STATEMENT OF
RICHARD A FALKENRATH
VISITING FELLOW
THE BROOKINGS INSTITUTION
BEFORE THE
UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

APRIL 27, 2005

Introduction

Good morning, Madam Chairman, Senator Lieberman, and Members of the Committee. I am grateful for the opportunity to be here today to provide my views on the vulnerability of toxic industrial chemicals to terrorist attack and the steps which could be taken to better protect this target set.

For the record, my name is Richard A. Falkenrath and I am presently a visiting fellow in foreign policy studies at the Brookings Institution. I am also Senior Director of the Civitas Group LLC, a strategic advisory and investment services firm serving the homeland security market; a security analyst for the Cable News Network (CNN); and a member of the Business Advisory Board of Arxan Technologies. Until May 2004, I was Deputy Assistant to the President and Deputy Homeland Security Advisor on the White House staff. Previously, I served as Special Assistant to the President and Senior Director for Policy and Plans within the Office of Homeland Security, and as Director for Proliferation Strategy on the National Security Council staff. Prior to government

service, I was an Assistant Professor of Public Policy at the John F. Kennedy School of Government, Harvard University.

Caveats

Before beginning my analysis of this matter, I would like to offer three general caveats.

First, and most importantly, I am in general against calling attention to America's most serious vulnerabilities. I believe that information relating to these vulnerabilities should be carefully guarded – and should never be sensationalized – because of the possibility that it will be used against us. Knowledgeable private citizens should discuss this information in public only when the government manifestly fails to address a pressing danger – and even then should do so with great care. I regret that I have come to the conclusion that, in my current capacity as a private citizen, a blunt public discussion of my analysis of this issue is a better course of action than silence.

Second, I was among those who were responsible for this policy issue on the White House staff after September 11, 2001, until mid-May 2004, when I left the government. My testimony today will be critical of the results the Administration has achieved in reducing the vulnerability of chemical targets in the United States. I will not, however, offer any testimony that would betray the confidentiality of the privileged internal discussions to which I was privy. I also will not attempt to assign responsibility within

the Executive Branch for this lack of results except to acknowledge, regretfully, that some portion of this responsibility clearly belongs to me.

Third, my only interest in this matter is the security of the U.S. homeland. I have no present or prior association with the environmental movement that has for years sought tighter regulation of the chemical industry, or with the industry that would be affected by such tighter regulation.

A New Mission: Critical Infrastructure Protection, Prioritization, and Protection

The basic strategy employed by Al Qaeda on September 11, 2001, was to strike a common, poorly secured commercial system in a manner that would cause catastrophic secondary effects. The terrorists did a better job identifying the particular vulnerability associated with the suicide hijacking of fully fueled commercial airliners than the government did, and then exploited this vulnerability to terrible effect. In the aftermath of the attack, the Administration and the Congress acted quickly and aggressively to reduce the vulnerability of U.S. commercial aircraft to suicide hijacking. I now think it is safe to say that our commercial aircraft are virtually impossible to hijack; only a very foolish terrorist would even try.

Suicide hijacking of commercial aviation is, of course, only one of many different tactic/target combinations available to a terrorist organization. Because terrorists are adaptive enemies, we must assume that they are continually searching out other

catastrophic vulnerabilities in our society. One central question in homeland security is whether the terrorists will again locate another major vulnerability in American society, exploiting it to catastrophic effect just as they did on September 11, 2001.

Prior to the creation of the Department of Homeland Security, no government department or agency was responsible for the broad-based strategic protection of the United States from high-consequence terrorism. Today, as a result of the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7, the Secretary of Homeland Security is responsible for identifying and prioritizing potentially catastrophic vulnerabilities in the U.S. homeland, analyzing their present security schemes, and effecting appropriate security enhancement wherever the current security arrangement is deficient. Beneath the Secretary, lead responsibility for this mission has been assigned to the Under Secretary for Information Analysis and Infrastructure Protection, though the successful implementation of this mission will require close collaboration with other parts of DHS, other federal departments and agencies, state and local government agencies, and the private sector.

