists to generate amplified effects. A shared focus on this explicit outcome must be the foundation for effective partnership. A second condition for effective partnering requires agreement on the roles and responsibilities of the parties. In this respect, it is important to remember that government is ultimately responsible for all activities undertaken to secure the homeland, even if it relies on its private sector partners to carry out some of these activities. The government also is responsible for making the case for partnership, establishing the conditions necessary

for launching and sustaining such partnerships, and managing public expectations as to what partnerships can and cannot accomplish. These responsibilities ultimately derive from the government's constitutional obligation to defend the nation against enemies at home and abroad.

Private industry is responsible for working with government to manage critical infrastructure risks that exist beyond the scope of normal business operations, support government operations during national crises or recovery efforts, and continue to manage, on its own, security risks that arise in the course of doing business. The responsibilities of private industry derive not from the Constitution, but from the government's ability to impose such responsibilities through laws and regulations to compel compliance.

Private sector participation cannot be relegated to a select few CEOs on advisory committees. These committees tend to stay away from taking any action that would obligate or commit the private sector to act. The administration, for its part, prepares its strategies and plans without meaningful participation from the private sector.

Industry's hands-off attitude is natural enough. The administration's reluctance is more complicated. The White House insists that the Federal Advisory Committee Act (FACA) prevents the government from engaging with industry on joint plans or operations. At first glance, this seems to be the case: FACA provides that all public-private planning sessions be open to the public unless otherwise exempt. However, Section 871 of the Homeland Security Act of 2002 authorizes the secretary of homeland security to exempt public-private planning from the open-meeting requirement under FACA. The secretary has thus far refused to exercise his authority. This is likely due to political considerations stemming from the administration's poor record on information sharing and public disclosure.

Given the strategic stakes, the administration would be wise to put political considerations aside and instruct the Department of Homeland Security to move quickly to establish joint planning committees for each sector. Exercising his authority under Section 871 of the Homeland Security Act of 2002, the secretary should exempt these joint planning committees from FACA. Once established, these committees should develop infrastructure security plans that specify the security end-state to be achieved, the goals and milestones for achieving it, the standards for implementation and compliance, and

the timelines for accomplishing intermediate actions. Provisions of relevant anti-trust laws must be amended to exempt explicitly standard-setting discussions and planning sessions that would necessarily be part of this joint process. Congress should establish an oversight subcommittee to ensure that partnering between the government and the private sector does not willy-nilly sanction collusion between or among market players.

Even with an open dialogue, the temptation to refer significant partnership disagreements to working group committees rather than resolve the disagreements will at times be irresistible. One way to minimize this is to ensure that chief executives are involved in planning and implementation. Chief executives bring perspective and authority to problems that mid-level officers find insurmountable. They also bear ultimate responsibility for the security of their company, as well as the role their company plays in securing their sector. Chief executive participation would also ensure that jointly developed strategies and plans are followed through. They should not only review and approve such plans, but also commit to implementing them and allocating the resources necessary for success. At this juncture, corporate chief executives—apart from the select few who are members of presidential advisory committees—do not generally view security as their responsibility, or give it much consideration. Their disregard could and should be countered by integrating chief executive review into the joint planning process and by obtaining CEO approval and commitment to carry out plans according to agreed upon timelines.

For individual infrastructure owners and operators, the partnering process should begin by examining their core business functions and operations, in concert with relevant federal partners, to determine which of their assets and systems, if any, qualify as HITS, essential systems, or both. Plans must then be jointly developed with government to manage the resulting security risks.

The Chemical Facility Anti-Terrorism Act of 2005 offers a framework for this joint planning process. The bill, sponsored by Senator Susan Collins (R-ME), would create infrastructure protection regional security offices in each of the eight Federal Emergency Management Agency (FEMA) regions. The bill would also create area security committees for urban areas within each of the regions to work with local partners, both private and public, to secure chemical facilities, share

information, and develop response plans. Though the bill would establish this structure explicitly for the chemical facility, it is clear that the drafters intend the regional approach to be used for other sectors. It is unfortunate that, due to the costs involved, these provisions are likely to be the first on the chopping block when the act is considered this spring. They would represent an immense leap forward in partnering and should be included in the final version of the bill.

SMART REGULATION

Despite appearances, partnership and regulation are not necessarily incompatible approaches to security. Smart regulation can create what the market alone cannot: a set of conditions and incentives that encourage proactive investment and adoption of necessary security measures. Seen in this light, smart regulation could make partnerships more effective. Whether smart regulation is needed, however, depends entirely on the economic and operating conditions that exist within each of the sectors. A one-size-fits-all approach to smart regulation and security will not work.

The development of an appropriate security posture for each of the sectors that need to be defended hinges on a detailed understanding of industry operations and risk management practices. Owners and operators are in a better position than the government to know how to translate homeland security goals and objectives into specific standards and operating procedures for their industries and companies. Close collaboration and coordination between the sectors and government are therefore indispensable.

