LEAVING THE NATION AT RISK:

33 Unfulfilled Promises From the Department of Homeland Security

AN INVESTIGATIVE REPORT BY THE
U.S. House Committee on Homeland Security Democratic Staff

PREPARED FOR:

Representative Bennie G. Thompson,
Ranking Member, Committee on Homeland Security

Representative Loretta Sanchez,
Ranking Member, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Representative Zoe Lofgren,
Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment

Representative Bill Pascrell,
Ranking Member, Subcommittee on Emergency Preparedness, Science, and Technology

Representative James Langevin,
Ranking Member, Subcommittee on Prevention of Nuclear and Biological Attack

Representative Kendrick B. Meek,
Ranking Member, Subcommittee on Management, Integration, and Oversight

Representative Edward J. Markey

Representative Norm Dicks

Representative Peter DeFazio

Representative Nita Lowey

Representative Eleanor Holmes Norton

Representative Sheila Jackson-Lee

Representative Donna M. Christensen

TABLE OF CONTENTS

Leaving the Nation At Risk: 33 Unfulfilled Promises Made by the Department of Homeland Security

---

INTRODUCTION

In the four years since the events of September 11, 2001, billions of dollars and countless hours of effort have been put into creating and strengthening the Department of Homeland Security. As a result of these efforts, the Department has achieved some successes, but it has also made numerous promises that have gone unfulfilled. Due to these unfulfilled promises, there are many security gaps that continue to leave our nation at risk. From critical infrastructure protection to border security, more work needs to be done to protect the homeland.

In order to hold the Department accountable for its promises and to ensure it carries through on them in the future, the Minority staff of the House Committee on Homeland Security has reviewed Department press releases, key Congressional testimony, and statements from the last 3 years, including from the signing ceremony creating the Department, in search of the most important promises made. Below is a listing of those promises in the words of the Department and its officials, and a description of how the failures to fulfill those promises have left security gaps in place.

This Administration must keep its promises to close security gaps and make the nation more secure. America deserves better.

CRITICAL INFRASTRUCTURE PROTECTION

PROMISE #1:
THE PRESIDENT AND THE DEPARTMENT PROMISED TO CREATE A COMPREHENSIVE PLAN TO IDENTIFY AND PROTECT CRITICAL INFRASTRUCTURE

"*Consistent with the Homeland Security Act of 2002, the Secretary shall produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives within 1 year [i.e. by December 2004] from the issuance of this directive.*"[1]

"The Office of Infrastructure Protection compiled a database with input from state and local governments and the private sector consisting of over 80,000 assets. The database is a key component of the National Infrastructure Protection Plan, which the Department is finalizing to implement better protective measures for key areas of critical infrastructure."[2]

SECURITY GAP #1:
WITHOUT A REAL PLAN TO PROTECT CRITICAL INFRASTRUCTURE, OUR NATION'S MOST VALUABLE ASSETS WILL REMAIN AT RISK

Homeland Security Presidential Directive 7 (HSPD-7), signed on December 17, 2003, required the development of a "National Plan for Critical Infrastructure and Key Resources Protection," which subsequently was referred to as the National Infrastructure Protection Plan (NIPP), by December 2004. That deadline was not met. In February 2005, an "Interim" NIPP was released, but that document was not a comprehensive plan for protecting critical infrastructure. Even the Department admits that the document merely "[e]stablished the risk management framework" and was only released to allow more engagement with security partners.[3]

The Department released the draft final NIPP in November 2005 for public comment. The final NIPP is supposed to be completed by February 2006.[4] A Department official recently testified that it may take another 6 months before the sector-by-sector plans are completed.[5]

---

[1] Homeland Security Presidential Directive 7, signed 17 December 2003, available at http://www.whitehouse.gov/news/releases/2003/12/text/20031217-5.html.
[2] Department of Homeland Security Press Release, 6 January 2005.
[3] National Infrastructure Protection Plan Status Update, U.S. Department of Homeland Security PowerPoint presentation provided to Committee staff on 1 November 2005.
[4] *Id.*

The one year delay in completing the NIPP has left the Department without a clear strategy for protecting critical infrastructure in the event of an attack. Unfortunately, this security gap may exist for another 8 months until all the sector-specific plans are completed, perhaps even longer as they are tested and refined. Furthermore, the long delay in completing the NIPP demonstrates the Department's inability to focus on key priorities—even those designated as such by the President.

In order to close the security gaps posed by the lack of a critical infrastructure protection strategy, the Department must complete the NIPP without missing any further deadlines. Most importantly, the NIPP must be a genuine plan for protecting critical infrastructure. It should address how to identify at-risk facilities, but other more difficult issues must also be included, such as recommendations on how certain facilities can be made secure.

PROMISE #2:
THE DEPARTMENT PROMISED TO CREATE A COMPREHENSIVE DATABASE OF CRITICAL INFRASTRUCTURE IN AMERICA

"Now we know, as do our partners, that vast, rich information sharing tools are critical to our ability to keeping our nation's critical infrastructure far from a terrorist's reach. And so, I'm announcing today that, by December of this year, together with our partners, we will create a unified, national critical infrastructure database that will enable us to identify our greatest points of vulnerability, existing levels of security and then add increased measures of protection where needed."[6]

"We will aid the private sector partners with a unified, national critical infrastructure database. And we, along with our state and local partners, will continue to improve and expand this Network."[7]

"We will also—by year's end—create a unified, national critical infrastructure database to identify vulnerabilities so we may better secure our symbols of freedom and the vast, complex systems that power them."[8]

---

[5] Testimony of Andy Purdy, Acting Director of the National Cybersecurity Division, Joint Hearing of the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity and the Subcommittee on Emergency Preparedness, Science and Technology, House Committee on Homeland Security, 18 October 2005.
[6] Statement of Secretary Ridge, 23 February 2004.
[7] Statement of Secretary Ridge, 24 February 2004.
[8] Statement of Secretary Ridge, 19 April 2004.

SECURITY GAP # 2:
WITHOUT A COMPREHENSIVE CATALOGUING OF CRITICAL INFRASTRUCTURE, OUR NATION CANNOT ASSESS WHICH ASSETS ARE MOST AT RISK

The National Asset Database is still incomplete. State governments have provided the Department with lists of so-called critical infrastructure that vary widely. For example, the list of critical infrastructure for one state includes gas stations and other locations that are not of critical significance.[9] The Department has not yet reduced these lists into one national list of critical infrastructure.[10]

Without creating a single list of the nation's critical infrastructure, there may be key facilities left without security plans or adequate terrorist response plans. Most importantly, this list should only have genuine critical infrastructure on it. The effort to identify critical infrastructure is useless if the Department cannot depend on the list as a reliable measure of at-risk facilities in the event of an emergency. Furthermore, the final list should be truly comprehensive, not just consisting of obvious critical infrastructure such as nuclear plants and dams. There may be facilities that are critical infrastructure for unique reasons, such as a transformer through which large portions of a city's power grid flows or a bridge that is the only major railroad crossing for hundreds of miles.

[9] Committee staff analysis of the June 2005 Mississippi portion of the National Asset Database.
[10] *See* Prepared Testimony of Bob Stephan, Assistant Secretary for Infrastructure Protection, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security, 20 October 2005.

PORT SECURITY

PROMISE # 3:
THE DEPARTMENT PROMISED TO PROVIDE MORE RADIATION MONITORING EQUIPMENT AT PORTS

"We're giving portable radiation detectors to each one of our primary inspectors, the first person you see at the border. That's more than 15,000 men and women who will be equipped with these. It's a first step. By the end of the year, we intend to have complete radiation screening of air and sea cargo as well."[11]

SECURITY GAP # 3:
UNTIL EVERY PORT OF ENTRY HAS RADIATION PORTAL MONITORS, WE WILL REMAIN AT RISK OF TERRORISTS SMUGGLING NUCLEAR MATERIAL INTO THE COUNTRY

Only 2 seaports have the capability to screen 100 percent of the cargo entering the country for radiological or nuclear material, and no airport has the capability to do so.[12] There is some progress being made to close this security gap. For example, the nation's busiest seaport, Los Angeles/Long Beach, California, will have complete Radiation Portal Monitor (RPM) coverage by year's end.[13] Despite these improvements, for a mere $280 million, the Department could install radiation portal monitors at every port of entry.[14] Yet the President has not requested this funding nor has Congress provided it.

In order to ensure that terrorists cannot easily smuggle radiological or nuclear materials into the United States, we must place radiation portal monitors at every port of entry. We must also improve the programs designed to identify high-risk cargo and invest in next generation technology for monitoring shipping containers and keeping them secure.

PROMISE #4:
THE DEPARTMENT PROMISED TO DEPLOY TRANSPORTATION WORKER IDENTIFICATION CARDS NATIONWIDE

"The Department of Homeland Security's Transportation Security Administration (TSA) today began testing the technology and business processes involved in the Transportation Worker Identity Credential

[11] Statement of Secretary Ridge, 3 March 2003.
[12] Department of Homeland Security briefing to Committee staff, 10 February 2005.
[13] "Nation's Busiest Seaports to Have Complete Radiation Detection Coverage by End of 2005," Department of Homeland Security Press Release, 3 June 2005.
[14] Congressional Budget Office Cost Estimate of H.R. 4312, December 6, 2005, p. 3.

(TWIC) Program at the Port of Long Beach Container Terminal. The Prototype will expand to 34 sites in six states and will last seven months."[15]

SECURITY GAP #4:
UNTIL A TRANSPORTATION WORKER IDENTIFICATION CARD IS EFFECTIVELY DEPLOYED NATIONWIDE, PORTS AND OTHER TRANSPORTATION FACILITIES WILL REMAIN AT RISK

Although a Transportation Worker Identity Credential (TWIC) prototype was conducted, in October 2005, TSA was still developing the regulation needed to issue the card nationwide. According to the Government Accountability Office (GAO), TSA originally planned to issue the TWIC cards nationwide in August 2004.[16]

Until the Department completes the TWIC program, there will remain a risk that terrorists could obtain employment or entry to transportation facilities, such as ports. To close this security gap, the Department must finish developing and deploying the TWIC card by early next year. At the same time, the Department must ensure the TWIC program does not duplicate other background checks workers must undergo, such as those needed to transport hazardous materials. The process for checking backgrounds must also focus on workers who are genuine terrorist threats, not regular people who have made mistakes in the past.

[15] Department of Homeland Security Press Release, 17 November 2004.
[16] "Port Security, Better Planning Needed to Develop and Operate Maritime Worker Identification Card (TWIC) Program," GAO 05-106, December 2004, p. 1.

CHEMICAL PLANTS

PROMISE #5:
THE DEPARTMENT PROMISED TO ENGAGE CONGRESS ON THE DEVELOPMENT OF CHEMICAL PLANT SECURITY REGULATIONS

"Well, we certainly do have, you know, some regulatory authorities. And I think, as I indicated in the area of chemical plants, there are obviously some times when you need to regulate in order to prevent people from free riding, basically; I mean, can -- you know, relying on others to enhance security and not doing it themselves. But we want to be -- as I said, we want to be judicious about it. I think there's a lot we can do. We clearly have to set good standards and we have to let people know what works and what doesn't work, and that's part of what we are trying to do right now."[17]

"We are proposing at this point in time over the next several weeks in an accelerated manner to figure out the principles we think should guide a measured regulatory framework for the chemical sector and work with you all and your colleagues in the Senate to develop a legislative proposal that would put that into effect."[18]

SECURITY GAP # 5:
UNTIL THE DEPARTMENT HAS THE AUTHORITY TO FORCE CHEMICAL PLANTS TO PUT SECURITY MEASURES IN PLACE, THEY WILL REMAIN A HIGH RISK

The Environmental Protection Agency estimates that over 100 chemical plants place more than 1 million people at-risk of harm in a worst-case chemical release.[19] Thousands are at risk from smaller plants.[20] As a result of these potential risks, chemical plants may be a target of terrorists. Yet neither the Department nor any other Federal agency has the authority to regulate the security of all chemical plants. Despite the Department's April and June testimony, it has still not begun serious negotiations with the House Committee on Homeland Security on a legislative proposal to grant the Secretary of Homeland Security this authority. Discussions of legislation are expected to begin in January of 2006—more than 6 months late. In order to close the security gap at chemical plants, the Administration and Congress must act quickly to negotiate and pass this legislation.

---

[17] Testimony of Secretary Chertoff, 13 April 2005.
[18] Testimony of Bob Stephan, Assistant Secretary of Infrastructure Protection, 15 June 2005.
[19] Belke, James C., "Chemical Accident Risks in U.S. Industry – A preliminary analysis of accident risk data from U.S. hazardous chemical facilities," Proceedings of the 10th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Stockholm, Sweden," Pasman, Fredholm and Jacobson (eds.) (2001).
[20] *Id*.

PROMISE #6:
THE DEPARTMENT PROMISED TO PLACE CAMERAS AT THE MOST HIGH-RISK CHEMICAL PLANTS

"And we will be monitoring, via web-enabled perimeter cameras, chemical facilities of greatest concern. The cameras will link to our Homeland Security Operations Center. They provide one piece of the real-time data that I spoke about earlier, and more are due to come on line by the end of the year."[21]

SECURITY GAP #6:
SURVEILLANCE EQUIPMENT MUST BE PLACED AT HIGH-RISK CHEMICAL PLANTS IN ORDER TO PREVENT A TERRORIST ATTACK

The Department initially planned to install cameras at 72 of the highest risk chemical facilities that could be monitored at the Homeland Security Operations Center through a secure internet connection. The Department later decided to narrow the scope of the initiative to a pilot of 12 plants. Ten of the plants approached with the idea agreed to participate and 2 declined. The pilot was conducted for a year, and the Department is now reviewing comments from participants, some of which have been positive and some negative. A decision on whether to expand the program or even continue the pilot is on hold, and there is no plan or funding to continue it at the present time.[22]

As previously discussed, up to a million people are at risk in the event of a terrorist attack on one of the 100 most at-risk chemical facilities in the United States. In order to close this security gap, once Congress provides the Secretary with authority to set security standards for chemical plants, he should act quickly to ensure the chemical facilities most at-risk of a terrorist attack have substantial surveillance systems in place. In the interim, the Secretary should continue the current pilot program and expand it to the 100 most at-risk chemical plants.

PROMISE #7:
THE DEPARTMENT PROMISED TO COMPLETE VULNERABILITY ASSESSMENTS AT HIGH-RISK CHEMICAL PLANTS

"Vulnerability assessments are underway for the nearly 300 [chemical] sites that could potentially affect more than 50,000 of local surrounding populations. To date, DHS officials have engaged these sites on more than 110 occasions by conducting a variety of assessments. The Department continues to visit these facilities on a

[21] Statement of Secretary Ridge, 8 July 2004.
[22] Committee Staff communications with a chemical industry association official, 25 October 2005.

priority basis in coordination with the state Homeland Security Advisors, state and local law enforcement, and sites owners and operators."[23]

SECURITY GAP # 7:
WITHOUT ON-SITE INSPECTIONS OF THE MOST DANGEROUS CHEMICAL FACILITIES, THE SECURITY OF THESE SITES WILL REMAIN IN QUESTION

As of June 2005, the Department had conducted assessments on roughly 150 chemical facilities, but only about 60 of these assessments involved actual "inside the fence" visits.[24] The remaining assessments were conducted by third parties, by phone, or by review of paperwork.[25]

Without assessments of the vulnerability of the most at-risk chemical facilities, including an on-site inspection of each facility's security systems, we cannot be assured that these sites are adequately protected for the event of a terrorist attack. To close this security gap, the Department must complete assessments of the vulnerability of the 300 most at-risk chemical facilities, including physical inspections, by early next year.

[23] Department of Homeland Security Press Release, 27 April 2005.
[24] Lawrence Stanton, Branch Chief (A), Protective Security Division, DHS IAIP Directorate, Briefing given the Homeland Security Committee Staff, 7 June 2005.
[25] *Id.*

AVIATION

PROMISE #8:
THE DEPARTMENT PROMISED TO HELP AIRPORTS ACQUIRE NEW EXPLOSIVE DETECTION EQUIPMENT

"In addition [the Administrator of the Transportation Security Administration (at the time) Admiral James] Loy announced that he would sign letters of intent for about 20 airports to provide federal assistance for the permanent installation of explosive detection equipment. The letters to airports commit nearly $1 billion of federal funds to pay for 75 percent of the cost of new or existing capital improvement projects. Airports on the list include Dallas - Fort Worth International Airport Boston Logan International Airport Seattle - Tacoma International Airport and Denver International Airport."[26]

SECURITY GAP # 8:
MANY AIRPORTS HAVE NOT RECEIVED THE ASSISTANCE NEEDED TO INSTALL MODERN AND EFFICIENT EXPLOSIVE DETECTION SYSTEMS

In-line explosive detection systems (EDS) are presently the most thorough, speedy, and cost-efficient method of screening checked baggage at airports. These systems use conveyor belts and other equipment to move the baggage quickly through sensors, thereby reducing the number of employees needed to lift and move the baggage; speeding the screening process; and reducing the number of false findings of trace amounts of explosives. Due to the high initial costs of installing EDS, airport operators rely on letters of intent as their principal method for funding them. Over the years, the need for Federal assistance to install in-line EDS has grown. In fact, as of July 2004, GAO reported that TSA had identified 27 additional airports that it believes would benefit from receiving letters of intent for in-line EDS because such systems are needed to screen an increasing number of bags due to current or projected growth in passenger traffic.[27]

Despite the benefits of in-line EDS systems, the Department has fallen far short of its promise to provide 20 airports with assistance to cover the costs of acquiring and installing them. To date, the Department has issued only 8 letters of intent to cover the costs of installing in-line EDS at 9 airports. Moreover, testifying before Congress on March 11,

[26] Transportation Security Administration Press Release, 30 April 2003.
[27] "Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems," GAO-05-365, 15 March 2005.

2004, Acting-TSA Administrator David Stone said that the Department had "[n]o plans for additional LOIs beyond the 8 that have already been signed."[28]

PROMISE # 9:
TSA PROMISED TO IMPROVE AIR CARGO SCREENING

"TSA will establish a Cargo Pre-Screening system that identifies which cargo should be considered "high-risk," and work with industry and other federal agencies to ensure that 100 percent of high-risk cargo is inspected."[29]

"TSA is employing a risk-based, layered approach to air cargo security that balances the twin goals of enhancing security without unduly impeding the flow of commerce."[30]

SECURITY GAP # 9:
CARGO IS STILL NOT ADEQUATELY SCREENED ON PASSENGER AIRCRAFT

Despite TSA's claims that its approach to air cargo security is sufficient to protect Americans from a terrorist attack that uses a bomb hidden in the cargo section of a passenger plane to devastate our nation, GAO recently identified significant problems with TSA's cargo security policies.[31] Additionally, a final regulation from TSA to enhance and improve air cargo security is more than 4 months overdue. It was supposed to be issued by August 14, 2005 under the Intelligence Reform and Terrorism Prevention Act of 2004.[32] Furthermore, TSA has still not developed a methodology to identify elevated risk cargo and ensure that 100% of it is inspected. Congress should require the screening of all cargo carried on passenger planes, just as all passengers and their baggage are screened before boarding.

Rep. Edward Markey (D-MA) and Rep. Christopher Shays (R-CT) have introduced H.R. 4373, the Safe Skies Cargo Security Act, to require a phased-in approach to 100 percent physical inspection of cargo on passenger planes, with one-third inspected in the first year, two-thirds in the second year, and 100 percent after three years.

---

[28] House Appropriations Subcommittee on Homeland Security, 11 March 2004.
[29] Testimony of Acting TSA Administrator David Stone before Senate Appropriations Committee, 23 March 2004.
[30] TSA air cargo briefing materials given to the staff of the House Committee on Homeland Security, September 23, 2005.
[31] "Federal Action Needed to Strengthen Domestic Air Cargo Security," GAO-06-76, 17 October 2005.
[32] P.L. 108-458, § 4053

PROMISE #10:
THE DEPARTMENT PROMISED TO IMPROVE SECURITY AND CREATE SURGE CAPACITY BY MOVING THE FEDERAL AIR MARSHALS TO IMMIGRATION & CUSTOMS ENFORCEMENT

"Federal Air Marshals and U.S. Immigration and Customs Enforcement (ICE) officers have previously operated independently of one another to disrupt threats to civil aviation - often with separate intelligence and regardless of the level of threats to specific targets.

To increase coordination and information sharing between the two and allow for a 'surge capacity' to effectively respond to specific threats, Secretary Ridge announced that the Federal Air Marshal Service (FAMS) and Explosives Unit from the Transportation Security Administration will transfer to ICE.

The move will enhance the security of the traveling public by:

- *Creating a 'surge capacity' to effectively deal with specific threats by cross-training FAMS and ICE agents to help disrupt aviation security related threats.*
- *Allowing for the real-time sharing of sensitive law enforcement information with the FAMS.*
- *Helping law enforcement agencies - federal, state and local - to investigate and respond quickly to incidents at the nation's airports and increase their ability to communicate swiftly and efficiently with DHS personnel involved in screening passengers and cargo leading to comprehensive coverage of the aviation environment.*

The movement of Federal Air Marshals to Homeland Security's U.S. Immigration and Customs Enforcement will significantly increase the number of federal law enforcement agents available to deploy during times of increased threats to aircraft ultimately providing a surge capacity during increased threat periods or in the event of a terrorist attack."[33]

"The recently announced movement of Federal Air Marshals to the Bureau of Immigration and Customs Enforcement will significantly increase the number of Federal law enforcement agents available to deploy during times of increased threats to aircraft, providing a surge capacity during these increased threat periods or in the event of a terrorist attack."[34]

[33] Department of Homeland Security Press Release, 2 September 2003.
[34] Statement of Department of Homeland Security General Counsel Joe Whitley, 7 October 2003.

SECURITY GAP # 10:
MOVING THE FEDERAL AIR MARSHALS DID NOT IMPROVE SECURITY, AND NOW THE DEPARTMENT HAS MOVED THEM AGAIN

The Federal Air Marshal Service (FAMS) was originally moved to Immigrations and Customs Enforcement (ICE) after the GAO found FAMS was facing a severe lack of resource and organizational support from TSA.[35] The move did not provide the promised improvements, as evidenced by Secretary Chertoff's decision to return FAMS to TSA in his Second Stage Review, announced in July 2005.

While the FAMS certainly plays a key role in protecting aircraft from terrorist hijackings, there are still considerable concerns about the level of resources and administrative support the agency is receiving from the Department. In order for the FAMS to continue to keep the skies secure, it will need more support from TSA and the Department than it has received in the past.

PROMISE #11:
THE DEPARTMENT PROMISED TO CREATE AN INTERNATIONAL REGISTERED TRAVELER PROGRAM

"Secretary Ridge and Dutch Minister of Immigration and Integration Rita Verdonk announced that their agencies will work together to develop and pilot an international registered traveler program." As announced by Secretary Ridge, the international registered traveler program would be available to U.S. citizens, U.S. legal permanent residents and foreign visitors who travel frequently to the United States, contingent upon admissibility to the United States and the completion of a background check. Participants would use dedicated kiosks when they arrive at JFK Airport. They would enter the United States without routine Customs and Border Protection (CBP) questioning, unless chosen for a selective or random secondary referral. They would present their machine-readable passport, submit their fingerprints for biometric verification, be photographed, and make a declaration at the kiosk. Once cleared at the kiosk, pilot participants would be allowed to claim their bags and exit the airport.[36]

[35] "Aviation Security: Federal Air Marshal Service is Addressing Challenges of Its Expanding Mission and Workforce, But Additional Actions Needed," GAO-04-242, November 2003.
[36] Department of Homeland Security Press Release, 13 January 2005.

SECURITY GAP #11:
NO PROGRESS ON AN INTERNATIONAL REGISTERED TRAVELER PROGRAM, AS THE FUTURE OF A DOMESTIC REGISTERED TRAVELER PROGRAM IS IN QUESTION

No pilot international registered traveler program was ever started at JFK Airport or elsewhere. International travelers and citizens who travel abroad frequently have no other option than to stand in line for screening by CBP. Considering that the domestic Registered Traveler program is still in the pilot phase, the likelihood of an international registered traveler program being created in the near future is slim. Moreover, the Department has still not adequately answered questions about whether any type of Registered Traveler program will improve aviation security and ensure that all travelers are treated fairly.

RAIL AND MASS TRANSIT SECURITY

PROMISE #12:
THE DEPARTMENT PROMISED TO CONDUCT VULNERABILITY ASSESSMENTS OF AT-RISK RAIL AND TRANSIT NETWORKS

"The Department of Homeland Security's Information Analysis and Infrastructure Protection division and TSA and DOT's Federal Railroad Administration and Federal Transit Administration have conducted comprehensive vulnerability assessments of rail and transit networks that operate in high-density urban areas. The risk-based assessments have provided information on where current and future security resources must be directed to reduce vulnerabilities to terrorism. As a result of these assessments, transit systems are producing robust security and emergency preparedness plans."[37]

SECURITY GAP #12:
UNTIL ALL HIGH-RISK RAIL AND TRANSIT NETWORKS HAVE RECEIVED VULNERABILITY ASSESSMENTS AND UNDERTAKEN SECURITY ENHANCEMENTS, THEY WILL REMAIN AT RISK OF TERRORIST ATTACK

According to the GAO, two different entities within the Department, using two different methodologies, are completing vulnerability assessments of the same transit systems.[38] These assessments are in addition to those completed by the Department of Transportation.[39] As a result, it is unclear whether the vulnerabilities of the rail and mass transit systems in the nation's largest urban areas have been adequately assessed, or whether these systems have taken adequate measures to prevent or respond to a terrorist attack.

[37] Department of Homeland Security Press Release, 22 March 2004.
[38] "Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts," GAO-05-851, September 2005, pp. 4-5.
[39] *Id*.

CYBERSECURITY

PROMISE #13:
THE DEPARTMENT PROMISED TO ENHANCE WARNING & RESPONSE TIME FOR CYBER ATTACKS

"Additionally, the US CERT will work closely with the private sector and technology experts to enhance our warning and response time to a cyber attack - speed action when action is critical . . . . And yet, now, through the U.S. CERT we will provide a range of information products with updates and reports on cyber vulnerabilities, as well as cyber security warnings that outline necessary steps to take in the event of a cyber attack."[40]

SECURITY GAP # 13:
UNTIL A BETTER SYSTEM IS DEVELOPED FOR IDENTIFYING CYBER ATTACKS AND VULNERABILITIES, THE NATION'S CRITICAL INFRASTRUCTURE WILL REMAIN AT RISK

A cyber attack can be designed to move quickly across the internet or other systems and cause substantial damage to critical infrastructure. As a result, it is important for the Department to develop a means for recognizing a cyber attack as quickly as possible and assessing the various systems that could be vulnerable to it. However, according to the Government Accountability Office, "DHS has not yet developed or deployed a national indications and warning architecture for infrastructure protection that would identify the precursors to a cyber attack, and [the National Cybersecurity Division's (NCSD)] analytical capabilities are still evolving and are not yet robust."[41] Moreover, the GAO found that the NCSD "has not yet completed the national cyber threat assessment and the sector vulnerability assessments – or the identification of cross-sector interdependencies – that are called for in the cyberspace strategy."[42]

In order to protect the nation from a potentially devastating cyber attack, the Department must correct these problems. The Department can start by finally appointing an Assistant Secretary for Cyber & Telecommunications. Democrats on the Homeland Security Committee advocated the creation of this position for more than a year, and Secretary Chertoff finally created it during his reorganization of the Department in July. However, during the last 6 months he still has not appointed a person to fill this important position. As a result, the Department's focus on all aspects of cybersecurity has remained weak.

---

[40] Statement of Secretary Ridge, 3 December 2003.
[41] "Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities," GAO 04-434, May 2005, p. 35.
[42] *Id* at 41.

PROMISE #14:
THE DEPARTMENT PROMISED TO IMPROVE PRIVATE SECTOR OUTREACH ON CYBERSECURITY THREATS & VULNERABILITIES

"From small businesses to large enterprises, from home users to owners and operators of critical infrastructures, all will be able to stay informed and improve security practices just by accessing the U.S. CERT website. This alert system is part of a larger, overall effort to raise public awareness about cyber threats."[43]

"The US-CERT will provide a coordination center that, for the first time, links public and private response capabilities to facilitate communication across all infrastructure sectors. In addition, the center will collaborate with the private sector to develop and implement new tools and methods for detecting and responding to vulnerabilities."[44]

SECURITY GAP # 14:
THE PRIVATE SECTOR CAN BE A VALUABLE PARTNER IN PREVENTING A CYBER ATTACK, BUT THE DEPARTMENT MUST DO MORE TO INVOLVE IT IN CYBERSECURITY EFFORTS

The private sector owns the vast majority of the critical infrastructure in the United States, much of which is at risk from a cyber attack. However, the Department must do a lot more to reach out to the private sector and seek its help identifying cyber vulnerabilities and responding to attacks. According to the GAO, "[a]lthough DHS has an active awareness and outreach program under way, more remains to be done to expand awareness of the department's roles, responsibilities, and capabilities. Multiple [critical infrastructure protection] stakeholders have reported that they were unaware of DHS's cybersecurity responsibilities."[45] Additionally, the GAO found that "[a]lthough NCSD has taken steps to develop partnerships and information-sharing mechanisms, the organization has not effectively leveraged its partnerships to increase the sharing of information . . . Regarding NCSD's efforts with the private sector, one [Information Sharing and Analysis Center] reported publicly that its information sharing with DHS was disintegrating."[46]

[43] Department of Homeland Security Press Release, 4 December 2003.
[44] Department of Homeland Security Press Release, 15 September 2003.
[45] "Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities," GAO 04-434, May 2005, p. 48.
[46] *Id* at 32.

CHEMICAL AND BIOLOGICAL THREATS

PROMISE # 15:
THE DEPARTMENT PROMISED TO USE PROJECT BIOSHIELD TO BUY THE COUNTERMEASURES NEEDED TO PROTECT AMERICANS FROM A BIOTERRORIST ATTACK

"And more help is on the way, if Congress approves the President's $6 billion BioShield Initiative, which will provide incentives for pharmaceutical companies to invest in new treatments for anthrax and other deadly diseases."[47]

"Project BioShield allows the Federal Government to pre-purchase critically needed vaccines and medications for biodefense as soon as experts agree that they are safe and effective enough to be added to the Strategic National Stockpile. The Administration is moving forward in purchasing the most important countermeasures and high on the list are next-generation vaccines for both smallpox and anthrax."[48]

SECURITY GAP # 15:
MILLIONS OF AMERICANS REMAIN AT RISK IN THE EVENT OF A CHEMICAL OR BIOLOGICAL ATTACK

Countermeasures will be needed to protect first responders and other vital personnel, as well as normal victims, in the event of a chemical or biological weapons attack. If developed properly and used quickly enough, many countermeasures could prevent injuries to victims or limit the extent of an attack.

Despite the need for the speedy development of chemical and biological countermeasures, to date, only four Material Threat Assessments (MTAs) – the first step in the BioShield process for developing and purchasing countermeasures – have been completed (Anthrax, Botulinum Toxin, Smallpox, and Radiation Exposure).[49] Of the four MTAs completed, only one – anthrax – has resulted in a contract for procurement.[50] Seventy-five million doses of next generation anthrax vaccine are due in 2006.[51] In the interim, the Strategic National Stockpile has ordered 3 million doses of an older vaccine.

---

[47] Statement of Secretary Ridge, 23 July 2003.
[48] Testimony of Secretary Ridge, 12 February 2004.
[49] Testimony of John Vitko, Director, Biological Countermeasures Portfolio, Science & Technology Directorate, Department of Homeland Security, Subcommittee on Emergency Preparedness, Science and Technology, House Committee on Homeland Security, 12 July 2005.
[50] *Id*.
[51] Frank Gottron, "Project Bioshield," Congressional Research Service, RS 21507, 10 June 2005, p. 2.

The Department must move more quickly to complete MTAs and begin the BioShield development and procurement process. Additionally, while the BioShield process is underway to develop the most effective countermeasures possible, the Federal government should stockpile whatever more limited medical devices are available, such as more doses of older versions of the anthrax vaccine.

INTELLIGENCE AND INFORMATION SHARING

PROMISE #16:
THE ADMINISTATION PROMISED THAT THE DEPARTMENT WOULD SERVE AS A LOCATION FOR ANALYZING INTELLIGENCE INFORMATION ON DOMESTIC THREATS

"For the first time in our history information on the threats to America will be gathered and analyzed, together with information on our vulnerabilities in one place. We've got a lot of good people working hard to collect intelligence. This new agency will analyze the intelligence to address vulnerabilities here in America."[52]

"This process will be substantially enhanced by the President's decision to create a terrorist threat integration center. For the first time, all intelligence-gathering agencies will have a central place in which their information is delivered and we'll have groups of analysts to be able to tie all that information."[53]

SECURITY GAP #16:
WITHOUT A WELL-DEFINED ROLE IN THE INTELLIGENCE COMMUNITY, THE DEPARTMENT MAY BE MISSING OPPORTUNITIES TO ASSIST IN INTELLIGENCE EFFORTS

Congress originally planned for the Department to include a collaborative intelligence analysis and integration center. Specifically, the Homeland Security Act created the Information Analysis and Infrastructure Protection Directorate (IAIP) in order to collect, analyze, and disseminate intelligence information about terrorist threats to the nation.[54] In early 2003, however, just months after the IAIP's creation, the Bush Administration began wrestling that function from the Department by creating a separate entity under the Director of Central Intelligence known as the Terrorist Threat Integration Center (TTIC).[55] The TTIC – staffed by representatives on assignment from the CIA, the FBI, the Department of Homeland Security, and other agencies – inherited many of the analysis responsibilities of the IAIP before it was even fully established.[56] In response to the 9/11 Commission's

[52] Statement of President Bush, 12 November 2002.
[53] Department of Homeland Security Press Release, 3 March 2003.
[54] Homeland Security Act, § 121.
[55] "The White House, Fact Sheet: Strengthening Intelligence to Better Protect America," Press Release, 8 January 2003, available at http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html; *see also* "DHS Challenges in Consolidating Terrorist Watch List Information," Department of Homeland Security Inspector General, OIG-04-31, August 2004, (describing reasons why DHS was unprepared to take on intelligence fusion role anticipated by Congress).
[56] *See* James J. Carafano & David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security*, The Heritage Foundation and the Center for Strategic and International Studies, available at http://www.csis.org.hs/041213_dhsv2.pdf (Dec. 13, 2004); Justin Rood, "A Curtain Comes Down on Homeland's Key Role in Counterterror Analysis," *Congressional Quarterly*, 12 October 2004; Justin Rood,

recommendations, the President subsequently shifted the analysis function to the National Counterterrorism Center (NCTC).[57] The Administration's actions essentially gutted the Department's intelligence role. The Department's authority problems have been compounded by the perception that it is only a "junior member" of the Intelligence Community with little to offer in terms of information assets.[58]

To strengthen the Department, Secretary Chertoff recently created a new Office of Intelligence & Analysis, headed by the Chief Intelligence Officer (CIO). However, it is unclear what this new office's intelligence mission or level of authority within the Intelligence Community will be. If the Department's CIO does not have a clearly defined intelligence mission, numerous opportunities to develop, analyze, or disseminate intelligence may be lost. Nonetheless, the Department can have a valid place in the intelligence community if its role is properly established. For example, the Department could be very useful to the Intelligence Community if it is given a stronger responsibility for distributing intelligence information to state and local officials.

PROMISE #17:
THE DEPARTMENT PROMISED THAT THE TERRORIST SCREENING CENTER WOULD BE AN EFFECTIVE, UNIFIED LOCATION FOR INFORMATION ON TERRORISTS

"The [Terrorist Screening] Center will ensure that government investigators, screeners and agents are working off the same unified, comprehensive set of anti-terrorist information - and that they have access to information and expertise that will allow them to act quickly when a suspected terrorist is screened or stopped."[59]

"Just a few weeks ago Secretary Ridge, Attorney General Ashcroft, Secretary of State Powell, and FBI Director Mueller announced the establishment of the Terrorist Screening Center to

- *Consolidate terrorist watchlists and*
- *Provide 24/7 operational support for thousands of Federal screeners, investigators, and agents across the country and around the world.*

"Analysis: New Counterterror Center Proposals Make DHS Intel Efforts 'Irrelevant,'" *Congressional Quarterly*, 30 September 2004; Seth G. Jones, "Terrorism and the Battle for Homeland Security," Foreign Policy Research Institute, 21 May 2004, available at http://www.fpri.org/enotes/20040521.americawar.jones.terrorismdhs.html; Michael Crowley, "Bush's Disastrous Homeland Security Department," *The New Republic*, 15 March 2004; Markle Foundation, *Creating a Trusted Information Network for Homeland Security, Second Report of the Markle Foundation Task Force* (2003), p. 2.

[57] "The White House, Reforming and Strengthening Intelligence Services," Press Release, 8 September 2004, available at http://www.fas.org/irp/news/2004/09/wh090804.html); "Making America Safer by Strengthening Our Intelligence Abilities," Press Release, The White House, 2 August 2004, available at http://www.fas.org/irp/news/2004/08/wh080204-fact.html.

[58] "Homeland Security Looks to Overhaul Intelligence Arm," *USA Today*, 18 June 2005.

[59] Department of Homeland Security Press Release, 16 September 2003.

- *The Center will ensure that all are working off the same unified, comprehensive set of anti-terrorist information and that they have access to expertise that will allow them to act quickly when a suspected terrorist is screened or stopped.*
- *The Center will also help to prevent false positive matches from causing unnecessary delay in the travel of law abiding persons.*
- *The job of the Center is to make sure DHS gets information from TTIC out to personnel on the borders and those who can put it to use on the front lines - and get it there fast.*
- *To provide increased security at the Nation's borders we are equipping our inspectors and Border Patrol Agents with state-of-the-art technology, including radiation pagers and non-intrusive inspection machines."*[60]

"We will integrate our watch lists so law enforcement will have comprehensive information to screen for potential terrorists."[61]

SECURITY GAP #17: EFFORTS TO DEVELOP AND MAINTAIN TERRORIST WATCHLISTS ARE STILL ENCOUNTERING PROBLEMS THAT MUST BE CORRECTED TO PREVENT TERRORISTS FROM ENTERING THE U.S.

Although the Terrorist Screening Center (TSC) is operating and has successfully created a single, consolidated terrorist watch list, the Department of Justice's Inspector General concluded that the TSC is plagued by deficiencies: (1) the TSC cannot ensure that that the information in its database is complete and accurate; (2) the TSC has no formal strategic plan by which to guide its progress, staffing, organizational structure and future planning; (3) the TSC is experiencing considerable staffing problems and managerial weaknesses (most employees are detailees); and (4) the TSC is riddled with training problems and poor quality controls.[62] Donna Bucella, the TSC Director, is also reportedly seeking additional funds in order to finance system improvements.[63]

The 9/11 Commission found that many of the 9/11 hijackers repeatedly entered and exited the United States using their real names.[64] Therefore, the TSC's responsibility for developing and maintaining a comprehensive terrorist watchlist is a vital part of the War on Terror. In order to ensure that the TSC successfully fulfills this role, the organizational, staffing, and funding problems it faces must be corrected.

---

[60] Statement of Department of Homeland Security General Counsel Joe Whitley, 7 October 2003.
[61] Statement of Secretary Ridge, 24 February 2004.
[62] Chris Strohm, "Terrorist Screening Center Plagued by Deficiencies, Audit Finds," *GovExec.com*, 14 June 2005, available at http://www.govexec.com/dailyfed/0605/061405c1.htm.
[63] Wilson P. Dizard III, "Bucella: More Funding Needed for Terrorist Watch List Center," *GCN.com*, 28 June 2005, available at http://appserv.gcn.com/vol1_no1/homeland-security/36235-1.html.
[64] Final Report of the National Commission on Terrorist Attacks on the United States (2004), p. 366

PROMISE #18:
THE DEPARTMENT PROMISED TO CREATE A SINGLE, EFFECTIVE NETWORK FOR SHARING INTELLIGENCE INFORMATION WITH STATE AND LOCAL OFFICIALS

"Homeland Security Information Network. Expanded this real-time computer based counter terrorism communications network to all 50 states, 5 territories, Washington, D.C. and 50 other major urban areas. Strengthens the two-way flow of current threat information to state, local, and private sector partners."[65]

SECURITY GAP #18:
WITHOUT A NETWORK FOR EFFECTIVELY SHARING INTELLIGENCE INFORMATION WITH LOCAL OFFICIALS, TERRORISTS COULD GO UNNOTICED OR EVADE CAPTURE

Although the Homeland Security Information Network (HSIN) is now operating, there are significant problems with its future development and deployment. The Department had planned for the Joint Regional Information Exchange System (JRIES), which is used by police intelligence units nationwide to share sensitive case information, to be a foundation for the HSIN. In May 2005, JRIES' executive board – which includes intelligence directors from New York City, Washington, D.C., and Los Angeles – broke off discussions with the Department and terminated efforts to assimilate the system into the HSIN. The disagreements essentially stemmed from different visions of how HSIN should operate. JRIES' executives wanted the HSIN to be a decentralized virtual analytical unit, while the Department wanted to set it up as a "one box" location where all information is stored. JRIES' executives likewise opposed for security and legal reasons the Department's inclusion of state homeland security advisers and other non-law enforcement sources in the network. JRIES' executives were frustrated by apparent leaks of sensitive case file information from at least one HSIN user earlier this year.[66]

Although police agencies still share information within the HSIN, JRIES' officials report that they are not sharing the most sensitive information. The Department has attempted to fully return JRIES to the HSIN effort through a Memorandum of Understanding, but efforts are ongoing and results are uncertain.[67]

---

[65] Department of Homeland Security Press Release, 6 January 2005.

[66] Alice Lipowicz, "Schism Downs JRIES Homeland Security Network," WashingtonTechnology.com , 5 October 2005, available at http://www.washingtontechnology.com/news/1_1/daily_news/27115-1.html.

[67] *Id.*

Without full cooperation of JRIES and its members, the Department's ability to create a truly universal mechanism for sharing intelligence information with local officials will be seriously reduced. This may reduce the chances of identifying and capturing terrorist cells.

PROMISE #19:
THE DEPARTMENT PROMISED TO STREAMLINE INTELLIGENCE INFORMATION SHARING

"Another immediate goal for the department is to streamline and strengthen information sharing. We will examine how we generate information and how we share it, not just within the federal family, but with the state and locals, as well."[68]

SECURITY GAP #19:
BY FAILING TO STREAMLINE INTELLIGENCE INFORMATION SHARING, OPPORTUNITIES TO IDENTIFY TERRORISTS WILL BE LOST

Given the problems identified with the HSIN, it is unclear whether the Department is doing all it can to streamline and strengthen information sharing. Moreover, a January 2005 survey conducted by the National Governors Association Center for Best Practices concluded that information disseminated by the FBI and the Department, "could be improved, as the majority of [survey] respondents are only somewhat satisfied with the timeliness, specificity and actionable nature of the information received."[69]

Until the Department strengthens its information sharing mechanisms, and the quality of the information disseminated through them, opportunities to provide local officials with the information they might need to identify and capture terrorists may be lost.

PROMISE #20:
THE DEPARTMENT PROMISED TO BETTER SHARE INFORMATION WITH PRIVATE OWNERS OF CRITICAL INFRASTRUCTURE

"First, we will improve our information sharing and infrastructure protection, namely by improving partnerships within the government and with the private sector to strengthen vertical communication systems and significantly increase permanent protections around our nation's most vital assets."[70]

---

[68] Department of Homeland Security Press Release, 30 January 2003.
[69] Jessica Toliver, *Homeland Security in the States: Much Progress, More Work*, NGA Center for Best Practices, 24 January 2005, available at http://preview.nga.org/Files.pdf/0502HOMESEC.pdf.
[70] Statement of Deputy Secretary Admiral Loy, 26 April 2004.

SECURITY GAP #20:
OWNERS OF CRITICAL INFRASTRUCTURE NEED INFORMATION ABOUT TERRORISTS AND VULNERABILITIES TO SECURE THEIR ASSETS

Over 80% of the nation's critical infrastructure is in private hands. However, the Department has not worked to effectively involve the owners of critical infrastructure in efforts to prevent terrorism. For example, a report prepared by the Heritage Foundation found that the Department has not clearly defined what it believes are reasonable actions for the private sector to take to reduce vulnerabilities in its critical infrastructure.[71] The Department has also failed to address private business fears about their homeland security-relevant information being disclosed to competitors.[72]

To address these problems, the Heritage Foundation recommended the creation of a position of Undersecretary for Protection and Preparedness (largely adopted as part of Secretary Chertoff's recent reorganization of the Department), as well as, among other things: (1) a removal of roadblocks to creating a risk-based system that engages the private sector, and (2) the development of an "effective means for sharing information among federal and state government agencies, the private sector, and other entities."[73]

H.R. 4009, introduced by the Ranking Member of the House Homeland Security Committee, Rep. Bennie G. Thompson (D-MS), would address many of the Heritage Foundation's recommendations by requiring the Secretary to develop policies and practices to better share information with owners of critical infrastructure. Congress should act quickly to pass this measure.

PROMISE #21:
THE DEPARTMENT PROMISED TO CREATE A NETWORK FOR COMMUNICATING CLASSIFIED INFORMATION

"The HSDN will significantly enhance DHS' capability to interact with other classified networks while simultaneously eliminating the department's dependence on networks external to DHS. Looking to the future, the [Homeland Security Data Network] will be designed to be scalable in order to respond to increasing demands for the secure transmission of classified information among government, industry, and academia crucial to defending America from terrorist attacks."[74]

---

[71] Alane Kochems, "Who's on First? A Strategy for Protecting Critical Infrastructure," *Backgrounder* 9 May 2005, available at http://www.heritage.org/Research/HomelandDefense/bg1851.cfm.
[72] James J. Carafano & David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security*, The Heritage Foundation and the Center for Strategic and International Studies, 13 December 2004, available at http://www.csis.org.hs/041213_dhsv2.pdf.
[73] *Id* at 4.
[74] Department of Homeland Security Press Release, 12 April 2004.

SECURITY GAP #21:
IF CLASSIFIED INFORMATION IS NOT SHARED WHEN APPROPRIATE, OPPORTUNITIES TO STOP TERRORISTS COULD BE MISSED

According to Matthew Broderick, director of the Homeland Security Operations Center, the Homeland Security Data Network (HSDN) will not be initiated until fiscal year 2007.[75] The Department must speed this process. While classified information should only be shared when relevant, local law enforcement officers and others may have opportunities to prevent a terrorist attack if they are exposed to it in a proper and secure way.

PROMISE #22:
THE DEPARTMENT PROMISED TO CREATE A NETWORK FOR SHARING SECRET AND UNCLASSIFIED INFORMATION BY THE END OF 2004

"The Department introduced the Homeland Security Information Network (HSIN) on February 24, 2004, a real-time counter terrorism communications network currently connected to all 50 states as well as more than 50 major urban areas. This program significantly strengthens the two-way flow of real-time threat information at the Sensitive-but-Unclassified level between the State, local and private sector partners. By the end of this year, information at the SECRET level will be able to be shared with HSIN users."[76]

SECURITY GAP #22:
DELAYS IN CREATING A NETWORK FOR SHARING SECRET INFORMATION DEMONSTRATES THE DEPARTMENT'S INABILITY TO MOVE QUICKLY TO ENLIST LOCAL AND PRIVATE SECTOR PARTNERS IN THE SEARCH FOR TERRORISTS

HSIN-Secret – the network on which Secret level information could be relayed to state and local partners – was not completed until July of 2005.[77] While the successful development of the HSIN-Secret network is good news, the fact that it was not completed until months after promised demonstrates that the Department still has difficulties sharing even low level intelligence information with local and private sector partners. If the Department does not better commit itself to sharing a variety of intelligence information with people and organizations in a position to identify terrorists, then opportunities to prevent another attack in the United States may be lost.

---

[75] Alice Lipowicz, "The Secret is Out: DHS Launches State-Local Network," *GCN.com*, 20 July 2005, available at http://www.gcn.com/vol1_no1/daily-updates/36443-1.html.
[76] Department of Homeland Security Press Release, 15 December 2004.
[77] Alice Lipowicz, "The Secret is Out: DHS Launches State-Local Network," *GCN.com*, 20 July 2005.

BORDER SECURITY

PROMISE #23:
THE ADMINISTRATION AND THE DEPARTMENT PROMISED TO CONTROL OUR BORDERS BY PROVIDING ENOUGH PERSONNEL AND TECHNOLOGY

"The new Department will control our borders. I mentioned the border – we need to know who's coming in, we need – but there's three agencies on the border right now, and they're all full of fine people. They wear different uniforms, they have different strategies. Sometimes they talk, sometimes they don't. There is a better way to enforce our border here in America."[78]

"And one of our first goals for the department this year is to integrate old functions in a new way, to make us stronger and safer. As a first step to accomplish this, we will restructure our border agencies."[79]

"We're also hiring 1,700 new inspectors and hundreds of Border Patrol Agents and equipping them with state-of-the-art technology, including non-intrusive inspection machines and radiation pagers."[80]

SECURITY GAP #23:
A COMPREHENSIVE STRATEGY FOR PROVIDING THE PERSONNEL, TECHNOLOGY AND OTHER RESOURCES NEEDED TO SECURE THE BORDER HAS NEVER BEEN DEVELOPED

The Administration and the Department have never developed a comprehensive border strategy that addresses personnel, technology, and other needs. The lack of a comprehensive strategy has led to many ad hoc or inexplicable actions. For example, although the former Commissioner of Customs and Border Protection, Robert Bonner, once told Congress that "We need more Border Patrol agents, there's no question about that,"[81] the President's proposed budget for fiscal year 2006 only requested funding for 210 new agents.[82] The President made this low personnel request even though the 9/11 Act authorized the hiring of another 2,000 Border Patrol agents per a year.[83]

The development of a comprehensive border security strategy would force the Administration to evaluate and provide the resources that are genuinely needed to secure the

[78] Statement of President Bush, 12 November 2002.
[79] Department of Homeland Security Press Release, 30 January 2003.
[80] Statement of Secretary Ridge, 23 July 2003.
[81] Testimony of Robert C. Bonner, Commissioner of U.S. Customs and Border Protection, House Government Reform Committee, 12 May 2005.
[82] Jennifer E. Lake and Blas Nunez-Neto, *Homeland Security Department: FY 2006 Appropriations*, Congressional Research Service, 5 October 2005.
[83] Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, § 5202.

border. It would also serve as a means for holding the Administration accountable for its successes or failures in securing the border. As a result, Congress should pass legislation quickly to force the Administration and the Department to produce this type of strategy.

PROMISE #24:
THE DEPARTMENT PROMISED TO CREATE A WORKING "ONE FACE AT THE BORDER" PROGRAM

"The One Face at the Border Initiative unifies the inspection process by cross-training CBP inspectors to perform all three inspection functions. Travelers will now meet a single primary inspection officer specially trained to determine who needs to go through secondary inspections – another significant step for Homeland Security to create efficiencies and unity around a single mission . . . . By utilizing one employee to perform all three primary inspection functions, the Department will be able to deploy additional employees into secondary inspection thus targeting our resources towards those passengers with suspicious indicators."[84]

SECURITY GAP #24:
IF STEPS ARE NOT TAKEN TO STRENGTHEN THE ONE FACE AT THE BORDER INITIATIVE, INSPECTIONS MAY NOT BE THOROUGH ENOUGH

Although the Once Face at the Border initiative is operating as personnel from several previously separate entities have been integrated into one inspection force, concerns have been raised about the loss of expertise as inspectors now have to focus on more areas. For example, a report published by the Migration Policy Institute (MPI) raised concerns about whether sufficient steps have been taken to ensure that customs, immigration, and agriculture expertise is retained as personnel from what was previously three separate entities are integrated into one workforce.[85] It also noted, among other things, that CBP should: (1) take steps to incorporate additional subject matter (i.e. customs, immigration, and agriculture) expertise into the training of new CBP officers; (2) accelerate delivery of cross-training for incumbent inspectors; (3) reconsider the minimum requirements for the CBP officer position; and (4) provide greater equity in the leadership and promotion opportunities available to former immigration employees now working in the field as part of the One Face at the Border initiative.[86]

The Department should act quickly to implement the MPI's recommendations and thereby ensure that the One Face at the Border initiative can successfully prevent the entry of terrorists while also enforcing customs, immigration, and agricultural regulations.

---

[84] Department of Homeland Security Press Release, 2 September 2003.
[85] Deborah Waller Meyers, *One Face at the Border: Behind the Slogan*, Migration Policy Institute, June 2005.
[86] *Id* at 54-57.

PROMISE #25:
THE DEPARTMENT PROMISED TO CREATE EFFECTIVE WAYS TO MOVE REGULAR TRAFFIC ACROSS THE BORDERS

"But here again, we've made great progress over the past 18 months. We have forged agreements with Canada and Mexico to create smart borders, 21st century borders, to keep terrorists out while letting legitimate goods and people through. One key to this is our Nexus program, which reduces border delays for people known to both sides as non-terrorists, and which is now in operation at most of our major crossings along the northern border."[87]

SECURITY GAP #25:
LOW RISK TRAFFIC ALONG THE NORTHERN BORDER IS NOT BEING MOVED QUICKLY ENOUGH, LEADING TO LONGER WAIT TIMES AND A LACK OF FOCUS ON MORE HIGH-RISK TRAFFIC

The NEXUS program is used at land ports of entry along the northern border to facilitate the speedy passage of low-risk, frequent travelers. Although the NEXUS program has been somewhat expanded along the northern border, the user base has not been broadened enough. The Department should move to promote a large expansion of the program. Wider enrollment would allow for the quicker movement of low-risk people and goods, thereby avoiding long wait-times and allowing the Department's border agents to concentrate on security concerns.[88]

PROMISE #26:
THE DEPARTMENT PROMISED MORE RADIATION SCREENING EQUIPMENT FOR BORDER INSPECTORS

"To provide increased security at our borders, we are equipping our inspectors and Border Patrol Agents with state-of-the-art technology, including radiation pagers and non-intrusive inspection machines."[89]

SECURITY GAP #26:
THE DEPARTMENT HAS NOT EQUIPPED ITS BORDER INSPECTORS AND AGENTS WITH ENOUGH MODERN TECHNOLOGY

Although the Department has provided basic radiation pagers to all of its inspectors and border agents, the promised "state-of-the-art" technology has been made less readily

[87] Statement of Secretary Ridge, 3 March 2003.
[88] Carolyn Thompson, "Bill Aims To Speed Border Passage, Congresswoman: N.Y. lags in signing up people in no-wait, security-check program," *Associated Press*, 9 July 2005.
[89] Department of Homeland Security Press Release, 20 August 2003.

available to them. A 2005 CBP fact sheet on the use of technologies along the border reveals a continuing widespread use of older, less reliable technologies.[90] For example, while there are more than 10,500 CBP officers with basic personal radiation detectors, there are only 500 radiation isotope identifiers in use.[91] These identifiers are hand-held instruments used by CBP officers to determine the exact identity of a radioactive source causing an alarm.[92] Additionally, there are only 166 Large-scale Gamma-ray/X-ray Imaging Systems in use.[93] These systems produce transmission and reflected images of the contents of a cargo container, rail car, vehicle or trailer-truck.[94] CBP officers analyze these images to determine where there are anomalies associated with the cargo listed on the manifest.[95]

The Department must move faster to equip border inspectors and agents with more of the most up-to-date technologies for screening people and cargo. More widespread use of modern technology will permit these officials to focus on real security risks while speeding normal traffic.

PROMISE #27:
THE DEPARTMENT PROMISED THAT IT WAS DEPLOYING EFFECTIVE UNMANNED VEHICLES TO SECURE THE BORDER

"The UAV program, as I understand, did work well. We are currently working now to begin the process of procuring UAVs. We'd like to get that done in a matter of months and start to put UAVs up and have them flying over the border."[96]

SECURITY GAP #27:
MORE EFFORTS MUST BE MADE TO STRENGTHEN AND EXPAND UNMANNED AERIAL VEHICLE RESEARCH AND PROCUREMENT TO MAKE THEM EFFECTIVE AT THE BORDERS

Although the Department recently began the procurement process to acquire unmanned aerial vehicles (UAVs) for the border,[97] there are still problems with UAVs generally, such as weather limitations.[98] More efforts must be undertaken to strengthen research, development

[90] "CBP: Securing Our Borders - Inspection and Surveillance Technologies," Press Release, 5 May 2005, available at http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/fact_sheet_cbp_securing.xml.
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] Testimony of Secretary Chertoff, 13 April 2005.
[97] "CBP Makes History with the Launch of Predator B Unmanned Aerial Vehicle Unveiled to Secure Border," CBP Press release, 29 September 2005, available at http://www.cbp.gov/xp/cgov/newsroom/press_releases/09292005.xml.
[98] Jason Blazakis, "Border Security and Unmanned Aerial Vehicles," *Congressional Research Service*, RS 21698, 2 January 2004, pp. 4-5.

and testing of UAVs. Moreover, no matter how effective, UAVs are still incapable of many enforcement actions for which a human officer is needed. Until this Administration fulfills the commitments in the 9/11 Act to hiring 2,000 new Border Patrol agents per a year, those needs will remain unmet.

PROMISE #28:
THE DEPARTMENT PROMISED TO TAKE A STRONGER LEAD IN VISA POLICY AND IN CORRECTING PROBLEMS WITH VISAS

"In the area of policy, DHS will now establish most visa policy, have final approval over most Department of State initiated guidance, review implementation of visa policy, and ensure that homeland security requirements are fully reflected in the visa process."[99]

SECURITY GAP #28:
THE DEPARTMENT'S ROLE IN THE VISA PROCESS REMAINS UNCLEAR

A September 2005 GAO report on the visa process indicates that while progress has been made to improve visa security, work remains to be done. According to the GAO, "Despite … improvements, we found that further actions are needed to enhance the process. Consular officers we interviewed said that guidance is needed on interagency protocols regarding DHS staff's roles and responsibilities overseas."[100] Furthermore, GAO indicated that the Department of State, not the Department of Homeland Security, is taking the lead in this process. For example, the GAO stated that "Since 2002 … the Assistant Secretary in the [State Department] Bureau of Consular Affairs has taken a leading role in implementing changes to the visa process and promoting its use as a screen against potential terrorists"[101] and "DHS has not provided guidance to consular officers regarding the roles and geographic responsibilities for its personnel."[102]

Until the role of each agency involved in the visa process is clarified, risks may remain that security problems could go unnoticed or uncorrected.

---

[99] Testimony of Under Secretary for Border and Transportation Security Asa Hutchinson, 30 September 2003.
[100] "Border Security, Strengthened Visa Process Would Benefit from Additional management Actions by State and DHS," Statement of Jess T. Ford, Director International Affairs and Trade, Testimony before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, 13 September 2005, p. 2.
[101] *Id* at 6.
[102] *Id* at 7.

PROMISE #29:
THE DEPARTMENT PROMISED TO MAKE US-VISIT A SYSTEM FOR TRACKING ENTRY AND EXIT AT THE BORDER

"…[W]e are on track to meet the December 31, 2004 deadline to integrate entry-exit databases at the 50 busiest land border ports of entry and to deploy biometric capabilities to verify certain visa holders."[103]

"US-VISIT is a continuum of security measures that begins overseas, when a person applies for a visa to travel to the United States, and continues on through entry and exit…"[104]

SECURITY GAP #29:
US-VISIT IS STILL NOT FULLY FUNCTIONING AND EVEN ONCE COMPLETE, IT WILL NOT SECURE ALL ENTRIES AND EXITS

Although the technology for entry procedures has been developed and put in place at many ports of entry, the technology for exit procedures is still not fully ready. For example, a GAO team traveled to Alexandria Bay, NY in October 2005 to inspect the US-VISIT test site there, one of five at which radio frequency exit processes are being tested. The test phase there is not scheduled to conclude until the spring of 2006. The GAO indicated that while the radio-frequency exit check technology appears to function, there are still several apparent problems, including that it does not meet Congress' demand for a biometric confirmation of exit. GAO also noted that the Department is not yet willing to provide any data on the technology's effectiveness.[105]

Additionally, US-VISIT's overall goal of securing the border will remain unfulfilled once the program is completed because neither entry nor exit data will be collected from Mexicans or Canadians at land borders. These two nationalities make up 78% of U.S. border crossings, meaning only 22% of those people entering and exiting the United States will fall under US-VISIT. [106]

---

[103] Testimony of Under Secretary for Border and Transportation Security Asa Hutchinson, 28 January 2004.
[104] Department of Homeland Security Press Release, 21 December 2004.
[105] GAO briefing given Committee Staff, 7 October 2005.
[106] Jessica M. Vaughan. "Modernizing America's Welcome Mat: The Implementation of U.S. Visit," *Center for Immigration Studies Report,* August 2005, p. 3.

PROMISE #30:
THE DEPARTMENT PROMISED THAT US-VISIT WOULD HELP PREVENT VISA OVER-STAYS

"US VISIT will also provide a useful tool to law enforcement to find those visitors who overstay or otherwise violate the terms of their visas.[107]

SECURITY GAP #30:
US-VISIT IS STILL NOT DESIGNED TO PRODUCE A LIST OF VISA OVER-STAYS THAT CAN BE TURNED OVER TO LAW ENFORCEMENT

The Department does not have a program in place to take exit data and compare it against entry documents, which would be necessary to create a list of visa overstays to be turned over to law enforcement. There are currently no plans to implement this feature. The Center for Immigration Studies has noted that "for the moment, DHS seems content to use the US-VISIT exit-recording feature primarily for workload reduction purposes rather than pro-active interior enforcement."[108]

[107] Department of Homeland Security Press Release, 29 April 2003.
[108] *Id* at 10.

DEPARTMENT MANAGEMENT

PROMISE #31:
THE DEPARTMENT PROMISED TO CREATE EFFICIENT PROCUREMENT PRACTICES

"The department has implemented new and consolidated acquisition policies and procedures (Homeland Security Acquisition Regulations and Homeland Security Acquisition Manual) that are among the most flexible in the entire federal government. Publication of this regulation and guidance was another major step in combining the cultures of 22 disparate agencies by ensuring that these organizational elements now operate under a single, department-wide program regulation."[109]

SECURITY GAP #31:
A LACK OF CENTRALIZED PROCUREMENT AUTHORITY HAS PREVENTED THE DEPARTMENT FROM PURCHASING THE MOST EFFECTIVE SECURITY MEASURES

The Department has implemented a new procurement system, but it is still understaffed and only one office that has the authority to procure goods and services directly reports to the Chief Procurement Officer.[110] Therefore, although the Department has used a system of interlocking rules to accomplish the appearance of cohesion, no overarching single authority currently exists over all procurements in the agency. As a result, the Department has suffered from numerous contracting scandals and errors, leading to a waste of taxpayer dollars and the loss of opportunities to purchase the best materials possible for securing the nation.

Democrats on the House Homeland Security Committee have introduced H.R. 4009, which would create more centralized procurement, financial management, and human resource management offices in the Department. Congress should act quickly to pass these measures in order to ensure the Department purchases and hires the best people and equipment possible.

[109] Department of Homeland Security Press Release, 11 February 2004.
[110] U.S. Department of Homeland Security FY 2005/2006 Acquisition Strategic Plan (provided to Committee Staff in a briefing on 23 September 2005).

PROMISE #32:
THE DEPARTMENT PROMISED TO IMPROVE RESOURCE MANAGEMENT

"The goal of eMerge2, which stands for 'electronically Managing enterprise resources for government effectiveness and efficiency,' is to improve resource management and enable the bureaus to move 'Back Office' effectiveness and efficiency to 'Front Line' Operations"[111]

SECURITY GAP #32:
THE DEPARTMENT STILL LACKS AN EFFECTIVE RESOURCE MANAGEMENT SYSTEM

After many false starts, the Department announced in July that it was reevaluating the eMerge2 program.[112] Although the eMerge2 program itself may not be the best solution to the Department's resource management needs, there is no question that the Department needs a more effective system for acquiring, tracking, and using resources. Until the Department fulfills this need, resources needed to secure the nation will continue to be wasted or unavailable.

PROMISE #33
THE DEPARTMENT PROMISED TO BUILD AN EFFICIENT, FAIR HUMAN RESOURCE SYSTEM

"The Human Resources System design team was appointed to develop options for a flexible and contemporary personnel system which meets the mission needs of the department while preserving fundamental merit principles. The team included department managers and employees, HR experts from Homeland Security and from the Office of Personnel Management, and representatives from the agency's three largest labor unions. The regulations to launch the new system will be announced shortly."[113]

"DHS and OPM have worked with the Director of the Federal Mediation and Conciliation Service to draft procedures to govern the legislatively-mandated "meet and confer" process -- we will be reaching out to employee representatives who commented on the proposed regulations to include them in this process as appropriate. Additionally, DHS and OPM have continued to have discussions with the three major unions representing DHS employees -- to ensure a clear understanding of their joint comments and to agree on the process going forward."[114]

---

[111] Testimony of Deputy Secretary James Loy, 6 May 2004.
[112] Amelia Gruber, "Homeland Security Financial Management Project in Limbo," *Govexec.com*, 16 August 2005.
[113] Department of Homeland Security Press Release, 11 February 2004.
[114] Testimony of Deputy Secretary James Loy, 6 May 2004.

"The implementation plan for MAXHR includes a multi-year schedule. Using the framework established in the regulations, work will begin in establishing new policies and procedures for labor relations, adverse actions, and appeals including the formation of the Homeland Security Labor Relations Board. The new performance management system is expected to launch in the fall of 2005 with pay and classification changes implemented the following year for some employee groups. Work will also be underway in the first year to develop HR information technology solutions to support this initiative.

Communicating these changes is a critical part of the MAXHR effort, and the Department of Homeland Security has made a serious commitment to ensure employees receive the information and training they need throughout implementation of the program. In the coming months, the department will roll out briefing sessions, satellite broadcasts, web-based training modules, classroom training, print materials, and frequent updates to the MAXHR Web site."[115]

SECURITY GAP #33:
THE DEPARTMENT RISKS EMPLOYEE MORALE BY CONTINUING TO DEVELOP THE UNFAIR MAXHR SYSTEM

Implementation of the MAXHR system has been blocked by the courts, which have found its provisions so lacking in fairness as to be a violation of collective bargaining rights.[116] If the Department continues to pursue implementation of the MAXHR system, it will risk undermining the morale of the people working on the front-line of homeland security. The Department should stop pursuing implementation of the MAXHR system and instead ensure that its employees have a truly fair and efficient human resource system.

[115] Department of Homeland Security Press Release, 26 January 2005.
[116] "Unions File Suit Over Pentagon Pay System," *Associated Press*, 7 November 2005.

This Page Intentionally Left Blank