This mission, which is one of the very few genuinely new missions of the Department of Homeland Security, is by presidential directive labeled "critical infrastructure identification, prioritization, and protection."[1] Critical infrastructure protection policy is, in

1. The term "critical infrastructure" became popular in the late-1990s, when it was the subject of Presidential Decision Directive 63, but it is somewhat misleading in the post-9/11 era. "Critical infrastructure" refers most appropriate to a few key technological systems, such as the Internet, electricity grid, or air traffic control system, upon which American society and government are highly dependent and which destroyed or damaged (in by a terrorist, natural disaster, or major technological failure) could cause cascading economic and operational effects. Since 9/11, the government's concern for critical infrastructure *per se* remains valid, but the government has had to expand the range of potential targets it

its essence, strategic defense against a notionally omniscient terrorist enemy. If Al Qaeda knew as much as we know about our own country, how and where would it attack us to achieve the highest expected damage? In its simplest form, the answer to the question will be a combination of potential damage and inherent difficulty of a particular terrorist tactic against a particular target. The highest priorities in our strategic defense against terrorism should be those tactic/target combinations that are least difficult to perpetrate and most likely to cause the highest levels of damage. Once we have answered this question, we will know where we should apply our marginal resources.

Four key criteria will determine the extent to which the Administration succeeds or fails in this new mission.

First, the responsible officials must understand the differences tactical offense and strategic defense – in other words, between preventing a threat and protecting a vulnerability – and must know that both are essential.

- Tactical offense, also known as prevention or counterterrorism, depends on threat assessment, which is the evaluation of indicators, usually derived from

---

is concerned about to include those which present the possibility of extraordinarily but essentially localized secondary effects, including mass casualties. Accordingly, in 2003 the President directed the Secretary of Homeland Security to attach "emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction." Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection,, para. 13.

intelligence, about particular terrorist groups, intentions, plans, and operations.

- Strategic defense in homeland security depends on vulnerability assessment, which is the analysis of the full range of potential terrorist tactics and targets – not just those which are the subject of current intelligence – for the purpose of determining which target/tactic combinations, if employed by terrorists, present the highest likelihood of causing the greatest damage.

The Executive Branch has a large and highly energetic system for tactical offense against terrorist threats. Literally thousands of U.S. officials are engaged in this activity around the clock every day of the year. Interagency information sharing and joint action is routine and extensive. Credible intelligence on current threats is immediately briefed to the very highest levels of the government and almost always results in some form of prompt operational response.

The system for identifying, assessing, and acting against vulnerabilities is far less mature and far less effective. The mid-level officials who should be focused on vulnerability assessment and target protection are too often pulled into the daily cycle of tactical offense against current threats. The senior officials who should concern themselves with both sides of the equation often focus only tactical offense.

Second, the officials responsible for target protection must set priorities. The country cannot protect all targets, all the time, against all manner of attack. Fortunately, not all potential tactic/target combinations are equally dangerous, and the differences can be revealed through a rigorous strategic vulnerability assessment of the sort I described above. Later in my testimony I will provide a simple strategic vulnerability assessment that illustrates how priorities could emerge from such an analysis.

Third, the responsible officials must be determined to get results – that is, real reductions in the inherent vulnerability of potential terrorist targets – against the highest priority (i.e., most dangerous) target/tactic combinations. This determination, if it exists, will manifest in hard objectives and deadlines imposed from above; outcome-based measurements of real-world progress that burn through the obfuscation of bureaucratic activity reports; and creativity about the means of achieving these concrete objectives. The U.S. government has an extraordinary range of instruments that can be used to achieve particular target protection objectives: many different legal authorities to regulate industries; the ability to appeal to state and local governments with their own regulatory authorities; the ability to set conditions on grants and participation on federal programs; the ability to offer many different kinds of grants and in-kind assistance; the ability to set standards; the ability to appeal to business and community leaders for cooperation; the ability to generate publicity (good or bad) for a particular company; etc. These instruments of course do not reside exclusively within the Department of Homeland Security, but by presidential directive the Secretary of Homeland Security is expected to coordinate “the overall national effort to enhance the protection of the

critical infrastructure and key resources of the United States,"[2] including those instruments and authorities which reside outside of the Department.

