



26

Securing the transnational movement of trade and people in the era of global terrorism

Remarks of Robert C. Bonner*

Former Commissioner, US Customs and Border Protection

* This text may vary from actual speech.

I am delighted to be here at this conference jointly hosted by the Australian Strategic Policy Institute (ASPI) and Unisys, addressing important national and homeland security issues. ASPI is one of Australia's foremost policy think tanks. And Unisys is a company that has been a partner of the US and the Australian Government and in the forefront of innovative homeland security solutions.



Former Commissioner, US Customs and Border Protection, Robert Bonner.

It is good to see some familiar faces of good colleagues and friends from my days as Commissioner.

I can't tell you how delighted I am to be back, to be 'down under' again in Australia, and here in the nation's capital.

Introduction

This morning, I want to discuss national and homeland security, in the post 9/11 era, in this age of global terrorism. And because I was, to use former Secretary of State Dean Anderson's phrase, 'present at the creation', I will offer a few comments about the Department of Homeland Security (DHS), the newest department of our federal government that stood up—a bit wobbly, I'm afraid—just over three years ago. Most importantly for this conference, I will discuss some of the key strategies and programs that the US Government launched in the wake of 9/11 and the technologies and systems that proved to be indispensable to the priority US strategic goal of preventing asymmetrical warfare; that is, preventing global terrorists from striking us at home. I will discuss what worked and what did not work and some of the wrong turns that seem to be inevitable when reacting

to a new threat, or finally coming face to face with a threat that materialised in the worst terrorist attack—in terms of loss of life—in the history of the world. That was 9/11. 2,933 innocent lives were lost that day. Or looked at differently, it was the most horrific attack ever perpetrated on US soil by a foreign enemy. In terms of loss of lives, 9/11 exceeded the attack on Pearl Harbor.

But I want to acknowledge at the outset that it is not just the US that has been thinking about and adjusting to the reality of global terrorism. You, here in Australia, have been in the vanguard. The Australian Government, for example, through Advance Passenger Processing (APP), e-passports, Regional Management Alert List (RMAL) and other initiatives, has been on the forefront of devising and implementing some of the best security programs in the world designed to prevent the entry of terrorists, terrorist weapons and criminals. We have learned much and continue to learn much from you. The national and homeland security issues I will discuss with you this morning consumed my energies and thinking for over four years.

A personal story

To understand how I—and the Bush Administration—came to approach the problem, let me take you back to—what was for me—the beginning; to the formative experiences that shaped our policy, or at least shaped my thinking and, at the risk of appearing a bit immodest, shaped US policy. I moved from California and ‘reported for duty’, so to speak, in Washington on September 10, 2001. Because I had not yet been confirmed by the US Senate as Customs Commissioner—that came one week after—I was given a temporary office at the Treasury Department, which, for those of you who know Washington, is next door to the White House.

On the morning of 9/11, I was in my office at the Treasury Department, when at about 9:35 am, the sirens went off to evacuate the building. There were two hijacked aircraft heading toward Washington.

On the morning of 9/11, I was in my office at the Treasury Department, when at about 9:35 am, the sirens went off to evacuate the building. There were two hijacked aircraft heading toward Washington. Just before exiting the Treasury Building, I glanced out the window and saw an enormous plume of black smoke rising from the Mall.

Shortly thereafter, I learned that that plume of smoke was emanating from the Pentagon, which had just been hit. Outside, on 15th Street, the Acting Treasury Secretary waved for me to get into his car and we proceeded to the command center at Secret Service Headquarters a few blocks away. US Customs itself was struck directly by the terrorists.

The aerial photo (on page 3) taken from a US Customs Blackhawk helicopter the day after 9/11 was the US Customs House at 6 World Trade Center. As you can see, it was destroyed when the North Tower fell upon it. Fortunately, all 800 Customs employees who worked there survived. The day after I was sworn in as Commissioner, I went to New York to speak with our Customs employees and to visit Ground Zero. The image of the Customs House—what was left of it, and of Ground Zero—will, of course, stay with me forever. On the morning of 9/11, I began running US Customs in earnest. My very first act as Commissioner came at about 10:05 am that morning. I approved and directed US Customs to go to Alert Level One, the highest level security alert at our border, short of actually shutting down our ports of entry.

I realised on the morning of 9/11 that the priority mission of US Customs... needed to dramatically and immediately change, from the interdiction of illegal drugs and regulation of trade—to a national security mission...

Two realisations

I came to two very important realisations during the week of 9/11. First, I realised on the morning of 9/11 that the *priority* mission of US Customs—as one of our government’s principal border agencies—needed to dramatically and immediately change, from the interdiction of illegal drugs and regulation of trade—to a national security mission—**preventing terrorists and terrorist weapons from getting into the United States**. The realisation that Customs had an anti-terrorist prevention mission was underscored that morning because a few

minutes after going to Level One Alert, I reviewed a list that US Customs was transmitting to the FBI; a list that contained the names of *nineteen* individuals tentatively identified by US Customs as the terrorist hijackers. Not twenty, not eighteen. It was 10:15 am. How had this been done so quickly? The answer: Passenger Name Record (PNR) data, which is essentially the reservation data the airlines obtain regarding passengers; data such as credit card used, prior travel, seating requests, name of travel agent used, home address and the like. Although we had the ability to do so, we had never accessed PNR data on a purely domestic or internal flight. But this was an emergency.

Given the need to understand what was happening, US Customs accessed PNR information for the first time for domestic flights—for the four domestic flights, three of which had done their carnage—the fourth one, which crashed in Pennsylvania, was heading toward Washington. How were the nineteen identified so quickly? Two had been identified by the CIA in the spring of 2000 as



Ground Zero and US Customs House at 6 WTC. Photo courtesy Customs and Border Protection

probable al-Qaeda terrorists, and provided to US Customs by the FBI for placement on our joint Customs–Immigration terrorist watchlist in August 2001. That eighteen month delay in sharing intelligence is another issue the US Government has attempted to rectify. But on the morning of 9/11, US Customs was able to immediately determine that two individuals who checked in on the four flights were on its terrorist watch list and were probable terrorists. So that was the start. Using PNR data and links to these two, the identity of all nineteen was quickly determined. Simple link analysis using PNR data allowed us to tie the nineteen together almost immediately. The implications of PNR data were not lost on me as a tool to prevent terrorists from getting into the US. You will now understand why one of my first acts as Commissioner was to ask Congress to promptly enact legislation requiring all airlines, foreign and domestic, to provide US Customs with Advance Passenger Information—that’s the passenger manifest, ie, name, passport number—and PNR data, and to electronically provide both types of data for every passenger at the time of departure of a flight from abroad for the US. That legislation was enacted in early November 2001. And since then, data concerning every person travelling to the US by commercial passenger aircraft is evaluated, not just against the Terrorist Watch List, but for terrorist risk factors.

I said I came to two realisations during the week of 9/11. The second realisation came the very next day. As a result of going to Level One Alert, by September 12 our borders began to shut down. Because of vastly increased inspections—we had no anti-terrorist targeting and no detection technology whatsoever at our seaports or at our northern border with Canada—by 9/12, wait times, for example, at our border with Canada—skyrocketed. Overnight they had gone from ten minutes on average

to over ten hours! Trucks were queued-up for 20–30 miles into Canada. By 9/14, the major American automakers—GM, Ford and Daimler Chrysler—dependent on just-in-time inventories, were beginning to shut down plants. And that underscored my second realisation. We definitely had to increase security in the post 9/11 era, in the age of global terrorism, but we had to find a way to do that without choking off the flow of legitimate trade and travel, without shutting down our economy in the process. We had to find ways, strategies to achieve what I’ve referred to as the ‘twin goals’: (1) achieving greater security, but also (2) facilitating the flow of legitimate cross-border trade and travel. Seeing the challenge of homeland security through this prism led to some of the most innovative, revolutionary homeland security initiatives launched by the US after 9/11.

We had to find ways, strategies to achieve what I’ve referred to as the ‘twin goals’: (1) achieving greater security, but also (2) facilitating the flow of legitimate cross-border trade and travel.

It led to the Container Security Initiative (CSI), Advance Passenger and Cargo Information (APCI), Advance Passenger Information System (APIS) and the 24-Hour Rule, to the National Targeting Center (NTC) and its Automated Targeting System (ATS), and to the Customs–Trade Partnership Against Terrorism (C-TPAT). It led to the use of detection technology for anti-terrorism prevention and the use of biometrics at our borders. It also led to US VISIT, Free and Secure Trade (FAST) and NEXUS; ‘smart border’ programs to expedite the movement of goods and people that pose no threat. Not one of these initiatives existed before 9/11.



The Initiatives.

The first step was to refocus the agency on the priority mission because Customs, like any bureaucracy, will continue in its old direction unless there is leadership ...

Steps taken; hurdles cleared

The first step was to refocus the agency on the priority mission because Customs, like any bureaucracy, will continue in its old direction unless there is leadership that says: 'We're changing. Here's why.'

I began with an 'all-hands' speech to all US Customs employees, worldwide, on my third day as Commissioner. I told everyone that our priority mission going forward is preventing terrorists and terrorist weapons from entering the United States. I repeated that mantra until I almost gagged, but I will tell you there is not a single frontline officer of Customs, now Customs and Border Protection (CBP), who does not know the priority mission, who does not go to work every day thinking about it. Implementing an ATS, expanding detection technology, implementing CSI and C-TPAT, of course, required funds. And funding and the budget process were also a challenge, starting with the very first Supplemental Budget Request post 9/11.

I started working on it from day one, the day I was sworn in as Commissioner, and submitted a supplemental request of over \$500 million to expand our technology, to support increased overtime to staff ports of entry 24/7 where necessary, to literally guard and harden low volume, unmanned, unsecured ports of entry along the Canadian border, unmanned when closed after 12 of 16 hours and secured before 9/11 with plastic orange cones placed in the middle of the roadway. I sought funds to start CSI and C-TPAT and to establish a NTC and an expanded Automated Targeting System. I presented this request to the Treasury Department, to which Customs belonged, in early October 2001. Astonishingly, I was zeroed on my request by the Treasury Department! Zeroed, except for funding to recover from the loss of the US Customs House in New York City. Congressional appropriators, however, granted my funding request, despite the objections of Treasury Secretary, Paul O'Neill.

The effects of 9/11 still reverberate in America, as witnessed by the flap over a Dubai company operating a few sea terminals at US seaports ...

Effects of 9/11

The effects of 9/11 still reverberate in America, as witnessed by the flap over a Dubai company operating a few sea terminals at US seaports just two months ago. 9/11 was, after all, the largest terrorist attack in the history of the world, and it changed the way we need to view national security. Before 9/11, the United States had been lulled into a false sense of security, perhaps under the illusion that we were somehow protected by:

- vast oceans to our east and west, and
- by peaceful neighbours to our north and south.

Today, another curtain threatens to separate Muslim countries from the rest of the world.

9/11 utterly shattered that illusion! As we now know, all of the nineteen terrorist hijackers were trained by al-Qaeda, an extremist Islamic group, whose brand of terrorism is global in scope, and goes beyond anything we had ever seen before. As Communism was the security threat that dominated much of the last half of the 20th century, this different ‘ism’—global terrorism—is likely to dominate the first half of this century. At the beginning of the Cold War, Winston Churchill warned of an ‘iron curtain’ being drawn across Europe. Today, another curtain threatens to separate Muslim countries from the rest of the world. That is exactly what al-Qaeda wants. Al-Qaeda wants to exclude all Western influence and globalisation from the Muslim world. Indeed, they want to restore an Arab-dominated caliphate of ten centuries ago, and they have and will continue to use like-minded terrorist organisations, like Jemaah Islamiya (JI), and asymmetrical warfare to achieve their goal.

Confronting the threat

This is the enemy America finally came face-to-face with on 9/11, but the threat of further attacks continues. *It would be unwise to underestimate al-Qaeda’s determination to strike again, or their patience. We cannot afford to become complacent.* Let us remember that the time between the first World Trade Center attack and the second was *eight* years. But al-Qaeda and its associated terrorist organisations are not only targeting the US, they are and have targeted Europe, Australia, and indeed, the global economy. But more, they are attacking the forces of globalisation that have the potential to lead to economic uplift,

democratisation and reform. 9/11 was only the most dramatic and brutal example of a long list of al-Qaeda-inspired attacks around the world, before and since:

- from the first attack on the World Trade Center in 1993
- to the bombing of the US Embassies in Kenya and Tanzania
- to the post 9/11 attacks in Bali—where over 200 innocent civilians were murdered including a large number of Australian citizens—to Istanbul, Morocco, Tunisia, Saudi Arabia, Djakarta, Madrid and last July, London.

The list would be even longer if other al-Qaeda plots had not been thwarted. In 2000, for example, an al-Qaeda terrorist named Ahmad Ressaam, who became known as the Millennium Bomber, was arrested by US Customs Inspectors as he tried to enter the United States from Canada. The trunk of his car was loaded with explosive materials. His target: Los Angeles International Airport (LAX).

After 9/11, one thing was immediately apparent: a policy of containment and mutual deterrence had no chance of being effective against this type of enemy.

The US response to global terrorism

After 9/11, one thing was immediately apparent: a policy of containment and mutual deterrence had no chance of being effective against this type of enemy. We needed a very different strategy to deal with this new kind of enemy. Lobbing a few cruise missiles into Afghanistan and Sudan, as we did after the bombing of the two US Embassies in East Africa, only served to embolden al-Qaeda.

A three-pronged strategy

After 9/11, under President George Bush's leadership, the United States adopted essentially a three-pronged strategy for responding to the threat of global terrorism. First, President Bush recognised that we must have an offense that goes after terrorists, terrorist leaders, and those who support them, and destroys the organisational infrastructure of al-Qaeda, root and branch. As a result of the efforts of the United States military and our allies—and Australia has been one of our best partners—we have deprived al-Qaeda of its base in Afghanistan. And, we have killed or captured a large number of al-Qaeda leaders.

... over the long haul, we must have an effective communication campaign to defuse the hatred and ignorance that motivates fundamentalist, fanatical Islamic jihadists to join the ranks of al-Qaeda and its affiliated terrorist organisations.

Second, we must have a strong defence. This is where the DHS comes in. Third, over the long haul, we must have an effective communication campaign to defuse the hatred and ignorance that motivates fundamentalist, fanatical Islamic jihadists to join the ranks of al-Qaeda and its affiliated terrorist organisations.

Although this may seem a bit distant now, a stable, democratic government in Iraq will do more to achieve the third objective of the strategy than anything else, because, in my view, a democratic Iraq would begin the collapse of al-Qaeda as surely as solidarity in Poland was the beginning of the end for Communism and the Soviet Empire.

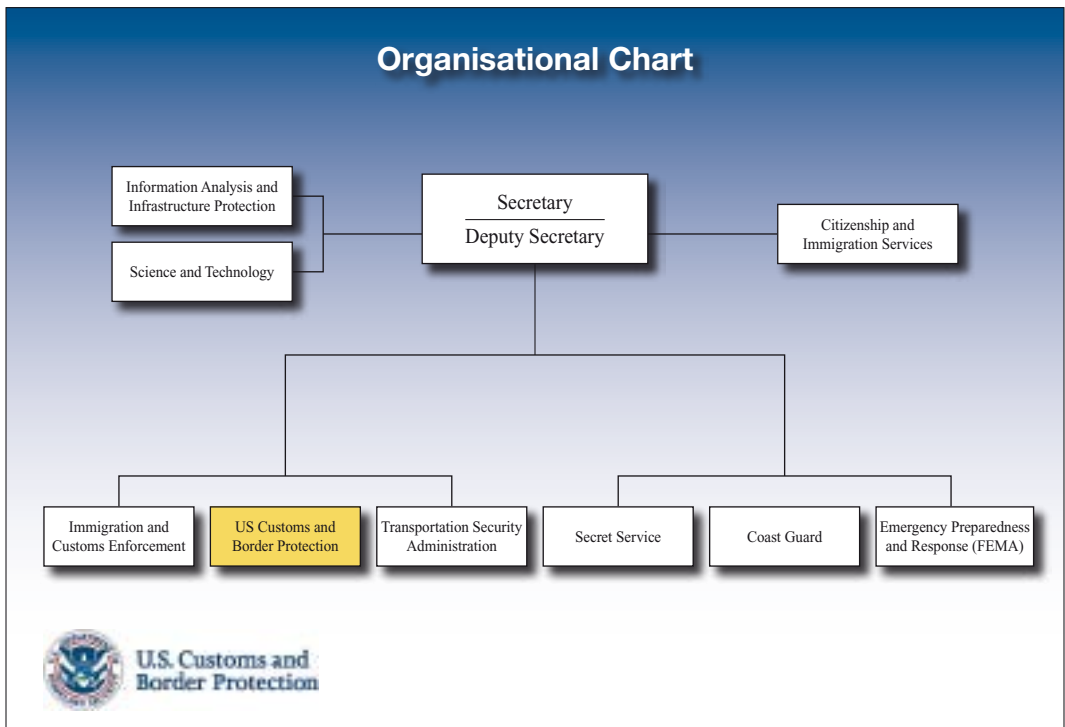
And Bin Laden and Zawahiri knows this. As does the al-Qaeda commander in Iraq, al-Zarqawi. In his video last month, Zarqawi described the formation of a unity government in Iraq under Mr Maliki as 'a dagger in the heart.' President Bush was right when he said recently: 'The stakes (in Iraq) are high!' The United States is moving forward on all *three* of these fronts, as we must, but I will address only the second one today; the defence. I thought it important, though, to remember that homeland security, for us, is part of a broader strategy for dealing with the threat of global terrorism.

