

STATEMENT of Clark Kent Ervin
BEFORE THE 9/11 PUBLIC DISCOURSE PROJECT
Securing the Homeland: June 28, 2005

Introduction

Thank you very much, Senator, for that introduction. It is an honor and a pleasure to join you and the rest of the panel today as we explore the important topic of the status of the 9/11 Commission's recommendations with regard to homeland security.

As I speak to various audiences, I'm often asked whether America is safer today than we were on 9-11. The good news is that the answer to that question is an unequivocal yes. Since the nation was attacked on 9-11 by means of airplanes, it is not surprising that the greatest strides have been made in the area of aviation security. Today, cockpit doors are hardened, some pilots are armed, the number of air marshals covering flights has significantly increased, the perimeters and interiors of airports are better protected, and airport screeners are better trained, more motivated, and more sensitized to the critical role that they play as the last line of defense before would-be terrorists board airplanes.

But, the bad news is that whether we're safer today than we were four years ago isn't the only question. And, in the greater scheme of things, it isn't even the most important question. The key questions are – are we as safe we need to be; are we as safe as we can be; and, are we as safe we think we are. In my judgment, the answer to all of these questions, sadly, is no.

Aviation Security

Even in the area where the most time, attention, and resources have been invested, aviation security, serious vulnerabilities remain. One of the first things I did as Inspector General of the Department of Homeland Security in 2003 was to ask my audit staff to follow up on the work of the Department of Transportation's Office of Inspector General in 2001 to assess the ability of airport screeners, in the immediate aftermath of 9-11, to detect guns, knives, and explosives concealed on the bodies or in the carry-on luggage of undercover auditors. To my dismay, we found that it was far easier, two years after 9-11, to sneak these deadly weapons past the by then federalized screener workforce than it should have been. We made a number of recommendations in the areas of training, policy and procedure, management and supervisory attention, and equipment and technology, which TSA promised to implement. One of the last things I did as Inspector General was to ask my staff to conduct a second round of undercover tests at the same airports to see whether screener performance had improved. The tests were conducted, the results came in, and the conclusion was reported this past March. In short, the OIG found no improvement in screener performance. The report went so far as to suggest that we have reached the limit of what training and greater management and supervisory attention can do; the only hope of significantly improving screener performance now lies in the wider

deployment of equipment and technology like backscatter machines, multi-dimensional x ray machines, and walk-through explosive detection “puffer machines” that are presently only either in the pilot stage or deployed on a limited basis.

In addition to screener performance, I remain concerned about what we found during my time as DHS Inspector General about the issue of criminal background checks for airport screeners. When we looked into the issue early last year, we found that some screeners had been hired before their criminal background checks were completed, and that a number of screeners had committed rather serious crimes. We further found that a number of screeners were allowed to continue working for weeks or even months at a time **after** their criminal backgrounds had been discovered. That criminals had been in the ranks of screeners raised the question for me of whether terrorists might have been, and TSA’s laxity in vetting procedures at the time gave me little comfort as to the likelihood of that terrible possibility. In response to our report, TSA pledged to hire screeners only after a thorough criminal records check is completed, and, needless to say, I hope that TSA has kept this promise. In due course, the Office of Inspector General or the Government Accountability Office should do a follow-up inspection or audit to determine that.

With regard to air marshals, while as noted above, the number of marshals has increased significantly, numbers alone are not sufficient. We need people with the right skills and clean backgrounds. When we looked into the air marshal program last year, we found that the department had knowingly hired air marshals with questionable backgrounds, and that it had placed some marshals on paid leave when those marshals could and should have been fired for serious and, sometimes, even dangerous, misconduct, like drug and alcohol abuse and sleeping on the job. So, due to the department’s laxity, a program designed to increase the safety of the flying public had, ironically, an element of risk that endangered public safety. Again, the department pledged to implement the recommendations in our report, and a follow-up inspection or audit should be conducted by OIG or GAO to determine whether the department has in fact done so.

And, there’s the separate issue of how effective air marshals can be if their identity can easily be discerned by their dress code, the order in which they board flights, where they sit on flights, and what hotels they may check into while on the road. To his credit, the new Secretary, according to news reports, has worked with air marshals to address the dress code issue; the hotel policy issue remains unresolved, however.

On the issue of airport security, the degree to which perimeters are vigorously patrolled varies from airport to airport. And, the degree to which vendors, delivery personnel, and repair and maintenance workers are vetted before they are hired, and the degree to which they are permitted to access secure parts of the airport without adequate screening is unclear. It is disappointing in this regard that the production of the TSA’s TWIC (Transportation Worker Identification Credential) card has been halted only a month before TSA planned to complete manufacturing, distributing, and testing a prototype version. The card is designed to verify the identity of transportation workers and to confirm that they have undergone the requisite background checks.

With regard to cargo on passenger planes, the department makes a point of saying that all cargo is “screened” before it is loaded onto flights, but the term is misleading. “Screened” does not mean “inspected.” What the department means is that all cargo manifests are scrutinized to see whether any red flags are raised that would argue for physically inspecting a particular container. And, there are occasional random inspections. But, the vast majority of cargo on passenger planes is not inspected, and this is a huge security vulnerability. The recent legislation proposed by Reps. Markey, Maloney, and Shays to inform the public of this problem and to phase in 100% inspections over time is a step in the right direction.

With regard to international flights bound for the U.S., there continue on a regular basis to be mid-flight diversions when the name of a passenger matches or appears to match the name of someone on the no-fly list. This will continue to happen unless and until DHS succeeds in working out an arrangement with international airlines and foreign governments to transmit passenger manifests **before** flights take off. At present, airlines have up to fifteen minutes after planes take off to transmit passenger manifests to DHS. If a terrorist is intent simply on blowing up a plane, as “shoe bomber” Richard Reid was, as opposed to hijacking the plane and flying into a target in the U.S., as the 9-11 hijackers did, fifteen minutes may be more than enough time to accomplish his goal.

Finally, the department is to be applauded for the idea of the Immigration Security Initiative. Reminiscent of the Container Security Initiative (CSI) with respect to seaports, through ISI, the Customs and Border Protection bureau stations some of its inspectors in some foreign airports to inspect passengers who may pose a risk for admissibility and to ensure that they have valid, genuine entry documents before they board U.S.-bound aircraft. But, the program is only as effective as a counterterrorism tool to the degree that our inspectors are actually permitted by foreign countries to do their work. Any limitations on the degree to which the inspectors can scrutinize passengers and their travel documents limit the protection afforded by the program. With this caveat, it is to be hoped that the program will be expanded as rapidly as possible to as many countries as possible.

Maritime Security

In the area of port security, the vulnerability dramatically exposed by an ABC News investigative team’s ability in 2002 and 2003 to smuggle the very same shipment of uranium (albeit depleted, not weapons grade) into our ports undetected continues. Just last week, a government auditor warned in a House subcommittee hearing that the federal government’s efforts to prevent terrorists from smuggling a nuclear weapon into the United States are so poorly managed and reliant on ineffective equipment that the nation remains vulnerable to a catastrophic attack, despite the passage of four years’ time and the expenditure of about \$800 million. Radiation detection monitors are unable to distinguish between innocuous, naturally occurring radiation in substances like ceramic tiles, and dangerous material like enriched uranium. Nationally, less than a quarter of the radiation detection devices needed to check all goods crossing the borders have been

installed, according to federal officials. In New York, none of the cargo that moves through the largest ship terminal or goods leaving the port by rail or barge is inspected for radiation, according to the security manager for the Port Authority of New York and New Jersey. The Secretary of Homeland Security's recent announcement that the nation's busiest seaports, Los Angeles/Long Beach, California, will have complete radiation portal monitor coverage by year's end is a step in the right direction certainly, but, this needs to happen at all of the nation's ports, and the equipment deployed, needless to say, has to work.

The department is to be commended for the idea of the Container Security Initiative, mentioned above. The idea is to "push the borders out" by stationing CBP inspectors at foreign ports to see to it that high-risk cargo is inspected for weapons of mass destruction before it sails for the United States. But, according to a GAO report released late last month, there are a variety of problems with the program in practice. Thirty-five percent of U.S. bound shipments from CSI ports were not targeted to determine whether they were high risk enough to merit inspection, and, therefore, were not subjected to inspection overseas. In addition, as of last September 11, 28% of the containers that were referred to host governments for inspection were not inspected overseas for various reasons. And, with regard to containers that are inspected, there is limited assurance that the inspections are effective in detecting WMD because of variances in the capability of the detection equipment employed.

CBP's Customs-Trade Partnership Against Terrorism, or "CTPAT," initiative likewise came in for criticism by GAO in that report. In returning for committing to making enhancements in to the security of their shipments, C-TPAT members reduce the possibility that their shipments will be extensively inspected. But, instead of being a "trust but verify" program, the program is in fact a "verify but trust program." In other words, CBP grants benefits **before** members' security programs are validated. Although CBP's goal is to validate members within three years, to date it has validated only 11% of them. Further, the validation process is not rigorous, as the objectives, scope, and methodology of validations are jointly agreed upon with the member, and CBP has no written guidelines to indicate what scope of effort is adequate for validation.

Late last week, the World Customs Organization, a group of 166 nations that account for 99% of global trade, adopted standards for the submission of electronic cargo manifests and for the identification and inspection of high-risk cargo. Certainly there need to be global standards; but, the fact that the standards are based on the flawed CSI and CTPAT programs is a cause for concern.

Finally, as demonstrated by an OIG report released in January, monies awarded in earlier port security grant rounds have on occasion been misdirected to projects of dubious security value. The latest \$140 million award is, according to the department, to be allocated competitively and strictly on the basis of risk, and that is exactly as it should be.

Mass Transit Security

With regard to mass transit security, despite the attack on a train station in Spain in March of last year, which Europe considers to be its 9-11, relatively little has been done in this country to secure this key transportation sector. Secretary Chertoff's recent announcement of the devotion of \$141 million to this task is to be commended, but more urgently needs to be done.

Border Security

In the area of border security, the department is to be applauded for the progress that it has made on the U.S. VISIT entry-exit biometrics based immigration system. For the first time in our history, we are moving toward keeping track of who is entering our country through legal immigration channels, and whether they are leaving when they are supposed to. But, as a February OIG report points out, most visitors who enter our country by land do so from Mexico and Canada, and most of those countries' citizens aren't subjected to U.S. VISIT. And, while the system has been extended to the 50 busiest land crossings, it is probably even more important that it be made operational as soon as possible at the smallest and most remote crossings, since it is there that terrorists' chances of undetected entry are, presumably, easiest. Moreover, the exit feature is still only in the pilot stage. Finally, the vast majority of foreign travelers are not checked against the FBI's 10 print based criminal database. This is important because the FBI database contains 47 million prints, including those of non-Americans suspected of terrorism.

Also worth mentioning is the department's pushing back by one year the deadline for the countries in the Visa Waiver Program to issue "e-passports" capable of containing and storing biometrics to confirm the identity of the bearer of the passport. It is good that digital photographs in such newly-issued passports will be required by this October, since digital photographs are less susceptible to fraud than non-digital ones, and they can be stored electronically for future use. But, this is no substitute for biometrics, and the deadline for a biometric-ready passport has now been pushed back a year for the second time.

Of course, the foregoing comments relate solely to vulnerabilities in border security that can be exploited by people who are attempting to enter our country legally. So, it is to say nothing of the ease with which millions of illegal aliens continue to enter our country, among whom the former DHS Deputy Secretary suggested in congressional testimony earlier this year might be Al Qaeda operatives.

Because the border is so vast, it is critical that the number of Border Patrol agents be increased as much as possible as rapidly as possible. Given the vastness of our southern and northern borders, there can never be enough agents to cover the entire area. The wide

deployment of effective technology like sensors and unmanned aerial vehicles (UAVs) is critical. The department has begun to deploy this technology, but more needs to be done and more quickly. But, the technology has to work, and the government should not be overcharged. Little comfort in this regard can be taken from recent news reports about the expenditure of some \$239 million on the “Integrated Surveillance Intelligence System,” a camera and sensor system so defective and riddled with problems that it has proved to be virtually worthless. The \$2.5 billion follow-on program known as “America’s Shield Initiative” must be closely watched to ensure that it, too, does not turn out to be an expensive and embarrassing failure.

Intelligence

Another challenge is ensuring that the department has access to the intelligence it needs to protect the homeland. It is clear that the roles now played by the National Counterterrorism Center (and, before that, the Terrorist Threat Integration Center) in synthesizing and analyzing all information from across the various intelligence agencies concerning threats against the homeland, and the Terrorist Screening Center in consolidating the various terrorist watch lists, were initially intended to be played by the Department of Homeland Security’s Information Analysis unit. In any event, now that these entities are a reality, and that the entire community has been reorganized and, to one degree or another, subjected to the overarching authority of a new Director of National Intelligence as recommended by the 9-11 Commission, it is critically important that the Secretary of Homeland Security work out an arrangement with the DNI to ensure that DHS is more than a bit player when it comes to homeland security related intelligence. This is no merely theoretical concern. The Silberman-Robb commission on various intelligence failures found that, even though DHS now literally has a seat at the same table as the CIA and the FBI at both the NCTC and the TSC, the CIA and FBI continue to keep important information from DHS on occasion. But, the problem goes both ways. The commission also found that DHS itself, an entity created largely because other agencies weren’t sharing homeland security related information, doesn’t always share information it should with its federal, state, and local partners.

Preparedness

The foregoing having been said, Secretary Chertoff is to be commended for beginning to move the department in the right direction on a number of fronts. Quite rightly, he makes the point that we can’t protect America from every conceivable threat, and we shouldn’t try to. Some threats are likelier to materialize than others, and, within that subset of threats, some would have greater consequences in terms of death and economic damage than others. We should concentrate our necessarily limited resources on these threats, and focus our deterrence and preparedness efforts accordingly. According to a recent New York Times report, the department is moving in exactly this direction by using intelligence to devise likely terrorist scenarios which, were they to materialize, would have serious consequences. The department is working with its state and local partners to ensure that they have the planning, training, and resources they would need in the event that any of those scenarios materializes.

In addition to this, the department recently completed the latest TOPOFF exercise, TOPOFF Three, to test the response capabilities of the federal, state, and local governments to terrorist attacks and natural disasters, and it completed a Continuity of Operations exercise just last week to test operations and procedures for performing essential government functions in emergencies. These kinds of exercises are critical to ensuring that the nation is as prepared as possible against the possibility of another attack.

A critical piece of preparedness is devising an accurate and prioritized list of the nation's most critical infrastructure. According to news reports late last year, the then current version of the plan was a hodgepodge of sites that have little strategic importance like golf courses and theme parks, and sites of strategic importance but ones not listed in any particular order of importance. The latter point is critical, because, again, we can't protect everything, at least not to the same degree. The Heritage Foundation report on this subject released last month shows that the list as presently constituted continues to be broader than it should be.

The role of the private sector in protecting the nation's critical infrastructure is, of course, hugely important, because about 85% of that infrastructure is owned or controlled by the private sector. During the first two years of its existence, the department was cool to the notion of legislation or regulation to mandate steps by the private sector to protect itself. In the area of chemical plants, the new department leadership has shown a welcome willingness recently to move in this direction in the absence of significant steps by industry itself. While government must always be careful not to over-regulate, it is to be hoped that the government will move in this direction increasingly with regard to other elements of critical infrastructure if the private sector continues to resist calls to do more to protect itself.

Funding Formula

Also to be applauded is Secretary Chertoff's focus on encouraging Congress to allocate homeland security funding entirely on the basis of threat, risk, and consequence, as opposed to pork barrel politics. Both the House and Senate (notably the Homeland Security Forward Funding Act of 2005 introduced by Sen. Feinstein of California and a bipartisan group of colleagues from New York, New Jersey, Texas, and Florida) have increasingly moved in this direction recently, and further steps in this regard are vitally important. That said, once jurisdictions get homeland security funding, it is critical that they spend it as quickly as possible, and that they spend the funds only on the items intended. OIG and other government and media studies and investigations have shown that state and local jurisdictions are sometimes slow to spend allocated money, and they don't always spend it on homeland security related purposes.

Conclusion

Now for some final thoughts. Increasingly, there are signs that the nation is growing complacent. Fewer Americans fear a terrorist attack on the US in the next several weeks than at any time since 9-11, according to a recent USA Today/CNN/Gallup Poll. Overall, 35% say another attack is likely soon, down from 39% in January, and a high of 85% in October 2001. We lack a sense of threat, and a sense of urgency about taking the steps that we need to take to protect ourselves against the likelihood of another attack. Some in our country have attributed the lack of an attack since 9-11 to the mere existence of the Department of Homeland Security, as if all it takes to secure the homeland is creating a new government agency called the “Department of Homeland Security.” The fact that the President was not told until after the end of the recent incident that, at least initially, appeared to be another 9-11 style attack on the capital, and the fact that, at least officially, the White House continues to defend the Secret Service’s failure to inform him right away, graphically demonstrates that the nation is in danger of going back to sleep.

We certainly shouldn’t frighten the American people needlessly, but we mustn’t become lackadaisical and complacent, either.

The key, it seems to me, to striking the right balance, between concern and complacency is coming up with metrics to measure success, or the lack of it, in the war on terror here at home. In Iraq, for example, we measure success by whether the number of insurgent attacks are increasing or decreasing. In the global war on terror, likewise, we measure success by whether the number of terrorist attacks is increasing or decreasing. But, if we were to use this criterion for the fight against terrorism here at home, we would conclude not only that we’re winning it, but that we’ve already won it, since we haven’t had another attack in four years. But, we all know instinctively and intuitively that this isn’t and can’t be the case. Equating, as some have done, the absence of an attack since 9-11 with the establishment of the Department of the Homeland Security is a false and dangerous syllogism. It seems to me that the metric should be the gap between terrorist’s capacity to strike us, and our ability to detect, deter, and defend against any such strike, what might be called “the vulnerability gap.” Of course, we’ll never eliminate the gap entirely, and, to be sure, we’ve made strides in the last four years, and since the 911 commission report, in closing the gap. But, as demonstrated by the shortcomings identified above, the gap remains far wider than it has to be, and it is urgent that we reduce the gap to as close to zero as possible as soon as possible.

Clark Kent Ervin
Director, Homeland Security Initiative
The Aspen Institute
Former Inspector General of the U.S. Dept. of Homeland Security