DHS must be given the authority to regulate industries that could endanger the public if targeted by terrorists. The kind and type of intervention, however, does not necessarily need to follow a traditional regulatory model. To prevent terrorism, security must be dynamic and adaptable. Countermeasures must be designed to thwart adversaries who will engage in reconnaissance and planning. A regulatory model that sets universal standards may be well suited to stopping acid rain, but will do little to prevent a determined terrorist. If regulation requires an eight-foot fence, terrorists will know to bring a ten-foot ladder.

Smart regulation focuses on results or end-states rather than dictating how those results should be achieved. Smart regulation relies on auditors and best practices, rather than government inspectors. In the financial industry, the Securities and Exchange Commission (SEC), with a staff of just 3,100, oversees the \$500 billion securities industry. It does this by requiring that certified accounting agencies audit industry reports against Generally Accepted Accounting Practices. A small number of federal auditors then follow up to verify that the self-regulatory regime is in fact working. While the Enron trial may remind readers of the recent failings of this model in the securities industry, those failures are indicative of poor management and execution, not of any flaw in the design itself.

Applying this to the private sector for security, the Department of Homeland Security should be empowered to certify security-auditing firms, which in turn would evaluate the security of private sector operations and judge whether they meet general standards, given potential threats and consequences. DHS needs the resources to train and certify the auditors and to audit the auditors, as in the SEC model. Such an approach will allow dynamic security regimes to be built cooperatively with industry and tailored to individual facilities and operations. The system would focus on results, rather than dictate how to achieve them. Auditors would certify that companies have assessed their vulnerabilities and taken reasonable measures to remedy them.

USING THE FEDERAL BACKSTOP TO PROMOTE SECURITY

In December, Congress passed a two-year extension of the Terrorism Risk Insurance Act (TRIA) with only minor modifications. The act provides a federal backstop for insurance companies in the event of a terrorist attack, while requiring no action on the part of the private sector to reduce vulnerabilities. Passed as a stopgap measure, TRIA was intended to allow the insurance markets to recover following September 11 and adjust policies and pricing for the newly realized risk of terrorism. Under the program, commercial insurers must offer coverage for terrorist incidents and would be responsible for paying an “insurer deductible”

before federal assistance begins. The federal government will then pay the remainder of insured losses. In the current revision these provisions remain largely unchanged.

The structure of the program, however, disrupts the normal market incentives that insurance companies need to promote risk reduction. When these incentives are properly aligned, insurance companies can actively promote risk reduction. This is why insurance companies give consumers discounts on auto insurance for safe driving records, anti-lock brakes, and airbags, or give non-smokers discounted rates on health and life insurance. For terrorism, however, TRIA removes the market incentive for the insurance industry to quantify the risk, determine the appropriate price of insurance, and provide incentives to reduce risks. In short, TRIA does not promote a “managed care” approach to the problem of terrorism.

If the federal government continues to subsidize terrorism insurance through TRIA as currently enacted, it will effectively encourage the private sector to continue to defer the costs of adjusting to the threat of terrorism. The likely result of this policy will be that losses from future attacks will be greater than they would have been if no federal program were available at all. An insurance program in which the insurer collects no premiums, where the majority burden falls on the government and the taxpayer, and where premiums do not vary with risk or reduction of risk is not in the best interests of the American people.

To fix TRIA, intervention should be retargeted so that companies in critical sectors and high-risk areas are encouraged to invest in reducing their vulnerabilities in exchange for lower insurance premiums. Companies that buy into this insurance program would receive federally backstopped insurance. That insurance would cover damage to property, business continuity losses, group life insurance, and protection from negligence lawsuits. The program would also cover acts of domestic terrorism, which are currently excluded from TRIA. Premium reductions would be tied to mitigation efforts. Participating companies would be granted access to a victim’s compensation fund if an attack succeeds. Insurance companies offering policies under the program would be required to contribute a percentage of the terrorism premium to a federal terror reinsurance pool, with the goal of fully capitalizing the federal government’s obligation without the use of general revenues over a ten-year period. Such a program could reinforce partnering and regulatory approaches, raising security to altogether higher standards.

The insurance industry as a whole has resisted steps to make insurance more of a player in reducing the risk of terrorism. Industry associations maintain that without adequate data from the federal government on the threat of terrorism, they cannot appropriately determine the value of policies on their own. This argument is not without merit. The Department of Homeland Security should establish an office for TRIA, staffed with industry veterans, and should work to provide usable threat data to insurance brokers so that they can make informed decisions on issuing terrorism insurance.