Reorganisation: Department of Homeland Security and the creation of Customs and Border Protection

One of the most profound steps taken by President Bush and the US Congress to defend against global terrorism was to establish the DHS, which stood up just over three years ago, in March 2003. This was and is, as you may know, the largest reorganisation of our federal government in over 50 years, since the reorganisation of 1947 to fight the Cold War.

The creation of the DHS—and I was 'present at the creation'—involved the transfer of all or parts of two dozen government agencies. This is a streamlined organisation chart of DHS (see page 8).

The Department has three missions: first, to prevent further large-scale terrorist attacks in the United States; second, identify and better secure truly critical infrastructure; and third, although it assumes failure, prepare for and respond to large-scale terrorist attacks, and other catastrophic disasters, a mission that involves organising first responders, such as local and state police and fire departments and emergency medical personnel.



DHS Organisational Chart.



DHS Missions.

The power to deny admission was held by the Immigration and Naturalization Service (INS) which, before 9/11, focused primarily on potential economic migrants, not on potential terrorists. The homeland security reorganisation rectified this.

The 'One Border Agency' idea

One of the most important ideas of the Homeland Security reorganisation, though, was the creation of one border agency for our government. One agency to manage, control and secure our nation's borders, all its official entry points—and between, for all purposes—customs, trade, immigration, agriculture protection *and* terrorist prevention. That agency—that one border agency—is United States Customs and Border Protection.

Shortly after 9/11, it was clear to me that while Customs, as a border agency, had enormous authority to inspect cargo, vehicles and people entering, or seeking to enter the United States, the agency lacked the authority to deny entry to persons seeking to get into the US. As I pointed out at an inter-agency meeting in November 2001, this frustrated the implementation of a coordinated anti-terrorism border strategy, and I proposed merging all immigration enforcement functions and personnel with US Customs.

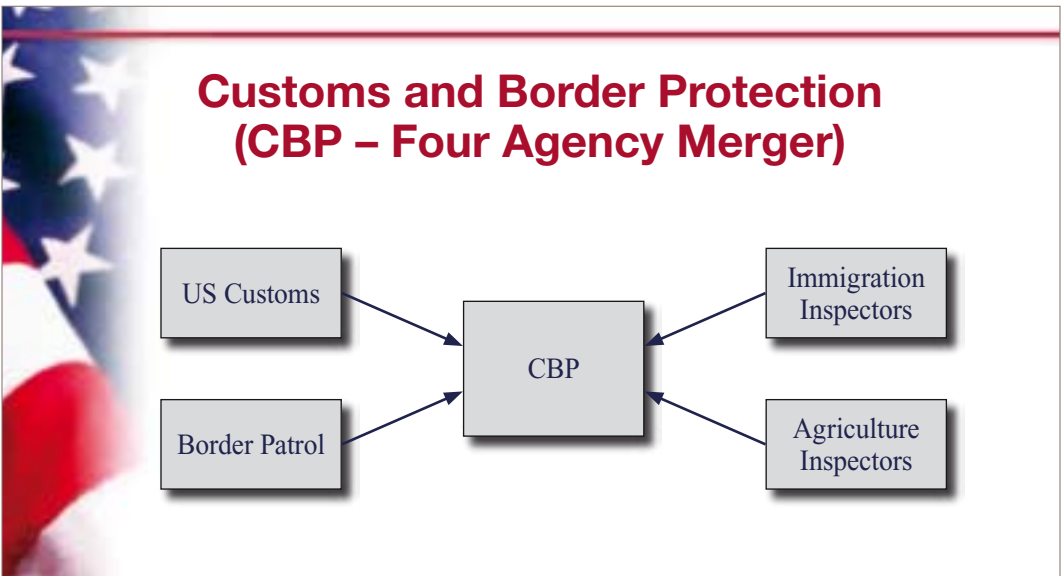
The power to deny admission was held by the Immigration and Naturalization Service (INS) which, before 9/11, focused primarily on potential economic migrants, not on potential terrorists. The homeland security reorganisation rectified this. First, under the Homeland Security Act, the INS was abolished. The *coup de grace* for the INS was when the INS issued visas to several of the terrorist hijackers in 2002, six months after 9/11.

The creation of one border agency was one of the least noticed, yet one of the most important ideas of the Homeland Security reorganisation.

And so, on March 1, 2003, all the frontline personnel of the former INS, including the entire Border Patrol, were merged with US Customs to form a new federal agency, US Customs and Border Protection, to create—for the first time in our nation’s history—one agency of the federal government to manage and secure our country’s borders. As you can see, even the border inspectors

of the US Department of Agriculture were transferred to CBP. This was important, by the way, to aid efforts to prevent bio and agro terrorism, e.g. intentional contamination of food products by global terrorists. The creation of one border agency was one of the least noticed, yet one of the most important ideas of the Homeland Security reorganisation. As I used to remind Tom Ridge (former Secretary, Department of Homeland Security), frequently, CBP was the largest, actual merger of people and functions taking place within the DHS. With 42,000 employees, CBP has one-fourth of all of the employees of the DHS, which is not surprising at all when you consider the importance of the security of our ports of entry and borders to the security of our homeland.

As you can see, CBP is one of just seven agencies of DHS. And over 99% of the employees of DHS are in these agencies. They all have relatively distinct homeland security missions, and quite different traditional missions. The priority mission of CBP, like US Customs before it, is homeland security and that means preventing terrorists and terrorist weapons from getting into the United States.



Merger of Four Border Agencies.

The primary strategic goal of DHS

That is the DHS's *first* strategic goal. That preventative goal reflects the fundamental responsibility of government to protect its citizens and homeland. It is that strategic goal that drove our government to reorganise itself and to implement initiatives, programs and technology to make it exceedingly difficult, far more difficult, for foreign terrorist operatives or terrorist weapons, particularly Weapons of Mass Effect (WME), to enter the country. Concurrently, our government, principally the FBI must take and has taken appropriate steps, within our laws and our Constitution, to identify and disrupt the formation of terrorist cells and training of terrorists within the existing immigrant population. The Patriot Act and the expansion of the Foreign Intelligence Surveillance Act (FISA) to cover foreign terrorist organisations has been important to our success.

The goal ought not to be stated as preventing any further terrorist attacks, for that would be an impossible goal. Yet the goal of dramatically and substantially reducing the ability of al-Qaeda and al-Qaeda associated terrorist organisations to attack in our homeland is achievable, and we had made real progress in achieving that national security and homeland security goal. The fact that we have not been attacked within the US since 9/11 comes down to this: al-Qaeda has not been able to get terrorist operatives into the US, nor has it been successful in recruiting and training home grown jihadi terrorists. Moreover, al-Qaeda has not been able to deliver terrorist weapons of mass effect across our borders. No car, truck or container bomb has been introduced across our border, nor has any Radiation Dispersal Device (RDD), or the like. I do not say it cannot be done. There is no foolproof system. I do say that we have made it far more difficult. We are attacking them abroad, and we are preventing asymmetrical attacks at home.

... we can easily misfocus precious resources on so-called infrastructure protection because of our political process that focuses so much on local or individual Congressional districts.

The *second* mission of DHS is protection of critical infrastructure. Here, I believe we have fallen victim to a good deal of fuzzy thinking and paralysis. There are serious practical and budgetary limits to protecting infrastructure within a country from terrorist attacks. Of course, steps have been taken to increase protection and harden national icons and a few symbolic governmental buildings; the Capitol and the White House. Steps have been taken to further limit access to nuclear power plants, and we need further progress protecting chemical plants that produce Bhopal-type chemicals. And, as everyone knows, huge efforts have been made to better secure commercial air travel. But as Beslan demonstrated, there are not sufficient resources to protect all infrastructure, bridges, stadiums, schools, etc. And yet we can easily misfocus precious resources on so-called infrastructure protection because of our political process that focuses so much on local or individual Congressional districts.

Indeed, it has skewed how US federal funds for port security, infrastructure protection and first responders are spent. These decisions should be made based on objective, risk/consequence assessments.

While there are no guarantees, the fact remains—for us—one of the best ways to prevent terrorist attacks is to prevent terrorists from getting into the US in the first place. Let me give you the example of Raed Mansour Al-Banna (see text box on page 11).

The Al-Banna story

Al-Banna was a passenger who was denied entry by US CBP officers at O'Hare Airport in July 2003, after arriving on a flight from Amsterdam's Schipol Airport. He was run through APIS which had revealed six hours earlier to the National Targeting Center and to our Passenger Analysis Unit at O'Hare that Al-Banna was a 30-year-old Jordanian national, who had a genuine Jordanian passport and a genuine and valid B1/B2 visa. He was not on anyone's terrorist watch list. He was flagged for Counter Terrorism Response (CTR) questioning, because he presented multiple terrorist risk factors. After questioning by CBP officers in secondary, we did not believe his stated purpose for entry. And for this passenger, we denied entry and detained him until the next flight back to the Netherlands the following day.

As is our protocol, Al-Banna's fingerprints and photo were taken, and the next day, he was escorted by armed CBP officers onto the airplane for Amsterdam. Dutch authorities, through our Immigration Advisory Team at Schipol Airport, were alerted. Last year, CBP denied entry into the US to 499 potential terrorists. Often, like Al-Banna, we don't know for sure whether such an individual is actually a terrorist, but we *now know* that Al-Banna was not only a terrorist, he was a suicidal jihadi terrorist seeking martyrdom. After US CBP denied him entry into the United States, Al-Banna entered Iraq and joined the ranks of the Qaeda's man in Iraq, al-Zarqawi. In February 2005, Al-Banna drove a vehicle loaded with explosives into a Shiite City; about 60 miles from Baghdad, where he blew himself up, and murdered 132 innocent Iraqis. In terms of loss of life, that was the largest single terrorist attack perpetrated in Iraq since the fall of Saddam Hussein.

The identity of Al-Banna may have gone unnoticed, except we have his hand. That's all that's left of him. He had one of his hands chained to the steering wheel of

the vehicle. Evidently, even jihadi terrorists need to make sure they don't change their minds. Al-Banna is not the only potential terrorist we have turned around. Indeed, since CBP was created, we've denied entry to hundreds of Al-Bannas annually. Not all of whom, but undoubtedly some of whom, were terrorist operatives. The keys to our ability to do this are:

- (1) Advance Passenger Information and PNR data
- (2) Evaluating that data with our ATS to identify terrorist risk factors; three or more requires a look, i.e. counterterrorism questioning and a border search of luggage, carry-ons and pocket litter. We call this Counter Terrorism Response (CTR)
- (3) Frontline CBP officers trained in CTR, behavioral reads, and search techniques
- (4) Empowerment of frontline CBP officers and supervisors to detain and deny entry if there is any credibility issue
- (5) And capturing biometrics on all foreign nationals entering the US.

