COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021
Tel 212 434 9400 Fax 212 434 9875

"Ending the Post 9/11 Security Neglect of America's Chemical Facilities"

Written Testimony before

a hearing of the

Committee on Homeland Security and Governmental Affairs

United States Senate

on

"The Security of America's Chemical Facilities"

by

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies

Room 562
Dirksen Senate Office Building
Washington, D.C.

10:00 a.m.
April 27, 2005

"Ending the Post 9/11 Security Neglect of America's Chemical Facilities"

by
Stephen E. Flynn
Jeane J. Kirkpatrick Senior Fellow
for National Security Studies

Chairman Collins, Senator Lieberman, and distinguished members of the Committee on Homeland Security and Governmental Affairs, I am the Jeane J. Kirkpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations. I am honored to appear before you this morning to discuss the vitally important issue of assessing the security of America's Chemical Facilities and to provide recommendations for moving beyond the tepid federal government effort since 9/11 to reduce the vulnerability of this critical sector to terrorism.

There is no more important work this Committee can undertake than holding hearings such as this one . With the passage of time, it has become tempting for many in Washington to become self-congratulatory about the efforts that have been made to date to deal with the catastrophic terrorist threat. Some would like to believe that our post-9/11 military operations in Iraq and Afghanistan have dissuaded terrorists from doing their worse on U.S. soil or at least distracted them from attacking the U.S. homeland. Others would like to assign a deterrent value to the very modest measures that have been taken to date to bolster security at home.

On the other end of the spectrum, as Americans become aware of just how "target-rich" we are as a nation, many simply become fatalistic. One view holds that a determined terrorist will succeed no matter what measures we put in place so any effort is hardly worth the effort. Some go so far as to argue that the expense of safeguarding what is valuable and vulnerable in our midst is itself a concession to terrorism; i.e., "the terrorists have won" if we have to make post-9/11 adjustments to the way we conduct business or go about our daily lives.

When the optimists who believe America is winning the war on terror by way of its overseas exertions are combined with the pessimists who believe efforts to protect the U.S. homeland are futile, what is left is a very small constituency who support tackling the complex issue of critical infrastructure protection. This is why it so important that this committee continues to exercise leadership on these issues.

It is my conviction that al Qaeda or one of its many radical jihadist imitators will attempt to carry out a major terrorist attack on the United States within the next five year. At the top of the list of likely targets is the chemical industry. I also believe that there are practical steps that can be taken right now at a reasonable cost that can reduce the risk that the next terrorist attack will be catastrophic. We must necessarily begin with a far more active role by the federal government in advancing security within an industry that has long been accustomed to managing its own affairs.

The case for purposeful federal leadership to bolster security in the chemical industry, rests on two legs. First, is the attractiveness of the industry as a potential terrorist target. Second, are the inherent limits of the marketplace—left on its own—to advance security within this sector.

THE THREAT

One of the questions that is asked with growing frequency today, is why there has not been another attack since 9/11? If America is indeed vulnerable, why have the terrorists not struck again? Implicit in this question are both: (1) a critique that perhaps observers like me are overstating the threat and underestimating what the U.S. government has accomplished since 9/11 to reduce the risk, and (2) a concern that new investments in added security may end up being wasteful.

There is a compelling explanation for a lengthy interval between the 9/11 attacks and the next attack that should serve as an antidote for the quickening slide back towards national complacency. Al Qaeda has made clear that they want to carry out a more devastating attack then those on New York and Washington. Launching such an attack requires developing a plan and mobilizing the capacity to carry out that plan. This includes setting up a logistics cell, surveillance cell, and attack cell to scope out the target, conduct dry runs, and ultimately to execute the attack. Establishing this organizational capacity takes time, particularly within the United States where al Qaeda must work from a much smaller organizational footprint than it has in Western Europe or countries like Indonesia. Going after lesser targets puts that organization at risk because any attack exposes terrorist cells to enforcement action. This is because it is impossible to carry out an attack without leaving a forensic trail that can put a carefully built organization at risk. In short, while it is true that there are many easy targets within the United States that terrorists could have struck since 9/11, carrying out a truly catastrophic terrorists attack requires more time.

Of the carefully selected potential targets that al Qaeda or its imitators might seek to attack, the chemical industry should be at the top of the list. There are hundreds of chemical facilities within the United States that represent the military equivalent of a poorly guarded arsenal of weapons of mass destruction. Terrorists do not need to produce or procure chemical weapons and smuggle them into the United States. Just as on 9/11 they converted domestic airliners into missiles that destroyed the twin towers, they can target facilities that manufacture or conveyances that transport such lethal chemicals as chlorine, anhydrous ammonia, boron triflouride, cyanide, and nitrates. These facilities are found around the country in industrial parks, in seaports, and near the major population centers. Dangerous chemicals routinely travel along our highways, inland waterways, and on railcars that pass through the heart of major cities including Washington, D.C. just a short distance from Capitol Hill. Terrorist attacks on the U.S. chemical industry have the potential to kill tens of thousands of Americans and seriously injure many more. In many instances, these attacks hold the potential for having a cascading effect across other infrastructures, particularly in the energy and transportation sectors. This is both because of the damage that can be caused by the attack, and the

enormous expense and effort associated with the clean-up to an affected area in its aftermath. The four metropolitan areas that deserve the most federal attention and support are Newark, New Orleans, Houston, and Los Angeles.

THE LIMITS OF THE MARKET

The White House National Strategy for Homeland Security, released on July 16, 2002, assigns most of the responsibility for funding the protection of potential targets within U.S. borders to the private sector. In Chapter Six, "The Costs of Homeland Security," the strategy lays out "the broad principles that should guide the allocation of funding for homeland security (and) help determine who should bear the financial burdens." It declares:

> *"The government should only address those activities that the market does not adequately provide—for example, national defense or border security. . . . For other aspects of homeland security, sufficient incentives exist in the private market to supply protection. In these cases we should rely on the private sector."*

Unfortunately, this expression of faith in the market has not been borne out by security investments within the private sector. According to a survey commissioned by the Washington-based Council on Competitiveness just one year after September 11, 92 percent of executives did not believe that terrorists would target their companies, and only 53 percent of the respondents indicated that their companies had increased security spending between 2001 and 2002. With the passing of each month without a new attack, the reluctance of companies to invest in security has only grown.

If there were indeed "sufficient incentives in the private market to supply protection," there would be no need for the hearing we are having today. 3 ½ years after the September 11 attacks we should be seeing the chemical industry making substantial investments in addressing longstanding security weaknesses. But, there are two barriers to this kind of investment taking place. First, executives in this increasingly competitive industry worry that such investments will place them at a competitive disadvantage. Second, there are unique liability issues associated with industry-led efforts to define and implement adequate security.

Security is not free. A company incurs costs when it invests in measures to protect the portion of a vital sector it controls. If a company does not believe other companies are willing or able to make a similar investment, then it faces the likelihood of losing market share while simply shifting the sector's vulnerability elsewhere. If terrorists strike, the company will still suffer the disruptive consequences of an attack right alongside those who did nothing to prevent it. Those consequences are likely to include the cost of implementing new government requirements. Therefore, infrastructure security suffers from a dilemma commonly referred to as the "tragedy of the commons."

The "tragedy of the commons" applies to the chemical industry in this way: By and large, chemical manufacturers have had an impressive safety record. They routinely work with and transport some of the most dangerous substances known to man, but accidents that result in serious loss of life and damage to the environment are rare. However, the post 9/11 security imperative poses a special challenge for them. Operating on thin profit margins and faced with growing overseas competition, most companies have been reluctant to incur the additional costs associated with improving their security. Consider the case of a hypothetical manager of a chemical plant who decides to spend a day looking around his facility to access its security and discovers many serious lapses. After a fitful night of sleep, he wakes up and decides to invest in protective measures that raise the cost to his customers by $50 per shipment. A competitor who does not make that investment will be able to attract business away from the security-conscious plant because his handling costs will be lower. Capable terrorists and criminals will target this lower-cost operation since it is an easier target. The result is that the terrorist threat is only displaced, not deterred.

Even if the chemical industry could agree amongst itself to a common set of security measures and felt confident that good faith efforts would be made across the sector to abide by them, it still faces the unique uncertainties associated with liability when it comes to deciding, "how much security is enough." Since all security measures follow the rule of diminishing returns; i.e., higher investments buy incrementally less additional security; at some point a decision about the cost-benefit trade-off must be made. When executives make decisions about safety or other business issues, they can refer to empirical data from reliable open or proprietary sources. But decisions about adequate security require information about the threat. Typically, that information/intelligence is carefully controlled by the public sector and often lacks specificity. So the private sector is left essentially making their best guess about how much security they should invest in. However, a successful attack on their sector in the wake of new investments to protect it, will inevitably lead to a public judgment that the bar was set too low.

The only way to prevent the tragedy of the commons and to address the liability issue is for the public sector: (1) to be intimately involved in the decision about what security measures should be taken, (2) to have a credible enforcement role in assuring industry compliance with these measures, and (3) to provide a reasonable level of indemnification should agreed upon security measures be found wanting following a terrorist attack; i.e., to provide the industry with a measure of "Good Samaritan" protection as long as they abide by agreed upon standards . In short, security of critical infrastructures such as the chemical industry requires an effective performance-based regulatory regime developed at the federal level. To this end, I recommend this committee consider holding hearings and drafting legislation that incorporates the following:

(1) Provides the necessary resources for the Department of Homeland Security to work with (a) the Local Planning Emergency Committees created under the Emergency Response and Community Right to Know Act (EPCRA) and (b) the FBI's district-based "INFRAGARD" program to identify minimal standards for the industry to:

- Establish physical security, communications capabilities, and access control at chemical facilities based on the quantity and lethality of the chemicals produced and stored within a facility, its proximity to major population centers, and its proximity to other critical infrastructure such as energy and transportation.
- Conduct regular exercises to test the adequacy of security measures to prevent intrusions.
- To conduct community outreach on incidence management with neighbors to the facilities who would be directly affected in the aftermath of a successful attack.
- To set minimal intervals for emergency response training involving local firefighters, police, and emergency healthcare based on the likelihood of large-scale casualties in the aftermath of a successful attack.

(2) To authorize the creation of bonded, third-party inspectors to audit compliance with these minimal standards at intervals appropriate to the risk posed by a successful attack on the chemical facility.

(3) To create within the Department of Homeland a chemical security compliance office that conducts periodic inspections of facilities to determine both the adequacy of their compliance and the care at which third-party inspectors have conducted their compliance audits. In carrying out this "auditing-the-auditors" program, DHS must possess the authority to swiftly sanction third-party inspectors who it finds to be providing substandard audits.

(4) To sponsor research and development and to provide tax incentives which reward the adoption of less dangerous processes for making, handling, and storing the most lethal chemicals.

(5) To sponsor research and development of new technologies to mitigate the risk of chemical releases beyond a chemical facility.

(6) To sponsor research and development of lower-cost, more user-friendly protective equipment for emergency responders.

(7) To create a task force that recommends a new protocol for resolving the conflict associated with the pre-9/11 community outreach requirements of EPCRA and the post-9/11 trend towards restricting public access to information deemed to be sensitive by DHS. The need for advanced information to be available for communities to take necessary life-saving measures in the aftermath of an attack should be assigned as much of a priority as DHS's tendency to treat public disclosure of details associated with high-risk/high-consequence facilities as sensitive information. This is especially the case in the near term to medium term, given the low-probability that DHS will have actionable intelligence to prevent a terrorist attack.

(8) To require security risk assessments that are reviewed by the senior homeland security official at the state level before new non-industrial development is allowed in the vicinity of existing chemical facilities. This is designed to provide the means for an

appropriate evaluation of decisions such as the one made this year by the Los Angeles Community College District to build a campus to accommodate up to 12,000 students in the southeast Los Angeles community of South Gate, next to one of southern California's largest chemical plants.

CONCLUSIONS:

While this hearing has focused on the issue of chemical facilities, it is important that the issue of transportation of chemicals receive equal attention by this committee and by the federal government. At the end of the day, precursor chemicals must be shipped to manufacturing facilities to produce their final products, and those products need to reach consumers for them to have commercial value. This means that virtually all of the chemicals that we should be concerned with at industrial facilities are concurrently moving about on railcars, barges, and trucks, often in close proximity to major population centers. There are even some chemicals that are so hazardous that they become unstable if they do not reach their destination within prescribed timeframes; i.e., they will explode.

The limited progress there has been made to date within the chemical industry has primarily involved efforts to improve physical security. While these "gates, guards, and guns" issues warrant the attention they have been receiving, they represent only a small part of the overall security agenda. At the end of the day, determined terrorist organizations will be able to compromise any existing industrial security regime. This does not mean these measures are futile because the harder a target becomes to compromise, the more expertise, money, planning, and dry-runs a terrorist organization requires to compromise it. This translates into improved odds that they will do things that will allow them to be detected by vigilant law enforcement.

However, the best way to protect both the American people and an industry as critical to the U.S. economy and our modern way of life as the chemical sector is to reduce the probability that targeting chemical facilities or the transport of hazardous chemicals is the equivalent of constructing and deploying a weapon of mass destruction. We can accomplish this by adding a new security lens to the safety lens that is already well entrenched within the industry. The safety lens which has evolved from training, professional protocols, regulation, and liability law, requires that the industry automatically anticipate the possibilities and potential consequences of an act of God, human error, or mechanical error and devise means to mitigate those risks. In our post-9/11 age, the new requirement must be that the industry also automatically asks: "What is the possibility and what are the potential consequences that we could be targeted by someone with malicious intent?" Based on the answer to that question, they must incorporate appropriate safeguards to lower the risk.

In the end, given that it will be several years before the recent reforms to our intelligence community will bear fruit, we must accept that while a "threat-based" approach to homeland security may be desirable, it will be elusive for some time to come. The only prudent alternative to dealing with our intelligence shortcomings is to look at the sectors

where the consequences of an attack would be greatest and assume that our adversaries are interested in attacking those targets. This means that we must put in place, as quickly a possible, reasonable safeguards to both protect those targets and to reduce the consequences should our prevention efforts fail.

One of the central conclusions of the 9/11 Commission noted the pervasive lack of imagination across the U.S. government in anticipating that organizations like al Qaeda would use aircraft as instruments of terror. What should be guiding our efforts on homeland security today is not whether there is explicit evidence that demonstrates that our adversaries are thinking how and when to harm us, but whether there are in place credible measures that would prevent an attack from happening. As I look at the chemical industry today, I do not see credible barriers to a determined and resourceful terrorist organization. This is clearly an unsatisfactory state of affairs in our post-9/11 world.

Stephen Flynn is the author of *America the Vulnerable*, published by HarperCollins in July 2004. He is the inaugural occupant of the Jeane J. Kirkpatrick Chair in National Security Studies at the Council on Foreign Relations. Dr. Flynn served as Director and principal author for the task force report "*America: Still Unprepared—Still in Danger*," co-chaired by former Senators Gary Hart and Warren Rudman. He spent twenty years as a commissioned officer in the U.S. Coast Guard including two commands at sea, served in the White House Military Office during the George H.W. Bush administration, and was director for Global Issue on the National Security Council staff during the Clinton administration. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy.