Testimony of Carol Ashley

for the

United States Senate
Committee on Homeland Security and Governmental Affairs

on

Ensuring Full Implementation of the 9/11 Commission's Recommendations

Washington, D.C.

January 9, 2007

My name is Carol Ashley. My daughter, Janice, was killed in the World Trade Center on September 11th. She was 25. Thank you for giving me the opportunity to speak today about implementation of the 9/11 Commission recommendations.

Along with other members of the Family Steering Committee, I worked for passage of intelligence reform legislation in 2004 based on the recommendations of the 9/11 Commission. Our goal was to make our nation as secure as possible to reduce the chances that any other American families would lose a loved one to terrorism. Unfortunately, that bill did not fully implement the 9/11 Commission recommendations. Some that were included were not as strong as they should have been. The result is that more than five years after 9/11 there are still gaps in our security.

The safety and security of all Americans rests in your hands, and those of your colleagues. I commend Senators Lieberman and Collins for once again drafting bi-partisan legislation to address some of those security gaps. I respectfully ask you to endorse their effort.

Tightening our security and upgrading preparedness is urgent. Although five years have passed with no terrorist attack on our soil, there is no way to know when, where or how the terrorists will strike again. To fulfill its foremost obligation to protect the American people, Congress must ensure through legislation and oversight that comprehensive security safeguards are in place; and if the terrorists succeed in breaching our security, that our federal, state and local agencies are fully trained, equipped and prepared to respond cohesively.

Urgent Issues

REORGANIZATION OF CONGRESS FOR BETTER OVERSIGHT

Effective Congressional oversight is crucial to ensuring the safety, security and rights of the American people.

The 9/11 Commission recommended that Congress reorganize itself for more effective oversight of the intelligence community and homeland security. You are urged to devise a plan for effective oversight. If the actions of our intelligence and other information gathering agencies are ineffective or inappropriate, Congress should take steps to correct the problems. The same is true for the performance of the Department of Homeland Security (DHS). Unfortunately, it often appears the only way for Congress to enforce its will is by withholding appropriations. For this reason both the authorizing and appropriations committees must work collaboratively and from the same knowledge base.

To an outside observer, it appears that Congress is in many ways like our intelligence community before 9/11. Each committee has its specific area of oversight, but no committee sees the big picture. This Senate Committee on Homeland Security and Governmental Affairs should logically be the one which oversees *all* the various aspects of homeland security.

In the House, Speaker Pelosi is developing a plan which appears to partially address the problem of "*separation between committees with substantive authority over particular departments or agencies (authorizers) and those who wield the power of the purse (appropriators*)." [1] The Senate is urged to consider implementing a similar plan.

Hampering oversight is the fact that the top line of the intelligence budget is classified because it is within the defense department budget. Congress is urged to declassify that aggregate figure to facilitate effective oversight.

Further hindering oversight is that some agencies within our security network ignore Congressional deadlines with apparent impunity. DHS has been late, years late in some cases, in responding to Congress. 118 security plans for mass transit, rail, aviation, ports and borders, for example, were due in 2003, but still had not been received as of May, 2006. [2] Although one would hate to see funding slashed to those agencies which ignore deadlines, if that is the only control Congress has, it should use it ruthlessly.

PRIORITIES

Government Accountability Office Comptroller General David M. Walker listed priorities for the 110th Congress. Many of them were among the 9/11 Commission recommendations released in 2004. Congressional action, or lack or it, on these priorities will have a direct impact on the safety and security of America.

- *Ensure the Effective Integration and Transformation of the Department of Homeland Security;*
- *Enhance Information Sharing, Accelerate Transformation, and Improve Oversight Related to the Nation's Intelligence Agencies;*
- *Enhance Border Security and Enforcement of Existing Immigration Laws;*
- *Ensure the Safety and Security of All Modes of Transportation and the Adequacy of Related Funding Mechanisms;*
- *Strengthen Efforts to Prevent the Proliferation of Nuclear, Chemical, and Biological Weapons and Their Delivery Systems (Missiles);*
- *Ensure a Successful Transformation of the Nuclear Weapons Complex;*
- *Enhance Computer Security and Deter Identity Theft;*
- *Ensure the Effectiveness and Coordination of U.S. International Counterterrorism Efforts;*
- *Ensure a Strategic and Integrated Approach to Prepare for, Respond to, Recover, and Rebuild from Catastrophic Events;*
- *Ensure the Adequacy of National Energy Supplies and Related Infrastructure;*
- *Ensure Transparency over Executive Policies and Operations.* [3]

We are looking to the 110th Congress to implement needed safeguards.

Privacy vs. Security

THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

The 9/11 Commission recommended a strong, independent Privacy and Civil Liberties Oversight Board to oversee the Information Sharing Environment. Its goal is to monitor the collection and sharing of information to prevent abuse. However, the Privacy and Civil Liberties Oversight Board established by Congress is not the strong, independent board envisioned by the 9/11 Commission. Members of this board were appointed by the President without needing Senate confirmation. The Board has no subpoena power. Both the Attorney General and the Department of Defense can halt an investigation of alleged abuse.

Outrageously, the Privacy and Civil Liberties Oversight Board

> *" didn't even get a formal briefing on the administration's eavesdropping on American citizens until October — almost a year after the warrantless surveillance program had been uncloaked…[and the] board's initial report to Congress in March will first be vetted by administration factotums."* [4]

This is not the definition of a strong independent Board.

Congress is urged to strengthen the independence and authority of the Privacy and Civil Liberties Oversight Board and empower it with credible oversight capability by

- **Giving the Board subpoena power;**
- **Prohibiting any person or agency from interfering with its investigations;**
- **Requiring Senate confirmation of its members;**
- **Balancing the representation of both political parties on the Board;**
- **Providing adequate funding for staff and investigations.**

Recently, DHS' privacy office reported that in 2004 during a test phase of Secure Flight which screens passengers against terrorist watch lists, the Transportation Security Administration (TSA) violated federal law when it gathered and stored 100 million commercial data records on passengers. The TSA had said the data would not be stored. [5]

The collection of travel data is a legitimate tool for combating terrorist travel. But the pursuit of security must be balanced with the right to privacy. The key is to ensure that what is done with private information stays within the parameters of the law.

Surveillance of Americans suspected of terrorist ties is also a legitimate counterterrorism tool. However, warrantless spying in which government agents listen in on the conversations and read the e-mails of Americans, in violation of the 1978 FISA Court law, is dangerous to a free society. The FISA law protects the privacy rights of Americans by requiring a warrant within 72 hours of the initiation of surveillance. Requiring warrants for surveillance does not prohibit government surveillance of suspected terrorists.

Unfortunately, to further emphasize the danger of spying in contravention of the law, and the need for an effective Privacy and Civil Liberties oversight board, surveillance was not confined to suspected terrorists. A Freedom of Information request revealed that a Joint Terrorism Task Force spied on Americans who demonstrated against the Iraq war and against other administration policies. [6]

The FISA law protects the privacy rights of Americans which are a hallmark of our country. Secrecy, even that which is integral to national security, must not be allowed to trump America's system of checks and balances as it did last year when a Department of Justice probe into the NSA's warrantless eavesdropping was thwarted when DOJ attorneys were denied the necessary security clearance. No government entity should have the power to stop a legitimate investigation into its activities. [7]

Unfettered clandestine surveillance increases the potential for abuse, and with it the potential for insidious erosion of our rights to privacy and dissent. The freedoms we take for granted are at stake.

It is not only terrorists about whom we should be concerned. There is danger to America from within when unsupervised, possibly illegal government surveillance of American citizens continues unchecked.

Before allowing warrantless spying, Congress is urged to determine the nature and scope of the warrantless spying program, what has been done with the information, and its efficacy. Consideration should also be given to the presidential directive on warrantless spying which appears to circumvent the law, in terms of its impact on the balance of power, as well as its impact on the concept of America as a nation of laws. Further, Congress is urged to explore whether other hidden programs are monitoring Americans. If our government does not adhere to the law, what mechanism is there to protect our rights? Immediate effective Congressional oversight is needed.

Chemical and Biological Threats

Early warning of chemical and biological attacks is essential. Sensors and real time data concerning possible chemical or biological attacks are essential to minimizing casualties, particularly for crowded mass transit locations where an attack would have the most severe impact. The military has some amazingly sophisticated sensors, which could perhaps be adapted for civilian use. Among them are an infrared device that scans for blister and nerve gas in a 60 degree arc for a distance of up to 5 kilometers. It sounds a horn and illuminates the agent. Another is the portable chemical detector kit which tests for blister agents, blood agents, nerve agents, and lewisite (a component of mustard gas). [8]

TOXIC EXPOSURE SURVEILLANCE SYSTEM (TESS)

To improve surveillance of chemical exposures, the CDC and the American Association of Poison Control Centers are using TESS, a national real-time

surveillance database that contains all reported cases of human exposure to toxic substances.

By monitoring daily clinical effects, TESS facilitates early detection of illness from chemical exposure. The frequency of each clinical event is compared to a historic baseline. Aberrations result in notification of respective poison control centers.

TESS can identify illnesses from isolated chemical releases or from multiple locations. [9]

While early detection is crucial to effective response,

> *"The only way to guard against the use of chemical and biological weapons is to increase safeguards. Protocols should be strengthened and there should be stringent control over the manufacture and distribution of weapons-grade material. For chemical agents, markers like those used for plastic explosives to identify the country of manufacture, permit tracing the movement of these chemicals. Technological surveillance needs to be increased over the purchase of storage equipment and precursors."* [10]

ISSUES REGARDING BIOLOGICAL WEAPONS

In 2002, the president signed Public Law 107–188. The goal of that legislation was "*to improve the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies*."

It mandated

> *" improving state, local, and hospital preparedness for and response to bioterrorism and other public health emergencies with supporting grants; emergency authorities; enhancing controls on dangerous biological agents and toxins communication streamlining and clarifying communicable disease quarantine provisions and reporting deadlines."* [11]

Biological events are particularly dangerous because the effects of an attack cannot be detected immediately.

The information sharing concept applies to biological surveillance as well as to intelligence and oversight. Optimally, biological surveillance streams would feed into a centralized location accessible to all monitoring agencies.

Some interagency communication has already been established. For example, the Food Emergency Response Network (FERN) links state and federal laboratories that analyze food samples in the event of a biological, radiological, or chemical terrorist attack. FERN laboratories are hooked into the Electronic Laboratory Exchange Network (eLEXNET), an integrated information network that allows health officials across the country to compare, share and coordinate laboratory findings.

DHS' National Bio Surveillance Integration System is a step in the right direction. Established in 2005 as part of the National Biosurveillance Initiative, its goal is to

> "*combine and analyze information collected from human, animal and plant health, food and environmental monitoring systems. Such an analysis, combined with evolving threat and intelligence information, will provide greater context for those making critical homeland defense decisions*." [12]

The National Bio Surveillance Integration System, based on integrated information sharing, alerts authorities to a disease outbreak by recording biological events in real time from across the country. Such a program should be encouraged and adequately funded.

In addition, Congress is urged to expand funding for laboratories to enable rapid identification of human and animal disease pathogens and appropriate rapid response.

Protecting America's Chemical Facilities

In America, there are 15,000 facilities that produce, use, or store dangerous quantities of hazardous chemicals, according to the Environmental Protection Agency (EPA). Many of these plants are in densely populated areas making them targets for terrorists. Seven thousand of these chemical facilities have the potential to affect more than 1,000 people. 123 of these facilities, if attacked, could affect more than 1,000,000 people.

Besides the devastating human cost, a terrorist attack on a chemical plant could disrupt commerce because many chemical plants and refineries are located near ports and/or major highways.

Transportation of hazardous chemicals through heavily populated urban areas is another opportunity for a terrorist strike.

Some chemical facilities have begun to institute "Inherently Safer Technologies" (ISTs) in which dangerous chemicals are replaced by safer ones. Not only does IST improve security, it also reduces the danger posed by shipping large amounts of extremely toxic chemicals. [13]

CONGRESSIONAL ACTION

Although legislation concerning chemical plants was passed in 2006, it was not strong enough.

> *"Congress passed an appropriations bill giving the Department of Homeland Security (DHS) interim authority until 2009 to review and approve chemical sites' security plans. The measure does not allow DHS to require specific measures, and provides a mere $10 million to improve chemical plant security."* [14]

Under the legislation, which reflected the recommendations of the chemical industry, America's chemical companies would assess their own vulnerabilities and provide a plan for addressing them.

Chemical companies will be required to conduct background checks on employees. But is there mandated standardization of acceptable criteria for access to the all U.S. plants? Is there a rule that requires biometric identification cards like the ones that will be mandatory for our maritime workers?

Although the companies are required to institute better control access or face fines of up to $25,000 a day, or even being shut down, they are allowed to contest the government's disapproval of their security plans. [15]

Who has the final say on security?

DHS can strengthen security at chemical companies by setting industry wide standards for employee screening, immediate implementation of biometric identification cards, and rigorous binding standards for compliance. In addition standards for risk and vulnerability assessments, with strict deadlines for submission will heighten safety. Finally, for enhanced security, no flight paths should be allowed over the facilities.

Coastal Defense

The Coast Guard is an integral component of border security.

A layer of security was added by the rule that ships approaching the United States must provide notice 96 hours before arrival. It allows the Coast Guard to determine whether to board a vessel before it lands (which it did about 10,000 times in 2005.) [16]

The latest security initiatives are designed to thwart a terrorist attack by sea. To defend against a terrorist attack, for example, in which terrorists crash a fast boat packed with explosives into a liquefied natural gas tanker, the Coast Guard is arming helicopters with machine guns, training security teams to rappel onto moving ships and to gain control of a hostile vessel by force. It is using technology such as sensors, satellites, and surveillance cameras to convey information to harbor based command centers. [17] These are valuable tools to defend against terrorism.

The Coast Guard needs to be equipped with state of the art technology and a fast efficient fleet. But the Coast Guard's fleet is aging. It uses a 43-year-old ice-breaking tug boat to patrol around the Indian Point nuclear power plant on the Hudson River, 24 miles north of New York City. The tug boat's top speed is 10 knots. It has no weapons except handguns. [18]

Unfortunately, the Coast Guard's Deepwater program to refurbish its aging fleet has encountered problems. A number of cutters are out of service. Some ships have deformities and structural cracks; surveillance cameras have blind spots; and communications systems are not secure. [19]

There are other problems as well:

- Its radar system is unreliable. Sometimes waves are mistaken for boats and the image of large ships is split in two.
- Communications and surveillance systems are less effective than expected.
- There is no unified command of the coasts and waterways. Control is divided among at least 15 federal agencies.
- The Coast Guard does not have enough armed vessels or planes.
- The Automated Identification System used to identify approaching ships is not secure. Those intent on avoiding detection can send out false information about the location or identity of the vessel, or even turn the system off.
- The Coast Guard has not yet developed an efficient system for collating the maritime threat information it collects and receives.
- There are turf issues regarding jurisdiction during maritime events. [20]

The Deepwater program is being investigated by the General Accountability Office. (GAO).

Congress is urged to consider streamlining oversight of the Coast Guard. The Coast Guard and other agencies with jurisdiction over maritime events should establish an incident command structure to define responsibilities. Congress should consider what can be done to eliminate substandard contract work and equipment failures which compromise national security. It is also urged to consider ways to prevent outrageous cost overruns.

Border and Transportation Security

The complexity of border and transportation security makes management difficult.

A 2005 CRS Report on "Border and Transportation Security: Possible New Directions and Policy Options", discussed the value of a layered approach to border and transportation security. The layered approach focuses on both logistics, which control the flow of goods, information, and travelers from one point to another, and on intermodal points of vulnerability across the transportation network. Layered security increases the opportunity for intercepting terrorists or terrorist activity at multiple points along the way.

On September 11th, 2001, none of the layers of security — intelligence, passenger prescreening, checkpoint or onboard screening— stopped 19 terrorists from boarding four airplanes at three different airports, For that reason, the 9/11 Commission cautioned that

> "*Each layer must be effective in its own right. Each must be supported by other layers that are redundant and coordinated*." [21]

LAYERED SECURITY MEASURES

For optimal effectiveness, the CRS recommended security measures at these points of vulnerability.

STAFF AUTHENTICATION AND SCREENING AT ALL POINTS ALONG THE TRANSPORTATION CHAIN

The identity of all transportation staff should be verified to ensure that terrorists cannot gain access to, or control of, any part of the transportation system.

SECURE IDENTIFICATION OF TRANSPORTATION WORKERS

Although President Bush signed legislation mandating the new identification cards for transportation workers in 2002, only now are the cards beginning to be issued. [22]

The Transportation Worker Identification Card (TWIC) rule issued by TSA and DHS on January 3rd, 2007, should help protect our ports and add a layer of security when fully implemented. The TWIC rule requires seaport and maritime workers, port owners and port operators to undergo background checks for criminal history and immigration status, and to submit all ten finger prints. Any applicants whose criminal history might place them in the "nexus of terrorism," will be banned. [23]
Federal law enforcement officials are increasingly concerned about the potential interchangeability of smuggling networks and their possible nexus with terrorist networks. [24]

Once the applicant is approved, he or she will be credentialed.

> "*The credential will be a "smart card" containing a photograph and name of each worker, expiration date and serial number. An integrated circuit chip will store the holder's fingerprint template, a personal identification number and a unique identifier*." [25]

Without the credentials there will be no unescorted access to secure areas of vessels and facilities.

In addition to monitoring access, biometric credentials should be used to provide "*a record of …every instance of request for entry, grant of entry, denial of entry and other data; a record of personnel movement; asset protection; and flexible security*." [26]

The ID credentials will be gradually phased in beginning in March. Ultimately more than 750,000 employees, union workers, mariners and truckers will be credentialed. The TWIC fee is $159 and valid for five years. The fee is high, especially for truckers who have a high turn over rate and may not use them for the full five years.

Incredibly, the TSA rule does not require port operators to install the machines to read the cards that verify employees' identities. [27] That defeats the purpose of requiring the card.

Why didn't the rule require card readers at the same time as implementation of the TWIC rule?

Ultimately the plan is to apply a single standard to approximately 5 million transportation workers at seaports, airports, chemical plants, and other protected facilities in the United States. [28]

TSA and DHS should issue an immediate supplementary TWIC rule requiring installation of machines capable of reading the TWIC smart cards.

As soon as its efficacy is proven, implementation of this credentialing program should be accelerated and expanded to include workers in all vulnerable industries.

ADVANCE ELECTRONIC CARGO MANIFEST REQUIREMENT

Security was improved when Customs implemented the "24 hour rule" requiring submission of specific manifest information 24 hours in advance of cargo being laden on a US bound vessel at a foreign port. This rule gives Customs enough time to do a risk assessment of arriving cargo. [29]

SECURE FREIGHT INITIATIVE

Another security program which should heighten port security is the Secure Freight Initiative which will begin this year. The Departments of Energy and Homeland Security announced that all US-bound cargo sent by container ships from three ports in Pakistan, Honduras and Southampton, England, will be scanned for hidden nuclear weapons or components.

The containers will be scanned by a radiation detection machine and an X-ray device and have their identification numbers read by an optical character reader. The combination of radiation detection and X-rays is supposed to find bomb-making materials that have been shielded. The radiation scan and X-ray images will be transmitted electronically to U.S. Customs and Border Protection officials, who can request that local law enforcement at the foreign ports to do a more comprehensive search of suspicious findings.

However, some antiterrorism experts have expressed concern:

- The screening will take place only on container ships, not on ships carrying millions of tons of other cargo, including cars, fuel or goods placed on pallets;
- The detection equipment is unable to see through many items that might be inside a container, like frozen food;
- The equipment is prone to false positives;
- Not all of the X-ray images will be checked, so a bomb could still get through.
- Since the equipment is installed in only a small number of ports, terrorists could send a bomb by container from somewhere else. [30]

Homeland Security Secretary Michael Chertoff said the department will also install radiation detection and X-ray scanners at three other ports — in South Korea, Oman, and the Port of Singapore. However, not all containers at these ports will be scanned using the combination of radiation scanning and X-ray technology. [30a]

Other possible safeguards to protect the vulnerability of cargo in transit include "smart-container" technology which can detect and record when a container is opened and the use of Global Positioning System (GPS) technology to track container location at any given point in time. [31]

Screening of Travelers

The Commission noted that when people travel, they usually move through defined checkpoints. Each checkpoint is an opportunity to verify the identity of the traveler and to intercept terrorist suspects: when they acquire a passport, apply for a visa, check in at ticket counters and gates, stop at exit controls at airports and seaports, and pass through immigration inspection points. Or interception can occur when the traveler seeks another form of identification or to change his immigration status in order to remain.

Onboard security worked in the recent case of six imams who were ejected because their behavior was alarming to the flight crew and passengers.

> *"Flight attendants said they were concerned that the way the imams took seats that were not assigned to them -- two seats in the front row of first class, exit seats in the middle of the plane and two seats in the rear -- resembled the pattern used by September 11 hijackers, giving them control of the exits."* [32]

The airline acted correctly.

INTEGRATED TERRORIST WATCHLIST

For optimal security, an integrated terrorist watch list should be made available to those who are monitoring activity at our borders.

On Sept. 16, 2003, President Bush signed Homeland Security Presidential Directive-6 directing that more than a dozen federal terrorist watch lists be integrated into a single master list of "known and suspected terrorists" maintained by the FBI. The deadline for creating the integrated master list was Dec. 1, 2003.

As a result of the directive, the FBI's Terrorist Screening Center was created. The FBI master list was to become a subset of the database maintained by the joint FBI-CIA Terrorist Threat Integration Center (TTIC).

When new information was added to the database, DHS was to review it and decide whether it would be made available to state and local law enforcement and to those responsible for critical infrastructure.

TTIC was also directed to "promptly assume responsibility" for the State Department's TIPOFF database which has more than 110,000 names of known and suspected terrorists. TIPOFF is used by consular officials to screen foreign visitors to the US. [33]

Noting that the watch lists had not been integrated and shared, the 9/11 Commission recommended in 2004 that

> "*Every stage of our border and immigration system should have as part of its operations the detection of terrorist indicators on travel documents. Information systems able to authenticate travel documents and detect potential terrorist indicators should be used at consulates, at primary border inspection lines, in immigration services offices, and in intelligence and enforcement units".* [34]

Where are we now? The lists have been consolidated but not merged.

Nominations from both the intelligence agencies and law enforcement, including the FBI, and state and local police, are submitted to Terrorist Screening Center for inclusion on the Terrorist Watch List. The CIA makes most of the nominations from the intel side.

But as for sharing of information and access by state and local law enforcement, as of June, 2006, DHS was still in the " 'early stages' of developing a strategic plan for capturing and disseminating intelligence along the nation's borders" and that Customs and Border Protection officers do not have access to all watch list databases. [35]

It is scandalously negligent that an effective plan for sharing integrated watch list data, and "capturing and disseminating data" along our borders is not in place more than 5 years after 9/11. Development of such a plan should have started immediately after the terrorist attacks.

An integrated terrorist watch list is integral to protecting our borders and our nation.

In evaluating terrorist screening, Congress is urged to

- **Explore how best to integrate and share the various watch lists;**
- **Direct DHS to implement an intelligence information sharing plan along our nation's borders as soon as possible;**
- **Examine the criteria used to accept a nomination for inclusion on the watch list;**
- **Determine who has access to the watch list and how that information is used;**
- **Address the difficulty of removing an innocent person's name that has been included on the watch list. Redress is currently very difficult.**

SCREENING PASSENGERS BY OBSERVATION TECHNIQUES (SPOT)

One credible new screening program which should be expanded and adequately funded is SPOT. It is race neutral and adds another layer of security. Trained TSA

workers identify suspicious passengers by observing unusual or anxious behavior reflected in mannerisms, excessive sweating, or changes in the pitch of a person's voice. So far, SPOT has resulted in the arrest of more than 50 people for drug possession, illegal entry or having fake identification.

Suspicious passengers will receive more thorough screening which might include face-to-face interviews with local police and national criminal database checks to help determine if a threat exists. If terrorist ties are suspected, Federal counterterrorism agents will become involved.

The TSA is considering deploying SPOT teams to other transportation systems like train and bus stations. [36]

Because the SPOT program is successful, the TSA should expedite expanding SPOT to include screening in all modes of transportation, including intermodal nexus points. To broaden the scope, SPOT training should be mandated for state and local police to add another layer of protection, especially for mass transportation. Congress is urged to ensure adequate funding for the program.

BIOMETRIC IDENTIFICATION

Securing our borders while simultaneously facilitating the movement of people to and from our country without unnecessary delays or intrusion into their privacy is a priority.

The State Department's implementation of new passport rules beginning this year is a welcome initiative. New electronic passports embedded with a smart chip that stores the traveler's photo and personal information will add a layer of security at our borders. To counter the possibility that hackers will compromise security by skimming personal data as it is being transmitted wirelessly, the State Department added metallic anti-skimming material to the passport covers and encrypted the information.

Another positive is the requirement beginning January 23rd that air travelers to and from Canada, Mexico and the Caribbean will need a passport except for those travelers who have a "Nexus Air card", issued through a joint US-Canada program which prescreens travelers.

Undermining these security initiatives though, is America's extraordinary leniency regarding the kind of documentation that is acceptable for crossing our borders. Diverse forms of acceptable documentation and multiple exceptions to the rule do not enhance our security. For example, a passport is required now for air travelers — unless they have a Nexus air card for travel to and from Canada. Land and sea travelers will need a passport by June, 2009 to travel to Canada, Mexico and the Caribbean —unless they don't want to pay the $97 passport fee and opt instead for a $20 "passport card" to be introduced later this year. [37]

Then there are those who enter through the Visa Waiver Program (VWP). A visa is required for entry— unless you come from one of 27 visa waiver countries. President

Bush wants to increase the number of countries included in this program. You are encouraged to quash that effort. [38]

The Government Accountability Office (GAO), concluded in a July report that the Department of Homeland Security (DHS) cannot keep up with the 27 visa waiver countries already approved. [39]

In addition, travelers admitted through the VWP do not have background checks prior to their arrival in the U.S.. That means there is only one opportunity— during immigration inspection at the port of entry— to identify terrorists or others who should not be admitted. [40]

Visa waivers offer a loophole for terrorist entry. England, Germany, Spain, and other friendly nations have terrorist cells, as evidenced by attacks and arrests there. Requiring visas of everyone who enters our country would add an extra layer of protection, providing another opportunity for interdiction at which a terrorist could be screened and stopped.

Leniency of admission standards, variable standards for entry and failure to enforce current immigration laws contribute to our porous borders and compromise our security.

Congress is urged to mandate uniform requirements for entry into America.

US-VISIT PROGRAM

US-VISIT was designed verify the identity of visitors and record their arrival to and departure from the United States using biometric identifiers (fingerprints of two index fingers) and digital photographs. Information collected is compared to watch lists to screen for criminals, suspected terrorists and visitors who stay in the country illegally.

Of 170 U.S. land Ports Of Entry (POEs), 154 have US-VISIT entry capability. Although there are statutory requirements for exit capability, US-VISIT officials have concluded that biometric US-VISIT exit monitoring cannot be implemented at this time due to technical difficulties, impact on the flow of traffic across the border and the cost of expanding facilities and infrastructure that would be needed. [40a]

The only proven technology for verification of an exiting visitors' identification is the same one which is used for entry verification. CBP officers at land POEs would follow the same screening procedures as for US-VISIT entry:

> "*examine the travel documents of those leaving the country, take fingerprints, compare visitors' facial features to photographs, and, if questions about identity arise, direct the departing visitor to secondary inspection for additional questioning*." This would result in "*additional staffing demands, new infrastructure requirements, and potential trade and commerce impacts*." [40b]

Non-biometric exit technology was tested using radio frequency identification (RFID) technology in the interim, but the failure rate was high and RFID could not verify that visitors who enter the country are the same as those who leave. In RFID trials, a microchip with a single number was embedded in a tag on the departure form. This unique ID number was linked to the visitor's biographic information but did not verify the identify of the holder. [40c]

US-VISIT officials are expected to announce soon that plans for verifying visitors' identification upon exiting will be dropped. [40d]

DOMESTIC FLIGHTS

One of the first lines of defense against terrorism is determining who is on the flights, whether they are international or domestic.

International passengers are checked before boarding against the No Fly List. Once the plane leaves the ground all names on the passenger manifest are checked against DHS' Custom and Border Protection's Selectee list, which is a comprehensive watch list. CBP can then decide whether to admit someone or contact the FBI. **To strengthen security, Congress should mandate that the manifests be checked *before* the plane leaves the ground.**

On domestic flights, the airlines check passenger names against the No Fly list. Once the plane leaves the ground, there is no parallel process to that of international flights. Passenger manifests are not checked by government agents against a comprehensive watch list. Today, once a potential terrorist boards a domestic flight, one layer of security is missing, even though it was four *domestic* flights that were hijacked on September 11th. This lapse in security is unacceptable, especially since we know from the 9/11 Commission investigation that two of the 9/11 terrorists were on a CIA watch list in 2001, and could have been stopped if the information had been shared in time.

The first objective is to keep potential terrorists from entering our country. If that security layer fails, then domestic security must be stringent enough to succeed in stopping them. To increase the chances of interception, Congress should mandate that domestic passenger manifests be checked by government agents against a comprehensive watch list.

INTERNAL TRAVEL

America would be more secure if state issued documents such as drivers' licenses adhered to consistent standards from state to state. A driver's license often serves as proof of identity, enabling the holder to travel within the country and conduct business.

The 9/11 Commission recommended setting national standards for state-issued documents — including birth and death certificates and driver's licenses. This recommendation was only partially implemented in the Intelligence Reform and Terrorism Prevention Act of 2004. Although the House passed H.R. 418, The Real ID Act, on February 10, 2005, the Senate took no action. [41]

Illegal immigration poses a threat to our security because it is impossible to verify the identity of those who do not come through America's official ports of entry. Standardization of legally acceptable proof of identity would add another layer of security to combat terrorist travel and would help stem identity theft.

Congress is urged to standardize legally acceptable proof of identity; to investigate lax enforcement of current immigration laws; and to fully fund the building of a fence on our southern border, technology to provide virtual barriers, and the hiring additional border patrol agents.

IMPROVED TRAINING FOR BORDER INSPECTORS

Border inspectors should receive updated training that highlights terrorist travel methods and document falsification techniques. Fifteen of the 19 hijackers carried documents that would have made them vulnerable to interception by border inspectors. [42]

Screening for Other Modes of Transportation

RAIL AND MASS TRANSIT SECURITY

Since 9/11 the government has spent $18 billion in aviation security and less than $500,000,000 on rail and transit security combined.

Government attention and leadership in this area is needed. Although mass transit is locally owned, protecting those modes of transportation and the intermodal connections is a national security issue and thus the federal government's responsibility.

Currently, within the executive branch, there is no single entity responsible for rail and mass transit. Responsibility is shared by the DHS and DOT.

Screening passengers on trains and mass transit is extremely difficult because of the numbers of people involved, and the speed with which passengers board and disembark. However, as evidenced by the Madrid and London bombings, rail and mass transit are especially vulnerable to attack.

Congress is urged to establish a leadership position whose responsibility is rail and mass transit issues, comparable to the FAA Administrator, within the executive branch.

VEHICLE SECURITY

In addition to the above security measures, the CRS report advised monitoring the physical security of all the various kinds of vehicles and vessels that carry passengers and cargo.

Steven Flynn author of *America the Vulnerable* recommends the use of transponders to track the location and route of vehicles transporting hazardous material. Others have proposed an automatic shutoff device for large rigs hauling such material. [43]

These two proposals would add another layer of security and are worth exploring.

Additional Security Tools Suggested by CRS

RED TEAMS AND WAR GAMES

As proposed by 9/11 Commission staff tasked with aviation and transportation security, Congress should create covert Red Teams outside the TSA and DHS to pinpoint and explore potential vulnerabilities in all transportation modes and use war-games to devise counter measures to those vulnerabilities.

In the two years preceding the terrorist attacks on 9/11, there were no Red Team exercises at Logan and Newark airports.

EXPAND RESEARCH AND DEVELOPMENT FUNDING FOR COMPATIBLE RADIATION AND EXPLOSIVES SCREENING DEVICES

There should be increased funding for research and development of radiation and explosives detection devices that can be used across all transportation modes. The ability to use Non-Intrusive Inspection (NII) technology at rail and transit terminals to detect explosives carried by a passenger at a distance would significantly improve security, as would “puffer” type explosive screening for passengers, sensors for chemical and biological materials, and bomb-sniffing dogs. Congress is urged to ensure adequate funding for all these security initiatives.

INVESTIGATE WAYS TO STRENGTHEN SECURITY AT NEXUS POINTS

Security should be strengthened at every juncture where cargo moves from point to point — from truck to container to ship to train to truck to delivery. Security should also be improved for smaller pallets to prevent tampering at these vulnerable points. [44]

Nuclear Danger

Nuclear danger is two-pronged.

EXTERNAL DANGER

The first involves the accessibility of radioactive and fissile material. The US must be more aggressive in securing the loose nuclear and radiological material especially in the former USSR to prevent it from falling into the hands of terrorists. Nuclear smuggling has increased sharply. In 2005 alone, there were more than 100 confirmed incidents of trafficking and unauthorized access to nuclear and fissile materials. [45]

A report released in 2005 by the John F. Kennedy School of Government at Harvard says that there is enough material in the former Soviet Union to build 80,000 nuclear weapons. Only half of it was secured. [46]

Interestingly, Dr. Igor Bolshinsky of the U.S. Department of Energy's National Nuclear Security Administration said during an ABC News taping that weapons-grade, highly enriched uranium can be picked up with one's bare hands, making it very attractive to terrorists. [47]

Between 2005 and 2010, the United States expects to spend more than $500 million to reduce the nuclear threat globally. Critics contend that is not enough. However, Ambassador Linton Brooks, former head of the National Nuclear Security Administration, said,

> *"Our problems are not primarily money…Our problems are access in the Russian Federation. Our problems are convincing other countries that they need to take the threat as seriously as we are, and we keep working through that. The greatest incentive in the world is to understand that we're all in the cross hairs, and therefore we want to take away the bullets."* [48]

Al Qaeda has repeatedly tried to obtain nuclear material and recruit nuclear scientists. Improved tracking of nuclear and radiological material has helped security, along with the use of radiation monitors at airports, ports and tunnels leading into major cities, but more needs to be done, and quickly. [49]

INTERNAL DANGER

The second involves internal security lapses at our nuclear facilities. Knowing that there is the threat of nuclear terrorism, it is inconceivable that security at Los Alamos and other nuclear weapons facilities is so lax. In a report dated Nov. 27, 2006, the Energy Department's inspector general criticized the National Nuclear Security Agency (NNSA), saying, "In a number of key areas, security policy was nonexistent, applied inconsistently, or not followed." [50]

Two striking security breaches occurred within the past year. Police responding to a domestic dispute uncovered drug paraphernalia and computer flash drives containing thousands of classified documents in a former Los Alamos worker's home. The other breach occurred when a computer hacker stole Social Security numbers, birth dates and other sensitive information about 1500 Energy Department contractors. [51] For nine months, neither those whose data was compromised, nor top officials were notified of the breach. [52]

It is not only federal facilities that are lax. In 2005, over a four month period an ABC News investigative team visited 25 universities with nuclear reactors. It found

> *"gaping security holes at many of the little-known nuclear research reactors operating on 25 college campuses across the country. Among the findings: unmanned guard booths, a guard who appeared to be asleep, unlocked building doors and, in a number of cases, guided tours that provided easy access to control rooms and reactor pools that hold radioactive fuel".* [53]

Congress is urged to invite expert witnesses to testify regarding the nuclear threat to gain their perspective on stumbling blocks that are slowing the process of securing accessible nuclear material and their recommendations on how Congress can help.

In addition, Congress is urged to make securing nuclear materials, a high priority and emphasize to the President and the Secretary of State that strong leadership is needed to convince all nations to cooperate in diminishing the nuclear threat.

Regarding internal security at our nuclear facilities, please consider dispatching Red Teams to evaluate security flaws, and act on their evaluations without delay.

For an added layer of security, flight paths should not be allowed over America's nuclear power plants.

Risk Based Homeland Security Funding

In the past both the House and the Senate have proposed legislation allocating to each state a percentage of the total funding for homeland security assistance. The differences between them lie in the criteria and formulas for distribution.

As explained in CRS Report RL 33050, *Risk-Based Funding in Homeland Security Grant Legislation: Analysis of Issues for the 109th Congress,* the House would guarantee each state a minimum amount after risk-based state allocations are determined. The Senate would guarantee each state a base amount without regard to risk. [54]

After weighing all the information it obtained about the 9/11 attacks—including the terrorists' targets and goal of killing as many people as

possible with nearly simultaneous multiple attacks— the 9/11 Commission concluded that Homeland Security assistance should be risk-based. For this reason, Congress is urged to mandate risk based distribution.

Emergency Preparedness

Two aspects of emergency preparedness must be considered. The public must be prepared and informed about protective measures it can take, and the first responders must have an organized emergency plan and the best available interoperable communications system.

To prepare the public for an emergency, in addition to detailing the contents of an emergency go-bag, emergency evacuation drills should be required in the private sector, preferably unannounced. Some drills should include blocked exits. These drills should be held several times a year so that occupants are familiar with both usual and unusual escape routes. High rise buildings should be required to hold full evacuations which exit on the ground.

In the event of a terrorist attack, or other mass casualty disaster, first responders must be prepared to act as quickly and efficiently as possible to minimize the loss of life and limit destruction. These key elements are needed:

INCIDENT OR UNIFIED COMMAND

Mandating rigorous training in either Incident or Unified Command Systems which define leadership responsibilities and allow each group of first responders across multiple jurisdictions to understand their unit's role, will make rescue efforts will more organized and efficient.

INTEROPERABLE COMMUNICATIONS

An interoperable communications system which enables state and local emergency responders to talk across jurisdictions is needed to prevent a tragedy such as happened on 9/11. Hundreds of firefighters died when they did not hear Police department evacuation orders prior to the collapse of the Towers because their radios were incompatible with police radios.

One official knowledgeable about DHS grant programs remarked "The interoperability goal is fine but how is it going to be paid for?" [55]

Some members of the House Homeland Security Committee urged Congress to address the problem by creating a grant program to help cities update their emergency communications. 56]

It is hoped the Senate will also address the interoperability issue, especially since a DHS report just released revealed that there are still major problems

with how well emergency agencies communicate. DHS evaluated 75 cities and surrounding suburbs on their emergency response capabilities in three categories: operating procedures; communication; and coordination. Only 6 cities received a top rating. [57]

The twin issues of interoperability and unified command must be resolved for the safety of both victims and first responders.

SIMULATED ATTACKS

Simulations and drills sponsored by Homeland Security are needed, but it is important for Congress to evaluate the effectiveness of the various exercises before it designates funding.

Top Officials program (TOPOFF) incorporates seminars, planning events and large-scale national exercises to train and drill government leaders and responders. It focuses on preventing, responding to and recovering from various types of large-scale terrorist attacks.

The scope and cost of TOPOFF exercises have increased rapidly, from 18 federal agencies participating in the first drill (pre-9/11 at a cost of $3 million) to 27 federal agencies, dozens of state and local departments and 156 private sector organizations (at a cost of $21 million) in the last full-scale event.

There are valid criticisms of TOPOFF:

- Its high cost and inefficient use of funds. Critics contend that for the cost of a two-city TOPOFF event, exercises could be done in 30 cities.

- Its use of consulting companies to run and evaluate disaster exercises. Critics believe that invalidates the simulations because contractors approach all locations the same way, without considering the unique variables of a specific location.

- Simulations that give advanced warning. This results in an unrealistic picture with fewer unforeseen problems. Critics believe more valuable emergency response insight is gained from real-life false alarms.

Critics argue that rigorous, independent evaluation is needed to accurately assess both the positive and negative of response capabilities. An after-action report on the exercise should be mandatory to aid in critical follow-up needed to correct deficiencies, either through additional training or policy changes.

Positive steps taken by the DHS include its Lessons Learned Information Sharing Web site (www.llis.gov) where registered users have access to preparedness information and after-action reports, and its Homeland Security Exercise and Evaluation Program (www.hseep.dhs.gov), which standardizes policy, methodology and language for designing, conducting and evaluating exercises.

Also positive is that DHS, Health and Human Services (HHS), and the Centers for Disease Control and Prevention (CDC) are beginning to require

use of the Homeland Security Exercise and Evaluation model before funding an exercise. [58]

Critical Infrastructure

To protect critical infrastructure, standards for risk assessment and well defined protective strategies and warning devices must be in place. If target dates for compliance are missing, DHS should set immediate deadlines for receipt of this information from critical infrastructure elements such as oil refineries, chemical facilities, nuclear power plants, and those who manage metropolitan area transportation systems, energy networks, and our food and water supply.

Recently, an analysis done for the New York-New Jersey Port Authority, a bi-state public agency that manages bridges, tunnels, bus terminals and airports, determined that the train tunnels running under the Hudson River are more vulnerable to a bomb attacks than previously thought. A relatively small bomb would flood one tube within 6 minutes, and within hours, produce significant flooding of the rail system. To address this vulnerability, the Port Authority plans to lay concrete blankets atop the tubes to plug holes caused by a blast, strengthen critical sections of the tubes and install floodgates.

However, neither the DHS, the governors, the Mayor of New York City, nor the New York Police Department were told of the vulnerability analysis. [59]

Congress is urged to determine how best to ensure that public authorities and others responsible for critical infrastructure report risk assessments to DHS (and other pertinent officials) in real time.

If the public authorities receive separate homeland security funding, that would be a place to start.

A Clearly Articulated Plan for Information Sharing

When this legislation is passed, it is hoped it will include a clearly articulated plan for information sharing.

Frustrated by the lack of federal leadership and harmonization, cities and states in 37 states have established their own "fusion centers" which collect and analyze information from local, state and federal law enforcement officials. The centers have received $380 million in federal support since the 2001, but with little concomitant federal guidance, training, and standards. [60]

To strengthen the Information Sharing Environment, Congress is urged to:

- **Extend the term of the Program Director and make the position permanent;**
- **Require Senate confirmation for the appointment;**

- **Give the Program Director the ability to issue government wide standards;**
- **Move the Program Director's office to NCTC;**
- **Provide for training of state and local law officers by experienced professionals in preparing and interpreting intelligence data so that there is some consistency and cohesiveness between the fusion centers and federal agencies. Such training would**
    - **improve the usefulness of data sent to the NCTC by state and local authorities;**
    - **increase state and local authorities' ability to interpret intel products correctly;**
    - **better integrate the state and local law enforcement with the federal government agencies;**
- **Determine the quality of interaction between state and local police and the FBI. Communication between these agencies is critically important. State and local police may be the first to encounter terrorists. For example, in Oklahoma, a trooper stopped 9/11 terrorist Nawaq al Hazmi for speeding on April 1, 2001.** [61] **Another terrorist, the pilot of Flt. 93, Ziad Jarrah, was stopped on September 9, 2001, in Maryland doing 90 mph.** [62] **Unknown to the police officers at the time, Al Hazmi, his passenger fellow terrorist Hanjour, and Jarrah all were in violation of immigration laws and could have been detained, perhaps unraveling the plot.**
- **Establish a federally funded intelligence institute for training of state and local law enforcement;**
- **Authorize additional funding for improving the Information Sharing Environment.**

Define What We Stand For

> *"The U.S. government must define what the message is, what it stands for. We should offer an example of moral leadership in the world, committed to treat people humanely, abide by the rule of law, and be generous and caring to our neighbors."* [63]

As Congress moves forward under new leadership, it also needs to look back at the actions of our government, and ask whether those actions best represented the ideals of our nation. If not, what changes need to be made?

After the devastation of 9/11, the families who lost so much were overwhelmed by the outpouring of support from across the country. Americans are compassionate, generous, caring people. We need to show that face to the rest of the world.

Conclusion

Congress shoulders a huge responsibility when it comes to national security. There are so many agencies and issues involved: 17 intelligence agencies, federal state and local law enforcement; security across all modes of transportation; port and coastal security; protecting the infrastructure, energy and communication networks; preparedness, and emergency response. The American people depend on our government—on Congress, the Executive and the Judiciary branches—to protect us from external and internal threats to our safety, our security and our Constitutional rights.

Decisions which you make today will affect American families now and in the future. Six or seven years ago, the FAA yielded to pressure from industry lobbyists who objected to heavy fines for egregious airline security violations. The purpose of the FAA fines was to force the airlines to correct identified security problems. What if the FAA had not reduced the fines to 10 cents on the dollar? Suppose those in Congress tasked with aviation oversight had disallowed any fine reductions for security lapses and instead called for full imposition? If the airlines had hardened security in response to heavy fines for violations, would that have stopped the terrorists on 9/11? We will never know. But in your oversight capacity, please remember the lessons of 9/11, and hold all government entities accountable for protecting the American people.

You are urged to approve full implementation of the 9/11 Commission recommendations. They were designed to make America safer. It is only a matter of time before terrorists breach our security network again. Our level of protection will depend on the safeguards and defense mechanisms that you, the members of Congress, mandate, along with your oversight to ensure compliance.

References

[1] "Intelligence Ignorance," Editorial. *The Washington Post*. December 17, 2006. B06 http://www.washingtonpost.com/wp-dyn/content/article/2006/12/16/AR2006121600662.html

[2] Alexander, Keith L. "2 Congressmen Seek Security Plans." *The Washington Post*. May 22, 2006; A07 http://www.washingtonpost.com/wp-dyn/content/article/2006/05/21/AR2006052100934_pf.html

[3] Mandel, Jenny. "GAO offers oversight advice to new Congress." *GovExec.com*. November 20, 2006. http://www.govexec.com/story_page.cfm?articleid=35532&dcn=e_gvet

[4] "Under-the-Rug Oversight," Editorial. *The New York Times*. December 29, 2006. http://www.nytimes.com/2006/12/29/opinion/29fri3.html?_r=1&th&emc=th&oref=slogin

[5] Nakashima, Ellen and Del Quentin Wilber. "Report Says TSA Violated Privacy Law." *The Washington Post*. December 22, 2006; A07 http://www.washingtonpost.com/wp-dyn/content/article/2006/12/21/AR2006122101621_pf.html

[6] Noyes, Andrew. "Democratic victory may kill surveillance bills." *National Journal's Technology Daily*. *GovExec.com*. November 8, 2006. http://www.govexec.com/dailyfed/1106/110806tdpm1.htm

[7] "Garfinkel, Simson L. "Phone Calls Are Just the Start." *The Washington Post*. May 14, 2006; B02. http://www.washingtonpost.com/wp-dyn/content/article/2006/05/13/AR2006051300043_pf.html

[8] "Detection." *Edgewood Chemical Biological Center*, A U.S. Army RDECOM Laboratory. http://www.ecbc.army.mil/ps/products_detection.htm

[9] Funk, Amy B., J. Schier1, M. Belson, M. Patel, C. Rubin, W. Watson, T. Litovitz, E. Kilbourne. "Using the Toxic Exposure Surveillance System To Detect Potential Chemical Terrorism Events." Abstract. *Morbidity and Mortality Weekly Report* (MMWR) September 24, 2004 / 53(Suppl); 239. http://www.cdc.gov/mmwr/preview/mmwrhtml/su5301a51.htm

[10] Gupta, Sonika. “Weapons of Mass Destruction and Terrorism.” *Institute of Peace and Conflict Studies*, WMD Seminar. Article no. 637. November 17, 2001. http://www.ipcs.org/Nuclear_seminars2.jsp?action=showView&kValue=126

[11]*Public Law 107–188*—June 12, 2002 Public Health Security and Bioterrorism Preparedness and Response Act of 2002. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ188.107.pdf

[12] *Office of Management and Budget*. “Protecting America.” http://www.whitehouse.gov/omb/budget/fy2006/protecting.html

[13] Kaplan, Eben. “Targets for Terrorists: Chemical Facilities” *Council on Foreign Relations*. December 11, 2006. http://www.cfr.org/publication/12207/targets_for_terrorists.html

[14] Id.

[15] “Proposed Rules for Securing Chemical Plants Released.” *The Washington Post*. Associated Press Article. December 23, 2006; A22. http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122201306.html?referrer=email

[16] Lipton, Eric. “Security Effort by Coast Guard Is Falling Short.” *The New York Times*. December 30, 2006. http://www.nytimes.com/2006/12/30/us/30domain.html?_r=1&th&emc=th&oref=slogin

[17] Savage, Charlie. “US arms Coast Guard terror units.” *The Boston Globe*. March 27, 2005. http://www.boston.com/news/nation/articles/2005/03/27/us_arms_coast_guard_terror_units/

[18] Lipton, Eric. “Security Effort by Coast Guard Is Falling Short.” *The New York Times*. December 30, 2006. http://www.nytimes.com/2006/12/30/us/30domain.html?_r=1&th&emc=th&oref=slogin

[19] Candiotti, Susan reporting. Segment on the Coast Guard. “*Lou Dobbs Tonight*.” CNN Transcript. December 26, 2006. http://transcripts.cnn.com/TRANSCRIPTS/0612/26/ldt.01.html

[20] Lipton, Eric. “Security Effort by Coast Guard Is Falling Short.” *The New York Times*. December 30, 2006. http://www.nytimes.com/2006/12/30/us/30domain.html?_r=1&th&emc=th&oref=slogin

[21] Robinson, William H.; Jennifer E. Lake; and Lisa M. Seghetti, Domestic Policy Division. *CRS Report for Congress Order Code RL32841*. “Border and Transportation Security: Possible New Directions and Policy Options.” March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32841.pdf

[22] Witte, Giff. “TSA Nears Decision on Contract for Government ID Cards” *The Washington Post*. January 2, 2007; D02. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/01/AR2007010100764.html?referrer=email

[23] Marino, Jonathan. “Union blasts final TSA rule on port ID cards.” *GovExec.com*. January 4, 2007. http://www.govexec.com:80/story_page.cfm?articleid=35798&dcn=e_gvet

[24] Lake, Jennifer E., William H. Robinson, and Lisa M. Seghetti, Domestic Policy Division. *CRS Report for Congress, Order Code RL32839*. “Border and Transportation Security: The Complexity of the Challenge” March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32839.pdf

[25] “DHS sets rules for port ID cards.” from *National Journal's Technology Daily. GovExec.com*. January 3, 2007. http://www.govexec.com/dailyfed/0107/010307tdpm2.htm

[26] Robinson, William H.; Jennifer E. Lake; and Lisa M. Seghetti, Domestic Policy Division. *CRS Report for Congress, Order Code RL32841*. “Border and Transportation Security: Possible New Directions and Policy Options.” March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32841.pdf

[27] Marino, Jonathan. “Union blasts final TSA rule on port ID cards.” *GovExec.com*. January 4, 2007. http://www.govexec.com:80/story_page.cfm?articleid=35798&dcn=e_gvet

[28] Robinson, William H.; Jennifer E. Lake; and Lisa M. Seghetti, Domestic Policy Division. *CRS Report for Congress, Order Code RL32841*. “Border and Transportation Security: Possible New Directions and Policy Options.” March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32841.pdf

[29] Seghetti, Lisa M., Jennifer E. Lake, and William H. Robinson, Domestic Policy Division. *CRS Report for Congress, Order Code RL32840*. “Border and Transportation Security: Selected Programs and Policies.” March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32840.pdf

[30] Lipton, Eric. “U.S. to Expand Cargo Scans to Detect Nuclear Material.” *The New York Times*. December 8, 2006. http://www.nytimes.com/2006/12/08/us/08cargo.html?ex=1323234000&en=c04339abf719a149&ei=5089&partner=rssyahoo&emc=rss and

Strohm, Chris. “Six foreign ports to scan cargo for nuclear devices.” *National Journal's Technology Daily . GovExec.com.* December 7, 2006. http://www.govexec.com/dailyfed/1206/120706tdpm1.htm

[30a] Strohm, Chris. “Six foreign ports to scan cargo for nuclear devices.” *National Journal's Technology Daily . GovExec.com.* December 7, 2006. http://www.govexec.com/dailyfed/1206/120706tdpm1.htm

[31] Robinson, William H.; Jennifer E. Lake; and Lisa M. Seghetti, Domestic Policy Division. *CRS Report for Congress, Order Code RL32841*. "Border and Transportation Security: Possible New Directions and Policy Options." March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32841.pdf

[32] Hudson, Audrey. "Marshals decry imams' charges" THE WASHINGTON TIMES. November 29, 2006. http://insider.washingtontimes.com/articles/normal.php?StoryID=20061129-121812-1240r

[33] Verton, Dan. "Bush orders integration of U.S. terrorist watch lists." *Computerworld.com*. September 22, 2003. http://www.computerworld.com/databasetopics/data/story/0,10801,85233,00.html

[34] Robinson, William H.; Jennifer E. Lake; and Lisa M. Seghetti, Domestic Policy Division. *CRS Report for Congress, Order Code RL32841*. "Border and Transportation Security: Possible New Directions and Policy Options." March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32841.pdf

[35] Strohm, Chris. "Border intelligence plan still in 'early stages,' official says." *CongressDaily. GovExec.com*. June 28, 2006. http://www.govexec.com/story_page.cfm?articleid=34441&ref=rellink

[36] Donnelly, Sally B. "A New Tack for Airport Screening: Behave Yourself." *TIME.com*. May. 17, 2006. http://www.time.com/time/nation/article/0,8599,1195330,00.html

[37]Yu, Roger. "Travel to Canada, Mexico is about to change with new passport rules." *USA TODAY*. January 2, 2007. http://usatoday.com/travel/news/2007-01-01-passport_x.htm?POE=click-refer

[38] Dinan, Stephen. "Bush seeks to ease visa requirement." *THE WASHINGTON TIMES*. November 29, 2006 http://insider.washingtontimes.com/articles/normal.php?StoryID=20061129-121704-2202r

[39] Id.

[40] Seghetti, Lisa M., Jennifer E. Lake, and William H. Robinson, Domestic Policy Division. *CRS Report for Congress, Order Code RL32840*. "Border and Transportation Security: Selected Programs and Policies." March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32840.pdf

[40a] Hsu, Spencer S., "U.S. Preparing to Drop Tracking of Foreigners' Departures by Land." *The Washington Post*. December 15, 2006; A05 http://www.washingtonpost.com/wp-dyn/content/article/2006/12/15/AR2006121500092.html

[40b]*GAO-07-248 report*, BORDER SECURITY: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry. December 2006.http://www.gao.gov/htext/d07248.html

[40c] Id.

[40d] Hsu, Spencer S., "U.S. Preparing to Drop Tracking of Foreigners' Departures by Land." *The Washington Post*. December 15, 2006; A05 http://www.washingtonpost.com/wp-dyn/content/article/2006/12/15/AR2006121500092.html

[41] Robinson, William H.; Jennifer E. Lake; and Lisa M. Seghetti, Domestic Policy Division. *CRS Report for Congress, Order Code RL32841*. "Border and Transportation Security: Possible New Directions and Policy Options." March 29, 2005. http://www.fas.org/sgp/crs/homesec/RL32841.pdf

[42] Id.

[43] Id.

[44] Id.

[45] Townsend, Mark, Antony Barnett and Tom Parfitt. "Spy death linked to nuclear thefts" *The Observer*. November 26, 2006. http://observer.guardian.co.uk/uk_news/story/0,,1957279,00.html

[46] "Hunting Loose Nukes in Eastern Europe." "*Nightline." ABC News*. Oct. 13, 2005. http://abcnews.go.com/Nightline/LooseNukes/story?id=1208241

[47] Id.

[48] Id.

[49] Meserve, Jeanne, reporting on Nuclear Smuggling. "*Lou Dobbs Tonight." CNN Transcript*. December 26, 2006. http://transcripts.cnn.com/TRANSCRIPTS/0612/26/ldt.01.html

[50] Wald, Matthew L. "Administrator Is Dismissed From Nuclear Security Post." *The New York Times*. January 5, 2007. http://www.nytimes.com/2007/01/05/washington/05nuke.html?th&emc=th

[51] Mufson, Steven. "After Breaches, Head of U.S. Nuclear Program Is Ousted." *The Washington Post*. January 5, 2007; A07. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/04/AR2007010401813.html?referrer=email

[52] Wald, Matthew L. "Administrator Is Dismissed From Nuclear Security Post." *The New York Times*. January 5, 2007. http://www.nytimes.com/2007/01/05/washington/05nuke.html?th&emc=th

[53] "Loose Nukes." *ABC News*. 2005. http://abcnews.go.com/Technology/LooseNukes

[54] Reese, Shawn. *CRS Report for Congress, Order Code RL 33050*. "Risk-Based Funding in Homeland Security Grant Legislation: Analysis of Issues for the 109th Congress." August 29, 2005, p. 6. http://www.fas.org/sgp/crs/homesec/RL33050.pdf

[55] Strohm, Chris. “Chertoff gets ahead of Hill, sets interoperable radio goals.” *CongressDaily. GovExec.com*. November 28, 2006. http://www.govexec.com/dailyfed/1106/112806cdpm1.htm

[56] Strohm, Chris. “Key Democrats back communications grant program.” *National Journal's Technology Daily* . *GovExec.com*. January 3, 2007. http://www.govexec.com:80/story_page.cfm?articleid=35794&dcn=e_gvet

[57] Barrett, Devlin. “6 of 75 cities get top disaster rating.” Associated Press. Jan 2, 2007 http://news.yahoo.com/s/ap/20070102/ap_on_go_ca_st_pe/emergency_communications

[58] Phillips, Zack. “Emergency preparedness exercises remain an imperfect science.” *GovExec.com*. Nov. 22, 2006. http://www.govexec.com/dailyfed/1106/112206z1.htm

[59] Rashbaum, William K. and William Neuman. “PATH Tunnels Seen as Fragile in Bomb Attack.” *The New York Times*. December 22, 2006. http://www.nytimes.com/2006/12/22/nyregion/22security.html?_r=1&th&emc=th&oref=slogin

[60] Sheridan, Mary Beth and Spencer S. Hsu. “Localities Operate Intelligence Centers To Pool Terror Data.” *The Washington Post*. December 31, 2006; A03 http://www.washingtonpost.com/wp-dyn/content/article/2006/12/30/AR2006123000238.html?referrer=email

[61] Phucas, Keith. “Sept. 11 riddles remain.” *Times Herald*. August 29, 2005. http://www.timesherald.com/site/news.cfm?newsid=15114089&BRD=1672&PAG=461&dept_id=33380&rfi=6

[62] Kobach, Kris W. “Terrorist Loophole: Senate Bill Disarms Law Enforcement.” *The Heritage Foundation*. May 24, 2006. http://www.heritage.org/research/immigration/wm1092.cfm

[63] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. W.W. Norton & Company, New York. 2004; p. 376.