We did none of this before 9/11. The INS didn't even look for potential terrorists. US Customs used its broad border search authority to hunt for illegal drugs, not terrorists. I cannot overstate the importance of the organisational change of combining the legal authorities and expertise of US Customs and frontline immigration has had on making us more effective in preventing terrorist entry into the US. That change would not have come about without the Homeland Security reorganisation of 2003. After creating CBP, we were also able to develop—for the first time—a *national* border control strategy, that takes a comprehensive approach to border security at all of our nation's 'ports of entry', and between the official entry points, especially along our long land borders with Mexico and Canada. The US Coast Guard continues to have the primary responsibility for protecting our coastal areas between seaports and for physical security of the seaports.

Importance of technology and automated targeting

Everything we did recognised the importance of technology in protecting our nation in the post 9/11 era. Indeed, we could not have succeeded in achieving the twin goals without technology and integrated systems. Technology, for example, to secure our ports of entry and, at the same time, keep legitimate trade and people moving.

There were 10 million containers offloaded at US seaports last year, 30,000 a day, on average. It is virtually impossible, and quite unnecessary, to mandate that CBP inspect every cargo container arriving at our nation's seaports...

There were 10 million containers offloaded at US seaports last year, 30,000 a day, on average. It is virtually impossible, and quite unnecessary, to mandate that CBP inspect every cargo container arriving at our nation's seaports, as some in our Congress have called for. Not if you have advance electronic information and you risk-manage for the terrorist threat. Likewise it is unnecessary to physically inspect all 11 million commercial tractor trailer trucks arriving at our borders from Canada and Mexico.

Using advance electronic information and our Automated Targeting System at the National Targeting Center, Customs and Border Protection selects the cargo shipments and people that pose a potential terrorist threat, and 100% are inspected or subject to Counter Terrorism Response. The ATS for cargo and for people is the key to reducing the haystack to a manageable size, whether the haystack be



Container Ship. Photo courtesy Customs and Border Protection



CBP's National Targeting Center. Photo courtesy Customs and Border Protection

cargo shipments or people. Unisys has been a partner with CBP. It has supported ATS with requirements analysis support, systems and software design and artificial intelligence technologies. Yet the ATS can be improved with greater visibility into the supply chain. More visibility, more data translate into greater security *and* fewer inspections. The twin goals, again. With detection technology, we can and do inspect far more cargo shipments, far more rapidly than ever before. Using this technology, and our ATS, about 2½ million trucks and containers were inspected last year alone. That is far more inspections than before 9/11, on the order of a six fold increase, but all of these inspections, except for some random ones, are targeted based on risk. We are smarter about what we inspect.

This detection technology includes large-scale, whole container imaging

equipment, like you see here (page 14), that gives an x-ray type image of what's in a container or truck. Under the Bush Administration, we quadrupled the number of these large imaging machines since 9/11 and they are now at every significant US seaport and land border crossing. Before 9/11, because of the drug smuggling, almost all the large x-ray imaging machines of US Customs were at our ports of entry along the Mexican border.

The detection technology also includes highly sensitive, Radiation Portal Monitors (RPMs). There are over 1,000 of the radiation monitors at our ports of entry and most trucks, vehicles, and containers now pass through RPMs *before* they enter our country. In June 2002, we literally invented and mandated the minimum security inspection for 'high risk' cargo shipments: an x-ray scan and a radiation detection sweep. In the seaport environment,



X-Ray Type Imaging Machine. Photo courtesy Customs and Border Protection



Radiation Portal Monitor. Photo courtesy Customs and Border Protection

including at overseas CSI ports, CBP has required this security inspection, both x-ray and radiation scans, for ‘high risk’ containers, before they leave foreign CSI ports for American ports. Before I left Washington last November, we had already implemented CSI at forty-two of the largest foreign seaports of the world.

Ports like Singapore—the largest container port in the world—and Shanghai, Rotterdam, Hamburg, and yes, even Dubai—now the tenth largest container port in the world.

Why did we implement CSI? Because most US seaports, like Seattle, are right smack in the middle of our country’s largest urban areas. Finding a terrorist weapon *after* a container is offloaded here would probably be too late. Using those five initiatives I mentioned, CBP launched the FAST program to expedite secure truck shipments, secured at point of origin, across our land borders.

Using ‘smart border’ technology, advance manifest information and the Automated Targeting System, C-TPAT participants, who meet security criteria get the ‘fast lane’ and are cleared across our border, on average, in seventeen seconds, as opposed to a process that can take up to an hour for unsecured shipments of shippers and importers not participating in FAST. Again, the twin goals. Unisys has provided CBP with technical and functional support to help manage the FAST program. The concept is equally applicable to the movement of oceangoing containers, and, importantly to the FAST processing of people arriving at our ports of entry.

All US bound passengers are bounced against the Terrorist Watch List, which is now one integrated, all-source list, long before they arrive.

CONTAINER SECURITY INITIATIVE (CSI)

CURRENT OPERATIONAL PORTS (42)

EUROPE

Algeciras, Spain
 Antwerp, Belgium
 Bremerhaven, Germany
 Felixstowe, UK
 Genoa, Italy
 Gioia Tauro, Italy
 Gothenburg, Sweden
 Hamburg, Germany
 La Spezia, Italy
 Le Havre, France
 Lisbon
 Liverpool, UK
 Livorno, Italy
 Marseille, France
 Naples, Italy
 Piraeus, Greece
 Rotterdam, Netherlands
 Southampton, UK

EUROPE (cont'd)...