RESPONSE AND RECOVERY

Finally, the administration's approach to the private sector fails to provide a system for managing economic reconstitution in the aftermath of catastrophic events. The administration established the National Incident Management System (NIMS) to enable the federal government to manage national crises and their consequences. In its National Response Plan (NRP), DHS recognizes the potential for large-scale incidents of national significance—caused by cyber or physical attack—to overwhelm government and private-sector resources by disrupting and taxing critical infrastructure systems. DHS also acknowledges, especially in the aftermath of the botched response to Hurricane Katrina, continuing challenges to the effective management of nationally significant incidents, including weak government coordination with the private sector and the uneven availability of secure and reliable communications needed to coordinate response and recovery efforts.

While the effects of some terrorist attacks may be felt immediately, potentially larger and more significant impacts could develop over time and across the economy. For example, many manufacturing systems dependent on critical infrastructure could cease operations, creating further cascading effects down the economic food chain; financial transactions might be halted and coordination of the delivery of goods, especially those dependent on just-in-time delivery systems, could be seriously disrupted. In the event of a catastrophic cyber event, software patches and other IT solutions designed to address specific cyber vulnerabilities and security problems might not get to their intended destinations because the

normal electronic delivery processes provided by the Internet are degraded or disabled.

Neither the NRP nor the NIMS address the complicated problems arising from the need to maintain an orderly functioning national economy in the event that, at the same time, enormous recovery demands are being made in specific affected areas. Administration planning does not consider the question of how two different economies—one market, the other command—might have to coexist during long periods of recovery and reconstitution.

Given the vast amount of corporate resources involved, chief executive involvement is essential; yet there is no process in place to engage executives in an organized and timely way. Indeed, the very magnitude and complexity of reconstituting economic assets and sustaining macroeconomic functionality under these circumstances appears to have led DHS to deem this sort of contingency unfeasible, and thus ineligible for systematic planning and organization.

RECOMMENDATIONS

The root cause for the lack of progress of public-private partnerships is a failure of administration leadership to create the conditions necessary for establishing and supporting those partnerships. If the administration means what it says—that homeland security is a national priority and public-private partnerships are essential to securing the homeland—then establishing effective partnerships with the private sector must also be afforded the status of a national priority.

Below is an eight-point plan for the administration to promote security in the private sector:

5.1. FOCUS ON SECURING HIGH-IMPACT TARGETS AND ASSURING CONTINUITY OF ESSENTIAL SYSTEMS OVER A BLANKET APPROACH TO CRITICAL INFRASTRUCTURE.

5.2. ESTABLISH JOINT PLANNING COMMITTEES FOR EACH HITS AND ESSENTIAL SYSTEM SECTOR. Exercise authority under Section 871 of the Homeland Security Act of 2002 to exempt joint planning committees from FACA. Amend provisions of relevant anti-trust laws to

exempt explicitly standard-setting discussions and planning sessions. Establish a congressional select committee to oversee joint planning.

5.3. ONCE ESTABLISHED, THESE COMMITTEES SHOULD DEVELOP INFRASTRUCTURE SECURITY PLANS THAT SPECIFY THE SECURITY END-STATE TO BE ACHIEVED, goals and milestones for achieving it, standards for implementation and compliance, and timelines for accomplishing intermediate actions.

5.4. INTEGRATE CHIEF EXECUTIVE REVIEW INTO JOINT PLANNING PROCESS; obtain approval and commitment to carry out plans according to agreed-upon timelines.

5.5. IMPLEMENT THE INFRASTRUCTURE PROTECTION REGIONAL SECURITY AND AREA SECURITY FRAMEWORK as set out in the Chemical Facility Anti-Terrorism Act of 2005.

5.6. ADOPT SMART REGULATION ON A SECTOR-BY-SECTOR BASIS TO ENCOURAGE THE DEVELOPMENT AND IMPLEMENTATION OF APPROPRIATE SECURITY MEASURES.

5.7. REVAMP TRIA TO PROMOTE RISK MITIGATION and create a safe harbor against litigation following a terrorist attack where targeted companies have complied with government-approved security standards.

5.8. DEVELOP A CEO-LEVEL SYSTEM FOR MANAGING RESOURCE ALLOCATIONS during recovery and reconstitution phases following a catastrophic national event to allow a coordinated effort with the federal government.



Securing the nation's homeland and critical infrastructure requires a new social contract among government, industry, and the public. All three parties are essential to this contract, because all three have obligations to fulfill. The government must assure the private sector and the public that it recognizes its responsibility to manage all aspects of homeland security competently and effectively. It must create the conditions for the

private sector to carry out its security responsibilities. The government and public must assure the private sector that, if it fulfills its responsibilities to secure HITS and assure essential systems, in the event companies are attacked, they will be shielded from liability. The public must recognize that there is no such thing as perfect security in a free society. It must develop reasonable expectations about what the government and the private sector can accomplish through managing risks to high-impact targets and essential systems. It must also develop the resilience and confidence to go on with life in the wake of an attack, knowing that government and industry are working together in partnership to do all they can to secure the homeland.