A quality critical infrastructure protection operation at DHS will need to be aware of all of these different instruments – including those which reside on other federal departments and agencies – and skillful at employing them to achieve particular, high-priority target protection objectives. A poor vulnerability assessment and target protection operation at DHS will act as if it can only employ those governmental instruments that reside in the information analysis and infrastructure protection directorate; will mistake activity for accomplishment; and will exhibit none of the determination that is so readily apparent among U.S. counterterrorism officials.

Fourth, if the Executive Branch lacks the legal authority or the financial resources necessary to achieve some particular, high-priority target protection objective, then it must ask the Congress to confer the authority or appropriate the resources. Once the request has been made, it is up to the Congress to consider the issue and take appropriate legislative action. If the Congress declines the Administration's requests for additional authority or resources, then it must share responsibility for the government's failure to achieve results.

---

2. Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, para. 12.

The Danger of TIH Chemical Targets in Context

Of the all the various remaining civilian vulnerabilities in America today, one stands alone as uniquely deadly, pervasive, and susceptible to terrorist attack: toxic-inhalation-hazard (TIH) industrial chemicals, such as chlorine, ammonia, phosgene, methyl bromide, hydrochloric and various other acids. The IDLS (immediately dangerous to life standard) for the two most common industrial TIH chemicals, ammonia and chlorine, is 500 and 10 parts per million, respectively.[3] These are extraordinarily dangerous substances: several are identical to those used as weapons on the Western Front during the First World War.

TIH industrial chemicals are essential to our economy and are routinely shipped through and stored near population centers in multi-ton quantities. Storage facilities for these ultra-hazardous chemicals routinely contain thousands of tons. The security that exists at any particular facility is essentially the outcome of voluntary, discretionary decisions made by the owners and operators of the facilities. There is no security whatsoever along TIH transportation routes. There exists no comprehensive, authoritative assessment of the quality of the security of U.S. chemical facilities and the conveyance systems, but anecdotal information of poor or non-existent security in this sector is overwhelming. The contrast to the security at commercial airports and nuclear power plants, both of which are strictly regulated by the federal government, is telling.

3. The IDLS is a regulatory value defined as the maximum exposure concentration in the workplace from which one could escape within 30 minutes without suffering symptoms which would interfere with escaping ans without suffering any irreversible health effects. http://www.cdc.gov/niosh/intridl4.html

A cleverly designed terrorist attack against a TIH chemical target would be no more difficult to perpetrate than was the simultaneous suicide hijacking of four commercial aircraft by 19 terrorists, four of whom had pilot training, on September 11, 2001. Without going into details, it should suffice to say that there are a large number of possible terrorist tactics for triggering a large-scale release of a TIH chemical in proximity to a dense population concentration, none of which are particularly difficult.

Although many variables would determine the lethality of such an attack, the loss of life could easily equal that which occurred on September 11, 2001 – and might even exceed it by an order of magnitude or more. Although there is some debate about just how dangerous are the most dangerous facilities, even the most conservative estimates of the Department of Homeland Security concede that there is at least one TIH chemical facility which, if successfully attacked, could result in more than one million human deaths. Specific scientific estimates of attack scenarios that could result in tens or hundreds of thousands of human deaths are commonplace.

In short, the casualty potential of a terrorist attack against a large TIH chemical container near a population center is comparable to that of a fully successful terrorist employment of an improvised nuclear device or effective biological weapon. The key difference is that TIH chemical containers are substantially easier to attack than improvised nuclear devices or effective biological weapon are to acquire or fabricate.

Figure 1
Illustrative Comparison of Select Terrorist Tactic/Target Combinations

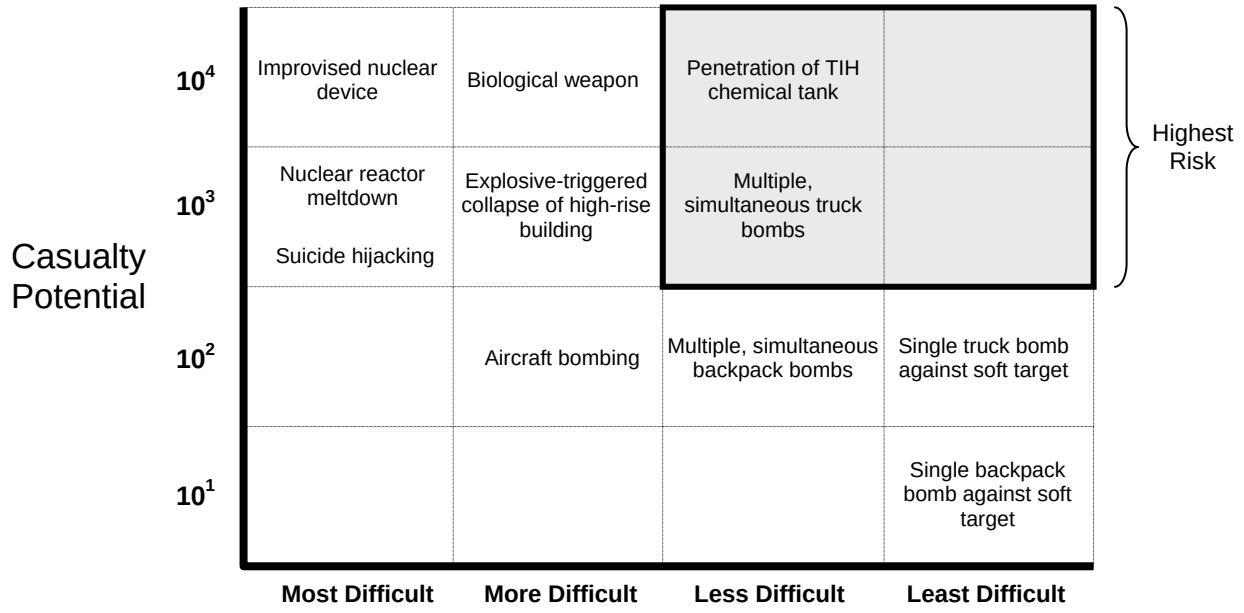

Figure 1 presents a simple but essentially accurate comparison of a few noteworthy terrorist tactic/target combinations. (A similar illustration could be constructed for tactic/target combinations that present major economic risks, but I personally believe that attacks which could result in significant human casualties deserve priority (ceteris paribus) for the simple reason that the country can recover from economic losses but cannot bring back the dead.)

In sum, I am aware of no other category of potential terrorist targets that presents as great a danger as TIH industrial chemicals.

Summary Assessment of Chemical Sector Vulnerability Reduction since September 11

There been no significant reduction in the inherent vulnerability of the most dangerous TIH chemical facilities and conveyances to terrorist attack since September 11, 2001.

What little progress has occurred at the largest chemical facilities owned by the largest, best-known chemical corporations, some of whom have undertaken select security enhancements on a voluntary basis. These facilities tend to be large, with considerable set-back from public roads, and are usually located away from major population concentrations. The voluntary security enhancements implemented by many of the larger chemical firms – in some cases with assistance from the Department of Homeland Security – are a step in the right direction but are insufficient because of their limited scope.

I have noticed two disturbing tendencies among many of the government officials who have been responsible for this issue. The first is that they tend to confuse bureaucratic activity with results. Measurements of progress, if they are offered at all, almost invariably focus on inputs, not outcomes.

The second is that they seem to believe that their only options for improving the security of chemical facilities and conveyance systems in the United States are voluntary

measures conducted in cooperation with the chemical industry. Clearly, where results can be achieved on a voluntary basis, they should be. But it is a fallacy to think that profit-maximizing corporations engaged in a trade as inherently dangerous as the manufacture and shipment of TIH chemicals will ever voluntarily provide a level of security that is appropriate given the larger external risk to society as a whole. Nor is this is an especially radical point of view: the body politic does not trust nuclear power plant or commercial airport operator to provide appropriate levels of security on a voluntary basis, and for good reason.

Proposed Outline for Chemical Site Security Legislation

When I testified before this committee on January 26, 2005, I called upon the Congress to pass comprehensive chemical site security legislation that would confer powerful new regulatory authorities upon the Secretary of Homeland Security. I will now provide my views on how such legislation should be structured.

First of all, I want to make clear that I do not believe the federal government currently has sufficient legal authority to regulate the security measures at chemical plants and storage facilities. Some have argued that sufficient authority has already been conferred to the Executive Branch by the general duty clause of the Clear Air Act.[4] I do not agree: the legal merits of this claim are suspect, but more importantly, as a practical political matter, any new regulatory initiative with enormous economic implications

4. Linda Greer, *New Strategies to Protect America: Securing Our Nation's Chemical Facilities*, Center for American Progress, 2005, pp. 10-11.

requires unambiguous statutory authorization.[5] The Administration also does not agree, which is why President Bush has twice called upon Congress to pass legislation that would unambiguously confer chemical security authority upon the Department of Homeland Security.

I favor a new chemical site security statute that would establish a regulatory approach with six basic parts:

1. A comprehensive, compulsory, and detailed inventory of all chemical facilities in the United States, organized into tiers according to each facility's risk;

2. Mandatory, graduated federal standards for the security of chemical facilities in each tier;

3. A time-phased certification procedure by which the owners or corporate directors of chemical facilities would vouch that they have attained the mandated security standard for their facility;

4. A verification procedure by which the government would confirm that the certifications provided for each chemical facility is complete and accurate;

5. Similarly, it could be argued that the Maritime Transportation Security Act of 2002 (MTSA) provides the authority to regulate chemical facilities at the waterline. While the legal merits of this argument appear to be stronger than those relating to the Clean Water Act, the legislative history of the MTSA makes clear that the Congress did not contemplate that this legislation would used to address the security risks of the chemical sector in particular.

5. A compliance procedure by which the government could compel the owners or corporate directors of chemical facilities to meet the mandated security standards through escalating civil and criminal penalties; and

6. An appeal procedure by which the owners or corporate directors of chemical facilities could contest and seek relief from governmental findings and penalties related to the security of their facilities.

I believe that this regulatory regime should be administered by the Department of Homeland Security, which should be proscribed by law from using these powerful new authorities for purposes that do not directly relate to the protection of chemical targets from terrorist attack.

1. Inventory

DHS should be required to develop and maintain a comprehensive, highly detailed computerized inventory of all chemical facilities and systems in the United States. Congress should impose a deadline for the establishment of this inventory, certainly no more than one year after enactment of the statute.

To create the inventory, each chemical facility in the country should be required to provide (and, as needed, update) to DHS a comprehensive data declaration concerning the types and volumes of chemicals present, movements of these chemicals, site layout, security systems, and any other information deemed pertinent by the Secretary

of Homeland Security. The data declarations should be compulsory; inaccuracies should be punishable by civil and criminal penalties against the owners or corporate directors of the facility in question. These data declaration should be consistent with, but expand upon, the Risk Management Plans that chemical companies are already required to provide to the Environmental Protection Agency. All information in this inventory should be protected from public release by the authorities already granted to the Secretary of Homeland Security by the Critical Infrastructure Information Act of 2002.

Once the inventory has been established, the Secretary should be required to organize it into a limited number of tiers (no less than four, no more than ten) according to objective, analytically based criteria. For instance, a high-throughput facility next to a dense population center and containing extremely large quantities of the most toxic chemicals would rank in the top tier, while a small, relatively inactive facility in an uninhabited area with only mildly toxic chemicals would rank in the bottom tier. The criteria for each tier should be transparent to the chemical industry so that individual facilities could have the opportunity to be reclassified into a lower tier by modifying their business operations.

2. Tiered Standards

The importance of the tiered structure of the DHS chemical facility inventory lies in the standards the Secretary of Homeland Security would be required to promulgate -- again, according to a statutorily prescribed deadline, in this case of no more than 18

months after enactment. In recognition of the different risk presented by different facilities, the Secretary should be required to establish graduated security standards for each tier of facilities. The standards should be operational, pragmatic, and measurable: for example, strength and height of exterior fencing; set-back distances; number of guards per acre; training standards for security personnel; quality of alarms and lighting; extent of sensor systems; manner of employee background checks; communication systems with local police agencies; nature of access control system; frequency and rigor of security drills; etc. These standards would become progressively more stringent for the more dangerous facilities in the higher tiers of the inventory.

Because compliance with these standards would be costly, and because facilities could apply for reclassification based on modifications in their business operations, a regulatory regime of this kind would create market-based incentives for the chemical industry to reduce the inherent danger of their facilities and practices.

Given the importance of these standards to the overall security scheme for the chemical sector, each new Secretary of Homeland Security should be required to review the standards he or she inherited from the outgoing Secretary, should have the opportunity to amend the standards as needed, and should be required to certify personally to the President and the Congress that the standards are sufficient to hold the risk of a terrorist attack against a U.S. chemical facility to an acceptable level.

3. Certification procedure

Once the Secretary's security standards have gone into effect, the owners of chemical facilities should have a limited, statutorily prescribed period to bring each of their facilities into compliance with the standard. At the end of this period, the owners or corporate directors of each facility should be required to certify that the standard has been attained, to attest that the standard will be maintained indefinitely, and to acknowledge that they bear civil and criminal liability for any failure to maintain the standard.

Although the principle of corporate responsibility should remain inviolate, the chemical industry should be granted substantial flexibility to design efficient processes for complying with the new federal chemical site security regulations. For instance, the owners or corporate directors of chemical facilities should have the opportunity to retain – individually or collectively – external review boards or independent auditors to assist them in determining that their facilities have in fact met the appropriate federal security standard.

4. Verification procedure

Once a certification has been filed for each chemical facility in the country, DHS should then be required to begin a process of verifying that the certification, as well as the underlying data declaration, is correct. Such a process would proceed in phases, starting with an initial baseline phase and then followed by annual maintenance phase, and should be governed by statutorily defined deadlines. Throughout the process,

highest priority should be afforded to verifying the certifications of the highest tier (i.e., most dangerous) facilities.

In order to minimize the Department's need to hire new staff, DHS should have a high degree of flexibility in designing its verification procedures, including the option to employ other federal agencies, state and local agencies, private firms, and industrial associations as its agents in the verification process. DHS or its agents should have the unlimited right to demand additional information from chemical facilities and to conduct on-site inspections, including no-notice on-site inspections; indeed, DHS should be required by statute to conduct regular no-notice, on-site inspections of the most dangerous facilities in its inventory.

5. Compliance procedure

The Secretary of Homeland Security should be required to establish a system of escalating civil and criminal penalties for failure to comply with federal chemical security standards. The Secretary's authority to fine non-compliant facilities should be extremely powerful, comparable to the strongest U.S. regulatory agencies, and sufficient to compel even the largest corporation to comply. The criminal liability associated with non-compliance with the federal chemical security standards should certainly be no less stringent than that imposed by the Sarbanes-Oxley Act of 2002 for fiduciary malfeasance.