Thamesport, UK
 Tilbury, UK
 Zeebrugge, Belgium

ASIA

Dubai, United Arab Emirates
 Hong Kong
 Kaohsiung
 Kobe, Japan
 Laem Chabang, Thailand
 Nagoya, Japan
 Port Klang, Malaysia
 Pusan, Korea
 Shanghai
 Shenzhen
 Singapore, Singapore
 Tanjung Pelepas, Malaysia
 Tokyo, Japan
 Yokohama, Japan

AFRICA

Durban, South Africa

AMERICAS

Halifax, Canada
 Montreal, Canada
 Vancouver, Canada
 Buenos Aires, Argentina
 Santos, Brazil



As of July 31, 2005



Port of Seattle. Photo courtesy Customs and Border Protection

Securing the movement of people

Let me mention the movement of people, and the layers of security we've put into place to prevent terrorist operatives from getting into the US. Last year, over 70 million people flew into the US from abroad on commercial passenger airplanes. Better screening of people seeking to enter the US also depends, in part, on use of biometric identifiers and advance targeting. All US bound passengers are bounced against the Terrorist Watch List, which is now one integrated, all-source list, long before they arrive. And all passengers are also evaluated, through ATS, for terrorist risk factors. All those identified as posing a potential risk get CTR, extra anti-terrorism scrutiny on arrival, or, similar to CSI, overseas in those countries where we have pre-clearance or the Immigration Advisory Program.

...biometrics are an important element of our strategy to achieve the twin goals for expedited, but more secure movement of people through ports of entry.

Moreover, under the US VISIT program—another layer of defence—all foreign nationals when they arrive at US airports provide CBP with digitised finger scans, and these scans are automatically checked against those taken when our embassy overseas issued the visa, and against prints of major crime violators, deportees and prints of known terrorists. We also capture a digitised photo. So, biometrics are an important element of our strategy to achieve the twin goals for expedited, but more secure movement of people through ports of entry.

In the final analysis, identity authentication with one or more biometrics is a key part of our strategy to meet the twin goals regarding the transnational movement of people. Identity authentication and the use of terrorist risk factors, as you can see, becomes especially important for foreign nationals traveling under our Visa Waiver Program.

The land border challenge: Secure Border Initiative

Australia has all of the challenges we have, except we have the additional challenge of land borders—a 2,000 mile border with Mexico and a 4,000 mile plus border with Canada. No strategy of preventing terrorist entry can ignore illegal access, between ports of entry, along our long land borders. As you may have read, one of the biggest debates going on now in the US Congress is controlling our land borders, as well as immigration reform, and all of the extremely contentious political issues that relate to that issue. Controlling our borders has always been a desirable goal, but in the post 9/11 era, it is absolutely essential. Understanding this led to the decision to include the Border Patrol, formerly under INS, as one of the key operational elements of US CBP. We have greater control over our land borders now than we had, say, ten years ago, but we still have unacceptably high numbers of aliens crossing our borders—especially our border with Mexico—*illegally*. This is not just an illegal immigration issue; it is a national security issue.

Al-Qaeda understands this vulnerability and, indeed, has considered moving terrorist operatives into Mexico and then illegally across the Mexican border into the US. This is why; CBP and the DHS have developed a comprehensive national strategy for gaining control of our nation's borders between the ports of entry, between the official entry

points. This strategy is part and parcel of the comprehensive Secure Border Initiative (SBI) discussed by President Bush in his address to the nation a week ago last Monday. SBI involves more Border Patrol Agents, to be sure—there are currently 12,000 Border Patrol Agents within CBP—but it recognises that control of our borders involves more than just more Border Patrol Agents, and more than fences. Rather, it involves the right combination of technology, infrastructure, improved processes and law enforcement, that is to say, Border Patrol personnel. It would include detection technology that tells CBP's Border Patrol where and when intrusions of our border have occurred, so that the Border Patrol can rapidly respond and interdict the intruders—those illegally entering our country. This will assist in increasing the apprehension rate, the key to effective law enforcement and control. The border security piece of SBI is an area that DHS is actively pursuing right now. A Request for Proposal was issued last month by DHS for an integration contract.

One of the thorniest issues we have dealt with is ... how to achieve—in a way that is credible to the American public—the right balance between anti-terrorism security and privacy concerns.

Security vs privacy

One of the thorniest issues we have dealt with is the issue of privacy, or put differently, how to achieve—in a way that is credible to the American public—the right balance between anti-terrorism security and privacy concerns. The recent revelations and flap concerning the National Security Agency (NSA) and its

reported listening in on phone conversations involving callers or callees in the US and a party abroad, where there is an al-Qaeda connection to the caller or callee, illustrates the difficulty, from a public policy perspective. This issue is playing out at a number of levels, the 'right' to privacy advocates are out in force. But in the final analysis, this issue probably has more to do with the powers of the President vis-à-vis the powers given to the Congress under our Constitution. There is a strong case for the President's executive authority in this situation. Perhaps the issue that has most bedeviled the DHS, and the Transportation Security Agency (TSA), is the Computer Assisted Passenger Prescreening System (CAPPS II), an improved CAPPS program, that seems so directly related to preventing another 9/11 type attack, that has been impaled, several times, on the privacy spear.

Why, one might ask. At essence, CAPPS II would capture and use PNR-type data provided by the airlines and run that data against the Terrorist Watch List and against a targeting system for terrorist risk. A high risk passenger would presumably be given extra scrutiny at the TSA screening stations, and if on the 'No Fly' List, the airline could be directed to NO BOARD. It would remove the so-called No Fly list from the airlines, which would actually add security regarding names on the No Fly List. Every attempt by TSA to secure the necessary data has failed. True, there have been several 'bumps in the road'. For example, the revelation that several airlines had, without any disclosure to their passengers, voluntarily disclosed PNR data to TSA so CAPPS II could be piloted. When that came out, the whole process had to start over. But it has been nearly five years, and no CAPPS II—no better screening of the people who get onto airplanes in the US than there was before 9/11. Yes, checked luggage is now inspected by x-ray and even for explosives.

The screeners are now employees of the federal government, of TSA. And cockpit doors have been hardened. The reason we are still struggling with CAPPS II, in my view, is that the reasons and benefits of CAPPS II, and what it consists of, have not been adequately explained to the American public.

...the majority of people worldwide, including Americans, are willing to share personal data, e.g. PNR data, if (1) the government will protect the information, and (2) there is a clear benefit in the form of convenience gained... Where we have failed, I believe, is the unwillingness, as a policy matter, to articulate clear convenience benefits.

As Unisys research has shown, the majority of people worldwide, including Americans, are willing to share personal data, e.g. PNR data, if (1) the government will protect the information, and (2) there is a clear benefit in the form of convenience gained. I do not believe the first issue is insurmountable. Where we have failed, I believe, is the unwillingness, as a policy matter, to articulate clear convenience benefits. For border security, as I have explained, we have risk managed for the terrorist threat. We have collected PNR data, pursuant to Congressional legislation, and no one—in the United States—has raised a serious concern. Of course, this is, in part, due to the extraordinary powers that the US Government has at its borders, under our Constitution. For example, CBP has the broadest search authority of any law enforcement agency in the US—the power to search luggage, carry-ons and establish identity, without warrant, cause or suspicion. And the power to deny entry.

Still, the public knows, generally, that more advance information and the use of biometrics reduce the number of inspections and the amount of time for questioning.

What trade-offs has TSA offered? If an American must still go through a magnetometer and take off his shoes, and wait in long lines for the privilege of doing so, there is no convenience gain. Unfortunately, the security benefits of identity authentication and knowing that suspected terrorists will not be allowed to board your airplane may not be enough. But I ask: if the government has enough information, in advance, to verify identity and rule out an individual, why require that person, or every one, to go through a magnetometer? Convenience will, if the data is protected, win the day.

Conclusion

Let me wrap up my remarks by noting that we may be locked in a struggle against global terrorism for many years. Some have suggested it may last as long as the Cold War.

I have talked mainly about the defence today, that is, homeland security, but our strategy includes a strong offense with our allies and coalition partners carried out overseas. No ally has shown stancher than Australia. We thank you for that. And our strategy must also include an effort to diffuse the hatred and misunderstanding in Muslim world that fuels al-Qaeda. That's a huge task, I know, but we must address it. But when I am asked whether we will succeed in defeating the forces of global terrorism, I am reminded about another perilous time in the history of our nation—a time of grave danger—the American Civil War. Toward the end of the war, President Lincoln traveled to see General Grant. As the two men were seated around a camp fire at night, Grant asked Lincoln, 'Mr President, did you ever doubt the ultimate success of our cause?' Lincoln leaned forward,

the light of the campfire flickering against his face, and replied: 'No, never for a moment.' Likewise, I firmly believe that America and our allies, working together, will defeat the forces of global terrorism. I do not doubt it, even for a moment.

Acronyms

APIS	Advance Passenger Information System
APP	Advance Passenger Processing
ATS	Automated Targeting System
CAPPS	Computer Assisted Passenger Prescreening System
CBP	Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs–Trade Partnership Against Terrorism
CTR	Counter Terrorism Response
DHS	Department of Homeland Security
FAST	Free and Secure Trade
INS	Immigration and Naturalization Service
NTC	National Targeting Center
PNR	Passenger Name Record
RMAL	Regional Management Alert List
RPM	Radiation Portal Monitors
SBI	Secure Border Initiative
TSA	Transportation Security Agency

About this edition

The Australian Strategic Policy Institute and Unisys held a seminar on National Security policy at Old Parliament House, Canberra, Australia, on 24 May 2006 which has been turned into a special edition *Strategic Insight*.

The seminar addressed and discussed how the balance between free movement of trade and commerce and border and national security are balanced. Always dynamic, these two opposing perspectives are often difficult to reconcile, yet the effects of policy on commerce and economic growth can be dramatic.

Key to resolving this tension is the ability for agencies and jurisdictions to share and use information effectively while still maintaining security and privacy of citizen information.

The keynote speaker was Robert Bonner, former Commissioner of US Customs and Border Protection who presented his thoughts and experience of how US federal and state agencies worked in concert over the four years that followed the attacks on the US in September 2001 to strengthen homeland security. The graphics were part of this presentation.



Unisys offers clients solutions for secure business operations by aligning technology with business strategy. Drawing on a history of industry innovation and expertise, Unisys provides specialised services delivered by trusted consultants.

www.unisys.com.au

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

About the Author

Robert C Bonner is a partner in the Los Angeles and Washington, DC offices of Gibson, Dunn & Crutcher.

Mr Bonner was appointed by President George W Bush to serve as Commissioner of US Customs Service in September 2001. From 2003 through December 2005, Mr Bonner served as the first Commissioner of US Customs and Border Protection, the agency of the Department of Homeland Security responsible for managing, controlling and securing the United States' borders, while facilitating global trade and travel.

Following the terrorist attacks of 9/11, Mr Bonner created and launched the Container Security Initiative (CSI) and the Customs–Trade Partnership Against Terrorism (C-TPAT), the 24-Hour Rule and built the National Target Center—all of which continue to revolutionize the secure and more efficient movement of trade around the world.

About Strategic Insights

Strategic Insights are intended to provide expert perspectives on specific current issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

© The Australian Strategic Policy Institute Limited 2006

This publication is subject to copyright. Except as permitted under the *Copyright Act* 1968, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers.