"The Role of Border Technology in Advancing Homeland Security"

Written Testimony before

a joint hearing of the

U.S. Senate Judiciary Subcommittee on
Technology, Terrorism, and Government Information
and
the U.S. Senate Judiciary Subcommittee on Border Security, Citizenship, and Immigration

on
"Border Technology: Keeping Terrorists Out of the United States – 2003"

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies and
Director, Council on Foreign Relations Independent Task Force
on Homeland Security Imperatives

Room 226
Dirksen Senate Office Building
Washington, D.C.

10:00 a.m.
March 12, 2003

Chairman Kyl, Senator Feinstein, Senator Chambliss, and Senator Kennedy and distinguished members of the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information and Subcommittee on Border Security, Citizenship and Immigration. I am the Jeane J. Kirkpatrick Senior Fellow for National Security Studies at the Council on Foreign Relations where I recently directed the Independent Task Force on Homeland Security, co-chaired by former Senators Warren Rudman and Gary Hart. In June 2002, I retired as a Commander in the U.S. Coast Guard after 20 years of active duty service. I am honored to be appearing before you this morning on the issue of Border Controls, Technology, and Terrorism.

We find ourselves in paradoxical times. On the one hand, our prosperity and that of our neighbors and international trade partners depends on an open global system that facilitates the free movement of people and goods. On the other, appropriate concern about our ongoing exposure to catastrophic terrorist attacks has fixated Washington's attention on the security of the nation's borders. Consequently, there is a potential train wreck in the making. Moving in one direction are those who have been keen to make national borders as seamless as possible so as to spawn greater economic integration. From the other are officials charged with the new homeland security mandate who look to the border to hold back would-be terrorists, contraband, criminals, and illegal migrants.

Now that the September 11 attacks have let the catastrophic terrorist genie out of the bottle, the United States is rightly concerned about its security at home. Just this past November, I was privileged to testify before this subcommittee with former Senator Warren Rudman on our homeland security task force report. In that report we concluded that: "America remains dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. soil. In all likelihood, the next attack will result in even greater casualties and widespread disruption to American lives and the economy. The need for immediate action is made more urgent by the prospect of the United States going to war with Iraq and the possibility that Saddam Hussein might threaten the use of weapons of mass destruction (WMD) in America." In my view, that chilling finding holds true today.

Yet, however compelling the homeland security imperative may be, it should not mean a derailment of the continental engine of free trade and travel. U.S. prosperity—and much of its power—relies on its ready access to North American and global networks of transport, energy, information, finance, and labor. It is self-defeating for the United States to embrace security measures that end up isolating it from those networks. In addition, there is little value to focusing singularly on bolstering the defenses of only those parts of those networks that lie within or along the borders of U.S. jurisdiction. Such an approach is much like building a firewall only around the computer server physically nearest to a network security manager, while leaving the remaining more remote servers unprotected.

Further, the experience over the past decade of stepped-up enforcement along the Mexican border suggests that U.S. efforts aimed at hardening its borders can have the unintended consequence of creating precisely the kind of an environment that is conducive to terrorists and criminals. On the face of it, an emphasis on tighter border controls appears logical. Stopping

threats at the frontier is better than trying to cope with them once inside the country. Customs inspectors and immigration officials also have the strongest legal authority for inspecting and searching people and goods. But, draconian measures to police the border invariably provide incentives for informal arrangements and criminal conspiracies to overcome cross-border barriers to commerce and labor movements. In addition, unilateral measures pursued on one side of the border create political impediments for enforcement cooperation on the other. The result is that the border region becomes more chaotic which makes it ideal for exploitation by criminals and terrorists.

The alternative is to look beyond national borders as a line of defense. Terrorists and the tools of terrorism do not spring up at the border. Instead, they generally arrive via hemispheric and international trade and travel networks. Advancing a continental and international approach to deterring, detecting, and intercepting illicit actors seeking to exploit those networks would accomplish two things. First, it would provide some strategic depth for responding to a threat before it arrived at a critical and congested border crossing. Second, it would allow the ability to segment risk so that the cross-border movements of people and cargo deemed to present a low-risk could be facilitated. Then limited enforcement resources could be targeted more effectively at those that present a high risk.

Based on a two-year project that I directed from 1999-2001 that involved field research all along the U.S.-Canada and U.S.-Mexican border, I am convinced that the 21st century imperatives that fuel both the incentives for advancing hemisphere economic integration and satisfying the new homeland security mandate do not inevitably involve trade-offs. On the contrary, the shared risks of loss of life and massive economic disruption presented by the catastrophic terrorist threat should provide the basis for trilateral cooperation that can remove many longstanding barriers to continental commerce precisely because those barriers themselves can elevate security risks. For example, the longstanding neglect of the border in terms of limited infrastructure investment and tepid efforts at customs and immigration modernization and harmonization made no sense in purely economic terms. But the resultant inefficiencies that carry substantial commercial costs also create opportunities that thugs and terrorists can exploit. Thus, there is a national security rationale to redress those inefficiencies. The agendas for both promoting security and greater continental commerce can be and must be mutual reinforcing.

That brings me to the issue of border technology which is the focus of the hearing today. Let me begin by citing a caveat contained in our "Hart-Rudman" Task Force report: "*Proceed with caution when embracing technological security 'fixes':* Technology can often serve as an enabler, but it must belong to a layered and dynamic system of defense that incorporates the contribution of human intuition and judgment. Any proposed technological 'solution' must be evaluated against the costs and consequences if it should be compromised. In the end, security is not just about protecting American lives. It is also about sustaining systems that support our way of life in the face of designs to exploit or target those systems. This means that the security protocol must be able to manage any suspected or real terrorist breach without imposing costs so high as to compromise the very network it is designed to secure. Ultimately, the end game must be to continue to live and prosper as an open, globally engaged society, not to become a nation trapped behind the modern versions of moats and castles."

The complexity of the border control agenda practically guarantees that initiatives that place excessive reliance on border technology to keep terrorists at bay, especially at the nation's border crossing and maritime ports of entry, will prove impractical. Substantial investments in technologies such as (1) deploying non-intrusive inspection equipment and radiation detection devices; (2) using transponders and proximity cards in programs such as SENTRI, and NEXUS, and (3) incorporating biometric devises into identity documents will be helpful only if pursued as a part of a comprehensive approach that is mindful of four facts of border control life:

First, ports of entry cannot be separated from the international transport system to which they belong. Border crossings and seaports are, for all practical purposes, simply nodes in an international network that moves people and cargo. Therefore, border controls must be pursued as a subset of a broader commitment to transportation and cargo security. In other words, efforts to improve security at the border require that parallel security efforts be undertaken in the rest of the transportation and logistics network. If security improvements are limited to the border, the result will be to generate the "balloon effect"; i.e., pushing illicit activities horizontally or vertically into the transportation and logistics systems where there is a reduced chance of detection or interdiction.

Take the case of Laredo, Texas—the busiest commercial border crossing on the U.S.-Mexican border. In 1999, 2.8 million trucks crossed the border there, up from 1.3 million in 1993. Many of these trucks operating at the border are old, poorly maintained, and owned by small mom-and-pop trucking companies. This situation prevails because waiting hours at a border crossing in order to make a 20-mile round trip, with an empty trailer on the return, is not a lucrative business. The drivers of these short-haul rigs tend to be younger, less skilled, and are paid only nominal wages—as little as $7 to $10 per trip. Not surprising the turnover-rate among these drivers is also extremely high.

The prevalence of a fragmented, semi-anarchical trucking sector to service the border is itself a direct consequence of the delays associated with crossing the border. Long-haul truck companies like Yellow and Roadway Express simply cannot afford to run their state-of-the-art rigs near the border. As a consequence, trailers are usually offloaded at depots near the border. In the case of south-bound traffic, a short-haul truck is then contracted to move the freight to a customs broker who will then order another short-haul truck to transport the freight to another depot across the border. A long-haul truck will then pick up the load and carry it into the interior. All this conspires to create almost ideal conditions for organized criminal networks—and potentially terrorists—to exploit.

Now if there were no real delays at the border, state-of-the-art long-haul trucks with experienced drivers that are easier to regulate and monitor would be responsible for these cross-border flows. With fewer short haul trucks tying up local roads and the border inspection stations, the border and the border region would become easier to police. In other words, the more efficient the border crossing—which is a an outcome of there being adequate infrastructure on both sides of the border—i.e., access roads, bridges, state-of-the-art inspection facilities, and the more efficient the inspection processes, the more secure the border will become. Alternatively, pursuing

improvements in only one of these areas without parallel efforts in the other will have suboptimal—maybe even counterproductive outcomes.

Second, since the bridges and seaports that link the United States to its neighbors and the world are among America's most critical infrastructure, they should not be viewed as a primary line of defense in an effort to protect the U.S. homeland. The last place we should be looking to intercept dangerous cargo on a truck or ship is in a busy, congested, and commercially vital seaport or at the base of a bridge. For instance, the Ambassador Bridge that links Detroit, Michigan to Windsor Ontario is the lifeline of the U.S. automotive industry. This bridge alone carries more trade into the United States than all the trade that arrives by sea from China. Thus, initiatives such as the Container Security Initiative and the next generation of the Automated Passenger Information System that push the border inspection out towards the port of origin should be pursued with a greater sense of urgency.

Third, inspections processes at a port of entry must be an exercise in *risk management*. There will never be enough inspection resources and it would prove self-defeating to subject every person, conveyance, and cargo to the same inspection regime. An age-old axiom in the security field is that if "you have to look at everything, you will see nothing." At its heart, risk management requires quickly clearing the inspection queues of traffic that is deemed low risk so that limited enforcement resources can focus on that which is deemed to be high risk. But, ultimately determinations of low or high risk are only as good as the integrity of the information, the targeting algorithms and intelligence that underpin them.

The assessment of a person as low or high risk is best done when an application is first made for a visa or passport. Technology can support a good assessment of the baseline documents that prove an applicant's identify, but the quality of the interview conducted by a U.S. consular officer is likely to be more an issue of the time that officer has available to meet with the applicant plus his or her training and experience. An investment in this human resource intensive part of the application process deserves equal billing with vast expenditures on new technologies such as biometrics.

The assessment of the relative risk of an inbound conveyance and cargo is dependent upon verifying the integrity of that conveyance from its point of origin to its arrival at the port of entry. It does not matter that a truck or cargo container originated from a legitimate company or that its paperwork is in order if there is no way to verify that the vehicle and shipment were not compromised once it left the loading facility. Technologies that can track the vehicle and ensure that neither it nor the freight it carries has been tampered with will be essential to confirming that these shipments are indeed low risk. Thus, initiatives such as "Operation Safe Commerce" that look to embed technologies into the transportation and logistics system at large should be pursued with the same vigor as efforts to advance inspection technologies at the border crossings themselves.

A determination that a person, conveyance, or freight shipment deserves to be considered as high risk is dependent on good intelligence. Good intelligence, in turn, is heavily dependent upon close coordination and cooperation with the stakeholders who are vested in legitimate trade and travel. Incentives are key—there must be rewards for good

behavior. Accordingly, technology or any security measure which is indiscriminately applied across a particular sector or that singles out a particular population group will almost certainly backfire by undermining the basis for information sharing and cooperation. For instance, a rush to deploy the Exit-Entry system at our borders is likely to produce considerable disruption and angst among the overwhelming majority of the people who are perfectly legitimate. Their frustration will translate into less cooperation, making the exercise of policing them more daunting for border inspection officials. The better approach is to draw frequent travelers and shippers into programs like NEXUS, SENTRI, and the INSPASS that offer facilitation across the border as a reward for undergoing vigorous pre-screening.

A final border control fact of life is that people matter. Any conversation about investing in new technologies at the border must not be divorced from a concurrent discussion about investing in the quantity and quality of the people who work at the border. Identifying and intercepting criminal or terrorist activity at the border places a premium on the people who populate the front-lines agencies that are tasked to do this. We must be candid in acknowledging that these agencies have been sorely neglected in recent years. This neglect has translated into limited personnel training and advancement opportunities. Most of the inspectors who work along the border have traditionally relied heavily on "on-the-job-training" and promotions from within on the basis of time-in-grade. This approach is clearly out of step with the much more complicated and technology-intensive border management environment of today and tomorrow. Today's inspectors and managers must have the same kind of formal training and education opportunities that we provide our military services. Failing to do that means that large investments in border technologies will end up being essentially white elephants.

Conclusion

Ultimately a focus on border technology in isolation from a broader national, continental, and multilateral conversation that reexamines the very ends and means of border control is self defeating. Accordingly, we should not fall into the trap of embracing technologies that rely on the border itself as the primary locus of inspection activity. Such an approach inevitably will foster only a more chaotic environment at our already congested border crossings and thereby create more fertile circumstances for criminals or terrorists to exploit.

Instead the post-9/11 focus on our borders should be seen as an opportunity to reinvent our borders with our neighbors. Such an exercise is long overdue. The evolution of commercial and social patterns of interaction throughout North America have made our continental relationships more dynamic, organic, and integrated. For some time the issue of border management should have been at the top of the national agenda. Our aim must be to invest in the kind of "smart border" initiatives being embraced on the northern border, not to try and replicate and make more technological efficient the inherently flawed and self-defeating approach that we pursued along the southwest border in the 1990s.

The outline for transformed border management is clear. It requires a risk management approach to policing cross-border flows which includes the close collaboration of the major beneficiaries of an increasingly open North American continent—the United States, our neighbors to the North and the South, and the private sector. The stakes of getting this right are also clear.

Transforming how the border is managed is an essential step towards assuring the long-term sustainability of hemispheric economic integration within the context of the transformed security environment of the post-9-11 world.

Thank you and I look forward to responding to your questions.