6. Appeal procedure

Any grant of regulatory authority as powerful as the one proposed here requires careful thought about how best to ensure that the new authorities are not abused. The regulated community has a right to the fair and even-handed application of federal power, and to contest in court any capricious, unjust, or overly broad federal action. While the Secretary's authority to demand information on chemical facilities, conduct on-site inspections, classify facilities into tiers, and establish security standards should be under his or her exclusive authority, with no opportunity for appeal to the courts, the regulated community should have the right to contest the procedural fairness of civil penalties imposed by the Secretary in federal court. Criminal prosecution for non-compliance with the chemical security standards, of course, would be handled by the Department of Justice according to normal criminal procedures.

A critical element in a chemical security appeal procedure, however, will the statutory provisions for protecting sensitive information relating to the vulnerability of particular chemical facilities or systems. A referral of a chemical security issues to the courts should not result in the publication of information which could assist a terrorist organization in locating and attacking a target which presents the potential for catastrophic civilian casualties. Accordingly, the authorizing statute should establish a regime for protecting this information in judicial processes, for example by extending the procedures of the Classified Information Protection Act (CIPA) to cases involving chemical security vulnerability information.

Chemical Security in Transit

In contrast to chemical facilities, the federal government already has the authority to regulate the security of chemicals as they are being transported on our roads, railways, and waterways. These authorities, which are vested in both the Secretary of Transportation and the Secretary of Homeland Security, have been conferred by the Hazardous Materials Transportation Act, the Federal Railroad Safety Act, the Aviation and Transportation Security Act, and the Homeland Security Act, among others.

The Administration has not exercised its authority to enhance the security of toxic chemicals in transit in any significant way since the terrorist attacks of September 11, 2001. There has, as a result, been no meaningful improvement in the security of toxic-by-inhalation chemicals moving through our population centers.

The Administration can and should act immediately to mandate a systematic, nationwide reduction in the vulnerability toxic chemicals in transit nationwide. Specifically, the Departments of Homeland Security and Transportation should promulgate regulations that over time will, at a minimum:

- require chemical shippers to track the movement of all hazardous chemicals electronically;
- to report this positional data to DHS in real time;
- to deploy fingerprint-based access controls for all chemical conveyances;

- to adopt an inapparent placarding system;
- to perform rigorous background checks on all employees;
- to strengthen the physical resilience of chemical containers;
- to reduce chemical loads;
- to ship empty, decoy containers alongside filled containers;
- to install perimeter security at loading and switching stations; and
- establish significant civil and criminal liability for noncompliance with these regulations.

Although no new legislation is required is required for the Administration to take this regulatory action, a new statutory mandate to move in this direction could certainly not slow the administrative process any further. In addition, if the 109th Congress does in fact act to confer chemical facility regulatory authority, then it would be sensible to require the facility and transport security regulations to be developed and implemented in concert.

Costs

Federal action along these lines that I have proposed here would be costly. Although there would be some implementation cost for the government, most of the cost of these regulations would be borne by the chemical industry. Over time, the costs would be passed on to consumers and the market would adjust to a new, more socially responsible equilibrium. It is right and proper for the government to require industries

to internalize the external security costs of their activities. The real losers would be Al Qaeda and its successors, who would be deprived of the astounding killing potential of toxic-by-inhalation industrial chemicals.

Conclusion

I do not make this recommendation for a new chemical security regulatory regime lightly. I am a believer in small government and private enterprise. But I also understand the economics of externalities and the character of America's vulnerabilities to catastrophic terrorist attack. The chemical sector is unique both in the danger it poses as a terrorist target and in its extraordinary freedom from governmental security oversight. Given the ease with which TIH chemical targets could be attacked and their enormous potential for secondary civilian casualties, I am convinced that the actions I have outlined are warranted. I have no doubt that the government would go at least this far in the aftermath of an attack that kills thousands.