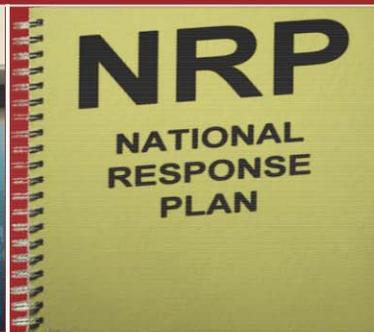

THE STATE OF HOMELAND SECURITY 2006



2003



2004



2005



2006

*An Annual Report Card on the
Department of Homeland Security*

*Prepared by the Democratic Staff of the Committee on Homeland Security
Rep. Bennie G. Thompson (MS), Ranking Member*

TABLE OF CONTENTS

Table of Contents	Page i.
Executive Summary	Page ii.
Report Card	Page vi.
 <u>Subject Areas:</u>	
Port Security	Page 4
Aviation Security	Page 10
Surface Transportation Security	Page 16
Border Security	Page 21
Emergency Preparedness and Response	Page 28
Emergency/Interoperable Communications	Page 32
Information Sharing	Page 37
Biosecurity	Page 42
Chemical Plant Security	Page 45
Critical Infrastructure Protection	Page 48
Cyber Security	Page 50
Science & Technology	Page 55
Privacy Protection	Page 58
Watch Lists Redress	Page 63
Organization, Execution and Staffing	
of Procurement Operations	Page 67
Employee Morale	Page 71

EXECUTIVE SUMMARY

Three years ago this month, the Department of Homeland Security opened its doors and promised to protect Americans from terrorism and provide leadership at all levels of government – federal, state, and local – to protect and secure the homeland. More than 180,000 employees from 22 agencies and offices were brought together under one roof.

As Members of the Congressional Committee that has overseen the Department from its earliest days, we are charged with monitoring the Department's progress since its creation. What we have seen does not inspire much confidence. In the past three years, the Department's evolution has been a troubled one. While thankfully the Department has not yet been tested by another terrorist attack, its performance fell well below expectations in the face of Mother Nature and Hurricane Katrina last year. Its failure to prepare and respond to this disaster created serious questions about how much more secure our nation is five years after 9/11. Emergency response failures, a porous border, contract mismanagement, and, most recently, the agency's role in approving a foreign government's purchase of U.S. port terminals have left many Americans questioning our government's homeland security efforts. In our oversight capacity, we have more questions than answers on the Department's progress.

In order to fully understand the agency's progress, Committee Democrats are instituting this annual report card for the Department of Homeland Security. In each of the significant 16 homeland security issue areas for which the Department has responsibility, we are grading the agency's performance, and identifying what the agency must do to improve and raise its grade.

This, the first annual report card, reveals the Department of Homeland Security to be a poor student, simply getting by with average and below average grades, focused more on announcing accomplishments than on protecting America's homeland. Unfortunately, being below average or getting "gentlemen's Cs" is not acceptable in the War on Terror here at home. The agency charged with our protection must be a stellar performer, not a C-student.

The Department's performance in each of the 16 areas can be summarized as follows:

- **Port Security:** The Department's grade in this area is a **C-/D+**. In addition to the recent uproar over the Dubai port terminal sales, there are many gaps remaining in our port security. As some experts have noted, the current port security regime is a "house of cards," in which containers are often not inspected and the government does not truly know which containers are "high risk." Likewise, the federal government remains unaware of security arrangements at foreign ports and vessels shipping goods to the United States.

- **Aviation Security:** The Department's grade in this area is a **C+**. Congress, the Government Accountability Office, the Department's Office of Inspector General, and the 9/11 Commission have each identified vulnerabilities in aviation security that remain unaddressed. The three most significant identified in this study are sabotage by "sleepers" among airport workers, a terrorist being allowed to board a U.S.-bound plane before being checked against the terrorist watchlist, and an attack emanating in the air cargo hold.
- **Surface Transportation Security:** The Department's grade in this area is a **C-**. The Department's proposed FY 2007 budget currently allocates less than 1% of the Transportation Security Administration (TSA) funds to surface transportation security, despite the recent subway bombings in London last year, and train attacks in Madrid the year before. At the same time, TSA has failed to mandate security plans, risk assessments, and training for surface transportation.
- **Border Security:** The Department's grade in this area is a **C-**. The Department urgently needs a comprehensive border security strategy for identifying and securing the nation's most porous and vulnerable land borders and ports of entry. At the same time, the Department urgently needs to develop a comprehensive vision for border screening that harmonizes and integrates the many initiatives underway.
- **Emergency Preparedness and Response:** The Department's grade in this area is a **D**. Hurricane Katrina exposed significant flaws in our ability to prepare for and respond to catastrophic events. Emergency plans at all levels of government, including the National Response Plan (NRP), failed the nation. Current plans underway by Secretary Michael Chertoff to separate response and preparedness functions cause us concern and raises questions about whether our nation will be prepared for the next hurricane season, which is less than 100 days away.
- **Interoperable Communications:** The Department's grade in this area is a **B-**. Emergency responders at all levels of government cite the ability to communicate as being one of the most basic functions of any response and recovery effort. Interoperable communications would be best achieved if the Department elevated the visibility of the issue by providing necessary resources to achieve full interoperability. To date, the Department does not have a dedicated interoperability grant program.
- **Information Sharing:** The Department's grade in this area is a **C-**. We found that the Department has not effectively bridged the information sharing gap between intelligence and law enforcement communities. In order to detect terrorist attacks before they occur, law enforcement must be capable

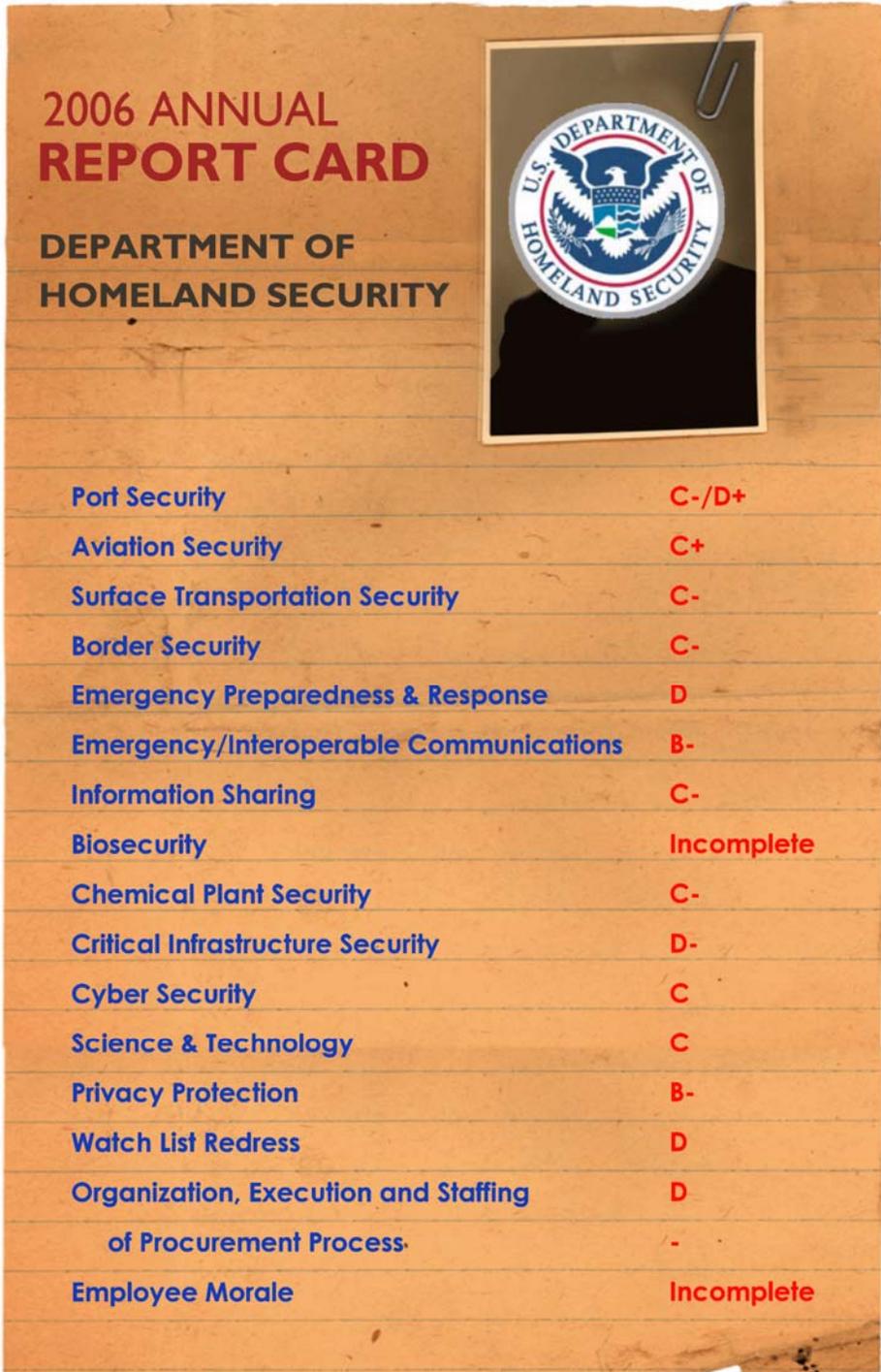
of sharing information and getting it into the hands of those who need it most.

- **Biosecurity:** The Department's grade in this area is an **incomplete**. A bioterrorist attack on the United States could have devastating consequences. Furthermore, bioterrorism and naturally occurring biological events, such as a SARS or avian influenza pandemic, could possibly be indistinguishable. As such, our biodefense should be constructed using an "all hazards" approach. Unfortunately, as the current scramble to prepare for a possible avian influenza pandemic demonstrates, the federal government is not prepared for a biological emergency—whether natural or manmade.
- **Chemical Plant Security:** The Department's grade in this area is a **C-**. Currently, the Department of Homeland Security does not have legal authority to enter a chemical facility and ensure that security programs are in place. The Department must have regulatory authority to ensure that chemical plants are putting the necessary security practices in place.
- **Critical Infrastructure Protection:** The Department's grade in this area is a **D-**. For almost a decade the federal government has been tasked with working with the private sector to secure the mostly-privately owned critical infrastructure. Yet, there have been many plans and strategies and little progress. Since assuming this responsibility, the Department has failed to catalogue the nation's most vulnerable assets and infrastructure.
- **Cybersecurity:** The Department's grade in this area is a **C**. The agency has made limited progress towards securing our nation's cyber infrastructure. For the past sixteen months, the National Cyber Security Division has been led by an acting director, and the Assistant Secretary for Cyber Security and Telecommunications remains vacant. Failure to find permanent replacements for both positions raises serious concern about the Department's ability to lead the nation in securing cyberspace.
- **Science & Technology:** The Department's grade in this area is a **C**. The Science & Technology Directorate lacks an overall strategy for research, development, testing and evaluation. The Directorate's work must be mission-driven, not process-driven as it is presently. More strategic planning will resolve many of the Directorate's problems fulfilling long-term projects. HSARPA must be allowed the flexibility to be more innovative in its approach to research and development.
- **Privacy Protection:** The Department's grade in this area is a **B-**. The agency's Privacy Officer must be provided with all the authority necessary to carry out the responsibilities laid out by the Congress in the Homeland Security Act. The Secretary must appoint a permanent Privacy Officer without delay and assure that the Officer has the independence and the

ability to obtain documents and other information relevant to safeguard privacy.

- **Watchlists and Need for Redress:** The Department's grade in this area is a **D**. Currently, the agency lacks a "one stop" redress process for innocent Americans misidentified as terrorists. In order to allow these individuals to clear their names, the Department must implement better policies and procedures to ensure watch lists are comprehensive and accurate.
- **Procurement:** The Department's grade in this area is a **D**. **Every tax dollar that is wasted on a mismanaged Department contract is one dollar less for homeland security.** For an agency that purchases an average of \$10 billion per fiscal year in goods and services from private contractors, a "D" is far from acceptable.
- **Employee Morale:** The Department's grade in this area is an **incomplete**. The Department must engage with employees' representatives to resolve ongoing problems that have hampered implementation of its new personnel system. The Department's ability to attract and retain a talented and professional workforce will be seriously impeded if it continues to be dogged by circumstances that lead to low employee morale.

While we offer this progress report to the Department's leadership, we offer our gratitude and thanks to the employees of the Department of Homeland Security. These brave men and women go to work every day to make your and our lives a little safer.



THIS PAGE INTENTIONALLY LEFT BLANK

I. STATEMENT OF PROBLEM HISTORICALLY:

America's ports are the gateway to the global economy. Our country's economic prosperity rests on the ability of tens of thousands of containers arriving unimpeded at U.S. ports to support the "just-in-time" delivery system that stock the shelves of Wal-Mart, Target, and Home Depot, to name a few. For example, over 12,000 containers arrive at the Port of Los Angeles/Long Beach every day. Not only do our ports support our retail economy, but they also serve as the entry point for America's oil and gas supply. In addition, America's ports and waterways carry over thirty-four million citizens a year on cruise ships and ferries.¹ According to the American Association of Port Authorities, ports generate five million jobs and move more than \$2 trillion in freight every year.²

Globalization forced ports to change their operations, shifting from a system that stored goods in warehouses to the storing of goods in containers. The focus on speedy movement of cargo caused port operators to put a premium on efficiency. As a result, our port system cannot afford disruptions or slow downs. A 2002 simulation of a lockout at West Coast ports cost the American economy an estimated \$5 billion per day.³ While the overall costs of the recent hurricanes cannot yet be calculated, the economic impact of Hurricanes Katrina and Rita was felt at the gas pump when oil tankers could not enter the ports of New Orleans and Houston. The need for efficiency at our ports and the economic consequences of disruptions of port operations make them attractive terrorist targets.

When ports made improvements to facilitate the movement of vessels and cargo they failed to take security into account, becoming even more vulnerable to terrorist attacks. As port security expert Stephen Flynn states, America's port system was "built without credible safeguards to prevent it from being exploited or targeted by terrorists or criminals."⁴ The economic consequences of a disruption combined with the loss of life caused by an attack serves the purposes of groups like Al-Qaeda who want to kill

¹ American Association of Port Authorities (AAPA), *Press Release: Port Leaders Respond to President's FY '07 Budget Request* (Feb. 7, 2006), at <http://www.aapa-ports.org/pressroom/feb0706.htm>; see also WASHINGTON STATE DEPARTMENT OF TRANSPORTATION, *Washington Ferries: History* (2006), at http://www.wsdot.wa.gov/ferries/your_wsf/index.cfm?fuseaction=our_history.

² AAPA, *supra* note 1.

³ Mark Gerencser, Jim Weinberg, and Don Vincent, *Port Security War Game: Implications for U.S. Supply Chains* 5, Booz-Allen-Hamilton (February 2003), at <http://extfile.bah.com/livelink/livelink/128648/?func=doc.Fetch&nodeid=128648>.

⁴ *The Fragile State of Container Security, Hearing on Cargo Containers: The Next Terrorist Target?* Before the Senate Governmental Affairs Committee, 109th Cong. (Mar. 20, 2003) (statement of Commander Stephen Flynn, USCG (ret), and Jeane J. Kirkpatrick, Senior Fellow in National Security Studies and Director, Council on Foreign Relations Independent Task Force on Homeland Security Imperatives), at <http://hsgac.senate.gov/index.cfm?fuseaction=Hearings.Testimony&HearingID=85&WitnessID=310>.

Americans and hurt the U.S. economy. Port security exercises have found that a terrorist attack at a major U.S. seaport would cause \$60 billion in economic damages.⁵

Terrorist groups have already targeted ports and vessels to carry out attacks. Some examples of terrorists using ports to carry out attacks include:

- The hijacking of the cruise ship Achille Lauro in 1986.
- The attack on the USS Cole in 2000.
- The attack of the French oil tanker Limburg in 2001.

In 2004, terrorists smuggled in a container killed 10 people at the Port of Ashod, Israel. In addition to these conventional attacks, security experts are concerned that our ports could serve as a point of entry for a nuclear weapon. While the likelihood that terrorists would smuggle a nuclear weapon in a shipping container is low, it is not an impossibility. In fact, the A.Q. Khan nuclear smuggling ring moved components of nuclear weapons through Middle Eastern ports. A terrorist attack involving a nuclear weapon detonated at a port could result in a substantial loss of life and an economic damage of \$1 trillion.⁶

Congress has taken steps since September 11th to improve port security. This includes passage of the Maritime Transportation Security Act of 2002. This new law required the development of facility and vessel security plans, the issuance of employee identification cards, the creation of Coast Guard security teams and a grant program to assist ports with security costs.

II. THE STATE OF PORT SECURITY:

On January 6, 2006, the Committee on Foreign Investment in the United States approved the sale of Peninsula and Oriental Navigation to Dubai Ports World, a company that is owned by the government of Dubai, United Arab Emirates. This sale would result in a government which has past ties to terrorism, including the 9-11 attacks would operate terminals at six major seaports. The announcement of this sale caused public uproar, and the Administration, including the Department of Homeland of Homeland Security, has stated that all security concerns were addressed. Since the news of the approval became public, the Department of Homeland Security has stated that it is requiring Dubai Ports World to subject itself to additional port security requirements. In addition, Dubai Ports World has agreed to undergo an additional 45-day security investigation to evaluate all national security concerns associated with sale. The Chairman and Ranking Member of the Committee on Homeland Security, along with almost eighty other Members, has introduced legislation ensuring this review occurs and allowing Congress, if need be, to intervene should national security threats be found and the President not suspend or prohibit the deal.

⁵ Gerencser, *supra* note 3.

⁶ MICHAEL O' HANLON ET AL., PROTECTING THE AMERICAN HOMELAND (Brookings Institute Press 2003), at <http://www.brookings.edu/press/books/protectingtheamericanhomelandoneyearon.htm>.

Beyond the Dubai World issue, our ports have received greater attention from the federal government since September 11th. The White House issued a National Strategy for Maritime Security in September 2005. The Department of Homeland Security has issued security regulations and developed cargo security programs. Congress has approved over \$750 million in grants to seaports to pay for security improvements.⁷

In October 2003, the Coast Guard, which is responsible for port security, issued security regulations for America's 361 ports requiring ports to hire security officers and to install barriers and surveillance systems.⁸ As of July 1, 2004, all of the nation's port facilities had complied with these regulations. The Coast Guard screens all incoming vessels to determine if the vessels' crew or cargo poses a terrorist risk and has established maritime security teams, equivalent to police SWAT teams, to board high-risk vessels. The Coast Guard also developed Maritime Security Conditions that require port facilities to increase the screening of cargo and people entering the ports, and has also increased security patrols in our harbors. The Coast Guard has also undertaken an effort to replace its aging fleet of ships and aircraft that are currently patrolling our shores.

In response to the need to secure the supply chain while ensuring the flow of goods, the Department of Homeland Security is working with the private sector to initiate a series of programs designed to target high-risk vessels, better screen containers, and provide incentives to shippers to voluntarily enhance the security of the supply chain. U.S. Customs and Border Protection (CBP), which is charged with cargo security has established a screening system (Automatic Targeting System or ATS) that assesses the risk of incoming cargo by determining if information listed on the manifest contains anomalies that would give away that illegal goods are being smuggled inside a container. CBP has also created the Container Security Initiative (CSI), in which Customs inspectors are deployed to forty-two foreign seaports to inspect high-risk containers before they are shipped to the United States.

Another security program, the Customs Trade Partnership Against Terrorism (CTPAT), is designed to improve supply chain security by requiring companies to adhere to specific security requirements from the time a container is packed until it reaches its final destination. In return, the companies' cargo receives preferential treatment from CBP and is less likely to be inspected when it arrives in the U.S. CBP, in conjunction with the Department of Homeland Security's Domestic Nuclear Detection Office (DNDO), is deploying radiation portal monitors at seaports, which can screen containers for a nuclear or radiological weapons.

⁷ U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY, *Fiscal Year 2005 Port Security Grant Program Awards For Your State and District* (Sept. 2005).

⁸ Implementation of National Maritime Security Initiatives, 68 Fed. Reg. 60,448 (Oct. 22, 2003) (codified at 33 C.F.R. pts. 2, 101, and 102).

III. PRESIDENT'S BUDGET

The President's Budget continues to limit the Department of Homeland Security's progress on port security. The budget eliminates the port security grant program, the only source of funds committed to help ports pay for post-9/11 security requirements. Instead of dedicated port funds, the White House has proposed \$600 million in Targeted Infrastructure Protection Program (TIPP) grants, forcing ports to compete with rail, mass transit, and other critical infrastructure for funding. The budget also fails to increase funding from the previous year for CBP cargo security programs, such as C-TPAT, which received only \$75 million. CBP has performed security checks on only thirteen percent of the 10,000 C-TPAT businesses. The Administration's budget will delay the completion of these security checks for years. The President's budget also falls short in the area of container inspection technology. The President requested only \$157 million for radiation portal monitors, which means U.S. seaports won't have the ability to screen containers for nuclear weapons. Finally, the President's budget requested \$934 million for the Coast Guard's Deepwater program, delaying by twenty-five years the overhaul of the Coast Guard's cutters and aircraft, which are used to patrol and protect our ports and coastline.

IV. AREAS FOR IMPROVEMENT:

According to the Department of Homeland Security, Dubai Ports World will continue to participate in CSI, will join C-TPAT, and will likely have the security of its foreign port terminals assessed. As noted earlier, once this occurs Congress will evaluate the steps taken by the Department of Homeland Security and make a judgment on the deal. This deal has raised broader port security issues that will need to be addressed.

While a great deal of attention has been placed on the efforts of Dubai Ports World this past week, gaps in port security remain regardless of which nations operate at U.S. ports. These gaps have led experts, like Flynn, to describe the Department's port security regime as a "house of cards," in which high-risk containers are un-inspected and the government remains unaware of security arrangements at foreign ports and vessels shipping goods to the U.S.⁹

Customs and Border Protection does not really know which containers are "high-risk" because the Automatic Targeting System is flawed. According to the Department of Homeland Security's Inspector General and the Government Accountability Office (GAO), the system relies on manifest data, the least reliable piece of information to determine the risk of a container, according to security experts.¹⁰ The Department must take steps to

⁹ Stephen Flynn, *Port Security Is Still a House of Cards*, FAR EASTERN ECONOMIC REVIEW (Jan./Feb. 2006), at <http://www.feer.com/articles1/2006/0601/free/p005.html>.

¹⁰ *Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers: Hearing Before the Subcomm. on Oversight and Investigations of the House Comm. on Energy and Commerce*, 109th Cong. 11 (Dec. 16, 2003) (statement by Richard Stanna, Director, Homeland Security and Justice, General Accounting Office); see also DEPARTMENT OF HOMELAND SECURITY, OFFICE OF THE INSPECTOR GENERAL, *Audit of Targeting*

require industry to submit additional trade data to CBP that will give CBP Inspectors a better sense whether a container poses a threat.

The Department must also ensure that CBP receives more resources to inspect containers. Current staffing shortages at foreign seaports participating in CSI are resulting in thirty-five percent of “high risk” containers not being inspected before they are shipped to the U.S. In addition to ensuring adequate staffing overseas, CBP must have more inspectors at U.S. ports inspecting containers. Since terrorists may be able to evade the Automatic Targeting System, CBP must have more manpower at our ports to conduct random checks on low-risk containers, and be able to conduct more inspections on companies that are not in C-TPAT. The Department must also provide more support to CBP for the C-TPAT program. Currently, Customs and Border Protection has only eighty people to perform security checks on 10,000 C-TPAT companies. Without greater resources, CBP will never be able to hire the personnel or have the funding required for these individuals to travel to overseas locations to enforce compliance with the program.

The Department must also increase funding and set hard deadlines for the deployment of radiation screening devices at seaports. Seventy-five percent of our ports do not have the ability to screen a container for dirty bombs or nuclear weapons.¹¹ This technology must be deployed now. The Department must use innovative approaches like the screening equipment that is deployed in Hong Kong which x-rays the contents of a container and screens it for radiation.¹² Such equipment will ensure that containers receive adequate screening while they transit to the supply chain.

The Coast Guard must accelerate the compliance checks at foreign ports to ensure that our allies are implementing security measures. Currently, the Coast Guard has twenty people assessing security at 135 foreign ports.¹³ This is the area where DHS had the greatest failure in its evaluation of Dubai Ports World security efforts. The Department should triple the number of Coast Guard personnel that conduct the foreign port assessment to ensure that the foreign ports have adequate security measures in place. In addition, the White House must take steps to accelerate the Coast Guard’s Deepwater program. America’s port security is dependent on a Coast Guard that has the tools to detect and intercept threats to our ports, and the nation cannot afford to wait twenty-five years for this to happen.

Lastly, the Department must also support our port operators by having a fully funded grant program that can assist ports with the increasing security they have undertaken since 9/11. Since 9/11 some ports are diverting up to fifteen percent of their budgets for security, which is hurting our economy because ports cannot make investments

Oceangoing Cargo Containers 2 (OIG-05-26) (July 2005), at http://www.dhs.gov/interweb/assetlibrary/OIG_05-26_Jun05.pdf.

¹¹ DEPARTMENT OF HOMELAND SECURITY, *U.S. Customs and Border Protection FY 2007 Budget Briefing* (Feb. 2006).

¹² Honorable James M. Loy and Stephen Flynn, *OP-ED: A Port in the Storm Over Dubai*, N.Y. TIMES, Feb. 28, 2006, at http://www.nytimes.com/2006/02/28/opinion/28flynn.html?_r=1&oref=slogin.

¹³ *Id.*

that enhance their ability to move goods which in turn make the movement of goods more expensive for consumers.¹⁴ If defending the country against terrorist threats is the primary responsibility of the federal government, then the Department of Homeland Security cannot leave our ports alone with the check.

Thus, much more must be done if America's ports and supply chain are going to be as secure as they can be against the threat of international terrorism.

¹⁴ American Association of Port Authorities, *Press Release: Port Leaders Respond to President's FY '07 Budget Request* (Feb. 7, 2006), at <http://www.aapa-ports.org/pressroom/feb0706.htm> (remarks by Kurt Nagle, President American Association of Port Authorities and Bernard Groseclose, President and CEO South Carolina Ports Authority).

I. STATEMENT OF PROBLEM HISTORICALLY:

The conditions that led to the largest terrorist attack on our nation directly relate to known weaknesses in the security of commercial aviation. As retold in the 9/11 Commission Report, “The 19 men were aboard four transcontinental flights. They were planning to hijack these planes and turn them into large guided missiles, loaded with up to 11,400 gallons of jet fuel. By 8:00 A.M. on the morning of Tuesday, September 11, 2001, they had defeated all the security layers that America’s civil aviation security system then had in place to prevent a hijacking.”¹

One of the most significant steps Congress and the Administration took to signal to the American people that it was safe to fly again, was the federalization of airport security. Created just two months after the 9/11 terrorist attacks, the Transportation Security Administration (TSA) had the enormous task of recruiting, screening, and hiring up to 60,000 new federal screeners and procuring and installing new systems, predominately to screen checked baggage for explosives, at our nation’s 429 airports. In the absence of staff and infrastructure to plan and manage contracts, and under public pressure to get the agency up and running, TSA relied heavily and almost blindly on NCS Pearson, a contractor, to recruit federal screeners. As a result, a contract that was supposed to be capped at \$104 million ballooned to \$741 million in a very short period. Asked by TSA to audit this contract, the Defense Contract Audit Agency identified almost \$300 million in “deficient” or unsubstantiated billing.²

As with the recruitment of federal screeners, TSA had very little time to acquire and install new equipment into our nation’s airports to meet Federal mandates.³ Between November 2001 and September 2004, about 93 percent of TSA’s budget was dedicated to meeting the equipment challenge.⁴ Specifically, TSA worked with a contractor to procure and place about 1,200 explosive detection systems (EDS) machines and about 6,000 explosive trace detection (ETD) machines at over 400 airports, and modify airports for the installation of this equipment. The Government Accountability Office (GAO) found that the rush to install new equipment resulted in TSA placing “stand-alone ETD and the minivan-sized EDS machines—usually in airport lobbies— that were not integrated in-line with airport baggage conveyor systems. Some of these interim lobby solutions resulted in

1 *The Final Report of the National Commission on Terrorist Attacks Upon the United States* (The 9/11 Commission Report), at 4.

2 Kimberly Palmer, *Management Flaws Cited For Cost Hikes on Screening Hiring Contract*, GOVERNMENT EXECUTIVE (January 10, 2006).

3 The congressional mandate to screen all checked baggage using explosive detection systems by December 31, 2002 was later extended to December 31, 2003.

4 *Statement before the Senate Committee on Commerce, Science, and Transportation, TRANSPORTATION SECURITY: Systematic Planning Needed to Optimize Resources* (GAO-05-357T) 8 (February 15, 2005) (Cathleen A. Berrick, Government Accountability Office) (Berrick statement).

operational inefficiencies, including requiring a greater number of screeners, as compared with using EDS machines in-line baggage conveyer systems.”⁵

The Transportation Security Administration often refers to its approach to aviation security a “system of systems” or a “layered approach.” TSA has identified eight accomplishments in its aviation security program since 9/11. Among them are a federal airport security workforce that meet 100% of the national standards, the deployment of Federal Air Marshals (FAMs) flying on tens of thousands of high-risk flights, every month, hardened cockpit doors on commercial passenger planes, hundreds of armed pilots, referred to as federal flight deck officers (FFDOs), numbering in the hundreds; and 100% screening of the 1 billion bags checked annually.⁶ Not to diminish the importance of these advancements, but given that Congress has directed tens of billions of dollars to aviation security since 9/11, the American people have the right to expect more.

II. STATE OF AVIATION SECURITY:

There are three major significant gaps in aviation security that Congress, the General Accounting Office, and the Department’s Office of Inspector General (OIG), and the National Commission on Terrorist Attacks on the United States have all brought to TSA’s attention that continue to go unaddressed— sabotage by an airport worker, a terrorist being allowed to board a U.S.-bound plane before being checked against the terrorist watchlist and an attack emanating in the air cargo hold.

The Continuing Threat of Sabotage by an Airport Worker

The current reality at our nation’s airports is that while millions of passengers, pilots, and flight crews are subjected to checkpoint screening, tens of thousands of airport caterers, cleaners, mechanics, employees at airport restaurants and shops, gate agents and baggage handlers bypass the checkpoint entirely and gain unfettered access to secured and sterile areas of the airport, including airplanes themselves. The thought that an airport worker will exploit this gap in aviation security to plant an incendiary device or weapon is not far-fetched. Al Qaeda has tried it before. In 1995, Philippine authorities uncovered “Operation Bojinka,” a plot developed by Ramzi Yousef, the architect of the first World Trade Center bombing, to detonate explosives on 11 commercial air carriers in a synchronized manner. The plot was discovered by Phillipine police. A dry run of the attack was attempted on a Philippine Airlines flight to Tokyo, where a small bomb, a contact lens solution bottle containing nitroglycerin, detonated \under seat 27F.⁷ In the subsequent prosecution, U.S. federal prosecutors estimated that 4,000 passengers would have died had the plot been successful.⁸ Yet, TSA has not taken steps to close the gap in

⁵ *Id.* at 8-9.

⁶ TRANSPORTATION SECURITY ADMINISTRATION, *Aviation Security System of Systems: THEN and NOW*, available at http://www.tsa.gov/interweb/assetlibrary/System_of_Systems_web.pdf

⁷ Matthew Brzezinski, *Bust and Boom*, WASHINGTON POST W09 (December 30, 2001).

⁸ *Plane terror suspects convicted on all counts*, CNN (September 5, 1996), available at <http://www.cnn.com/US/9609/05/terror.trial/index.html>.

aviation security represented by a “sleeper” attack, where an airport worker exploits the trust or access granted to them as an employee to launch a terrorist attack from the inside.

In the absence of checkpoint screening protocols for airport workers, the establishment of stringent identification requirements and a secure badge program, with biometrics, is all the more critical. Programmatic delays, however, have plagued the development of an integrated, credential-based, identity management program, the Transportation Worker Identification Card (TWIC), to provide unescorted access to secure areas of transportation infrastructure to the over 12 million individuals working in the transportation sector.

Shortly after its establishment in 2002, TSA announced the development of the TWIC program to not only meet the statutory requirements of the Maritime Transportation Security Act of 2002 to create a credentialing program for maritime workers by August 2004, but create a system for transportation workers in all other modes, including aviation. The August 2004 deadline for deployment in the maritime sector was missed and by December 2004, GAO stated that “Each delay in TSA’s program to develop the card postpones enhancements to port security. . . .”⁹ The same can certainly be said for aviation security, insofar as deployment of TWIC in the maritime environment is the precursor to implementation for airport workers. In response to questioning about delays in the TWIC program, Michael Jackson, the then-nominee for the Deputy Secretary position at the Department stated: “I honestly don’t know and I wish I did. I have to say it is perhaps impolitic, but it is true that I just share your frustration in this area, and I am perplexed at why we have not been able to move this ball further and faster, because it is important.”¹⁰ As of June 30, 2005, TSA had little progress to report-- the prototype phase, conducted at 27 seaports, airports and other transportation facilities in five states, was completed and just 8,000 cards had been issued.¹¹

The Threat that a Terrorist Will Board A U.S.-Bound Plane Without Being Checked Against The Terrorist Watch List

At present, the Department requires air carriers to transmit full manifests of U.S.-bound flights fifteen minutes after departure to U.S. Customs and Border Protection (CBP). Passengers names are then checked against the consolidated watch list, including the “no fly” list. In instances where there appears to be a match, flights are diverted – either back to their airport of origin or to unexpected destinations en route. Six major international flights were diverted in 2005, and while many diversions are a result of “false hits,” in at least one incident, the individual had connections to Jihadist groups.¹² One of the eight key

⁹ GOVERNMENT ACCOUNTABILITY OFFICE, *PORT SECURITY: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106, 17-18 (December 2004).

¹⁰ *Statement of the Honorable Michael P. Jackson, Hearing before the Senate Committee on Homeland Security and Governmental Affairs*, S. Hrg. 109-44 (March 7, 2005).

¹¹ 24 Government Computer News 25, *Core Projects: DHS builds its foundation on IT initiatives*, (August 29, 2005), available at http://www.gcn.com/24_25/top-stories/36761-1.html.

¹² On May 31, 2005, a Korean Air flight to California was diverted to Japan because the name of a U.S. citizen of Pakistani descent matched the name of a suspect on the no-fly list. Subsequent investigations showed that the passenger, Hamid Hayat, had in fact attended a Jihadist training camp in Pakistan for approximately six

arenas of action in a strategy to disrupt terrorist mobility identified by Susan Ginsburg, former Senior Counsel of the 9/11 Commission, in *Countering Terrorist Mobility: Shaping an Operational Strategy*, is “[i]nvesting in the ability to track individuals *en route*.”¹³ Moreover, technology exists to fully automate pre-screening of passengers and restrict the issuance of a boarding pass until a passenger’s name is checked against the consolidated terrorist watch lists. Australia has had such a system since the Sydney Olympics in 2000.

Not only has the Department failed to tighten its pre-screening program to ensure that all U.S.-bound passengers are screened before departure but it has been slow to implement the Immigration Security Initiative, since renamed “the Immigration Advisory Program,” that deploys CBP inspectors to foreign airports with high volume of traffic to the U.S. to engage in critical information exchange and prevent travelers identified as security threats, and others deemed inadmissible, from continuing on to the United States.¹⁴

The Air Cargo Security Risk

Screening the 23 billion pounds of air cargo that is transported annually is critical to keeping America secure. In fact, the 9/11 Commission Report concluded that “More attention and resources should be directed to reducing or mitigating the threat posed by explosives in vessels’ cargo holds.”¹⁵ In recent years, TSA has increased the number of cargo inspectors and canine dog teams. It has also undertaken research and development of technologies and systems that could be utilized in the air cargo environment. Yet, TSA has not moved forward and issued a final air cargo rule, as required under section 4053 of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). The deadline for issuance was August 14, 2005. TSA’s approach to securing air cargo is predicated on air carriers and freight forwarder verifying known shippers and undertaking screening and physical inspections. GAO recently reported that there are a number of structural weaknesses with TSA’s plans to create a centralized Known Shipper Database and that a number of exemptions on the screening of air cargo may “create potential vulnerabilities in the air cargo security system.”¹⁶

Operationally, TSA continues to struggle to establish timely and effective communications about threats internally. The OIG found that two years after TSA failed to act upon an email sent by Nathaniel Heatwole, a 20-year-old college student, notifying the agency that he had evaded checkpoint security and was able to concealed box cutters and other prohibited items on six different Southwest flights, information about potential

months in 2004 and that his relatives had connections to various Jihadist groups. Hamid Hayat remains under investigation by the Department of Justice.

¹³ Susan Ginsburg, *Countering Terrorist Mobility: Shaping an Operational Strategy* 5, Migration Policy Institute (February 2006).

¹⁴ Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) §§ 7206, 7210.

¹⁵ 9/11 Commission Report at 393.

¹⁶ Government Accountability Office, *AVIATION SECURITY: Federal Action Needed to Strengthen Domestic Air Cargo Security* (GAO-06-76), at 6 (October 2005).

security violations, threats and criminal activity was not always reviewed and forwarded in a timely manner within TSA.¹⁷

Additionally, there is a lack of clarity as to the responsibilities of the Federal Security Director (FSD), TSA's top official in an airport environment, as relates to the Federal Bureau of Investigations and other Federal and State authorities during an aviation emergency. A recent GAO report found that "TSA's primary document outlining FSDs' authority is outdated, and neither it, nor other statements TSA has issued, delineates the authority of the FSD in various security situations relative to other parties."¹⁸ The surveys that GAO collected from FSDs reflected that the lack of clarity as to relative roles during security incidents "could result in conflict, confusion, and increased response time."¹⁹

It is too soon to tell whether the recent reorganization at TSA will address the operational weaknesses identified by the OIG and GAO, but these critical communications and command and control issues must be addressed for TSA to effectively secure the skies.

III. PRESIDENT'S BUDGET:

With respect to aviation security, the President's budget requests \$4.65 billion, a \$73.5 million increase over the FY 2006 level. This increase is largely dependant on Congress approving a doubling of the passenger ticket fee and TSA collecting additional air carrier security fees. This fee increase would disproportionately impact travelers on non-stop flights, doubling what they pay per round-trip from \$5.00 to \$10.00, and cost the flying public approximately \$1.3 billion a year.

It is also worth noting that the TSA budget provides no new funding for explosive detection systems (EDS). On April 30, 2003, Admiral James Loy, TSA's Administrator committed to nearly \$1 billion of federal funds to pay for 75 percent of the cost of new or existing capital improvement projects. The Department has fallen far short of its promise to provide 20 airports with assistance to cover the costs of acquiring and installing in-line detection equipment. To date, it has issued LOIs to nine airports but there are at least 27 airports that TSA has identified would benefit. TSA viewed the deployment stand-alone EDS systems in 2001 as an "interim solution" but five years later, hundreds of airports around the nation still do not have in-line EDS systems with baggage conveyors.²⁰

TSA's air cargo operations budget continues to be funded at \$55 million, the FY 2006 level. This is \$200 million less than what is authorized under the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) (9/11 Act) for air cargo security. The

¹⁷ THE DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, *Transportation Security Administration's Revised Security Procedures (Unclassified Summary)* (OIG-05-51) (September 2005).

¹⁸ GOVERNMENT ACCOUNTABILITY OFFICE, *TRANSPORTATION SECURITY ADMINISTRATION: More Clarity on the Authority of Federal Security Directors Is Needed* (GAO-05-935) 36 (September 2005).

¹⁹ *Id.* at 3.

²⁰ Berrick Statement at 9.

President's budget request will not provide TSA with the resources to add more cargo inspectors, over and above the 300 that are authorized, or deploy explosive detection equipment or other technology to improve air cargo screening and inspections.

IV. AREAS FOR IMPROVEMENT

To close the three major security gaps identified above, the Department must:

- Put systems in place to either restrict unescorted access to secured and sterile areas of the airport or screen airport workers;
- Deploy an automated system to pre-screen U.S.-bound passengers before they their flights depart; and
- Eliminate exemptions to the screening of air cargo and develop a multi-layered approach to cargo security where Known Shippers are verified and elevated risk cargo is identified and screened and watch list.

Additionally, as TSA implement organizational changes in accordance with the Secretary's Second Stage Review, it should address the communications and command and control issues identified above.

What Democrats Have Done

Legislation has been introduced by Democratic Members of the Committee on Homeland Security to address the three identified security gaps:

H.R. 2688, the Guaranteeing Airport Physical Screening Standards Act of 2005 - Introduced by Rep. Nita Lowey (D-NY), this legislation would require screening (at a minimum, screening for metal objects) or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of a U.S. airport.

H.R. 4512, legislation introduced by Rep. Peter DeFazio (D-OR) to direct the Department to initiate a pilot program to evaluate the use of automated systems for the immediate prescreening of passengers on flights in foreign air transportation bound for the United States.

H.R. 2044, the Air Cargo Security Act, legislation introduced by Rep. Ed Markey (D-MA) to requires the inspection of all cargo transported in aircraft operated by domestic and foreign air carriers.

I. STATEMENT OF PROBLEM HISTORICALLY:

The Transportation Security Administration (TSA) was created to oversee the nation's efforts to secure all modes of transportation. Since its inception, however, TSA has focused almost all of its attention on aviation security.

This focus continued even after the terrorist attacks in Moscow, Madrid, and London. On February 6, 2004, an explosion in a Moscow Metro rail car killed 41 people and wounded 129 others. The explosive device was thought to have been stored in a backpack or briefcase. Later that year on March 11, 2004, a coordinated series of ten explosions aboard four packed commuter trains in Madrid killed 191 people and injured over 1,500 others. The attacks were carried out by Al-Qaeda linked terrorists who boarded the system at outlying stations, deployed their device-laden packages on the trains, and exited before the predetermined time of detonation. On July 7, 2005, four suicide bombers detonated bombs on three London subway trains and one double-decker bus, killing 52 people and injuring 700 more. The suicide bombers claimed to have ties to Al-Qaeda. Later that month on July 21, 2005, four attacks were attempted on London's transit system in which only one person was injured, but the system, and to a great extent London, were crippled for a considerable amount of time.

These devastating attacks demonstrated the fact that terrorists viewed non-aviation transportation modes as potential targets and served as a wake-up call to U.S. mass transit, rail, and highway systems. While TSA and the Coast Guard have focused on securing aviation and maritime security, no entity has focused greatly on surface transportation. Indeed, TSA, while having primary responsibility, has not mandated the creation of security plans, risk assessments, or training for surface transportation.

II. THE STATE OF SURFACE TRANSPORTATION SECURITY TODAY:

Best Standards, Guidance, and Regulations. TSA has not yet issued any best standards, guidance, or regulations regarding security plans for mass transit, rail, or highway owners and operators. Instead, the industry, on its own initiative, has begun developing these plans. As the agency responsible for ensuring security of ALL modes, TSA should be taking a lead role and there are indications that TSA hopefully will do so in the future. In the Congressional justification submitted to Congress for the FY'07 TSA Surface Transportation security budget, the Administration states that "In FY'07, TSA and its partners will develop best practices, standards, and regulations to protect the transportation infrastructure. In addition to continued inspections monitoring and

enforcing compliance with standards and regulations will occur, along with designing and implementing vulnerability assessment models for all surface transportation modes.”¹

Risk Assessments and Duplication of Effort. TSA has conducted risk assessments, but these assessments are duplicative to those conducted by the Federal Transit Administration and the Office of Grants and Training (formerly known as the Office of Domestic Preparedness). The Government Accountability Office (GAO) highlighted this problem in an October 7, 2005 report.² This apparent duplication of effort has led to questions about what the various agencies are doing with the information that they collect; whether it is being shared; where it is being stored; and who has access to it.

The duplication of effort also exists in other areas. For example, TSA recently began approaching trucking companies to assess their vulnerabilities with regard to the transportation of hazardous materials. Since 9/11, the Federal Motor Carrier Safety Administration (FMCSA) has completed more than 40,000 security sensitivity visits and in fiscal year 2005, FMCSA completed more than 1,200 security compliance reviews. This apparent lack of coordination by TSA and FMCSA has created confusion and frustration for industry.³

Security Directives. In response to the terrorist attack in Madrid, TSA issued two Security Directives (SDs) on May 20, 2004.⁴ TSA developed these SDs without public comment and the GAO is currently examining the legal basis under which TSA issued the SDs.⁵ These SDs are the only SDs that TSA has issued for mass transit and rail security, despite the fact that the agency has issued 80 SDs for aviation security.⁶

Surface Inspectors. TSA has 43,000 aviation screeners.⁷ There are only 100 surface inspectors.⁸ The 100 inspectors are responsible for ensuring the security of the thousands of miles of railroad tracks and mass transit lines that crisscross our country. TSA must devote more personnel to non-aviation security if it wants to prevent surface

¹ Department of Homeland Security, Transportation Security, Fiscal Year 2007, Strategic Context, Congressional Justification, page 7.

² GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* (GAO 05-851) 4 (Sept. 2005), at <http://www.gao.gov/new.items/d05851.pdf>.

³ E-mail from American Trucking Association, to Democratic Staff, House Committee on Homeland Security (Feb. 23, 2006) (on file with Committee staff).

⁴ These SDs are classified as Sensitive Security Information. Individuals wishing to attain a copy of these SDs should contact TSA.

⁵ GAO, *supra* note 2, at 36 n.36.

⁶ E-mail from Transportation Security Administration, to Democratic Staff, House Committee on Homeland Security (Feb. 23, 2006) (on file with Committee staff).

⁷ These screeners have recently been reclassified as Transportation Security Officers. DHS, TRANSPORTATION SECURITY ADMINISTRATION, *Press Release: TSA Unveils Enhanced Security Screening Procedures and Changes to the Prohibited Items List* (Dec. 2, 2005), at

<http://www.tsa.gov/public/display?theme=44&content=090005198018c27e>.

⁸ Congress appropriated funds for these inspectors in the FY 2005 Homeland Security Appropriations Act. *See* An Act Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2005, and for Other Purposes, Pub. L. No. 108-334, 118 Stat. 1298 (Oct. 2004). The Conference Report accompanying the public law contains specific information about the inspectors. H.R. CONF. REP. NO. 108-774 (Oct. 2004).

transportation from becoming the weak link in the system. TSA must also develop regulations and security directives that can be enforced.

Training and Exercises. Despite the recent spate of attacks, TSA has not yet mandated security training for the men and women who drive the trains, subway, and trucks that move millions of people and cargo each day. Security training is mandated for the maritime sector.⁹ The International Brotherhood of Teamsters, in a fall 2005 report, called for mandatory training for all rail employees.¹⁰ TSA has taken some small steps. It has contracted with the National Transit Institute to develop training for passenger and freight rail employees.¹¹ In addition, Assistant Secretary Hawley told the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity on February, 16, 2006, that TSA is working with industry on this training. TSA, has not yet however, consulted labor organizations.¹²

Public Outreach. The Departments of Homeland Security and Transportation are beginning to work together on public outreach. These initiatives, however, did not prevent the breakdown in communication and coordination on October 5, 2005, when New York City (NYC) Mayor Michael Bloomberg announced that the city, in response to a credible threat, would be taking additional security measures to protect the NYC subway system. Department of Homeland Security officials told the press that the threat was not credible.¹³

Research and Development. TSA and the Department of Homeland Security have not progressed past the pilot stage with regards to mass transit and rail research and development (R&D). TSA developed a mass transit pilot program in 2004 but no additional steps were taken.¹⁴ In January 2006, the Department's Science and Technology Directorate announced that it was starting its own mass transit pilot program.¹⁵ To many, the Department's mass transit and rail R&D initiatives are reminiscent of mice which run on wheels without ever making any forward momentum.

Hazardous Material. The vulnerability of hazardous material has been of particular interest to several cities in the country, like Washington, D.C., who want to ban the transportation of certain hazardous materials through their respective cities. In their fall 2005 report, the Teamsters highlight the security gap that exists with regards to the

⁹ Security training for maritime professionals is required under Section 109 of the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, § 109(a), 116 Stat. 2064, 2090 (Nov. 2002).

¹⁰ International Brotherhood of Teamsters, Teamsters Rail Conference, *High Alert: Workers Warn of Security Gaps on Nation's Railroads* (Fall 2005), at <http://www.teamster.org/divisions/rail/pdfs/railsecuritybook.pdf>.

¹¹ E-mail from Transportation Security Administration, to Democratic Staff, House Committee on Homeland Security (Feb. 24, 2006) (on file with Committee staff).

¹² Amalgamated Transit Union, *ATU Action Weekly Update- 2/21/06* (Feb. 21, 2006), at http://www.unionvoice.org/atuaction/notice-description.tcl?newsletter_id=1551241.

¹³ Josh Getlin and Josh Meyer, *New York Mayor Defends Telling the Public About Subway Threat; Some Residents Question why Local and Federal Officials Differ Over What was Called an 'Imminent' Plot Against the City's Transit System*, L.A. TIMES, Oct. 8, 2005, at 14.

¹⁴ DHS, TSA, *Transit and Rail Inspection Pilot Programs* (Feb. 2006), at http://www.tsa.gov/public/interapp/editorial/editorial_1711.xml (information about the TRIP pilot)

¹⁵ E-mail from Science and Technology Directorate, to Democratic Staff, House Committee on Homeland Security (Jan. 25, 2006) (on file with Committee staff).

movement of hazardous materials.¹⁶ TSA, along with other Federal agencies, is working to close this gap but it still has not yet developed regulations or guidance to fully address this issue.

Surge Capacity. In December 2005, TSA piloted a surge capacity initiative designed to enhance security in the non-aviation modes of transportation. The surge capacity was piloted in Los Angeles, Houston, Atlanta, Washington, DC, Philadelphia, and Baltimore.¹⁷ This pilot initiative was not without controversy. According to Representative Allyson Schwartz, who was briefed by Philadelphia and Southeastern Pennsylvania Transportation Authority law enforcement officials, TSA told Philadelphia police about the initiative only hours before they arrived. TSA claimed that they briefed the police weeks before their arrival.¹⁸

High Turnover. Finally, TSA has suffered from a high level of personnel turnover for the past four years. In fiscal year 2004, 12,156 individuals left the agency. In fiscal year 2005, this trend continued as an additional 12,232 departed.¹⁹ Assistant Secretary Hawley is the 4th person to lead the agency in four years. This turnover at all levels of the agency has resulted in a lack of continuity, constant upheaval, and minimal progress with regards to surface transportation security.

III. PRESIDENT'S BUDGET

The President's budget request for Fiscal Year 2007 only allocates \$37.2 million in the TSA budget for non-aviation transportation security – less than 1% of the TSA budget. The Administration's budget also eliminates the dedicated grants used by public transportation systems to enhance security. Specifically, the President's budget eliminates rail and transit security grants and intercity bus grants, which were funded at \$144 million and \$9.6 million, respectively, in FY 2006. Instead of providing more direct funding, the Administration has yet again proposed to consolidate all critical infrastructure funding under the Targeted Infrastructure Protection Program (TIPP). The TIPP program will force surface transportation entities to compete against each other and with other critical infrastructure, such as ports. Moreover, the \$600 million will not meet the needs of our nation's transportation systems. The American Public Transportation Association estimates that \$6 billion is needed just for mass transit security.²⁰

¹⁶ Teamsters, *supra* note 10.

¹⁷ TRANSPORTATION SECURITY ADMINISTRATION, *Press Release* (Dec. 13, 2005) (on file with Committee staff).

¹⁸ Leslie Miller, *Undercover Air Marshals to Expand Work Beyond Airplanes to Trains, Buses*, ASSOCIATED PRESS, Dec. 15, 2005.

¹⁹ Letter from Under Secretary Kip Hawley, Transportation Security Administration, to Representative Bennie Thompson, Ranking Member, House Committee on Homeland Security (Dec. 9, 2005) (on file with Committee staff).

²⁰ American Public Transportation Association, *Statement on President Bush's Proposed FY 2007 DHS Budget* (Feb. 6, 2006), at http://www.apta.com/media/releases/060206dhs_response.cfm (a nonprofit international association of more than 1,600 transportation related entities).

IV. AREAS FOR IMPROVEMENT:

In order to secure our surface transportation system, TSA, working with its Federal, state, local, and tribal partners, industry and other stakeholders must develop best standards, guidance, and regulations concerning security plans. Mandatory training for employees must be a component of these plans. It has been four years since 9/11. TSA cannot continue to dawdle and delay this important step.

Additionally, TSA, working with its partners, must ensure that all surface transportation security issues – budget, grants, vulnerability assessments, R&D, and outreach -- are better coordinated and directly relate to the National Strategy for Transportation Security. A dedicated and sufficient funding stream for surface transportation grants and initiatives is important if our surface transportation system is to make adequate security enhancements.

The development of security standards for surface transportation security is another important benchmark the Department has yet to reach. As stated in its FY '07 budget justification, TSA should develop security standards for surface transportation security that reflect industry best practices. These standards must be monitored and enforced by TSA surface inspectors and, if appropriate, by asset owners and operators.

In conjunction with relevant stakeholders, TSA should establish guidelines for vulnerability assessments, including an agreed-upon methodology. These assessments should be protected and shared, as appropriate. In addition, TSA should work with fellow agencies to minimize the number of assessments completed of each individual asset.

Lastly, but perhaps most important, TSA must improve outreach, communication, and sharing of information with state and local officials, and the private sector, including industry and labor organizations. The Department's partners must know who is in charge and who they should contact if and when a transportation security incident occurs.

I. STATEMENT OF PROBLEM HISTORICALLY:

Over 400 million passengers, 130 million vehicles, and 23 million shipping containers cross between Mexico and Canada at U.S. ports of entry annually.¹ Hidden among the millions of travelers are those seeking to come to the U.S. for illegal purposes, including terrorists.² It is estimated that about 10 million immigrants are currently in the U.S. illegally.³ Since 9/11, over 4 million individuals were intercepted between U.S. Ports of Entry (POEs) for attempting to enter the U.S. illegally.⁴ Improving border security was a primary objective behind the establishment of the Department of Homeland Security (DHS) and was intended to address the ease with which terrorists entered the United States to plan for and carry out the 9/11 terrorist attacks.⁵ Since the establishment of the Department three years ago, billions of dollars and countless hours of effort have been put into strengthening our nation's borders.⁶ The Administration and the Department of Homeland Security have promised to control the nation's borders by providing the personnel, technology and effective border security strategy to screen travelers and cargo entering and exiting our country's borders.

II. THE STATE OF BORDER SECURITY TODAY:

Although some effort has been undertaken to enhance border security, such as the expansion of Container Security Initiative (CSI) agreements to 26 foreign countries,⁷ progress towards implementing a biometric entry system (US-VISIT)⁸, and efforts to

¹ U.S. Customs and Border Patrol (CBP), *Presentation at SBI-net Industry Day* (Jan. 26, 2006).

² Janice L. Kephart, *Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel*, CENTER FOR IMMIGRATION STUDIES (Sep. 2005), at <http://www.cis.org/articles/2005/kephart.html>.

³ Susan Ginsburg, *Countering Terrorist Mobility: Shaping an Operational Strategy* 9, Migration Policy Institute (Feb. 2006), at http://www.migrationpolicy.org/pubs/MPI_TaskForce_Ginsburg.pdf.

⁴ U.S. CUSTOMS AND BORDER PROTECTION, *FY 2007 Budget Briefing for Homeland Security Committee Staff* (Feb. 17, 2006) (materials on file with Committee staff).

⁵ Susan Ginsburg, *Countering Terrorist Mobility: Shaping an Operational Strategy 1*, Migration Policy Institute (Feb. 2006), at http://www.migrationpolicy.org/pubs/MPI_TaskForce_Ginsburg.pdf.

⁶ U.S. HOUSE COMMITTEE ON HOMELAND SECURITY, Democratic Staff, *Leaving the Nation At Risk: 33 Unfulfilled Promises Made by the Department of Homeland Security* (Dec. 2005) (investigative report prepared for Bennie G. Thompson, Ranking Minority Member).

⁷ CSI sets out to enable the U.S. Customs and Border Protection (CBP), in working with host government Customs Services, to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the United States. It is operational in forty-two foreign ports in Europe, Asia, Africa, the Middle East and North America, according to DHS. DHS, *Fact Sheet: Securing U.S. Ports* (Feb. 22, 2006), at http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0865.xml.

⁸ US VISIT currently applies to all visitors (with limited exemptions) entering the United States, regardless of country of origin or whether they are traveling on a visa or by air, sea or land. Most visitors experience the US VISIT biometric procedures – digital, inkless finger scans and digital photograph – upon entry to the United States. DHS, *US-VISIT: How it Works*, at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0525.xml.

implement more secure travel documents (the Western Hemisphere Travel Initiative),⁹ several promises remain unfulfilled. As a result, our borders remain porous. For example, in fiscal year 2005, the U.S. Border Patrol made over 1 million apprehensions of people attempting to cross U.S. land borders illegally, and the U.S. Customs and Border Protection (CBP) Field Operations officers stopped more than 600,000 individuals attempting to enter illegally at our POEs.¹⁰ In the same period, Immigration and Customs Enforcement (ICE) apprehended approximately 140,000 illegal immigrants in interior enforcement operations and 15,000 under its fugitive operations program.¹¹ Given the porous nature of our borders, much more needs to be done to reduce illegal entry and other criminal activity.

Among the broken promises and border security-related priorities that the current Administration needs to fulfill are:

- Providing border security personnel “state-of-the art” technology and radiation screening equipment to detect illegal entry of people and attempts to smuggle dangerous cargo and weapons into the United States;
- Moving forward with a Secure Border Initiative (SBI) only after adequately assessing the vulnerabilities of all U.S. land borders and ports of entry; and
- Developing a comprehensive border screening system and structure to ensure the successful implementation of the Western Hemisphere Travel Initiative and US-VISIT programs.

Border Security Personnel Lack “State-of-the Art” Technology and Radiation Screening Equipment

The Department promised that it would deploy *effective* technology to secure and enhance border security, including providing border security personnel with more radiation detection equipment to detect attempts by terrorists to transport Weapons of Mass Destruction across U.S. land borders and ports of entry.¹² To date, however, the

⁹ The Western Hemisphere Travel Initiative (WHTI), enacted by Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), mandated that the Secretary of Homeland Security, in conjunction with the Secretary of State, develop and implement a plan to require a passport or other documentation that shows both identity and citizenship for land border crossings at the U.S. borders with Canada and Mexico by Jan. 1, 2008, as well as travel to and from the Caribbean, areas previously excluded from the passport requirement. The goal is to limit the number of documents Border Patrol Agents must master in order to determine admissibility of travelers at the border, lessening opportunities for fraud. Currently, 50 U.S. State drivers’ licenses and as many as 8,000 different birth certificates can be presented as proof of identity and citizenship at the border. The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7209(b), 118 Stat. 3638 (2004).

¹⁰ *Comprehensive Immigration Reform II: Hearing Before the Senate Judiciary Committee*, 109th Cong. (Oct. 18, 2005) (statement of Secretary Michael Chertoff, Secretary, U.S. Department of Homeland Security), at http://judiciary.senate.gov/testimony.cfm?id=1634&wit_id=66.

¹¹ *Id.*

¹² *The Department of Homeland Security: Hearing on Promoting Risk-Based Prioritization and Management Before the House Committee on Homeland Security*, 109th Cong. (Apr. 13, 2005) (statement of Michael Chertoff, Secretary, U.S. Department of Homeland Security).

Department has not kept its promise to equip its border inspectors and agents with “state-of-the-art” technology that would enable its personnel to effectively secure U.S. borders.

Since the inception of the Department of Homeland Security, millions of tax dollars have been wasted as a result of failed border security-related technology initiatives undertaken by the Department. The Department already has two failed border security technology programs behind it, the discontinued Integrated Surveillance Intelligence System (ISIS)¹³ and the America’s Shield Initiative (ASI)¹⁴. These multi-million dollar efforts, as Table 1 shows, were to develop and deploy adequate border security technology.

Table 1: Funds Expended on Discontinued ISIS/ASI Programs (fiscal years 1997-2005)

Fiscal Years	Total ISIS/ASI Budgeted	Total ISIS/ASI Expended
1997-2000	\$78,330,495	\$78,330,495
2001-2005	\$376,297,427	\$263,968,377
Total (1997-2005)	\$454,627,922	\$342,298,872

The Department recently announced the launching of the Secure Border Initiative (SBI_{net}), which sets out to engage industry representatives in identifying solutions for securing our nation’s border that considers the use of people, technology, and infrastructure. As the Department moves forward with SBI, it is imperative given the past problems associated with contract management and deployment of ISIS and ASI, that the Department also put appropriate management controls and contract oversight systems in place to ensure that the government does not procure equipment and technology that will not fulfill its critical border security needs and lead to further waste.

Although the Department has provided basic radiation pagers to all of its inspectors and border agents, promised “state-of-the-art” radiation detection technology has been less readily available. A recently published DHS fact sheet on the use of technologies along the border reveals a continuing widespread use of older, less reliable technologies.¹⁵ While there are more than 10,500 CBP officers only about 500 of them have advanced radiation detection equipment to effectively screen cargo containers, rail cars, vehicles, and trucks.¹⁶

¹³ In 1997, the Immigration and Naturalization Service (INS) deployed the Integrated Surveillance Intelligence System (ISIS)—a system of sensors, cameras, and databases designed to prevent smugglers and illegal aliens from entering the United States along its northern and southern borders. Pursuant to the Homeland Security Act of 2002 (P.L. 107-296), INS was absorbed in the Department of Homeland Security and the ISIS program was moved into the department’s Customs and Border Protection (CBP) component. U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Border Security: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program 1* (GAO-06-295) (Feb. 22, 2006), at <http://www.gao.gov/new.items/d06295.pdf>.

¹⁴ *Id.* In September 2004, CBP established the America’s Shield Initiative (ASI) program. The goals of the program were to address ISIS capability limitations and support the department’s antiterrorism mission. *Id.*

¹⁵ U.S. CUSTOMS AND BORDER PATROL, *Press Release: CBP Securing Our Borders - Inspection and Surveillance Technologies* (May 5, 2005), at http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/fact_sheet_cbp_securing.xml.

¹⁶ *Id.*

The Department must move faster to equip border inspectors and agents with more of the most up-to-date technologies to expedite the screening of people and cargo so officials can focus on real security risks while facilitating expeditious movement of legitimate travel and trade.

The Administration is Moving Forward with a Secure Border Initiative without Adequately Assessing the Vulnerabilities of All U.S. Land Borders and Ports of Entry

We commend the Department for efforts to reevaluate its border security strategy and for efforts to reach out to industry stakeholders before moving forward with implementing its Secure Border Initiative. Effective strategic planning and a risk-based approach are vital to ensuring that we obtain the greatest possible benefit and security from our investment in technology, people, and tactical infrastructure. Concerns, however, remain that the Department may be moving forward with SBInet without first completing proper vulnerability assessments of land border crossings and ports of entry to determine the most porous areas of greatest risk to our national security. Minority Members of the Homeland Security Committee have called for the Department to complete vulnerability assessments at all U.S. land borders and ports of entry, a requirement incorporated in H.R. 4312, the Border Security bill reported out of the Committee in November, 2005.

In the absence of such assessments, the vigorous oversight of SBInet will be necessary--including the awarding and implementation of the main "integrator" contract. DHS will have to put in place a sufficient oversight function, with the right experts, to ensure that any SBInet solutions offered by industry are relevant and reliable solutions to securing our border.

A Comprehensive Border Screening System & Structure at Ports of Entry (POEs) is Needed to Ensure Border Security

The Department of Homeland Security urgently needs to develop a comprehensive vision for border screening that harmonizes and integrates the many initiatives underway. Issues include resolving biometric standards, making stove-piped systems interoperable, and achieving true data integration.

One key element of such a strategy is the Western Hemisphere Travel Initiative. The Departments of Homeland Security and State have cooperated on developing a plan to address this program, but are far from a final solution. Secretary Chertoff, in a January 17, 2006 joint briefing with Secretary Rice, announced a new "PASS" (People Access Security System) program to support this initiative, with the State Department developing an inexpensive and convenient "passport card" for land border crossings which would be a platform for expedited traveler programs such as NEXUS, SENTRI, and FAST. The Homeland Security Department committed to building a network of card readers and computer terminals to screen the cards at POEs. The Department, however, has not provided any resources to move forward on this commitment. In his February 15, 2006 testimony to the House Appropriations Homeland Security Subcommittee, Secretary

Chertoff was not able to specify where money for the PASS technology would come from. DHS spokesman Jarrod Agen, on February 17, 2006 said the Department has not yet decided on a source of funding.¹⁷ For a program of this magnitude and importance, mandated for implementation by January 1, 2008, to be missing from the President's FY 2007 budget is a glaring omission.

The US-VISIT program was established to collect information on foreign nationals who enter and exit the United States. It is a vital part of the Department's efforts to implement a comprehensive border screening system. According to the GAO, the US-VISIT program has met a number of mandated requirements. For example, a pre-entry screening capability has been achieved at 115 airports, 154 land ports of entry, and 14 sea ports.¹⁸ However, to date, the Department has only fully implemented 2 of the 18 recommendations made by the GAO for strengthening the US-VISIT program. Moreover, the Department has not made measurable progress on establishing an integrated biometric exit component within U.S. VISIT to ensure that foreign nationals do not overstay.

Among the area where key actions have yet to be taken are (1) assessing security risks and (2) adequately testing the system. The GAO concluded that "the longer that US-VISIT takes to implement its recommendations, the greater the risk that the program will not meet its stated goals on time and within budget".¹⁹

III. PRESIDENT'S BUDGET

Although the President's fiscal year 2007 budget provides increases in border security and immigration enforcement, as table 2 shows, the Administration continues to fall short of fully-funding the level of Border Patrol Agents, detention bed space, and Immigration and Customs Agent resources called for by the Intelligence Reform and Terrorism Prevention Act of 2004 (9/11 Act).²⁰ Funding in the President's fiscal year 2007 budget is 25 percent short of what is needed to hire the 2,000 Border Patrol Agents required by the 9/11 Act. It is 20 percent short of the funding needed to provide the 8,000 detention bed spaces authorized by Congress in that Act, and nearly 75 percent short of the funding levels needed for the 9/11 Act authorized increases of 800 Immigration and Customs Enforcement Agents.

¹⁷ Zack Phillips, *Dearth of Details About Border Crossing Card Irks Northern Lawmakers*, CONGRESSIONAL QUARTERLY, Feb. 21, 2006.

¹⁸ U.S. Government Accountability Office (GAO), *Homeland Security: Visitor and Immigrant Status Program Operating, but Management Improvements are Still Needed* (GAO-06-318T) 3 (Jan. 25, 2006).

¹⁹ GAO, *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to be Implemented* (GAO-06-296) 2 (Feb. 14, 2006).

²⁰ The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 5202-04, 118 Stat. 3734-35 (2004).

Table 2: Shortfalls in Fulfilling 9/11 Act Border Security-Related Commitments (FY 2006-2007)

Increases Authorized by 9/11 Act ²¹	FY 2005	FY 2006			FY 2007		
	End of Year Levels	9/11 Act Commitment Levels ²²	Projected Levels	Projected Shortfalls	9/11 Act Commitment Levels ²³	Projected Levels	Projected Shortfalls
Increase of 2,000 Border Patrol Agents each year (FY 2006-2010)	11,264 ²⁴	13,264	12,319 ²⁵	(945)	15,264	13,819 ²⁶	(1,445)
Increase of 8,000 Detention Bed spaces each year (FY 2006-2010)	18,500 ²⁷	26,500	20,800 ²⁸	(5,700)	34,500	27,500 ²⁹	(7,000)
Increase of 800 Full-Time ICE Investigators each year (FY 2006-2010)	5647 ³⁰	6447	6101 ³¹	(346)	7247	6341 ³²	(906)

IV. AREAS FOR IMPROVEMENT:

To further enhance the security of our nation's land borders and ports of entry, the Administration and the Department of Homeland Security should place a priority on the following:

- Developing a comprehensive strategy for identifying and securing the nation's most porous and vulnerable land borders and ports of entry as a part of the Department's efforts to implement its Secure Border Initiative and to deploy future resources;
- Putting an adequate internal control and management oversight system in place to ensure that the same contract procurement, deliverable, and deployment problems experienced by the Department during its past attempts to deploy border security-related surveillance systems and technology are not repeated;

²¹ The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 5202-04, 118 Stat. 3734-35 (2004).

²² Figures were derived at by adding the 9/11 Act increases in authorized levels to the level of resources DHS reported as on-board at the end of fiscal year 2005.

²³ *Id.*

²⁴ U.S. CUSTOMS AND BORDER PROTECTION, *FY 2007 Budget Briefing for Homeland Security Committee Staff* (Feb. 17, 2006) (materials on file with Committee staff).

²⁵ *Id.*

²⁶ *Id.*

²⁷ U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, OFFICE OF CONGRESSIONAL RELATIONS (Dec. 2005) (email on file with Committee staff).

²⁸ U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, OFFICE OF CONGRESSIONAL RELATIONS (Dec. 2005) (email on file with Committee staff).

²⁹ U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, *FY 2007 Budget Briefing for Homeland Security Committee Staff* (Feb. 13, 2006) (materials on file with Committee staff).

³⁰ U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, OFFICE OF CONGRESSIONAL RELATIONS (Feb. 2006) (email on file with Committee staff).

³¹ *Id.*

³² *Id.*

- Developing a sound strategy to enhance border security and to fully implement the GAO recommendations for enhancing the U.S. VISIT program; and
- Increasing the number of border patrol agents, detention bed spaces, and immigration and customs enforcement agents to fulfill the funding and resource recommendations of the bi-partisan 9/11 Act, and ensuring that these officers have the necessary resources to do their jobs.

I. STATEMENT OF PROBLEM HISTORICALLY

Emergency preparedness refers to the work done before an emergency in order to ensure state, local and federal agencies are as prepared as possible to manage protection, response, and recovery operations. Most of the emergency preparedness functions of the Department of Homeland Security currently are performed by the Preparedness Directorate, which was created last year as part of the restructuring of the Department ordered by Secretary Chertoff. The new Directorate's mission is to manage homeland security grants; oversee nationwide preparedness efforts; support first responder training; strengthen citizen awareness, public health, critical infrastructure and cyber security; and ensure proper steps are taken to protect high-risk targets.¹

Emergency response includes the actual activities conducted by a variety of federal agencies to rescue survivors of a disaster, provide assistance, and reduce damage. A variety of offices within the Department of Homeland Security respond to a disaster, though the most commonly known are the Coast Guard and the Federal Emergency Management Agency (FEMA). As a result of Secretary Chertoff's reforms of the Department, the director of FEMA now reports directly to the Secretary, but many of FEMA's programs to prepare for an emergency have been transferred to the Preparedness Directorate.

In August 2005, Hurricane Katrina, a Category 4 storm, struck the Gulf Coast, severely damaging parts of Mississippi, Alabama, and Louisiana and creating a storm surge that breached the New Orleans levee system. The storm resulted in over 1,300 deaths and damages are estimated at well over \$100 billion, making it the costliest storm in U.S. history.² The Department of Homeland Security and FEMA's response to Hurricane Katrina was a complete failure, showcasing how ineffective management, poor communications, and failing to take a true all-hazards approach to response have affected both preparedness and response capabilities.

II. THE STATE OF EMERGENCY PREPAREDNESS AND RESPONSE TODAY

Hurricane Katrina and the subsequent flooding of New Orleans exposed significant flaws in our government's ability to prepare for and respond to catastrophic events. Emergency plans at all levels of government, including the National Response Plan (NRP), failed the nation.

¹ Press Release, DEPARTMENT OF HOMELAND SECURITY, *DHS Organization*. Available at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0794.xml.

² National Oceanic and Atmospheric Administration, "Climate of 2005 Atlantic Hurricane Season," 13 January 2006. Available at <http://www.ncdc.noaa.gov/oa/climate/research/2005/hurricanes05.html>.

In February 2006, the White House released its review of the federal response to Hurricane Katrina.³ The report includes 125 specific recommendations for emergency preparedness and response reforms. It is not yet clear whether the Department can successfully implement the report's long-term recommendations, such as eliminating red tape and delays in providing federal assistance to disaster areas; strengthening homeland security education exercises, and training; and ensuring that homeland security assessments, lessons learned, and corrective action programs are institutionalized throughout the federal government.⁴ It is also unclear how achievable these goals are in, in light of the pending hurricane season, which starts June 1.

Additionally, the Department's past track record has left many local officials skeptical about whether they will be partners in implementing reforms. Mike Selves, President-Elect of the International Association of Emergency Managers observed, "At a time when the Administration is recommending decreases in assistance to State and local governments in the form of cuts to the Emergency Management Performance Grants, COPs, fire and homeland security grants, this report calls for greatly increased workload and accountability on our part. Without significant collaboration with our Federal partners, how do we 'sell' many of these recommendations to our elected officials as anything other than unfunded mandates?"⁵

Changes made late last year as a result of Secretary Chertoff's reform of the Department may also complicate emergency preparedness and response. In particular, the division of FEMA's preparedness and response programs, which are now split between FEMA and the Preparedness Directorate, respectively, have been opposed by many first responders and emergency managers. Bruce Baughman, who led the Office of National Preparedness prior to the creation of the Department, said the separation "was a big mistake. We tried that before, and it was a disaster."⁶ Similarly, FEMA Director Brown described the problem in June 2005, explaining the impact of withdrawing the preparedness functions from the rest of the emergency cycle he said, "Merging FEMA's small preparedness functions with the prevention mission of the department will destroy the emergency management cycle and lead to failure. I don't want to see us fail this President or the nation because of a desire to consolidate that which shouldn't be consolidated."⁷

³ Associated Press, *White House to issue its own Katrina report*, 22 February 2006.

⁴ THE WHITE HOUSE, *The Federal Response to Hurricane Katrina: Lesson Learned*, February 2006. Available at <http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf>.

⁵ "News Release: IAEM Responds to White House Report on Lessons Learned From Hurricane Katrina," 24 February 2006.

⁶ Robert Block, *Homeland Security Wrestles with Revamp*, THE WALL STREET JOURNAL, 13 June 2005, p. A4.

⁷ Letter from FEMA Director Michael Brown to Deputy Secretary of Homeland Security Michael Jackson, June 2005. Retrieved online at <http://www.pbs.org/wgbh/pages/frontline/storm/etc/brownconcern.html>

III. PRESIDENT'S BUDGET

The President's fiscal year 2007 budget does little to address the needs of local first responders and emergency managers, cutting \$612 million out of first responder grants and training programs administered by the Preparedness Directorate. Overall, funding levels for programs designed to assist state and local law enforcement agencies were slashed by more than \$1 billion compared to fiscal year 2006. Representatives of the National Sheriffs' Association and the International Association of Chiefs of Police have questioned whether these cuts demonstrate a lack of commitment to homeland security on the part of the Administration.⁸

Despite the lack of emergency planning Hurricane Katrina demonstrated, the President's budget proposes a \$15 million cut to Emergency Management Performance Grants (EMPG), a vital source of federal funding to state and local governments for emergency planning, training, exercising, and hiring of emergency management personnel. According to Bruce Baughman, President of the National Emergency Management Association (NEMA), it is "unbelievable in light of recent disasters that the federal government would propose a reduction of state and local disaster preparedness grants."⁹ Furthermore, the Administration proposes a sixty-six percent decrease from fiscal year 2006 for training offered by the National Domestic Preparedness Consortium, a critical means of delivering high-level training to first responders. The President even proposes cutting the Assistance to Firefighters Grant program by fifty percent, from \$545 million to \$293 million. This program has been very effective in providing local fire departments with the tools they need to perform their day-to-day duties, as well as enhancing their ability to respond to large disasters.

While the President's budget shows an increased commitment to FEMA in the wake of the 2005 hurricane season, the \$3.1 billion in discretionary funding for the agency may still fall short of what is needed to implement the White House's reforms, adequately address the agency's operational weaknesses, and ensure that the agency can lead efforts to prepare, respond, recover and mitigate disasters. Additionally, the President's budget flat funds the National Disaster Medical System (NDMS), a program consisting of thousands of volunteer medical professionals ready to be deployed in the event of a disaster, even though the drastic cuts to the program made last year affected its performance during Hurricane Katrina.

⁸ According to Edmund M. Sexton, President of the National Sheriffs' Association, these cuts have significantly impacted the first responder community. "While the President continues to state that he is committed to protecting the homeland, his budget does not reflect it." National Sheriffs' Association. White House Virtually Eliminate Local Law Enforcement Funding, February 8, 2006. The International Association of Chiefs of Police voiced similar opposition to the budget. "The proposed cuts continue the disturbing trend by both the Bush Administration and Congress of significantly slashing the funding for critical state and local law enforcement assistance programs. This proposal brings the total cuts to law enforcement to more than \$2.3 billion since September 11, 2001." International Association of Chiefs of Police, Capital Report, February 6, 2006.

⁹ National Emergency Management Association. Administration Proposes Budget Cuts for Emergency Management Despite Aftermath of Hurricane Katrina, February 6, 2006.

IV. AREAS FOR IMPROVEMENT

Hurricane Katrina demonstrated that federal, state, and local governments lacked adequate plans for preparing for or responding to emergencies. The best way to improve preparation and response efforts for the next disaster will be to reform FEMA's leadership and authority. For example, the FEMA director must be statutorily required to have an extensive background in emergency or disaster-related management.

In addition to reforming FEMA, citizen and community preparedness must be a national priority. Citizen Corps, a program that trains volunteers for use in an emergency, needs more funding.¹⁰ The Department's efforts to enhance school preparedness and evacuation planning efforts also needs improvement.¹¹ Federal efforts in these areas are uncoordinated and many local officials do not know who to turn to for help developing emergency plans.¹²

Finally, the federal government needs one clear emergency response plan that governs all federal agencies and makes cooperation with state and local officials successful. Hurricane Katrina showed that the current NRP does not meet this goal. Although the administration has advocated some reforms to the NRP and more funding for training officials on how to use it, these efforts will need more support and funding.

¹⁰ National Volunteer Fire Council, "NVFC Reaffirms Legislative Priorities for the 109th Congress." *Available at* <http://www.nvfc.org/news/2005-109.html>.

¹¹ Many of the school preparedness grants – like the Emergency Response and Crisis Management Plans Discretionary Grants – are located within the Department of Education's Safe and Drug Free Schools and Communities program (SDFSC). Though SDFSC state grant programs received \$437 million in fiscal year 2005, the program only received \$346 million in funding in fiscal year 2006 – over a \$90 million decrease. In fact, the SDFSC state grant program initially received no money under President Bush's fiscal year 2006 budget proposal. For fiscal year 2007, the Administration again requested no money for the program. See BUDGET OF THE UNITED STATES GOVERNMENT (Fiscal Year 2006), DEPARTMENT OF EDUCATION. *Available at* <http://www.ed.gov/about/overview/budget/budget06/06action.pdf>.

¹² According to a survey conducted by the Minority Staff of the Committee on Homeland Security of the U.S. House of Representatives in February 2006, only eighty-three percent of respondents told the Committee that they know who to ask for help with emergency planning. Thirteen percent of respondents do not know who to ask for help. See COMMITTEE ON HOMELAND SECURITY, U.S. HOUSE OF REPRESENTATIVES, MINORITY STAFF, *Reading, Writing, and Readiness: A Survey of School Emergency Plans in the 2nd Congressional District of Rhode Island*, January 2006. *Available at* <http://hsc-democrats.house.gov/NR/rdonlyres/7377CFCC-682E-453A-B10B-3D3E6966EB8B/0/LangevinSchoolReportFINAL.pdf>.

I. STATEMENT OF PROBLEM HISTORICALLY

In 1996, the Public Safety Wireless Advisory Committee (PSWAC), a blue ribbon committee created by Congress to examine the issue of interoperable communication, concluded that public safety agencies did not have sufficient radio spectrum to communicate with each other when they responded to emergencies. The PSWAC had called for congested spectrum to be cleared by September 11, 2001. Responding to the PISWAC report, Congress included a provision in the Balanced Budget Act of 1997 which called for the Federal Communications Commission (FCC)-to allocate portions of the 700 Mhz spectrum for public safety use by December 31, 2006.

When the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) released its final report, it found that the inability of first responders to talk with each other and their commanders resulted in a loss of life. The 9/11 Commission also identified the need for more spectrum as crucial to assist police, fire fighters and emergency responder communications during an emergency, such as a terrorist attack or a hurricane. Among the findings of the 9/11 Commission report was the fact that firefighters never received the police warning to evacuate the North Tower after the South Tower's collapse because their system was not interoperable with the police communication systems. Lack of interoperable communication also impeded the relay of the message that an open stairwell in the South Tower free of debris and obstruction could be used for evacuation. The report issued by the 9/11 Commission called for "Congress [to] support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes."¹ The report also recommended that federal funding for interoperable communication be given high priority by Congress.²

More recently, the catastrophic Hurricanes Katrina and Rita demonstrated the critical need for operable and interoperable communication. The damage to the communications infrastructure in the four Parishes surrounding and including New Orleans led to the operational failure of the interoperable communications network. During and after the storm, New Orleans communicated through the use of five or fewer mutual aid channels. Congress finally resolved to address the issue in the Fiscal Year 2006 Budget Reconciliation Act by setting a firm date of February 17, 2009 for the return of portions of the 700 Mhz spectrum to public safety.³ The Reconciliation Act further provided that \$1 billion of the monies collected from the auction of spectrum will be available to public safety agencies for equipment and other costs associated with deploying interoperable networks at 700 Mhz.

¹ *Final Report of the National Commission on Terrorist Attacks Upon the United States* at 397 (July 22, 2004).

² *Id.*

³ Public Law 109-171.

II. STATE OF INTEROPERABLE COMMUNICATIONS

In 2002, Project SAFECOM was created by the Presidential Management Initiative as the communications program at the Department of Homeland Security. SAFECOM was charged with strengthening interoperability at all levels of government by coordinating Federal programs, initiating a comprehensive standards program, and developing a national interoperable communications architecture. In 2004, the Department established the Office for Interoperability and Compatibility (OIC), where SAFECOM resides, to help improve Federal, State, local, and tribal public safety preparedness and response.

According to SAFECOM, interoperability directly impacts the first responder community which consists of over 61,000 public safety agencies including 960,000 firefighters, 830,000 EMS personnel, and 710,000 Law Enforcement Officers. The U.S. Conference of Mayors (USCM) conducted a survey of 192 cities regarding their interoperable communications systems in 2004 and found:

- Of the cities with a major chemical plant, 97% reported that they did not have interoperable communications capability between the chemical plant, police, fire and emergency medical services;
- 60% of the cities reported that they did not have interoperable communications capability with state emergency operations centers; and
- 75% of the cities pointed out that limited funding was preventing achieving full interoperable communications capability.⁴

The Office of Management and Budget (OMB) estimated interoperability solutions would cost more than \$15 billion. According to the USCM's 2004 survey on interoperable communications:

- Cities under 100,000 report an average of \$4.7 million in funding to achieve full interoperability,
- Cities of 100,001 to 400,000 require approximately \$5.4 million to achieve full interoperability, and
- Cities over 400,001 reported an average of \$30 million to achieve full interoperability.⁵

With a modest full-time staff of four to seven employees, SAFECOM in January 2005 initiated the National Interoperability Baseline study which it hopes will provide a

⁴ *The U.S. Conference of Mayors Interoperability Survey: A 192-City Survey*, at 5 (June 28, 2004).

⁵ *Id.* at 11.

statistically significant, quantitative measurement of the progress of communities in the area of interoperability. The baseline study is building on the success of its partnership with the Commonwealth of Virginia and the Department of Justice to develop a strategic plan for improving statewide interoperable communications. In addition, SAFECOM is implementing two regional communications interoperability pilots in Nevada and Kentucky, pursuant to Section 7304 of the Intelligence Reform and Terrorism Prevention Act of 2004.⁶

In 2004, SAFECOM coordinated with the Department of Justice's 25 Cities Program, and the Department's Wireless Management Office, to launch RapidCom - a program that assessed the communications interoperability capacity and needs of ten high-risk urban areas. RapidCom worked with the ten urban areas to provide requested assistance to help improve the incident level interoperability capabilities. Congress provided \$5 million in funding to expand RapidCom to other urban areas in the 2006 Department of Homeland Security Appropriations Act.

Project SAFECOM is a model for how the Department should be working with states and local entities on the problem of interoperability. SAFECOM, however, is a small office within the much larger OIC that has not yet elevated interoperable communication as its core function and mission.

III. PRESIDENT'S BUDGET

Although interoperable communications systems remain a critical need for emergency responders, the President's Fiscal Year 2007 Budget requests no funds for grants to enhance interoperability. The President's FY 2007 budget proposes to eliminate the Community Oriented Policing Services (COPS) Interoperability Grants. This key program awards technology grants to law enforcement agencies to enhance interoperability and information sharing. The COPS interoperability grant program was cut significantly in the FY 2006 budget where it was funded at \$10 million, down from \$99 million in FY 2005, when COPS awarded 26 local law enforcement agencies with interoperable communication grants. The City of New Orleans, a recipient of the COPS Interoperability Grant Program, was sixteen months from completing its emergency communications plan when it was struck by Hurricane Katrina.

In contrast, the President's budget proposes a modest \$3.5 million increase for the Office of Interoperability and Compatibility (OIC) in FY 2007, from \$26.2 million to \$29.7 million.⁷ While an increase, it is far less than what is necessary to remedy the weaknesses that were evident with the glaring failure of emergency communication systems during Hurricanes Katrina and Rita, and far from what SAFECOM, with four to seven full-time employees, needs to accelerate the standards and development of interoperable communications equipment.

⁶ Public Law 108-458.

⁷ Department of Homeland Security, FY 2007 Budget in Brief, at 81.

IV. AREAS FOR IMPROVEMENT

Emergency responders at all levels of governments cite the ability to communicate is the most basic function of any response and recovery effort. Interoperable communications would be best achieved if the Department elevated the visibility of the issue by providing the necessary resources to achieve full interoperability. To date, the Department does not have a dedicated interoperability grant program.

The goal of a nationwide interoperable network could best be achieved if the Congress passed authorizing legislation that would provide clear directives and resources to SAFECOM, within the Department. The Department would be best served if it would provided the appropriate resources to SAFECOM to have the dedicated full-time employees, with state and local experienced personnel, who have the background in communications to assist in the process. SAFECOM's success with its projects is due primarily because of that office's use of a "bottom-up" approach to achieving interoperability.

The Department should also make clear that interoperability is the sole responsibility of SAFECOM. Currently the full-time staff of four to seven employees is charged with responsibilities ranging for grant guidance, the development of standards and methodology, the implementation of pilot programs and expansion of the Rapidcom program, research and development, conducting a national interoperability baseline study, and most currently the re-assignment of disaster management from the Federal Emergency Management Agency (FEMA).

Building on the well-received interoperability continuum plan designed by SAFECOM and providing the resources to take the interoperability message nation wide should be another Department priority. Instructional seminars focused at state, local and federal partnerships to develop an exchange of ideas about interoperability projects would prove constructive.

While the Department took the steps of requiring the development of a state-wide communication plan as a condition for homeland security grants, greater efforts need to be made to tie future federal funding to performance measures. The Department should provide technical assistance and embrace the peer group reviews to assist grant applicants. The Department should also reward jurisdictions that have successfully implemented cooperative efforts by citing them as "best-practices" models.

Congress must be willing to provide the long term sustainable funding necessary to develop interoperable communication networks. The Department should develop metrics to assess the investments of federal dollars must measurable results. Additionally, the Department should allow more flexibility in the use of federal public safety funds for upgraded technology communication systems and training.

Finally, the Department needs to improve its ability of tracking the dollars appropriated for the deployment of interoperable communications.

I. STATEMENT OF PROBLEM HISTORICALLY
The Department Has Not Effectively Bridged the Information Sharing Gap Between the Intelligence and Law Enforcement Communities

The hundreds of thousands of law enforcement officers across the country offer the best hope for detecting and preventing terrorist attacks before they occur. Intelligence information about terrorists is useless, however, if we cannot get critical information to the front line police and sheriffs officers who need it most. As Congress recognized in the Homeland Security Act of 2002, those officers observe activities and conditions in the course of their day-to-day work that may be indicators of emerging terrorist plots.¹ They accordingly need at least some “homeland security information” to help prevent attacks.² Federal policymakers nevertheless have failed to develop policies and procedures for converting highly classified intelligence into an unclassified or “less classified” format that the Department of Homeland Security can share rapidly with those officers. They likewise have failed to create a mechanism by which those same officers can effectively share information from the field with the Department and the wider Intelligence Community.

Congress’ original plan was to locate a collaborative intelligence analysis and integration center within the Department. Specifically, it created the Information Analysis and Infrastructure Protection Directorate (IAIP) in order to collect, analyze, and disseminate intelligence information about terrorist threats to state, local, and tribal authorities – including law enforcement.³ In early 2003, however, IAIP ceded most of these functions to the Terrorist Threat Integration Center (TTIC)⁴ which was subsequently folded into the National Counterterrorism Center (NCTC) several months later.⁵ Former Department Secretary Tom Ridge acknowledged IAIP’s diminished status in September 2004 during a hearing before the Senate Governmental Affairs Committee, testifying that the NCTC would take over “a lot” of threat assessment responsibilities from the IAIP.⁶ NCTC today serves as the primary fusion center for all terrorism intelligence analysis and

¹ Homeland Security Act of 2002, Pub. L. No. 107-396, Title VIII § 891(b)(2), (4), 116 Stat. 2155 (2002) [hereinafter Homeland Security Act].

² *Id.*

³ *Id.*, § 201.

⁴ Press Release, The White House, *Fact Sheet: Strengthening Intelligence to Better Protect America* (Jan. 28, 2003), available at <http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html>.

⁵ Press Release, The White House, *Reforming and Strengthening Intelligence Services* (Sept. 8, 2004), available at <http://www.fas.org/irp/news/2004/09/wh090804.html>; Press Release, The White House, *Making America Safer by Strengthening Our Intelligence Abilities* (Aug. 2, 2004) available at <http://www.fas.org/irp/news/2004/08/wh080204-fact.html>.

⁶ Daily Open Source Infrastructure Report, *Department of Homeland Security IAIP Directorate, Daily Open Source Infrastructure Report for 15 September 2004* 10, available at http://www.cargosecurity.com/ncsc/ncsc_dotnet/uploads/DHS_IAIP_Daily_2004-09-15.pdf (Sept. 15, 2004); Dibya Sarkar, *DHS to Push Counterterror Info*, Federal Computer Weekly (Sept. 13, 2004), available at <http://www.fcw.com/fcw/articles/2004/0913/web-ridge-09-13-04.asp>.

integration, leaving the Department – until recently – without much of an intelligence mission to call its own. As James Jay Carafano, a homeland security expert with the Heritage Foundation noted, “If you look at the language in all of the bills, it’s like we forgot there was a Department of Homeland Security, and that it was supposed to play a central role” in intelligence analysis.⁷

During his Second Stage Review testimony before Congress on July 13, 2005, the Secretary appeared to set a new course – announcing the creation of a Chief Intelligence Officer (CINT) to head what has now become the Office of Intelligence and Analysis (I&A). The Secretary described I&A as an analytic entity empowered to coordinate activities and fuse information from all intelligence offices within the Department that accordingly would be able to create a common operations picture.⁸ The Secretary explained that I&A would serve as the primary connection between the Department and the wider Intelligence Community as well as a primary source of information for the Department’s state, local, and private sector partners.⁹

II. THE STATE OF INFORMATION SHARING

Cultural Differences Between the Intelligence and Law Enforcement Communities Continue to Hinder Effective Information Sharing

Among the key goals that CINT Charlie Allen subsequently identified during his October 19, 2005 testimony before the House Committee on Homeland Security was for I&A to act as the primary federal government intelligence information provider on homeland security issues to state, local, and tribal law enforcement officers while advocating on their behalf for access to information within the Intelligence Community.¹⁰ He nevertheless acknowledged the Department’s historical problems with consistent and effective dissemination of information to that community and mentioned that he would attempt to determine what a “communication center” within I&A would cost for Fiscal Year 2007 in order to disseminate intelligence information more promptly.¹¹ He likewise admitted that the Department, the FBI, and others could do “a better job” of sharing information with state, local, and tribal authorities.¹² Finally, he described a plan to expand I&A’s “reports officer program” – an information sharing initiative designed to extract and disseminate intelligence information generated during the day-to-day operations of the Department’s

⁷ Justin Rood, *Analysis: New Counterterrorism Center Proposals Make DHS Intel Efforts ‘Irrelevant’*, Page 15 (Sept. 30, 2004) available at <http://page15.com/2004/09/analysis-new-counterterrorism-center.html>.

⁸ Press Release, Department of Homeland Security, *Secretary Michael Chertoff U.S. Department of Homeland Security Second Stage Review Remarks* (July 13, 2005), available at http://www.dhs.gov/dhspublic/interapp/speech/speech_0255.xml.

⁹ *Id.*

¹⁰ Chief Intelligence Officer Charles Allen, *Written Statement to the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment* (Oct. 19, 2005).

¹¹ *Department of Homeland Security Second Stage Review: Hearing on the Role of the Chief Intelligence Officer Before the House Committee on Homeland Security*, 109th Cong. (2005) (statement of Chief Intelligence Officer Allen).

¹² *Id.*

various intelligence units, including Customs & Border Protection (CBP), Immigration & Customs Enforcement (ICE), and the Transportation Security Administration (TSA).¹³

It is not at all clear, however, that Mr. Allen or I&A have the capability of assessing what intelligence information would be of most use to law enforcement officers. Historically, most intelligence analysis conducted by the Intelligence Community has been destined for high-level federal policymakers – not first responders in the field.¹⁴ Without some input from the people on the frontline, however, the result might be useless data dumps on police and sheriffs’ departments nationwide made in the name of sharing information. “The caveat is to make sure the information in the intelligence products is essential and reaching the right consumer,” Professor David L. Carter, a law enforcement expert, observed.¹⁵ “If law enforcement officers are deluged with intelligence reports, the information overload will have the same outcome as not sharing information at all.”¹⁶ Carter added, “If officers are deleting intelligence products without reading them, then the effect is the same as if it had never been disseminated.”¹⁷ Peter A. Modafferi, Chief of Detectives of the Rockland County, New York, District Attorneys Office, likewise noted that turning homeland security information into specific, actionable intelligence that informs the work of officers in their communities is not solely the task of the Intelligence Community.¹⁸ “We, jointly, have to develop not only policies but also an implementation plan that will bring all law enforcement into the intelligence process,” he stated.¹⁹ “The biggest issue and obstacle to achieving this is not technology but history and culture.”²⁰

Compounding this problem is the fact that the various agencies that comprise the Intelligence Community – including the Department and the FBI – are still not fully cooperating in the information sharing realm. As one commentator observed during a 9/11 Public Discourse Project panel discussion regarding the information needs of state, local, and tribal law enforcement, “[W]hile information sharing has gotten to be considerably better, a lot of police officers, for instance, tell us that the biggest challenge they face is getting the FBI to share information with DHS and getting DHS to share it with them.”²¹ She added, “[T]hey don’t trust this relationship because of this incredible rivalry and turf wars between the two agencies. They’re unclear as to how much information is being shared . . .”²² The Safe Cities Project recently concluded, “Counterterrorism intelligence

¹³ *Id.*

¹⁴ See Deborah G. Barger, *Toward a Revolution in Intelligence Affairs* 21, RAND Corporation, National Security Research Division (2005), available at http://www.rand.org/pubs/technical_reports/2005/RAND_TR242.pdf.

¹⁵ See David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies; Chapter 6: Law Enforcement Intelligence Classification, Products, and Dissemination* 86 (November 2004) (citations omitted), available at <http://www.cops.usdoj.gov/mime/open.pdf?Item=1393>.

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ Telephone Interview with Peter A. Modafferi, Chief of Detectives, Rockland County, New York District Attorneys Office (Nov. 16, 2005).

¹⁹ *Id.*

²⁰ *Id.*

²¹ Chitra Ragavan, *Remarks at the 9/11 Public Discourse Project Panel Discussion on Proposed Changes to the CIA and FBI Following the Recommendations of the 9/11 Commission* (June 6, 2005), available at http://www.9-11pdp.org/ua/2005-06-06_ragavan.pdf.

²² *Id.*

sharing will not be effective until police have a single venue for two-way information sharing between local, state, and federal agencies.”²³ That venue accordingly must cut through the cultural barriers that presently impede effective information flows.

III. PRESIDENT’S BUDGET

Despite the organizational separation of I&A and the Directorate of Operations, the President’s budget request lumps the two offices together in order to avoid public disclosure of I&A’s classified budget and personnel numbers. Collectively, the President seeks \$298.663 million for both offices, along with 475 employees – an increase of 18% in combined funding (\$45.723 million more than the \$252.94 million enacted for Fiscal Year 2006) and an additional 69 employees (over the Fiscal Year 2006 enacted 406 FTE total). While these numbers are an improvement over Fiscal Year 2006, they were in large part developed prior to Mr. Allen’s arrival at the Department and prior to the announcement of his information sharing initiatives. Mr. Allen’s priorities in this regard should be fully funded on a going forward basis as should the Vertical Intelligence Terrorism Analysis Link (VITAL) Program described below.

IV. AREAS FOR IMPROVEMENT

I&A Needs a State, Local, and Tribal Law Enforcement Voice That Informs Its Information Sharing Process

I&A would be well-served by developing an information sharing program similar to what authorities in the United Kingdom (UK) have established at their new Joint Terrorism Analysis Centre (JTAC). JTAC is an entity that brings all of the UK’s intelligence agencies together under one roof to fuse and share intelligence information.²⁴ It is staffed by intelligence and law enforcement officers who, among other things, not only identify intelligence of interest to police officers but also work to convert it to a usable format.²⁵ JTAC does this work with the assistance of the Police International Counterterrorism Unit (PICTU) which is the voice of local police departments to the UK Intelligence Community.²⁶

Like JTAC, the National Counterterrorism Center (NCTC) brings all of our intelligence agencies together under one roof to jointly analyze intelligence information.

²³ Safe Cities Project, *Hard Won Lessons: Problem-Solving Principles for Local Police* 6 (May 2005) [hereinafter Safe Cities Project Report], available at http://www.manhattan-institute.org/pdf/scr_02.pdf.

²⁴ Frank Gregory, *Intelligence-Led Counter-terrorism: A Brief Analysis of the UK Domestic Intelligence System’s Response to 9/11 and the Implications of the London Bombings of 7 July 2005*, Real Instituto Elcano (2005), available at <http://www.realinstitutoelcano.org/zonas analisis.asp?zona=7&version=2&publicado=1>.

²⁵ Keith Weston, Police International Counter Terrorism Unit (PICTU) Background Document 3 (Aug. 19, 2005) (unpublished manuscript, on file with author) [hereinafter Weston Document]; Email from Keith Weston, Detective Chief Superintendent of Police International Counter Terrorism Unit (PICTU) to Committee Staff, House Committee on Homeland Security (Aug. 19, 2005, 04:34:00 EDT) (on file with author).

²⁶ Weston Document at 2-3.

We do not have any entity similar to PICTU, however, through which state, local, and tribal law enforcement officers can voice their needs and concerns to their federal partners. I&A accordingly should develop a PICTU-like initiative – called the VITAL Program – that would be operated within the I&A analysis shop itself. The VITAL Program would be staffed by state, local, and tribal law enforcement officers who would rotate periodically through I&A and who would have the same access to NCTC intelligence as I&A analysts.

Participating officers could educate I&A staff about what information is actually of interest to law enforcement in terms of thwarting terrorist attacks. Participating officers likewise could work with I&A staff to convert highly classified documents to an unclassified format that could be disseminated widely. Furthermore, the VITAL Program would not only help get such “sanitized” intelligence information to the officers in the field who need it, but also would be a mechanism for those officers to share information from the field with the Department. Accordingly, it would go a long way toward addressing the nation’s information sharing shortcomings.

I. STATEMENT OF PROBLEM HISTORICALLY

A bioterrorist attack on the United States could have devastating consequences. Furthermore, bioterrorism and naturally occurring biological events, such as a SARS or avian influenza pandemic, could possibly be indistinguishable. As such, our biodefense should be constructed using an “all hazards” approach. Unfortunately, as the current scramble to prepare for a possible avian influenza pandemic demonstrates, the federal government is not prepared for a biological emergency—whether natural or manmade.

II. THE STATE OF BIOSECURITY TODAY

Our nation’s biodefense capabilities are measured by the adequacy of bio-intelligence, bio-surveillance, countermeasures, and emergency planning within the Department of Homeland Security and other agencies.

Biointelligence and biosurveillance are the early warning systems necessary to detect the spread of disease, whether natural or intentional. Unfortunately, these systems are not adequately developed. For example, the United States needs to develop more international cooperation to conduct bio-surveillance. Although the H5N1 strain of avian influenza has been infecting humans since 1997, China was able to temporarily hide the level of its recent outbreaks from the United States and the international community.¹

Biological countermeasures are needed to protect and mitigate the effects of a biological incident. Project Bioshield (P.L. 108-276) is the primary federal program for developing biological countermeasures². Unfortunately, it has not lived up to expectations. To date, Project BioShield has only awarded contracts for treating anthrax and radiological sicknesses,³ even though the CDC has listed over 30 “select agents” of concern for possible bioweapons.⁴ While the real bottleneck in the process seems to be the Department of Health and Human Services, the Department of Homeland Security has still only completed six Material Threat Assessments (MTAs),⁵ the first step in the BioShield process.

¹ Tiaji Salaam-Blyther and Emma Chanlett-Avery, CRS Report 33219, *US & International Responses to Avian Flu – Issues for Congress*, at 18 (January 11, 2006) (noting international health experts continue to question Chinese transparency and referring to a specific possible outbreak in April 2005 which was not disclosed, but reported by Hong Kong virologists and the Washington Post months later).

² Frank Gottron, CRS Report RS21507, *Project BioShield*, (June 10, 2005)

³ DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF RESEARCH AND DEVELOPMENT COORDINATION, *Project BioShield Related Procurement Projects*, available at <http://www.hhs.gov/ophep/bioshield/PBPrctPrjct.htm>.

⁴ CENTERS FOR DISEASE CONTROL AND PREVENTION, *Agents, Diseases, and Other Threats*, available at <http://www.bt.cdc.gov/agent/>.

⁵ Information provided to the House Homeland Security Committee Minority Staff by DHS Office of Legislative affairs.

Finally, it is not clear who is in charge in the event of a biological event like a bioterrorist attack or pandemic flu. For example, there are many “influenza response plans” circulating at present. It is not clear how these plans would interact with the National Response Plan (NRP), which was created by presidential order to serve as the blueprint for federal responses to “incidents of national significance.”

III. PRESIDENT’S BUDGET

The President’s fiscal year 2007 budget wholly fails to recognize the threat of a bioterrorist attack or a naturally occurring disease outbreak.

In the area of biointelligence and biosurveillance, the National Biosurveillance Integration System (NBIS), which is designed to integrate biothreat and biosurveillance information, was cut from \$14 million to \$8.2 million. Without more funds, the NBIS will not be prepared to monitor for an attack or outbreak.

The President’s budget also fails to adequately fund key countermeasures programs. For example, the budget cuts funding from the Biological Countermeasures Portfolio by \$39 million, even though these funds are used for the development and deployment of environmental biosensors and to conduct Material Threat Assessments as part of Project BioShield.⁶ Even the newly created Chief Medical Officer, who is responsible for the final approval of all procurements under Project BioShield and is also the point person within the Department for avian influenza preparedness, only receives a total of \$5 million and 15 full-time-employees.⁷

The President’s budget also fails to fully fund biological preparedness and response programs. For example, the National Disaster Medical System, which consists of thousands of volunteer medical professionals ready to be deployed in the event of a disaster, is essentially flat-funded, even though the dramatic \$50 million cut it received between 2004 and 2005 affected its performance during Hurricane Katrina. Additionally, the Metropolitan Medical Response System (MMRS), which helps medical systems in major metropolitan areas prepare for catastrophic emergencies, has been completely zeroed out in the budget.⁸

IV. AREAS FOR IMPROVEMENT

First, a robust biointelligence and biosurveillance capability must be developed. Better connections must be created between the various entities at the Department of Defense, Department of Homeland Security, Centers for Disease Control and Prevention, World Health Organization, academia, state agencies and others that have some capability

⁶ *Id.*

⁷ Budget In Brief, Department of Homeland Security, FY 2007

⁸ *Id.*

in this area. Additionally, the NBIS attempts to fuse many of these sources of information, but it needs more support to succeed.

Second, Project Bioshield, which was created in order to promote development of vaccines and other medical countermeasures, must either be fixed or replaced with a program that will achieve this objective.

Even if the capacity to develop vaccines and countermeasures is strengthened, better planning is needed to distribute these protections or treat those who are exposed. For example, the medical infrastructure in the United States – especially hospitals – is insufficiently prepared for the large influx of patients that would occur during an avian influenza pandemic or biological attack.⁹ More efforts also need to be made to coordinate response plans both horizontally across the federal government as well as vertically from federal to state and local governments.

⁹ Lewis Rubinson *et al.*, *Augmentation of hospital critical care capacity after bioterrorist attacks or epidemics: Recommendations of the Working Group on Emergency Mass Critical Care*, 33 *Critical Care Medicine* 10 (2005).

I. STATEMENT OF PROBLEM HISTORICALLY

The Department of Homeland Security, while responsible for protecting America's critical infrastructure under Homeland Security Presidential Directive 7,¹ does not actually have any authority to ensure that chemical plants, or any critical infrastructure sector, have adequate security. Both Secretary Michael Chertoff and former Secretary Tom Ridge recognized this problem. In October 2002, then-DHS Secretary Ridge and then-EPA administrator Christie Whitman declared in a joint statement: "Voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve."²

Two and a half years later, during his appearance before the House Committee on Homeland Security in April 2005, Secretary Chertoff stated, "In the area of chemical plants, the President has indicated that if we could not get what we need in terms of security using these various kinds of market-based incentives and best practices, that we would look to the possibility of some kind of regulation."³

II. STATE OF CHEMICAL PLANT SECURITY TODAY

The overall state of chemical plant security today should be of concern to all Americans. Some facilities are voluntarily pursuing security enhancements, yet others have simply not increased their security precautions enough to stop a terrorist attack. As chemical plant security specialist Sal DePasquale stated in testimony before the House Committee on Homeland Security in June of 2005, "Surely we can do better than the mediocre and ineffectual practices that exist today...Although industry claims it has invested considerably in security since September 11, the investments have been little more than window dressing."⁴

The Government Accountability Office (GAO) agrees with Mr. DePasquale. In testimony before the Senate Committee on Homeland Security and Governmental Affairs in April 2005, GAO stated, "About 1,100 facilities participate in a voluntary industry effort in which they assess vulnerabilities, develop security plans, and undergo a third party verification that the facilities implemented the identified physical security enhancements.

¹ HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, available at <http://www.fas.org/irp/offdocs/nspd/hspd-7.html>.

² James V. Grimaldi, *Fearing Litigation, EPA Treads Lightly with Chemical Industry, Despite Terror Threat*, WASHINGTON POST (March 24, 2003).

³ Testimony before the House Committee on Homeland Security Hearing: "The Department of Homeland Security: Promoting Risk-Based Prioritization and Management," April 13, 2005.

⁴ Testimony before the House Committee on Homeland Security Hearing: "Preventing Terrorist Attacks on America's Chemical Plants," June 15, 2005.

The extent to which the remaining facilities are addressing security is unclear and the extent of chemical facilities' security preparedness is unknown.”⁵

In November 2003, *60 Minutes* completed an investigation of security at chemical plants in urban areas. The investigators "found gates unlocked or wide open, dilapidated fences and unprotected tanks filled with deadly chemicals that are used to manufacture everything from plastics to fertilizer." Regarding one plant, *60 Minutes* noted, "There was an open gate right in front of the most dangerous chemicals at the plant. We made it in, with plenty of time to find what they were looking for.”⁶

III. PRESIDENT'S BUDGET

The President's budget request includes \$10 million for a Chemical Site Security Office within the Preparedness Directorate. The office is supposed to “classify facilities into risk-based tiers, establish security standards for each tier, and ensure strong safeguards are in place to protect the public disclosure of any sensitive information gathered by the Office.”⁷ These activities are supposed to be carried out by the existing Office of Infrastructure Protection, so the budget request merely specifies that efforts specific to chemical plants will be given a special focus.

IV. AREAS FOR IMPROVEMENT

While the Office for Chemical Site Security is a good one, it is critical that the office receive necessary authority to accomplish its mission.

Additionally, the development of analytical metrics to properly categorize the risk posed by any specific plant has been a great improvement as well. The use of the Risk Assessment Methodology for Critical Asset Protection (RAMCAP) has allowed the quantification of threat, vulnerability, and consequence factors to be taken into account in a rational and systematic way. These metrics are of little use, however, if the information they provide is not acted upon. Under current law, the Department of Homeland Security does not even have the authority to enter a chemical facility. While the Department is providing guidelines and recommendations for security practices, according to the GAO, only a small fraction of plants, 7%, are following industry suggested (not imposed) guidelines.⁸ What is needed is to give the Department of Homeland Security the regulatory authority necessary to ensure that chemical plants put the necessary security practices in place.

Bob Stephan, the Assistant Secretary for Infrastructure Protection reaffirmed this recently in an interview with Congressional Quarterly. “Business writ large has made a lot of improvements, but the progress has not necessarily been even across the board,” Stephan

⁵ GOVERNMENT ACCOUNTABILITY OFFICE, *Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action is Needed* (GAO-05-631T) (April 27, 2005) (GAO Report).

⁶ CBS 60 Minutes (November 14, 2003).

⁷ Budget in Brief, Department of Homeland Security, FY 2007.

⁸ See GAO Report, *supra* note 5.

said. “We have to take care of that.”⁹ Chemical plant security has been addressed on a bipartisan basis in the Senate by, Senators Susan Collins and Joseph I. Lieberman who introduced S. 2145, the Chemical Facility Anti-Terrorism Act of 2005. Similar legislation should be introduced and passed in the House of Representatives.

Once such legislation is passed, we expect the Department to move quickly to promote a risk-based regulatory structure that clearly lays out the security performance requirements necessary for each chemical facility, and that the Department will ensure that all chemical plants fulfill those security requirements.

⁹ Benton Yves-Halperin, *DHS Budget Request May Portend New Authority Over Chemical Security*, CONGRESSIONAL QUARTERLY HOMELAND SECURITY (February 22, 2006), available at <http://homeland.cq.com/hs/display.do?docid=2054309&sourceType=31&binderName=news-all>.

I. STATEMENT OF PROBLEM HISTORICALLY

The private sector owns and operates more than 85 percent of the critical infrastructure in the United States. Former President Bill Clinton, recognizing the vulnerability of this infrastructure issued Presidential Decision Directive 63 on May 8, 1998. The President's intent in issuing this Directive was to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures."¹ Three years later, terrorists attacked the World Trade Center and the Pentagon.

In the months after the tragic attacks, Congress created the Department of Homeland Security (Department). In the Homeland Security Act (HSA), Congress charged the new Secretary with developing a "comprehensive national plan for securing the key resources and critical infrastructure of the United States . . . and the physical and technological assets that support such systems."² This plan and others required by President George W. Bush have yet been completed. The Department is still making plans to make plans.

II. STATE OF CRITICAL INFRASTRUCTURE PROTECTION TODAY

Critical infrastructure includes our drinking water, the food we eat, the gas we use to drive our cars, and the subways that we use to get to work. This infrastructure is vital to our everyday lives. If our food is tainted, our water poisoned, or our subways attacked, we as Americans will suffer unimaginable costs. 9/11 was only a preview of what could happen if terrorists successfully attack the critical infrastructure of the United States.

Although the President required the completion of the National Infrastructure Protection Plan by December 2004,³ the Department was working on the plan when terrorists attacked the London metro system and when Hurricane Katrina made landfall in New Orleans. The plan will not be completely finished for another six months.

In its final report issued on December 5, 2005, the 9/11 Commission gave the Administration a "D" for fulfilling its recommendations for critical infrastructure security and vulnerability assessments.

¹ Presidential Decision Directive 63, *Critical Infrastructure Protection*, available at <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

² Homeland Security Act, P.L. 107-296, Section 201(d)(5). Under this Section, the Assistant Secretary for Infrastructure Protection and Information Analysis was responsible for completing this task.

³ Homeland Security Presidential Directive -7, *Critical Infrastructure Identification, Prioritization, and Protection*, available at: <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>.

*A draft National Infrastructure Protection Plan spells out a methodology and process for critical infrastructure assessments. No risk and vulnerability assessments actually made; no national priorities established; no recommendations made on allocation of scarce resources. All key decisions are at least a year away. It is time that we stop talking about setting priorities, and actually set some.*⁴

The Department has also failed to create a National Asset Database that effectively catalogues critical infrastructure in the U.S. The current database contains 80,000 critical and non-critical assets such as shopping malls and local banks.⁵ Members of Congress – on both side of the aisle – have referred to the asset database as a “joke.”⁶ The government has only a finite number of resources that it can use in protecting our nation against terrorist attacks and natural disasters. There must be better management of the resources and tools that are used.

III. PRESIDENT’S BUDGET

The President’s fiscal year 2007 budget increases funding to complete the NIPP and critical infrastructure identification, but it does not provide any increases in funds for securing this infrastructure. In fact, the President proposed consolidating all critical infrastructure protection grants into one pool – known as the Targeted Infrastructure Protection Program – which will require ports, chemical plants, and other critical infrastructure to compete against each other for scarce resources.

IV. AREAS FOR IMPROVEMENT

The Department must make a drastic change in course. The inability to finish critical protection plans directly impacts the security of our nation’s critical infrastructure. The Department must complete work on the National Infrastructure Protection Plan, the National Asset Database, and other critical security plans. Additionally, more dedicated funding must be provided to secure ports, chemical plants, mass transit, and other critical infrastructure.

⁴ 9/11 Public Discourse Project, *Final Report on 9/11 Commission Recommendations*. <http://www.9-11pdp.org> (December 5, 2005).

⁵ Robert Liscouski, *Task of securing U.S. is complex, ongoing*, USA TODAY page 19A (December 15, 2004).

⁶ Mimi Hall, *Terror Security List Way Behind*, USA TODAY page 1A (December 9, 2004)

I. STATEMENT OF PROBLEM HISTORICALLY

Maintaining the integrity of our computer networks and systems has never been more important than it is today. Most Americans are dependent on the Internet, as well as its underlying structure for business and personal transactions of every kind. Here in the United States, federal, state, and local governments provide a variety of services – from running dams and power plants to maintaining court dockets – all using networked infrastructure and technology. Because of our reliance on these systems, disruptions in service, whether by virus, theft, or malicious command and control can and do have disastrous effects. For instance, in 2000, the “Love Bug” email virus cost the global economy an estimated \$8 billion.¹ Beyond economic costs, cyber attacks can have serious environmental consequences. An Australian hacker was able to send millions of liters of raw sewage into local waterways by changing the computerized valve settings of a local sewage plant.² Attacks may also threaten our national security. A series of coordinated attacks on American computer systems since 2003 – designated “Titan Rain” by the U.S. government – were most likely the result of Chinese military hackers attempting to gather information on U.S. computer networks, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA.³

To coordinate protection of the computer systems that support our nation’s critical infrastructure, the Homeland Security Act of 2002 established the Department of Homeland Security.⁴ The Department is responsible for preparing our nation for cyber threats, working with the private sector to protect our national cyber infrastructure, and responding to and recovering from cyber attacks on that infrastructure.⁵ The Department created the National Cyber Security Division (NCSA) to achieve those tasks.

¹ Laton McCartney, *Battling the Bad Guys: Worms and Anti-Worms Get Smarter*, Baseline Magazine, Dec. 13, 2005. Available at <http://www.baselinemag.com/article2/0,1397,1901716,00.asp>. Cost estimate provided by Mark A. McManus, vice president of technology and research at Computer Economics.

² Michael Crawford, *Conference tackles critical infrastructure issues*, COMPUTERWORLD TODAY (Australia), Feb. 10, 2006. Available at <http://www.itnetcentral.com/computerworld/article.asp?id=15539&leveli=0&info=Computerworld>. The attack on Queensland’s Maroochy Water Services in April 2000 saw multiple pump station shutdowns sending millions of litres of raw sewage spilling into local parks, rivers and the grounds of hotel resorts. After an extensive investigation, an ex-employee was found guilty of hacking into the SCADA control system. He was later fined and sentenced to two years in jail.

³ Nathan Thornburgh, *The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)*, TIME, Sep. 5, 2005. Available at <http://www.time.com/time/archive/preview/0,10987,1098961,00.html>.

⁴ P.L. 107-296.

⁵ *Id.* at §293.

II. STATE OF CYBER SECURITY TODAY

Since its creation in 2003, the Department has made limited progress towards securing our nation's cyber infrastructure. The NCSO established the United States Computer Emergency Readiness Team (US-CERT), to coordinate federal, state and local government preparedness and response to cyber security incidents. US-CERT maintains a Cyber Watch Center operating 24 hours a day that detects, analyzes, and responds to cyber events.⁶ Unfortunately, a national indications and warning architecture for infrastructure protection remains incomplete.

NCSO has undertaken several initiatives to foster partnerships and enhance information sharing between the public and private sectors and across all three levels of government. For instance, NCSO is also partnering with the various Information Sharing and Analysis Centers (ISACs), each representing a different critical sector, and the Multi-State ISACs (MS-ISAC), an information sharing organization among representatives of state and local governments, to analyze and disseminate information pertaining to cyber events and vulnerabilities to ISAC members and private industry. Unfortunately, the Department continues to struggle with its outreach efforts, and “has not effectively leveraged its partnerships to increase the sharing of information.”⁷ According to *Government Security News*, the Department's “failure to use its ‘bully pulpit’ on behalf of the ISACs comes amid continued confusion and turmoil over the centers’ relationships with the federal government.”⁸ In addition, the General Accountability Office (GAO) found flaws with the Department's information sharing mechanisms in a 2004 report prepared for the then-Select Committee on Homeland Security. The GAO found that the Department lacked “policies and procedures to ensure effective coordination and sharing of ISAC-provided information among the appropriate components.”⁹

The Department has created private-sector lead “sector-coordinating councils” to facilitate information sharing and sector cooperation.¹⁰ Currently, the GAO is reviewing these councils to determine what role they play in relation to the ISACs and information sharing. The GAO's findings will shed light on how successful the Department has been in this area.

The Department participates in cyber training and education, though on a limited basis. NCSO co-sponsors efforts to train professionals and recent graduates. The Centers of Academic Excellence in Information Assurance Education (CAEIAE) is designed to improve the nation's pool of educated information assurance professionals to help prepare for, mitigate, respond to, and

⁶ Homeland Security Fact Sheet: Protecting America's Critical Infrastructure – Cyber Security. Available at http://www.us-cert.gov/press_room/050215cybersec.html.

⁷ GOVERNMENT ACCOUNTABILITY OFFICE, *Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities* 28 (May 2005) (Cybersecurity Challenges Report).

⁸ Martin Edward Andersen, “Sector-wide ISACs have both critics and advocates,” *Government Security News*, Apr. 26, 2005. Available online at <http://www.offnews.info/verArticulo.php?contenidoID=1160>.

⁹ Government Accountability Office, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, (July 2004) (Improving Information Sharing Report).

¹⁰ U.S. Congress, House of Representatives, Committee on Science, *Cybersecurity: U.S. Vulnerabilities and Preparedness*, Testimony of Donald A. Purdy, 109th Cong., 1st sess., 15 September 2005. Retrieved online at <http://www.house.gov/science/hearings/full05/sept15/Purdy%20Testimony%20Final.pdf>.

recover from cyber attacks. NCSD is also a co-sponsor of the National Science Foundation Scholarship for Service Program, known as “Cyber Corps,” to expand the ranks of the federal cyber workforce by providing scholarship grants to CAEIAE and other universities to fund information assurance education in return for student commitments to work for the federal government for two years.¹¹ Unfortunately, the Department “co-sponsors” these efforts in name alone. Scholarships are funded entirely by the National Science Foundation.¹²

Lastly, the NCSD is engaged in measuring response capacity through national and regional cyber exercises. In October 2003, the agency participated in Livewire, the first-ever national-level cyber exercise to baseline government’s capabilities for responding to national cyber attack. More recently, in February 2006, the agency conducted its “Cyber Storm” exercise, a test of federal and private sector preparedness in the event of a cyber attack.¹³ The Department now must work quickly to release lessons learned to the participants. It must also better engage academic and private sector entities who have been conducting operational cyber exercises for communities and businesses. It is not clear that the Department has clearly integrated these efforts into their programs.

In spite of some encouraging developments, much work remains. A Government Accountability Office (GAO) report issued in May 2005 detailed the Department’s shortfalls in meeting thirteen key responsibilities contained in the Homeland Security Act, the Homeland Security Presidential Directive 7 (HSPD-7) and the *National Strategy to Secure Cyberspace*.¹⁴ Unfortunately, the Department lacks clear leadership in the field of cyber security. In July 2005, after significant pressure from Congress and the private sector, Secretary Michael Chertoff announced the creation of an Assistant Secretary for Cyber Security and Telecommunications, a position that would have the authority to set policy and improve partnerships with private industry. Unfortunately, the position remains unfilled. Furthermore, for the last sixteen months, the NCSD has been led by an acting director. Failure to find permanent replacements for both positions raises serious concern about the Department’s ability to lead the nation in securing cyberspace.

III. PRESIDENT’S BUDGET

The President’s fiscal year 2007 budget request represents a \$210,000 decrease for the National Cyber Security Division (NCSD), although the cyber security budget within the Science and Technology Directorate receives a \$6.2 million increase from fiscal year 2006.¹⁵ Under the President’s budget, the NCSD receives \$92.205 million, down from \$92.415. This decrease came as

¹¹ Homeland Security Fact Sheet: Protecting America’s Critical Infrastructure – Cyber Security. Available at http://www.us-cert.gov/press_room/050215cybersec.html.

¹² Federal Cyber Service: Scholarship for Service. Available at <http://www.sfs.opm.gov/default.asp>.

¹³ Press Release, DEPARTMENT OF HOMELAND SECURITY, *DHS Conducts First Full-Scale Cyber Security Exercise to Enhance Nation’s Cyber Preparedness* (Feb. 10, 2005). Available at <http://www.dhs.gov/dhspublic/display?content=5410>.

¹⁴ Cybersecurity Challenges Report, *supra* note 7.

¹⁵ Budget of the United States Government (Fiscal Year 2007), Department of Homeland Security, Preparedness Directorate 32; Science and Technology Directorate 98.

a surprise to the NCSA since Acting Director Andy Purdy had predicted that the budget for his organization would grow by \$25 million in fiscal 2007.¹⁶

Many observers believe that the Department's spending should focus more on research and development. Though the President's budget reduces funding within NCSA, it does provide the Science and Technology Directorate with \$22.733 million for cyber security research and development, a \$6.2 million increase from the previous year.¹⁷

IV. AREAS FOR IMPROVEMENT

The Department must demonstrate a sustained commitment to protecting cyberspace. "Cyber security clearly fell off the radar screen when they set up the Department, and the Department is trying to find its way," said Paul Kurtz, president of the Cyber Security Industry Alliance.¹⁸ The Department faces significant impediments in achieving its mission due to organizational instability.

It is difficult for the NCSA to effectively establish national cyber policy and for the public and private sectors to develop strategic partnerships with the Department under transient leadership. The GAO noted this problem in 2005, reporting that the Department has been slow to develop a national plan for critical infrastructure protection related to cyber security.¹⁹ In February 2005, the Department issued the Interim National Infrastructure Protection Plan (NIPP), a strategy for protecting critical infrastructures by conducting vulnerability assessments and establishing performance metrics. Unfortunately, the sector specific plans – that is, the detailed plans for protecting public and private cyber infrastructure throughout the country – will not be released until sometime in the fall of 2006. Each day that passes is another day that our infrastructure – including dams, power plants, and electric utilities – is less secure than it should be. Furthermore, countless private sector representatives have expressed frustration with their role in advising the Department in drafting the NIPP.²⁰ Because the private sector owns eighty-five percent of cyberspace, it is imperative that they work closely with the Department in achieving these goals.

¹⁶ Andy Purdy reported in January 2006, weeks before the budget was released, "We are pleased with the increase." Patience Wait, *DHS cyber security budget grows to fight computer crime*, GOVERNMENT COMPUTER NEWS (Jan. 26, 2006).

¹⁷ According to Marcus Sachs, Deputy Director of SRI International, the Science and Technology budget is an area in need of increased cyber spending. "Classic cyber security funding organizations seem to be getting more plus-ups while DHS/S&T is always forgotten. We need to dramatically increase what we are spending on transitioning basic cyber security research through the development, testing, evaluation, and deployment phases. DHS/S&T is the right place to do that, but they need help." Email on file with committee.

¹⁸ Declan McCullagh, *U.S. Cybersecurity due for FEMA-like calamity?*, NEW YORK TIMES (Oct. 10, 2005).

¹⁹ Cybersecurity Challenges Report, *supra* note 7.

²⁰ As the Internet Security Alliance noted in its draft comments, the private sector was not considered as a true partner in the effort: "We all know the private sector owns and operates the vast majority of the systems that make up cyber space. The private sector is not a down-stream 'stake-holder' in the effort to secure cyber space. If the NIPP is to be successful with respect to cyber security, the private sector must be recognized as a full and equal partner in its defense. If the private sector could be recruited as a full partner in the overall effort, including planning and operations, it could dramatically expand the resource base that would be available to secure cyber space." Comments of the Internet Security Alliance on the National Infrastructure Protection Plan v. 2.0, issued to the Department of Homeland Security in February 2006.

The Department is also experiencing difficulty developing partnerships with state and local governments. Surveys and reports issued in January 2006 by the National Association of State Chief Information Officers (NASCIO), the Metropolitan Information Exchange (MIX), and the Minority Staff of the House of Representatives Committee on Homeland Security found weaknesses in the relationship between state and local officials and the Department.²¹ NASCIO issued five strategic recommendations and eighteen lesser recommendations from NASCIO to the Department on ways to improve cyber security and relations between the information officers and the Department. For the Department to demonstrate a commitment to both the public and private sectors, it must fill its leadership positions with qualified personnel who bring a national outlook on securing cyberspace.

²¹ “I wouldn’t say the DHS has dropped the ball as much as it has neglected to make this a priority,” said Denise Moore, CIO of the state of Kansas. As a result, the DHS is rarely the go-to agency on cyber security issues, said Larry Kettlewell, the Kansas CISO. “We’ve had a couple of experiences here in Kansas where, frankly, the federal government wasn’t my first go-to. My first go-to was more out in the private sector” because of their greater expertise and experience in dealing with cyber threats, he said. Jaikumar Vijayan, *DHS cyber security efforts lacking; surveys find State, local CISOs seek more support from federal agency*, Computerworld (Jan. 26, 2006).

I. STATEMENT OF PROBLEM HISTORICALLY

Research and development of new technologies to strengthen homeland security is conducted by the Department of Homeland Security's Science and Technology Directorate (S&T). The S&T Directorate is also responsible for coordinating with research programs of other agencies, such as the Department of Energy's national laboratories and the Department of Health and Human Service's Project Bioshield.¹ The S&T Directorate has made advances, but has experienced significant problems in many areas, especially in producing technological solutions without delay.

II. STATE OF HOMELAND SECURITY SCIENCE & TECHNOLOGY TODAY

The S&T Directorate has been successful in a number of areas. For example, the first generation of environmental biosensors are deployed in over 30 cities across the country, and the second generation of biosensors have been deployed in 10 cities.² Pilot programs are expected in 2008 for the third generation of biosensors, which will be fully automated and offer higher resolution and dramatically reduced detection times (4-6 hours compared to 24).³ The S&T Directorate should also be commended for progress in nuclear detector development, chemical countermeasures production, and the founding of five University Centers of Excellence funded by the Homeland Security Advanced Research Projects Agency (HSARPA).⁴

On the other hand, the S&T directorate has failed to develop technological solutions to close serious security gaps. For example, although the S&T Directorate has made progress in developing counter-MANPADS to protect large aircraft like 747s from shoulder mounted missiles, most domestic flights are not made in these large planes, but in smaller, yet still very sizable aircraft, like 737s, the most widely used passenger airplane worldwide. The S&T Directorate has also struggled to fulfill its responsibility for making Material Threat Assessments (MTA), the first step in the Project Bioshield process designed to create countermeasures for a biological attack. To date MTAs have been completed for only 4 threats—botulinum toxin, anthrax, plague, chemical nerve agents, and radiological materials—even though there are approximately 30 high risk threats.⁵ The process

¹ Genevieve J. Knezo, CRS Report 21270, *Homeland Security Research and Development Funding, Organization, and Oversight* (November 9, 2005).

² *Department of Homeland Security Staff Briefing Before the House Committee on Homeland Security: Biological and Chemical Countermeasures in the S&T Directorate* (February 9, 2006) (Statements of Dr. John Vitko, Director, Biodefense RDT&E portfolio, and Robert Hooks, Deputy Director, Office of Research and Development).

³ *Id.*

⁴ Knezo, *supra* note 1.

⁵ Information provided to the Homeland Security Committee by DHS Office of Legislative Affairs.

typically takes 6-9 months per assessment, though S&T hopes to streamline the process to complete MTAs within four months.⁶ S&T appears to lack necessary funding to complete multiple MTAs.⁷

III. PRESIDENT'S BUDGET

The President's Fiscal Year 2007 budget request for the S&T Directorate is \$1.002 billion, compared to \$1.467 billion last year, a reduction of 32%.⁸ \$337 million of this reduction, however, is due to the movement of the Domestic Nuclear Detection Office (DNDO) and the radiological and nuclear countermeasures program to other sections of the Department. Another \$104 million of the cut can be attributed to the completion of the counter-MANPADS program. Leaving aside these three programs, the President's budget still cuts the S&T Directorate's remaining programs by \$24 million – 2.3% – compared to the amounts they received in fiscal year 2006.⁹

The S&T Directorate's problems may also be related to the lack of funding for full-time federal employees (FTEs) and an over-reliance on outsourcing to contractors. In Fiscal Year 2006, 387 full-time-employees were authorized for the Directorate.¹⁰ At present, only 195 of those FTE positions are actually filled.¹¹ The President's budget request for Fiscal Year 2007 continues this reliance on contractors by asking for funding for only 383 FTEs.¹² While there are some advantages in using contractors from time to time, the S&T Directorate needs more institutional knowledge in order to fulfill its research and development duties.

Finally, the budget does not break down according to the four major offices within the S&T directorate: Office of Plans Programs and Requirements (PPR); Office of Research and Development (ORD); the Homeland Security Advanced Research Project Agency (HSARPA); and the Office of Systems Engineering and Development (SED). Instead, they are broken down by portfolio, making it difficult to determine just who is in charge of what.

IV. AREAS FOR IMPROVEMENT

The S&T Directorate must develop an overall strategy for research, development, testing and evaluation. The Directorate's work must be mission-driven, not process-driven as it is presently. More strategic planning will resolve many of the Directorate's problems fulfilling long-term projects, such as MTAs. HSARPA must be given more ability to take

⁶ *Id.*

⁷ *Id.* at note 2.

⁸ Budget in Brief, Department of Homeland Security, FY 2007.

⁹ *Id.*

¹⁰ *Department of Homeland Security Staff Briefing for House Committee on Homeland Security: Science and Technology Directorate FY 07 Budget Briefing* (February 8, 2006) (statements of Kurt Hahn, S&T Budget Officer and Carol Dunham, S&T CFO).

¹¹ *Id.*

¹² *Id.*

risks in research, if it is to be as successful as DARPA, the agency within the Pentagon which it is modeled on. Finally, serious attention must be given to employee development and retention in order to build the sense of mission, skill sets, and institutional knowledge the S&T Directorate needs to fulfill its mission.

**I. STATEMENT OF PROBLEM HISTORICALLY:
The Department's Privacy Officer Has Played A Key Role in Bolstering
Public Confidence in the Department But Has Too Often Been Ignored**

In the wake of 9/11, Congress moved to make the most sweeping changes to the federal government's structure since 1947 when President Truman merged the War and Navy Departments into the Department of Defense.¹ The result was the creation of the Department of Homeland Security in the Homeland Security Act of 2002.

Not forgetting that homeland security is about reserving our citizens' most basic rights, privileges, and liberties, Congress included in the Act the first statutorily required Privacy Officer. This position, among other things, is responsible for ensuring that all new Department technologies and processes used for security purposes comply with federal privacy law. "The establishment of [the Privacy Officer position] is consistent with the DHS' fundamental responsibility to improve security while protecting the civil liberties of all Americans," one observer noted shortly after the Act's passage.² "As the DHS develops ways to prepare for and predict terrorist threats, it is also important that it not overreach and either infringe on civil liberties or lay the groundwork on which a future administration might restrict freedom."³ In addition to issuing systems of records notices, general privacy orders, and privacy memos, the Privacy Officer influences policy by conducting investigations when appropriate and through issuing Privacy Impact Assessments (PIAs) of Department initiatives.⁴ The consequences of failing to "operationalize" privacy were starkly revealed in several high-profile cases when Privacy Officer input was either not obtained or ignored:

Secure Flight. The Privacy Officer initiated an investigation of the Secure Flight passenger screening program after a July 22, 2005 memorandum prepared by the Government Accountability Office (GAO) stated that the Transportation Security Administration (TSA) "did not fully disclose its use of personal information in its fall 2004 privacy notices as required by the Privacy Act."⁵ In short, "the public was not adequately informed that a TSA contractor obtained over 100 million commercial data records."⁶

¹ Council on Foreign Relations, "Department of Homeland Security," Terrorism: Questions and Answers, (2004), available at <http://cfrterrorism.org/security/dhs.html>.

² Michael Scardaville, Principles the Department of Homeland Security Must Follow for an Effective Transition, The Heritage Foundation (February 28, 2003), available at <http://www.heritage.org/Research/HomelandDefense/bg1630.cfm> (last visited February 27, 2006).

³ Id.

⁴ Privacy Office- Privacy Impact Assessments (PIA), Department of Homeland Security, at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0511.xml (last visited February 27, 2006).

⁵ GAO; "Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information During Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public." GAO-05-864R Aviation Security, July 22, 2005, p. 1.

⁶ Id.

Making matters worse, TSA revised its original privacy notices only after the ensuing uproar.

CAPS II. The Privacy Officer initiated a separate investigation of the CAPPS II passenger screening program in April 2004 to determine if TSA violated the Privacy Act by not providing public notice of the type of information the system would use and how passengers could determine if their personal information was used to test it.⁷ After the government spent more than \$100 million to stand up the program, CAPPS II was killed – largely because of the unaddressed privacy concerns.⁸

JetBlue. The Privacy Officer likewise initiated an investigation in the spring of 2004 involving JetBlue Airways, “which admitted that it had turned over millions of passenger records to the government for a security project.”⁹ Although the Privacy Officer’s report criticized TSA managers and required them to undergo privacy training, it was not until after the report that TSA admitted that almost every other major airline also shared passenger records – some 270 million of them.¹⁰

Failure to infuse Department programs with appropriate privacy safeguards from the outset not only undermines public confidence in the work the Department is doing but also – in the case of CAPPS II – results in tremendous financial waste when they are canceled. As former Privacy Officer Nuala O’Connor Kelly noted, “I’m not positioning the privacy officer as against any collection of information, but I think the collection of information has to be well-thought-out, limited and relevant to the information at hand . . . We’re actually helping fine-tune programs to make better decisions for privacy, and to make better programs themselves. We can be enhancers of the business.”¹¹ In other words, better respect for privacy means better homeland security.

II. THE STATE OF INFORMATION SHARING: The Privacy Officer Has One Hand Tied Behind Her Back

The Privacy Officer’s ability to conduct investigations – and to prepare thorough PIAs at the outset of Department programs – has been significantly hampered by both a lack of independence of the position and an inability to get needed documents and

⁷ Larry Greenemeir, “CAPPS II is Dead, Says Ridge, But Door is Open for CAPPS III,” *Information Week* (July 15, 2004), available at <http://www.informationweek.com/showArticle.jhtml?articleID=23901115>.

⁸ See Mark Clayton, “US Plans Massive Data Sweep,” *Christian Science Monitor* (Feb. 9, 2006), available at <http://www.csmonitor.com/2006/0209/p01s02-uspo.htm> (last visited February 27, 2006); Cynthia L. Webb, “Uncle Sam Mothballs Screening Program,” *Washington Post* (July 6, 2004), available at <http://www.washingtonpost.com/ac2/wp-dyn/A54487-2004Jul16?language=printer> (last visited February 27, 2006).

⁹ Sara Kehaulani Goo and Spencer S. Hsu, “First Privacy Officer Calls ‘Experiment’ a Success,” *Washington Post* A21 (Sept. 29, 2005), available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/09/28/AR2005092802173.html> (last visited February 27, 2006).

¹⁰ *Id.*

¹¹ Sarah D. Scalet, “Five Things Every CSO Needs to Know About the Chief Privacy Officer,” *CSO Magazine* (Feb. 1, 2005), available at <http://www.csoonline.com/read/020105/fivethings.html> (last visited February 27, 2006).

information. The Privacy Officer has limited independence because she reports to the Secretary – not Congress. “That meant that certain items, such as the chief’s privacy reports about agency activities, first had to be cleared by the department’s top official.”¹² The Privacy Officer’s limited investigatory powers likewise have caused some Department heads to deny her access to internal documents needed to explore privacy complaints.¹³ Marc Rotenberg of the Electronic Privacy Information Center has noted that the Privacy Officer could do a better job if she had the power to issue subpoenas, a sentiment shared within the Privacy Office itself.¹⁴ Department attorney Elizabeth Withnell has stated, “Although the chief privacy officer by statute is required to investigate complaints of privacy violations, she does not have subpoena authority. She must therefore rely on voluntary submissions of information in order to conduct her investigation.”¹⁵ Former Privacy Officer Nuala O’Connor Kelly bemoaned this state of affairs when investigating JetBlue. “I had sent my first inquiry to TSA public affairs, my second to (the agency’s risk assessment office), but information has not been forthcoming,” she wrote in a November 2003 e-mail to Carol DiBattiste, TSA’s deputy administrator.¹⁶ “This is particularly disturbing . . . We’re getting better information from outside than we have from our own folks at this time.”¹⁷

According to Ari Schwartz of the Center for Democracy and Technology, the Privacy Officer nevertheless has done an “excellent job of consulting with as many experts as possible about a variety of difficult issues.”¹⁸ For instance, she created the Department’s Data Privacy and Integrity Advisory Committee, a 20-member group of privacy experts, to advise her and the Secretary about issues affecting privacy, data integrity and data interoperability.¹⁹ The Privacy Officer likewise has “created new privacy-protection practices and borrowed best practices from government and industry.”²⁰ Schwartz added that the Department, “now has the best privacy-impact assessments in government, even though they are still not perfect.”²¹

That progress, however, risks being undermined without a permanent Privacy Officer in place. Nuala O’Connor Kelly left her position at the end of September 2005, and the post has been staffed by an Acting Privacy Officer since that time.²² The Secretary

¹² Anne Broache, “Homeland Security Privacy Chief Leaves for GE,” CNET News.com (Oct. 3, 2005), available at http://news.com.com/2102-1029_3-5886525.html (last visited February 27, 2006).

¹³ Id.

¹⁴ Sara Kehaulani Goo and Spencer S. Hsu, “First Privacy Officer Calls ‘Experiment’ a Success,” Washington Post A21 (Sept. 29, 2005), available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/09/28/AR2005092802173.html> (last visited February 27, 2006).

¹⁵ Declan McCullagh, “Sidelining Homeland Security’s Privacy Chief,” CNET News (April 11, 2004), available at http://news.com.com/Sidelining+Homeland+Securitys+privacy+chief/2010-1071_3-5660795.html (last visited February 27, 2006).

¹⁶ Id.

¹⁷ Id.

¹⁸ Michael Arnone, “Wanted: New DHS Privacy Officer,” FCW.com (Oct. 10, 2005), available at <http://www.fcw.com/article91050-10-10-05-Print> (last visited February 27, 2006).

¹⁹ Id.

²⁰ Id.

²¹ Id.

²² Id.

must appoint a permanent Privacy Officer to effectively develop a privacy agenda and continue the Privacy Office's good work.

III. PRESIDENT'S BUDGET

The President's FY07 budget request essentially flatlines the Privacy Officer's budget at \$4,335,000 – a \$2,000 decrease from last year's \$4,337,000 request.

IV. AREAS FOR IMPROVEMENT

The Privacy Officer should be provided with all the authority necessary to carry out the job. As an initial matter, the Secretary should appoint a permanent Privacy Officer without delay. Unless the Privacy Officer is provided with greater independence and the ability to obtain documents and other information relevant to her work, he or she risks becoming a privacy also-ran. At least one expert has opined that the Privacy Officer's role already has been "pretty much reduced to flak absorption for [Department] screw-ups, and TSA in particular."²³

While the Secretary should direct all Department components to cooperate fully with the Privacy Officer's work, undefined authorities and powers can only go so far. This is especially true when details about Department missteps in the privacy arena are uncovered and jobs and reputations are on the line. As Jim Harper, the Cato Institute's director of information policy studies who serves on Homeland Security's privacy advisory committee has noted, the Privacy Officer "was not popular" within the Department after she issued her JetBlue report.²⁴ The Secretary accordingly should draft and issue a Management Directive defining clear powers for the Privacy Officer that insulate privacy from having to compete in a popularity contest. These should include the powers to:

1. Access all records she deems necessary to do her job;
2. Undertake any privacy investigation that, in her judgment, is appropriate for her office;
3. Subpoena documents from the private sector when necessary to fulfill her statutory mandate;
4. Obtain sworn testimony; and
5. Take the same actions that the Department's Inspector General may take in order to obtain answers to questions and responsive documents required for her work.

Congress, in turn, should pass legislation enacting these powers – along the lines set forth in H.R. 3041, the Privacy Officer With Enhanced Rights (POWER) Act – and should establish a

²³ Sarah Lai Stirland, "Homeland Security's Privacy Chief Resigns," [GovExec.com](http://www.govexec.com) (Sept. 28, 2005), available at <http://www.govexec.com/dailyfed/0905/092805tdpm1.htm> (last visited February 27, 2006).

²⁴ *Id.*

five-year appointed term for the Privacy Officer to ensure the independence of her office. Toward this end, the legislation should also require the Privacy Officer to submit reports directly to Congress.

An independent and effective Privacy Officer is precisely what the Department needs to avoid the problems of the past and to guard against the kinds of abuses recently reported with the National Security Agency's domestic spying program. "We understand that a truly vigorous and independent privacy officer can be inconvenient for government officials over the short term," ACLU attorney Tim Sparapani has noted.²⁵ "But over the long run, vigorous checks and balances will strengthen the Department of Homeland Security by inspiring greater public confidence in DHS programs . . ."²⁶

²⁵ Ryan Singel, "More on O'Connor Kelly's Departure," Secondary Screening (Sept. 28, 2005), available at http://www.secondaryscreening.net/static/archives/2005/09/more_on_oconnor.html (last visited February 27, 2006).

²⁶ Id.

**I. STATEMENT OF PROBLEM HISTORICALLY:
The Department Lacks a “One Stop” Redress Process for Innocent
Americans Misidentified as Terrorists to Clear Their Good Names**

For years, Americans have heard almost daily reports of babies, young children, senior citizens, and other unlikely terrorists being stopped unnecessarily at airports, border crossings, and ports of entry because they are “on the watch list.”¹ The vast majority are not “on the watch list” at all. On the contrary, they simply have the misfortune of sharing the same or a similar name as a known or suspected terrorist – prompting close scrutiny, delays, and major inconvenience whenever and wherever they are screened. A variety of Department of Homeland Security components – such as the Transportation Security Administration (TSA), Customs and Border Protection (CBP), and Immigration and Customs Enforcement (ICE) – operate highly publicized screening programs that often cannot distinguish innocent people from terrorists included on the watch list. Without some way to clear their good names, innocent Americans will continue to be harassed as they exercise their right to travel to and from the United States. Others who apply for jobs in certain sensitive employment sectors will also continue to suffer the indignity of being tagged as potential terrorists.² The Department’s plan to screen applicants for certain private sector critical infrastructure positions, moreover, faces a similar challenge.

Observers have long noted that the Department, “should take the lead in implementing processes, enforced by authorities, to develop comprehensive and accurate watchlists. This must include authorities and processes to correct errors, configuration control to enhance utility and interoperability of information across agencies, and regular review and oversight.”³ Although the Department recently acknowledged that “[s]ometimes mistakes are made” during screening and that “[t]ravelers need simpler ways to fix them,” it has failed to develop a Department-wide redress process through which

¹ See, e.g., *4-Year Old Turns Up on Government’s ‘No-Fly’ List*, MSNBC (Jan. 5, 2006), available at <http://www.msnbc.msn.com/id/10725741/>; Caroline Drees, *US No-Fly List Vexes Travelers From Babies on Up*, ABC NEWS (Dec. 15, 2005), available at <http://abcnews.go.com/US/wireStory?id=1408903>; Ryan Singel, *Nun Terrorized by Terror Watch*, WIRED NEWS (Sept. 28, 2005), available at <http://www.wired.com/news/privacy/0,1848,68973,00.html>; Rick Bowmer, *Terror List Snag Nearly Grounded Ted Kennedy*, USA TODAY (Aug. 19, 2004), available at http://www.usatoday.com/news/washington/2004-08-19-kennedy-list_x.htm.

² The Department’s Transportation Threat Assessment and Credentialing (TTAC) Office oversees the HAZMAT Threat Assessment Program, Alien Flight School Program, and aviation crew vetting programs. Automatic access to the watch list – and the names that have been cleared from it – would undoubtedly assist innocent Americans trapped in the watch list web. See Shaun Waterman, *Trucker Case Shows Vetting Redress Problem*, WASHINGTON TIMES (March 7, 2005), available at <http://www.washtimes.com/upi-breaking/20050302-123409-7769r.htm>.

³ James Jay Carafano and David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security*, Heritage Foundation/CSIS 22 (Dec. 13, 2004).

innocent people can distinguish themselves from real terrorists.⁴ For its part, the Terrorist Screening Center (TSC), which collects and shares much of the screening information available to the Department, acts only as a redress facilitator:

[While] privacy issues and redress procedures remain an integral part of TSC operations, the TSC will not establish an Office of the Ombudsman for redress issues. The ombudsman function will be at the nominating agency level. Each agency that has nominated an individual for inclusion in the TSDB [watch list] will ultimately be responsible for authorizing the continued inclusion or exclusion from the TSDB. The TSC will establish a Redress office to coordinate and facilitate that process among and between Federal agencies in the most efficient and effective manner.⁵

The TSC's website in fact directs innocent people misidentified as terrorists to the Department components most often encountered by the traveling public: TSA, CBP, and ICE.⁶ Because these components screen people not only for possible terrorism connections but also for a host of other reasons within their respective areas of expertise – including criminal status, immigration status, and the like – it makes sense to establish a “one stop” redress process at the Department where it can have the greatest impact. The failure of the Department to follow this course represents an ongoing missed opportunity to provide good customer service to a frustrated public and to build confidence in the Department's mission of protecting the homeland.

II. THE STATE OF THE REDRESS PROCESS TODAY

The seeds of a solution, however, may be sprouting. TSA recently unveiled its new Office of Transportation Security Redress (OTSR) which, among other things, is designed to expedite the TSA's redress process as it applies to airline passengers. By filling out a TSA Passenger Identify Verification Form (PIVF) and submitting various documents, innocent travelers who repeatedly register as potential “hits” whenever they attempt to board an airplane can distinguish themselves from actual or suspected terrorists included on the watch list. After TSA vets the submissions and determines that a traveler is not a risk, it adds the person to a cleared list that includes personal identifiers. TSA then shares that cleared list and identifiers with the airlines. When the traveler next attempts to board a plane and his name registers as a hit during screening, airport personnel can question him about his true identity using the information he supplied to OTSR. “The key point,” policy experts have noted, “is that the vetted individual holds the information to disambiguate

⁴ Press Release, Department of Homeland Security, *Fact Sheet: Secure Borders and Open Doors in the Information Age* (Jan. 16, 2006), available at <http://www.dhs.gov/dhspublic/display?content=5347>.

⁵ United States Department of Justice Office of the Inspector General Audit Division, *Review of the Terrorist Screening Center*, Audit Report 05-27, Appendix IV (June 2005) at 97 (USDOJ Audit).

⁶ Federal Bureau of Investigation, *Counterterrorism – Terrorist Screening Center Terrorist Watchlist Redress Procedures*, available at <http://www.fbi.gov/terrorinfo/counterterrorism/redress.htm>.

himself – and thus controls his own fate.”⁷ With the advent of Secure Flight, the innocent traveler who “hits” as a potential terrorist at the boarding gate will be automatically compared with the cleared list – expediting his screening experience significantly.

TSA, however, does not automatically share its cleared list with CBP, ICE, or any other Department components routinely engaged in screening. Instead of leveraging TSA’s resources and established methods, those entities often turn instead to the TSC for redress assistance on a case-by-case basis. In short, the Department lacks a common picture of who is and who is not a terrorist and at times relies on the TSC to handle redress issues – a task for which it admittedly has no plan to undertake on any mass scale.⁸ A better solution is warranted.

III. PRESIDENT’S BUDGET

The President’s FY07 budget request does not include any funding for a Department-wide redress process.

IV. AREAS FOR IMPROVEMENT

The Department should create an Office of the Ombudsman for Redress Issues that maintains a common cleared list in a centralized database accessible to all Department components. To facilitate redress, it should:

- (1) Establish, where feasible, a “swift, informal, administrative resolution” procedure at land borders, ports of entry, and other screening points in order to resolve as many misidentification issues as possible without requiring innocent people to undergo a formal redress procedure. Potential candidates for such an expedited process would include babies, small children, and others that pose no threat and could accordingly be placed on a Department-wide clearance list as a matter of course;⁹
- (2) Create a Department-wide administrative review process – based on the TSA model – that acknowledges and resolves complaints within a reasonable, specified time frame; accesses information from appropriate sources to distinguish the redress applicant from terrorists on the watch list, if possible; and captures, maintains, and publishes metrics of its performance;¹⁰ and

⁷ Paul Rosenzweig and Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum*, Heritage Foundation (June 17, 2005), available at <http://www.heritage.org/Research/HomelandDefense/lm17.cfm>.

⁸ US DOJ Audit, Appendix 4 at 97.

⁹ See Rosenzweig and Jonas, *supra* note 7.

¹⁰ *Id.*

- (3) Institute an administrative hearing process for redress applicants that allows them to contest adverse decisions on their watch list status – with appropriate due process protections and national security safeguards – and that preserves a record for purposes of federal district court appeals of adverse administrative rulings.¹¹

The ombudsman too will need an information technology network architecture that allows each Department component that conducts screening to submit redress applications from the screening site and provides those components with access to watch list information and the common cleared list simultaneously.

Finally, this information technology network architecture should provide a direct link to the TSC itself – not only to contribute to the accuracy and completeness of TSC records but also to help the Department develop a redress outreach program. Because the TSC maintains records of all hits on the watch list – including records of all innocent people who are misidentified as terrorists – the TSC could advise the Department on a periodic basis about who is repeatedly experiencing this problem.¹² The Department could then invite these victims of circumstances to initiate the redress process *before they have even contacted the Department to complain*. That would be a welcome and valuable service to the American people that the Department presently cannot offer.

¹¹ *Id.*

¹² USDOJ Audit, Appendix IV at 137.

The Department of Homeland Security has earned a “needs improvement” for its procurement operations. Unfortunately, for an agency that purchases an average of \$10 billion per fiscal year in goods and services from private contractors, a “D” is far from acceptable. The grading for this section is divided into 3 parts: organization, execution and resources.

I. ORGANIZATION

Grade: C

Procurement at the Department began with dismal prospects. Faced with the huge and often unwieldy undertaking of merging the process, operations, and culture of 22 distinct entities, the Department has earned an “A” for the incredible effort which has resulted in winnowing down 22 different procurement operations to eight. Of these eight procurement offices, seven serve separate units¹ within the Department while one office, Office of Procurement Operations, was designed as a catch-all to carry out acquisitions for units that lack independent acquisitions capacity. Despite this progress, a significant amount of work remains in the huge task of transforming the Department’s procurement operation, averaging \$10 billion per year in purchases of goods and services, into one integrated function.

At a minimum, to improve its performance and continue its work toward transformation, the Department must invest its Chief Procurement Officer (CPO) with the necessary authority to set and enforce standards and guidelines within the various agencies that retain independent procurement authority. Currently the department’s CPO does not have direct authority over the purchasing decisions or processes used throughout the agency. Instead, 3 years after this Department’s establishment, the authority to prioritize critical acquisition decisions, identify solutions and formulate Department-wide rules and policies affecting procurement is shared among a group of procurement officials that comprise the Chief Acquisition Officers Council, an organization composed of the Chief Procurement Officer and the senior acquisition managers of the seven agencies that continue to retain their own procurement shops. One need not be a cynic to posit that members of this Council may have entrenched interests in retaining autonomy, power and control over their respective procurement shops. Needless to say, a reluctance to relinquish decision-making authority and control over spending decisions will only exacerbate real or perceived turf battles within various legacy agencies and thus hinder the ultimate transformation of the Department into an entity that operates as one unit.

¹ The seven units with separate procurement operations are Customs and Border Protection (CBP); the Transit Security Administration (TSA); the Immigration and Customs Enforcement (ICE); the Federal Emergency Management Agency (FEMA); the U.S. Coast Guard (USCG); the Federal Law Enforcement Training Center (FLETC), and the U.S. Secret Service (USSS).

For these reasons the Department receives a “C” on its efforts to transform its procurement operations.

II. EXECUTION

Grade: D

The Department’s grade for execution of its procurement functions is significantly below average. Unfortunately, the Department has earned a “D” for its lax oversight and ineffective management of basic procurement processes. Both the U.S. Government Accountability Office (GAO) and the Department’s own Inspector General have expressed significant concerns about the manner in which procurement practices are implemented. In many instances, these operational failures have led to instances of waste and inefficiency, which if left unchecked, will hinder the Department’s ability to carry out its basic mission. The following are a few examples of problematic procurements which have hurt the agency and resulted in waste of taxpayer dollars. overall function:

- **ISIS** – The Integrated Surveillance Intelligence System (ISIS) envisioned using technology as a force multiplier to secure our borders. The basic idea was to employ a system of cameras and sensors to alert Border Patrol Officers to illegal crossings in real-time. ISIS was initiated by the Immigration and Naturalization Service, one of the Department’s legacy agencies. Since the establishment of the Department, the ISIS program has been renamed twice. Currently, the Department has stopped purchases under the program and is awaiting the publication of a new Request for Proposals (RFP) to continue these important border security efforts. Unfortunately, GAO and the Inspector Generals of GSA and the Department have raised serious concerns about the Department’s vision in executing a technology based border security program and the ability of their procurement operations to implement such a program.² To date, the Department has spent approximately \$429 million to secure only 4% of the border with technology.³ With close to 7,000 miles of land border shared with Canada and Mexico, the taxpayers of this nation cannot afford to spend \$100 million for every 1% of border coverage.
- **eMerge2**—The Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency project (eMerge2) began in 2003 and was to weave together the financial, budget, asset control and grant activities of the Department’s legacy agencies. Estimates were that it would cost about \$100 million and would be complete in 2006.⁴ Unfortunately, problems surfaced almost immediately with both

² GENERAL SERVICES ADMINISTRATION, *Compendium of Audits of the Federal Technology Service Regional Client Support Centers* (December 14, 2004); *A Review of Remote Surveillance Technology Along U.S. Land Borders* (OIG-06-15) (December 2005); OFFICE OF INSPECTOR GENERAL *Major Management Challenges Facing the Department of Homeland Security* (OIG-05-06) (December 2004); GOVERNMENT ACCOUNTABILITY OFFICE, *Border Security: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program* ([GAO-06-295](#)) (February 22, 2006).

³ GOVERNMENT ACCOUNTABILITY OFFICE, *Border Security: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program* ([GAO-06-295](#)) (February 22, 2006).

⁴ Wilson P. Dizard, *Back-Office IT deal has yet to Emerge at DHS*, GOVERNMENT COMPUTER NEWS (September 13, 2004).

the technical specifications in the procurement contract and in the overall feasibility of the plan. After working with a contractor for almost 2 years, the Department announced its intention to abandon eMerge2 in late 2005 and to replace it with a significantly scaled down version of a financial program that would systematically integrate only a few components at a time.⁵ At the time the decision was made to abandon eMerge2, the Department had spent approximately \$10 million.⁶ To date, the Department has neither set forth the details of the plan to replace eMerge nor has it established a viable framework to integrate its financial systems. The Department's failure to create a unified financial budget and asset control system is particularly troubling given that 5 of its legacy agencies⁷ had known financial management weaknesses and vulnerabilities. The inability of these agencies to adequately maintain and document budgeting and inventory activities may not only continue to prevent the Department from reporting a clear financial picture, but it will ultimately hamper the ability of the component agencies to make and track their procurement decisions.

- **Buy America Act Compliance**—American taxpayers expect their government to use American made goods whenever possible. The Buy American Act of 1933, 41 USC 10a-10d, requires that with certain exceptions only articles, materials and supplies that have been mined, produced or manufactured in the United States be utilized in fulfilling federal procurement and construction contract. One would assume that an agency charged with the security of the American homeland would be particularly concerned about fulfilling the requirements of this law and maintaining an awareness of the potential security hazards that may result from failing to follow this procurement measure. In June 2005, however, the Department's Inspector General found that the Department's internal procurement tracking system, the Homeland Security Contract Information System, did not have the capability to collect data about the amount and types of foreign end products that were procured by the Department.⁸ The IG also found that the Department's procurement personnel did not have adequate training to properly implement the Buy America Act.⁹ As a result of these failings, in 2004, the Department purchased approximately \$152 million in helicopters and almost \$4 million in pistols from foreign manufacturers.¹⁰ While these purchases did not represent an immediate risk, the Department's internal policies should not only abide by the law, but must recognize the overall effect of its purchases on domestic industries that manufacture defense and security related goods. There are simply some manufacturing capabilities that are too important to be outsourced and must remain on American soil.

⁵ Meeting with Deputy Chief Financial Officer, February 8, 2006, Notes on file with Committee Staff.

⁶ Meeting with Deputy Chief Financial Officer, February 8, 2006, Notes on file with Committee Staff.

⁷ The legacy agencies with known financial management weaknesses and vulnerabilities were Customs, Transportation Security Administration, Immigration and Naturalization Service; Federal Emergency Management Agency and the Federal Law Enforcement Training Center. See GOVERNMENT ACCOUNTABILITY OFFICE, *DHS Financial Management* (GAO-04-774) (July 2004).

⁸ Audit of Buy American Act Compliance, OIG-05-23 (June 2005).

⁹ *Id.*

¹⁰ *Id.*

The foregoing examples represent purchasing decisions involving approximately \$600 million in goods and services that have failed to perform adequately, return a real benefit to the taxpayer, or make the homeland more secure. Therefore, on the execution of procurement activities, the Department receives a “D”.

III. RESOURCES

Grade: F

The Department cannot function without an adequate number of well-trained employees. Unfortunately, the Department has consistently failed to hire and adequately train procurement personnel. Recently, the Department increased personnel for the Department’s Procurement workforce. Even the addition of \$8 million to hire 25 additional employees¹¹ is grossly insufficient to adequately run procurement operations worth billions of dollars. In a September 2005 letter prepared by the Inspector General at Secretary Chertoff’s request, the IG noted that “procurement staff throughout DHS is severely limited”¹² and cautioned that procurement offices may be “significantly understaffed”.¹³ Given that the Department’s current procurement workforce is made up of approximately 1100 employees,¹⁴ it is unlikely that an additional 25 people will have a significant impact on alleviating the concerns expressed by the Inspector General. In addition to increased staffing levels to meet an overwhelming workload, the IG found that there are significant training needs and that training and certification of procurement personnel to oversee internal practices and purchasing programs could significantly reduce the DHS’ vulnerability to waste, fraud and abuse.¹⁵

The Department’s failure to hire sufficient and competent procurement personnel can only be described as “penny wise and pound foolish.” In an attempt to hold down some personnel costs it has failed to commit the resources necessary to build a well functioning procurement workforce. Those decisions have left the agency vulnerable to waste, fraud and abuse in each purchasing decision it makes. For its failure to provide resources and training needed to develop a strong and competent procurement workforce that can safeguard the taxpayer’s money, the Department has earned an F.

¹¹ Budget in Brief, Department of Homeland Security, FY2007.

¹² Department of Homeland Security’s Procurement and Program Management Operations, OIG-05-53 (September 2005).

¹³ *Id.*

¹⁴ Document Provided in Meeting with Chief Procurement Officer, Copy on file with Committee.

¹⁵ See OIG-05-53, *supra* note 12.

I. STATEMENT OF PROBLEM HISTORICALLY: Department Fails to Address Employee Morale Issue

In the Homeland Security Act of 2002, the Department of Homeland Security was relieved from compliance with civil service regulations normally applied to federal employers.¹² Congress, at the Administration's urging, sought to create an employment system that would become a flexible and modernized personnel system which could meet the mission needs of the Department, while preserving principles of fundamental merit.³

Unfortunately, in the three years since its creation, the Department has failed to demonstrate that it is capable of creating a fair and flexible system. In an annual survey conducted by the Office of Personnel Management and distributed to 30 cabinet level departments and independent agencies, the Department has consistently ranked among the lowest in employee morale.⁴ In the most recent study, published in October 2005, the Department was ranked at the bottom of all federal agencies in the degree of employee satisfaction.⁵ Perhaps most disturbing, only 3% of Department employees felt that personnel decisions were based on merit, and only 4% felt that creativity and innovation were rewarded.⁶ Furthermore, the morale at the Department was far worse than that of the agency that immediately preceded it in the rankings, the Small Business Administration (SBA).⁷ A workforce that suffers from low morale is simply not likely to deliver peak performance.

To be fair, some of the morale issues within the Department may be due to the inevitable confusion and uncertainty that results from any large-scale merger, such as the one that created the Department. The source of the morale problems here, however, may not be limited to an anxiety solely related to change.

While employed by the Department's component legacy agencies, personnel worked under the federal civil service system, which governed pay, promotion and benefits. The new system the Department seeks to implement, dubbed MaxHr, will determine pay and promotion. Under development for approximately one year, this system has encountered substantial legal hurdles. Specifically, in August and October of 2005, the U.S. District Court for the District of Columbia ruled that parts of the Department's proposed personnel system violated collective bargaining rights and other employee protections and prevented

¹ Homeland Security Act of 2002, P.L. 107-296, § 841.

² *Id.*

³ OFFICE OF PERSONNEL AND MANAGEMENT, *Results from the 2004 Federal Human Capital Survey*.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ DEPARTMENT OF HOMELAND SECURITY EQUAL EMPLOYMENT OPPORTUNITY PROGRAM STATUS REPORT (2004).

the Department from implementing the central aspects of the program.⁸ Unfortunately, the Department has been reluctant to negotiate with employee representatives to seek agreement to resolve the issues raised by the court.

Adding to low employee morale is the Department's ongoing diversity challenge. According to the Department's numbers, its performance in securing diversity while it secures the nation has been less than stellar. Quite simply, the Department has not moved to enhance minority representation in any measurable manner.

The following chart with information provided by the Department of Homeland Security represents the ethnic, racial and gender breakdown of employees in the Department as of May 2005.⁹

American Indian/Alaskan Native	1,011
Asian/Pacific Islander	5,875
Black	20,646
Hispanic	24,251
White	76,310
Male	88,480
Female	43,637

By February 2006, the Department had substantially increased the number of employees by 6030, but had not substantially increased the number of women and minority employees. The table below details the February 2006 ethnic racial and gender division of employees.¹⁰

American Indian/Alaskan Native	1,148
Asian American/Pacific Islander	5,674
Black	20,931
Hispanic	25,356
White	82,308
Other Races	1,079
Male	92,751
Female	43,745

⁸ The Administration also plans to remove civilian employees at the Department of Defense from the federal civil service system, using a plan similar to MaxHr. However, on February 27, 2006, the U.S. District Court for the District of Columbia ruled that DOD cannot implement its plan. Judge Emmet G. Sullivan wrote the DOD plan would "entirely eviscerate collective bargaining." American Federation of Government Employees, AFL-CIO, et al. v. Department of Defense, et al., Civil Action No. 2005-2183. See also NTEU v. Chertoff, No. 05-201 (October 7, 2005) (D.D.C.).

⁹ Email from the Department's Office of Civil Rights and Civil Liberties, February 24, 2006. Copy on file with the Committee. Categorizations used in this report are those used by the Department.

¹⁰ *Id.*

While overall number of employees increased from 160,764 to 166,794, the number of minority employees did not increase substantially. As the chart reveals, during this period, the Department suffered a net loss from the employee population of Asian American/ Pacific Islanders, while the numbers of employees for all other minority groups remained virtually stagnant. Although the actual numbers of minority group employees remained stagnant, their overall percentage of representation decreased because of the increase in the total employee population.

Non-minority employees accounted overwhelmingly for the increase in the employee population, increasing their numbers from 76,310 in 2003 to 82,308 in 2006. Thus, of the 6030 new employees hired by the Department during the period, non-minority employees accounted for 5098 or 99%.

II. AREAS FOR IMPROVEMENT

The Department should engage with employees' representatives to resolve the ongoing problems that have hampered implementation of the new personnel system. These discussions should be substantive and should focus on resolving the serious deficiencies in the MaxHr blueprint which have been repeatedly raised by the court. If these deficiencies cannot be resolved in a manner that passes the muster of the federal courts, the Department must immediately embark upon ways to use aspects of the federal civil service system to supplement or replace MaxHr. The Department's ability to attract and retain a talented and professional workforce will be seriously impeded if it continues to be dogged by the circumstances that lead to low employee morale.

Further, the Department must immediately institute mechanisms that recognize employee contributions and achievement. Given the Department's Congressionally-authorized flexibility in the personnel arena, it might want to try a novel approach to recognize and award front line and other non-supervisory employees. For instance, the Department may want to place a moratorium on monetary awards or bonuses for all employees in the upper echelons of management and the Senior Executive Service for one year, while reserving those awards for front-line and non-supervisory employees. This kind of gesture would communicate that everyone's work is appreciated and valued. However, this kind of one-time stop gap measure will not provide a solution fix for the profound morale problems that beset the Department. The Department must engage in a host of measures that ensure that hiring and promotions are not only conducted in a fair manner but are perceived as fair and balanced. In attempting to re-make the civil service system, the Department may wish to retain many of the system's time-tested features, such as the use of career ladders, education and training opportunities that are tied to career advancement, flexible time, job-sharing and other practices that encourage family-friendly practices.

Finally, the numbers reveal that the Department's record of hiring and retaining non-white employees is abysmal. The Department must immediately **set and meet** targets to increase its racial and ethnic diversity.

END PAGE

This page intentionally left blank....

E N D