THE STATE OF HOMELAND SECURITY 2007

An Annual Report Card on the Department of Homeland Security

Prepared by the Majority Staff of the Committee on Homeland Security
Congressman Bennie G. Thompson (D-MS), Chairman

PREPARED FOR:

Representative Bennie G. Thompson,
Chairman of the Committee on Homeland Security

Representative Loretta Sanchez,
Vice Chair of the Committee and Chairwoman of the Subcommittee on Border, Maritime and Global Counterterrorism

Representative Jane Harman,
Chairwoman of the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment

Representative Sheila Jackson-Lee,
Chairwoman of the Subcommittee on Transportation Security and Infrastructure Protection

Representative James R. Langevin,
Chairman of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

Representative Henry Cuellar,
Chairman of the Subcommittee on Emergency Communications, Preparedness, and Response

Representative Christopher P. Carney,
Chairman of the Subcommittee on Management, Investigations, and Oversight

Representative Ed Markey

Representative Norman D. Dicks

Representative Peter DeFazio

Representative Nita Lowey

Representative Eleanor Holmes Norton

Representative Zoe Lofgren

Representative Donna Christensen

Representative Bob Etheridge

Representative Yvette D. Clarke

Representative Al Green

Representative Ed Perlmutter

TABLE OF CONTENTS

Subject Areas:

EXECUTIVE SUMMARY

On March 1, 2007, the Department of Homeland Security celebrated its fourth anniversary. More than 170,000 employees from twenty-two agencies were brought together to prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation. On February 12, 2007, the House of Representatives, and later the Senate, passed resolutions recognizing and honoring the employees of the Department for their efforts and contributions to protect and secure the Nation. Despite the valiant efforts of the employees at the Department, there are troubling signs that the Department's leadership is critically challenged with regard to executing the basics of strategic planning and organizational planning, financial management, integration and coordination.

Some areas of challenge include:

- A shortage of contracting and technical management personnel in the immediate term serving critical acquisition programs;
- The lack of a financial management system that can give timely, critical insight into all levels of department expenditures; and,
- Responding in a timely manner to requests for information.

In order to fully understand the Department's progress, the Committee Democrats have instituted this annual report card for the Department of Homeland Security. In each of the significant 17 homeland security issue areas for which the Department has responsibility, we are grading their performance, as well as identifying what the organization must do to improve and raise its grade.

The Department's performance in each of the 17 areas can be summarized as follows:

- **Border Security:** The Department's grade in this area is an **Incomplete**. The Department needs adequate SBI*net* procurement, management, and oversight resources in place to prevent the same procurement and deployment problems experienced by the Department with previous border security technology systems. The Department also needs to make adequate preparations, prior to the deadline for implementing the land and sea portions of the Western Hemisphere Travel Initiative, to meet the mandate of the program without disrupting legitimate travel and commerce.

- **Emergency Preparedness/FEMA:** The Department's grade in this area is a **C-**. Challenges still remain in the areas of operational planning, fraud, waste and abuse controls, disaster logistics, evacuation planning, command and control, and mass care for disaster victims. In addition to continuing to reform FEMA, the Department needs to continue refining its risk-based approach to awarding first responder grants to ensure that areas and assets that are most vulnerable are as secure as possible.

- **Emergency Communications:** The Department's grade in this area is a **C**. The Department should move quickly to establish the Office of Emergency

Communications and also work diligently to complete a National Emergency Communications Strategy by October 4, 2007, as outlined in law. Such actions will greatly improve intergovernmental coordination regarding emergency communication capabilities.

- **Aviation Security.** The Department's grade in this area is a **C**. The concerns outlined in this year's reports card remains largely unchanged from last year's assessment. The four most significant areas of vulnerability identified in our analysis are: sabotage by "sleepers" among airport workers, a terrorist being allowed to board a U.S.-bound plane without being checked against the terrorist watch list, an attack emanating in the air cargo hold, and the threat of an explosive device at the checkpoint.

- **Port Security.** The Department's grade in this area is a **C-/D+.** The Department should implement the Inspector General's recommendations regarding the management and oversight of two major programs, Deepwater and the Automatic Targeting System (ATS). It is also imperative that the Transportation Workers Identification Card (TWIC) program remains on schedule.

- **Surface Transportation Security.** The Department's grade in this area is a **C.** The Transportation Security Administration (TSA) must work with its Federal, State, local and tribal partners, industry and other stakeholders, to develop best standards, guidance, and regulations concerning security plans. The development of security standards for land-based surface transportation security is another important benchmark that the Department has yet to reach. Perhaps most important, TSA should improve its outreach, communication, and sharing of information with State and local officials, and with the private sector, including industry and labor organizations.

- **Critical Infrastructure.** The Department's grade in this area is an **Incomplete**. The Department must make every effort to ensure that the proposed Office of Infrastructure Protection has the resources to allow it to accomplish its mission. The Department also needs to continue to work on the National Asset Database and identify specific improvements. Finally, the Department must complete and share the sector specific plans required under the National Infrastructure Protection Plan with Congress.

- **Information Sharing.** The Department's grade in this area is a **C.** The Department has not effectively bridged the information sharing gap between the intelligence and law enforcement communities. The Office of Intelligence & Analysis needs to define the role it envisions for its State, Local, and Tribal law enforcement partners participating in its initiatives.

- **Science & Technology.** The Department's grade in this area is a **C.** The Department must produce the Science and Technology Directorate's strategic plan and national policy, as called for in the Homeland Security Act of 2002.

S&T must continue to develop a mature business model, involving financial management system accountability and prudent project management including performance metrics. Finally, the Under Secretary must become a strong intra-department coordinator for determining the R&D needs and performance of the various Department divisions.

- **The State of Biosecurity.** The Department's grade in this area is a **B-.** A robust biointelligence and biosurveillance capability must continue to be developed, with better connections created between the various agencies and organizations including academia. Also, Project Bioshield, which was created to promote development of vaccines and other medical countermeasures, must either be fixed or replaced with a program that will achieve this objective.

- **Chemical Plant Security.** The Department's grade in this area is a **B-.** Chemical site security must be increased, especially those that pose the greatest risk to the Nation's citizens and economy. The Department has made progress in this area; developing analytical metrics to categorize the risk posed by any specific plant has been a great improvement. 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.

- **Domestic Nuclear Detection Office.** The Department's grade in this area is a **B.** The Government Accountability Office was very critical DNDO methods to conduct Advanced Spectroscopic Portal Monitors (ASP) cost-benefit analysis. The Department must improve upon the methodologies applied toward radiation portal monitors. The Department should also examine the possibilities and implications of aggressive deployment of detection technologies; and, examine if proper internal procedures and independent evaluation have been established and followed to ensure the right technologies are deployed.

- **Management and Organization.** The Department's grade in this area is an **Incomplete**. The Department sorely lacks experienced procurement and contract management staff, and there is deep concern over the Department's results from the recent Federal government job satisfaction survey.

- **Employee Morale.** The Department's grade in this area is an **F.** The Department should promptly implement the recommendations from last year's report card, which include ways to use aspects of the federal civil service system to supplement or replace HCOP. The Department's ability to attract and retain a talented and professional workforce will be seriously impeded if it continues to allow circumstances that lead to low employee morale.

- **Procurement.** The Department's grade in this area is a **C-.** The Department needs to significantly increase its procurement workforce and develop its own in-house cadre of procurement professionals.

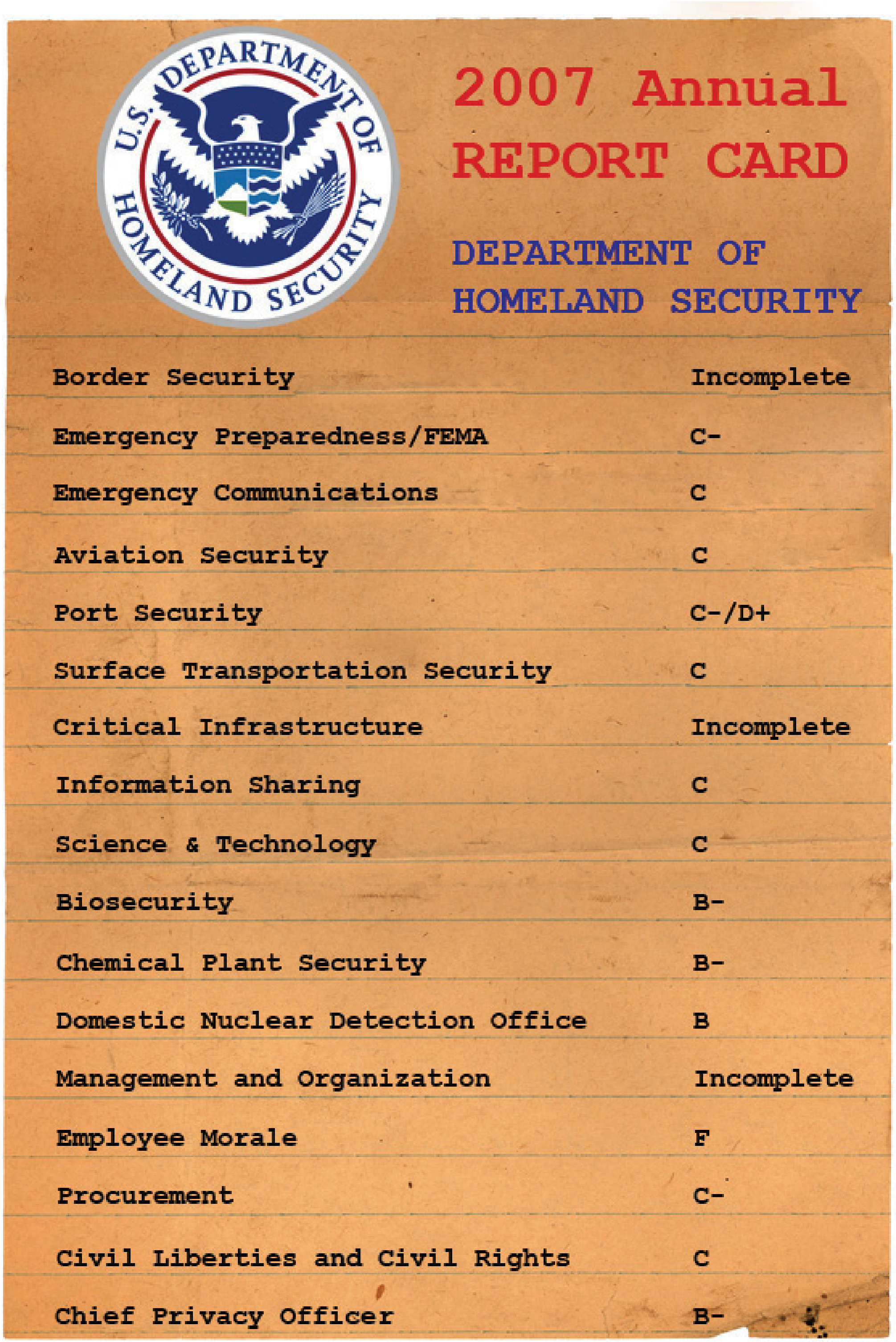
- **Civil Liberties and Civil Rights.** The Department's grade in this area is a **C**. The protection of citizen rights and liberties is paramount at a time when the Federal government is gathering, distilling, and collecting information for security purposes. The Secretary should direct all Department components to cooperate fully with the Civil Rights Civil Liberties (CRCL) Office. The CRCL Office must also exercise more oversight regarding the Department's internal equal employment policies to achieve more diversity in the Department's workforce. Additionally, the CRCL office must deliver its annual reports to Congress on a timely basis.

- **Chief Privacy Officer.** The Department's grade in this area is a **B-.** The Chief Privacy Officer must have enhanced authority to conduct investigations into privacy complaints. The Privacy Office must also submit its reports to Congress a timely fashion.

Overall, the Democrats on the Committee continue to have concerns regarding the Department's general lack of candor regarding its challenges regarding leadership and management. This was clearly echoed in the findings of the 2006 Federal Human Capital Survey. Although many excuses were offered for the poor showing of the Human Resources survey, the Secretary or Deputy Secretary did not state that they are ultimately accountable for the performance of the Department. Reorganizations, realignments and multiple changes in management and leadership have resulted in some organizational instability. The Department's management needs to evolve to support, develop, and invest in established long term, best business practices in organizational and program management.

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 who go to work every day to make all of our lives safer.

REPORT CARD



2007 Annual REPORT CARD

DEPARTMENT OF HOMELAND SECURITY

Border Security	Incomplete
Emergency Preparedness/FEMA	C-
Emergency Communications	C
Aviation Security	C
Port Security	C-/D+
Surface Transportation Security	C
Critical Infrastructure	Incomplete
Information Sharing	C
Science & Technology	C
Biosecurity	B-
Chemical Plant Security	B-
Domestic Nuclear Detection Office	B
Management and Organization	Incomplete
Employee Morale	F
Procurement	C-
Civil Liberties and Civil Rights	C
Chief Privacy Officer	B-

BORDER SECURITY INCOMPLETE

I. STATEMENT OF PROBLEM HISTORICALLY:

Over 1 million passengers and pedestrians, 327,000 vehicles, and 70,000 shipping containers come into the United States through ports of entry each day.[1] Hidden among legitimate travelers and trade are persons who seek to enter this country illegally or smuggle contraband, both at and between the ports of entry, including potential terrorists. A major component of the Department of Homeland Security's mission is to "ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce."[2] Since the Department was established over four years ago in the wake of the terrorist attacks of September 11, 2001, billions of taxpayer dollars have been spent toward achieving that mission.

II. STATE OF BORDER SECURITY TODAY:

The Department is implementing several initiatives toward securing the border, including the Secure Border Initiative (SBI) and the Western Hemisphere Travel Initiative (WHTI).

SBI takes a systematic approach to border security by integrating and unifying border security systems, and developing and coordinating programs and policies to secure the border and efficiently enforce customs and immigration laws. SBI focuses on:

- Intelligence and information sharing,
- Increased enforcement of immigration, customs, and agriculture laws,
- Increased compliance with immigration, customs, and agriculture laws, and
- Unification of the Department's efforts to resolve border security issues.

Within SBI, several program areas of interest to this Committee include:

- Implementing SBInet,
- Adding an additional 6,000 Border Patrol Agents over the next two years, and
- Ending catch-and-release for non-Mexicans.

Another program of interest is WHTI. The goal of WHTI is to strengthen border security and facilitate entry into the United States for U.S. citizens and legitimate foreign visitors by providing standardized, secure, and reliable documentation to allow the Department to quickly and accurately identify travelers.[3] WHTI began initial implementation for air travelers on January 23, 2007, with projected expansion to land and sea passengers as early as January 1, 2008.

[1] U.S. CUSTOMS AND BORDER PROTECTION, *Fact Sheet: On a Typical Day…*(Jan. 2007), *at* http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/typical_day.ctt/typical_day.pdf (last visited Mar. 9, 2007).

[2] DEPARTMENT OF HOMELAND SECURITY, *Strategic Plan -- Securing Our Homeland,* http://www.dhs.gov/xabout/strategicplan/index.shtm (last modified Mar. 8, 2007).

[3] DEPARTMENT OF STATE, *Western Hemisphere Travel Initiative (WHTI) Fact Sheet* (Feb. 2007), *at* http://travel.state.gov/pdf/whti_fact4.pdf (last visited Mar. 9, 2007).

Implementing SBI*net*

SBI*net* is intended to field the most effective mix of proven technologies, infrastructure, staffing, and platforms.[4] The Homeland Security Appropriations Act for fiscal year 2007 includes $1.2 billion for border fencing, vehicle barriers, technology, and tactical infrastructure for the program.[5] The SBI*net* contract was awarded in September 2006 to Boeing. For the upcoming year, the President's budget proposes $1.0 billion for SBI*net*.[6]

> Since the September 2006 contract award, Boeing has been given three task orders:
> 1) Management Task Order,
> 2) Project 28 Task Order, and,
> 3) Barry M. Goldwater Range (BMGR) Task Order Phase I.

The Management Task Order is a twelve-month, $44 million effort which includes overall systems engineering, mission engineering, and program management. Project 28 is a $20 million operational effort over an eight-month period that will demonstrate Boeing's concept of operation over twenty-eight border miles in the Tucson/Sasabe area along the Southern border. The BMGR Phase I Task Order was recently awarded $19.9 million to install a nine-mile physical barrier integrated with technology and infrastructure. The BMGR Phase I is to be completed no later than March 2007.

Department of Homeland Security Inspector General Richard L. Skinner has characterized the SBI*net* contract as a "high-risk, complex, system-of-systems" acquisition that requires the Department to "lay and oversee the foundation for contractor performance and control costs and schedules."[7] He has also expressed concern about a lack of contractor oversight on the project.[8]

In order to exercise close scrutiny over this large and complex SBI*net* contract, the Homeland Security Appropriations Act for fiscal year 2007 required that the Department submit to Congress an expenditure plan for the program. The plan was subsequently reviewed by the Government Accountability Office (GAO), which released its findings in February 2007. In its report, GAO stated that "because the Department's SBI*net* expenditure plan lacked sufficient details on such things as planned activities and milestones, anticipated costs and staffing levels, and expected

[4] U.S. CUSTOMS AND BORDER PROTECTION, *SBInet Timeline* (Feb. 21, 2007), *at* http://www.cbp.gov/xp/cgov/border_security/sbi/sbinet_information/sbinet_project_timeline.xml (last visited Mar. 9, 2007).

[5] Department of Homeland Security Appropriations Act, 2007, Pub. L. 109-295 (2006).

[6] THE WHITE HOUSE OFFICE OF MANAGEMENT AND BUDGET, Budget of the United States Government, Fiscal Year 2008, *at* http://www.whitehouse.gov/omb/budget/fy2008/ (last visited Mar. 9, 2007).

[7] *Procurement Practices of the Department of Homeland Security: Hearing Before the House Committee on Oversight and Government Reform*, 110th Cong. (Feb. 8, 2007) (statement of Richard L. Skinner, Inspector General, Department of Homeland Security).

[8] *Id.*

milestones, Congress and DHS are not in the best position to use the plan as a basis for measuring program success, accounting for the use of current and future appropriations, and holding program managers accountable."[9]

The Department proposes to measure SBI*net* progress by: developing Quality Assurance Surveillance Plans (mandated by Federal Acquisition Regulations for performance-based contracts), establishing milestones, and identifying performance measure criteria. Also, the Department is compiling a list of lessons learned from other major acquisition programs that it plans to implement. However, evaluation of the program cannot be completed due to the many unanswered questions. The Department's Inspector General and the GAO reports indicate concern and that without enhanced management and oversight the program has the potential to meet the same fate as its failed predecessor programs, the Integrated Surveillance and Intelligence System (ISIS) and America's Shield Initiative.

Adding 6,000 Additional Border Patrol Agents

As part of SBI, the Administration has committed to doubling the size of the Border Patrol during President Bush's term in office. To do so, it must add 6,000 additional agents over the next two years, which would bring the total number of agents at the end of calendar year 2008 to 17,819.[10] The President's fiscal year 2008 budget requests $647.8 million for the Border Patrol Staffing Initiative and $100 million for constructing or enhancing existing Border Patrol facilities to accommodate staffing increases.[11]

While there is significant support for expanding the ranks of the Border Patrol, it remains to be seen whether the Department has the capacity to recruit, hire, train, and retain a sufficient number of agents to meet this ambitious goal under a very short deadline.

Ending Catch-and-Release

As part of SBI, the Administration has also committed to ending the policy of catch-and-release for non-Mexican illegal entrants apprehended along the Southwest and Northern border. Under that policy, non-Mexicans apprehended by the Border Patrol were issued notices to appear at an immigration hearing and then were released instead of being detained, often due to a lack of detention space. The new policy has been implemented by re-engineering the detention and removal processes (i.e. using expedited removal), and by increased detention space. The Department has drastically reduced the use of catch-and-release over the last year.[12]

While ending catch-and-release is commendable, recent reports suggest management problems at the detention facilities, which are giving rise to allegations

[9] GOVERNMENT ACCOUNTABILITY OFFICE, *Secure Border Initiative, SBInet Expenditure Plan Needs to Better Support Oversight and Accountability*, GAO-07-309 (Feb. 2007).
[10] DEPARTMENT OF HOMELAND SECURITY, *Budget in Brief Fiscal Year 2008* (2007), at 29, *at* http://www.dhs.gov/xlibrary/assets/budget_bib-fy2008.pdf (last visited Mar. 9, 2007).
[11] *Id.*
[12] *Id.*

regarding the treatment of detainees, particularly with respect to children.[13] The Department must exercise greater oversight of the contactors that operate many of these facilities, or risk undermining their efforts to end catch-and-release.

Implementing the Western Hemisphere Travel Initiative (WHTI)

Mandated by the Intelligence Reform and Terrorism Prevention Act of 2004, WHTI requires citizens of the United States, Bermuda, Canada, and Mexico to have a passport or passport-like document when entering the United States by air, land, or sea.[14] The air portion of these requirements took effect on January 23, 2007, and the land and sea requirements are scheduled to take effect by January 1, 2008.[15] The President's fiscal year 2008 budget requests $252.5 million for WHTI. While the air implementation occurred without serious incident, there is concern that, due to the higher volume of travelers, the upcoming land implementation could be particularly problematic. It is incumbent upon the Department to have the personnel and infrastructure systems in place and to conduct appropriate public outreach prior to implementation. Otherwise, WHTI could have significant, detrimental effects on travel and commerce, particularly for border residents and communities.

III. AREAS FOR IMPROVEMENT:

To strengthen America's border security, the Department of Homeland Security should prioritize the following:

- Putting adequate procurement, management, and oversight resources in place to ensure that the same contract procurement and deployment problems experienced by the Department with previous border security technology systems do not undermine SBI*net* implementation;

- Effectively and efficiently expanding capacity to properly recruit, train, equip, and deploy an additional 6,000 Border Patrol agents over the next two years;

- Implementing protections to ensure the proper treatment of persons detained on immigration violations at Department or contractor-operated facilities; and

- Making adequate preparations, prior to the deadline for implementing the land and sea portions of WHTI, to meet the mandate of the program without disrupting legitimate travel and commerce.

[13] Suzanne Gamboa, *Groups Seek to Close Immigrant Center*, THE ASSOCIATED PRESS, Feb. 22, 2007.
[14] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638 (2004).
[15] DEPARTMENT OF HOMELAND SECURITY, *Western Hemisphere Travel Initiative: The Basics*, *at* http://www.dhs.gov/xtrvlsec/crossingborders/whtibasics.shtm (last modified Feb. 23, 2007).

EMERGENCY PREPAREDNESS/FEMA GRADE: C-

I. STATEMENT OF PROBLEM HISTORICALLY

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.[16] The Department of Homeland Security and FEMA's response to Hurricane Katrina was a complete failure, showcasing how ineffective management, poor communications, and failure to take a true all-hazards approach to response have affected both preparedness and response capabilities.

The process of integrating FEMA into the Department of Homeland Security was mishandled by the Administration and the Republican-controlled Congress. Many experts advocated for a Department with a robust FEMA at its core. However, this vision never materialized. FEMA was never given responsibility for managing more than $3.5 billion in funding the Department made available to emergency responders for preparedness grants and training. The efforts to create a strong FEMA were further undermined when, as part of his Second Stage Review, Secretary of Homeland Security Michael Chertoff elected to split preparedness and response into separate entities.

In an effort to address the glaring deficiencies demonstrated by the Department during Hurricane Katrina, Congress passed the Post-Katrina Emergency Management Reform Act of 2006. This act established FEMA as a distinct entity within the Department, created new leadership positions with clear position requirements, brought new missions within the scope of FEMA's authority, restored some responsibilities that had been removed, and directed the FEMA Administrator to undertake a broad range of activities before and after disasters occur.

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, mitigate, respond to, and recover from catastrophic events. According to the White House report on lessons learned from Katrina, the Federal effort lacked critical elements of prior planning, such as evacuation routes, communications, transportation assets, evacuee processing, and coordination with State, local, and non-governmental officials receiving and sheltering the evacuees. The Department's lack of advance planning, FEMA's inability to execute contracts in a timely manner or have contracts in place ready to execute, and the failure of the Department's senior leadership to coordinate with other Federal agencies

[16] NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION, *Climate of 2005 Atlantic Hurricane Season* (Jan. 13 2006), *at* http://www.ncdc.noaa.gov/oa/climate/research/2005/hurricanes05.html (last modified August 21, 2006).

severely constrained FEMA's ability to provide buses as required by the National Response Plan. [17]

Additionally, a GAO report published in December 2006, entitled "Transportation-Disadvantaged Populations: Actions Needed to Clarify Responsibilities and Increase Preparedness for Evacuations," recommended that the Department clarify the roles and responsibilities of Federal agencies for providing evacuation assistance when State and local governments are overwhelmed.[18]

GAO began an investigation of assistance provided after Katrina even while immediate recovery operations were still active. In June 2006, GAO issued a report detailing significant instances of fraud and duplicate payments in the expedited assistance program.[19] GAO asserted that of the 11,000 debit cards issued, duplicate payments were made to approximately 5,000 of the recipients. GAO also found registrants who applied for assistance using false social security numbers and bogus property addresses. Because FEMA had no identity verification program for phone applicants, potentially thousands of fraudulent payments were made.[20] According to GAO, while the recent changes being implemented by FEMA have been helpful, there is still an alarming lack of planning and trained staff to process initial applications, responses to applicant questions, and the ability to conduct inspections, as well as programmatic restrictions on the uses of funds that limited FEMA's flexibility to use assistance in the most efficient and effective manner.[21]

While there is much work to be done, FEMA is taking some steps in the right direction. Turning the organization around requires strong, experienced leadership and FEMA has begun to assemble a strong team of leaders with decades of emergency management experience. FEMA Administrator R. David Paulison came to FEMA with more than thirty years of fire and emergency services experience.

FEMA is also taking steps to strengthen its logistics management capabilities by ensuring that it knows where supplies are at all times and have the ability to deliver them to the right place. According to FEMA, pre-staged commodities such as food, water, tarps, and generators have been distributed to hurricane-prone areas. Additionally, FEMA has implemented the first phase of its Total Asset Visibility

[17] THE WHITE HOUSE*, The Federal Response to Hurricane Katrina: Lessons Learned* (February 2006), *at* http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf (last visited Mar. 9, 2007)

[18] GOVERNMENT ACCOUNTABILITY OFFICE*, Transportation-Disadvantaged Populations: Actions Needed to Clarify Responsibilities and Increase Preparedness for Evacuations*, GAO-07-44(Dec. 2006), at 1.

[19] GOVERNMENT ACCOUNTABILITY OFFICE, *Expedited Assistance for Victims of Hurricanes Katrina and Rita, FEMA's Control Weaknesses Exposed the Government to Significant Fraud and Abuse*, GAO-06-655 (June 2006).

[20] *Id.*

[21] GOVERNMENT ACCOUNTABILITY OFFICE, *Hurricanes Katrina and Rita: Unprecedented Challenges Exposed the Individuals and Households Program to Fraud and Abuse; Actions Needed to Reduce Such Problems in Future*, GAO-06-1013 (Sept. 2006).

program in the Gulf states, by procuring and installing 20,000 GPS units to enable the agency to track commodities and ensure they are going to the right places.[22]

FEMA has also taken significant steps to address the problems they have had in the area of communications and situational awareness. Federal Incident Response Support Teams have been created to be a highly responsive and flexible Federal incident management team ready to deploy and provide situational awareness of disasters.[23] In addition, FEMA is doing a better job utilizing advances in technology including satellite imagery and upgraded radios.[24]

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget does little to address the needs of first responders, emergency managers and state and local government preparedness efforts, cutting $835 million out of first responder grants and training programs administered by the Department.[25] The leadership of the National Sheriffs Association and the International Association of Fire Fighters have expressed grave concerns about a lack of commitment to homeland security on the part of the Administration.[26]

The President's fiscal year 2008 budget would eliminate funding for the $375 million Local Law Enforcement Terrorism Prevention Program, which plays a key role in assisting local law enforcement agencies in information sharing, target hardening, threat recognition and mapping, counter-terrorism and security planning, interoperable communications, and terrorist interdiction. The budget also includes a fifty-two percent cut (a decrease of $275 million) to the State Homeland Security Grant program (SHSGP), which provides grants to first responders in all fifty States and territories to help them prevent, prepare for, and respond to acts of terrorism and other emergencies.

Despite the enormous needs of our local firefighters, the President's fiscal year 2008 budget for the Assistance to Firefighters Grant program would cut funding by almost 50 percent even though the program has been critical in providing local fire

[22] R. David Paulison, Remarks at the National Press Club, *Director Paulison Lays out Vision for a New FEMA*, Nov. 30, 2006, *at* http://www.fema.gov/news/newsrelease.fema?id=31850 (last visited Mar. 9, 2007).

[23] *Id.*

[24] *Id.*

[25] DEPARTMENT OF HOMELAND SECURITY, *Budget-In-Brief Fiscal Year 2008*, 2007*, at* http://www.dhs.gov/xlibrary/assets/budget_bib-fy2008.pdf (last visited Mar. 9, 2007).

[26] According to Sheriff Ted Kamatchus, President of the National Sheriffs' Association, these cuts have significantly impacted the first responder community. "[W]e are deeply concerned that the President's budget as a whole fails to adequately fund the most effective law enforcement programs under both the Departments of Justice and Homeland Security." Sheriff Ted Kamatchus, Remarks at National Sheriffs' Association on the President's Proposed FY 2008 Budget. (February 5, 2007). The President of the International Association of Fire Fighters, Harold Schaitburger voiced similar opposition to the budget. "Make no mistake, this budget proposal puts the safety and security of the American people at risk." Harold Schaitburger, Remarks at the International Association of Fire Fighters, "Budget cuts threaten safety," (February 5, 2007), *at* http://firefightingnews.com/articleUN-US.cfm?articleID=25502 (last visited Mar. 9, 2007).

departments with the equipment and training they need to perform their day-to-day duties, as well as enhancing their ability to respond to large disasters. Additionally, the President's fiscal year 2008 budget proposes to eliminate the $115 million for the Staffing for Adequate Fire and Emergency Response (SAFER) grants program, despite clear evidence that additional firefighters are needed to adequately staff fire departments. According to International Association of Fire Fighters General President Harold Schaitberger, "fire fighters expect our elected officials to provide adequate staffing, equipment and resources they need to do their jobs – and once again the president's budget fails America's fire fighters."[27]

The President's fiscal year 2008 budget also cuts funding for the State and local training programs by $123 million, including a $50 million cut to the National Domestic Preparedness Consortium, which enhances the capacity of first responders to prevent, deter, and respond safely and effectively to incidents of terrorism involving weapons of mass destruction. In addition, despite the dangerous lack of emergency medical preparedness nationwide and the potential for an outbreak of pandemic influenza, the President's budget proposes to eliminate the Metropolitan Medical Response System (MMRS), which was funded at $33 million in fiscal year 2007. MMRS provides funds to more than one hundred metropolitan medical systems to enhance and sustain their preparedness to respond to mass casualties.

While the President's budget has shown an increased commitment to FEMA since the 2005 hurricane season, the $141 million increase for FEMA operations, planning and support still falls short of what is needed to implement the reforms mandated by Congress last year to address the agency's operational weaknesses, and ensure the agency can lead efforts to prepare for, respond to, recover from and mitigate disasters.

IV. AREAS FOR IMPROVEMENT

FEMA and the Department are in the process of implementing massive reforms to their emergency management capabilities. Nevertheless, challenges remain in the areas of operational planning, fraud, waste and abuse controls, disaster logistics, evacuation planning, command and control, and mass care for disaster victims.

In addition to completing necessary FEMA reforms, the Department needs to continue refining its risk-based approach to awarding first responder grants to ensure the most vulnerable areas and assets are as secure as possible. It must incorporate sound risk management principles and methodologies to successfully prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.[28] Additionally, citizen and community preparedness must become a national priority. In

[27] Id.

[28] DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, *Major Management Challenges Facing the Department of Homeland Security*, OIG-07-12 (Dec. 2006).

particular, Citizen Corps, a program that helps recruit and train volunteers for use in an emergency, must receive more funding.[29]

The Federal government needs to continue to enhance the National Response Plan (NRP), which governs all Federal agencies and makes cooperation with State and local officials successful. Hurricane Katrina showed that the NRP was flawed and not properly executed. The process of revising and updating the NRP must include heavy participation by State and local emergency managers and first responders. Additionally, the Department must build upon the Nationwide Plan Review. As part of the Review, the Department completed visits to 131 sites (50 states, 6 territories, and 75 major urban areas) and reviewed the disaster and evacuation plans for each. Now the Department must work with these states and urban areas to address their deficiencies.[30]

[29] NATIONAL VOLUNTEER FIRE COUNCIL, *Legislative Report: Priorities and Monitored Items*, updated October 2006, *at* http://www.nvfc.org/pdf/2006-nvfc-legislative-report.doc (last visited Mar. 9, 2007).
[30] DEPARTMENT OF HOMELAND SECURITY, *Fact Sheet: Select Homeland Security Accomplishments for 2006*, Dec. 29, 2006.

EMERGENCY COMMUNICATIONS GRADE: C

I. STATEMENT OF PROBLEM HISTORICALLY

Interoperable communications is "the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another on demand, in real time, as necessary."[31] The inability of first responders to communicate during emergencies persists despite high-profile events such as the bombing of the Alfred P. Murray building in Oklahoma City, al Qaeda's attack on the United States on September 11, 2001, and the devastating Hurricanes Katrina and Rita.

In 1996, the Public Safety Wireless Advisory Committee (PSWAC) called for the clearing of the congested radio spectrum by September 11, 2001 so that first responders could have the needed frequencies to communicate in times of emergency without interference. The National Commission on Terrorist Attacks Upon the United States (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."[32] The report also recommended that federal funding for interoperable communications be given high priority by Congress.[33] Congress addressed part of the 9/11 Commission's recommendation 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.[34] The Reconciliation Act further provided that $1 billion of the money collected from the auction of the spectrum will be available to public safety agencies for equipment and other costs associated with deploying interoperable networks.

Although more than 90 percent of the public safety communication infrastructure in the United States is owned and operated at the local and state level, there remains, according to the 2002 National Task Force on Interoperability (NTFI), five key challenges to interoperability:

1) Incompatible and aging communications equipment.
2) Limited and fragmented funding. (State and local governments have budget cycles, priorities and constraints that differ from the Federal government.)
3) Limited and fragmented planning, often due to fiscal constraints, complicate the implementation of long-term projects needed to achieve full interoperability.
4) Lack of coordination and cooperation. (Agencies are reluctant to give up management and control of their communication systems.)

[31] Pub.L. No. 108-458 § 7303(g)(1).

[32] 9/11 COMMISSION, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (July 22, 2004), at 397.

[33] *Id.*

[34] Deficit Reduction Act of 2005, Pub. L. No. 109-171, 120 Stat. 4 (2006).

5) Limited and fragmented radio communications spectrum. (Public safety is competing with every other interested party to have access to limited spectrum.)

The challenges to achieving interoperable communications were confirmed by the Department in 2005 when it found that "[a]chieving interoperability requires management and control, just as important as the technology is the need for uniform policies, procedures, standards, and training including exercises on communications interoperability in Weapons of Mass Destruction (WMD) or 'all-hazard' events." [35]

When discussing emergency communication capabilities, Dr. David Boyd of the Department of Homeland Security testified before Congress that "operability must be in place for interoperability to be possible."[36] During Hurricane Katrina, it was found that the entire communications infrastructure on the Mississippi Gulf Coast was destroyed and that thirty-eight 911 call centers collapsed.[37] Secretary Chertoff underscored the point by noting that "if all of the communications have been blown down, if the satellite phones are running out of power, if all the radio towers are down, then it's not a question of interoperability, it's a question of ability to operate at all."[38]

II. STATE OF EMERGENCY COMMUNICATIONS

On December 8, 2006, the SAFECOM Program at the Department of Homeland Security released the findings of the first National Interoperability Baseline Survey[39] to determine the level of operability and interoperability across the nation. The survey drew a 30 percent response rate, with the participation of 6,186 agencies representing randomly selected law enforcement, fire, and emergency medical services nationwide. The survey found that:

- Approximately two-thirds of emergency response agencies across the nation use interoperable communications.
- Respondents tended to be more developed in technology than they are in standard operating procedures and exercises.
- There is more interoperability between law enforcement, fire, and emergency medical services than is between state and local agencies.

[35] DEPARTMENT OF JUSTICE OFFICE OF STATE AND LOCAL GOVERNMENT COORDINATION PREPAREDNESS, *ICTAP Interoperable Communications Equipment Survey*, July 2005 *at* www.ojp.usdoj.gov/odp/docs/ICTAPJuly05Bulletin_att.pdf (last visited Mar. 9, 2007).

[36] *Protecting Homeland Security: A Status Report on Interoperability Between Public Safety Communications Systems: Hearing Before Subcommittee on Telecommunications, House Committee on Energy and Commerce*, 108th Cong. (June 23, 2004) (testimony of David G. Boyd, Ph.D., Director, SAFECOM Program Office, Directorate of Science and Technology, Department of Homeland Security).

[37] H. Rpt. 109-377, *A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, U.S. House of Representatives* (2006) at 164, *at* http://www.gpoaccess.gov/serialset/creports/katrina.html (last visited Mar. 9, 2007).

[38] *International Association of Fire Fighters Legislative Conference,* Mar. 21, 2006 (Remarks by Michael Chertoff, Secretary, Department of Homeland Security).

[39] SAFECOM, *National Interoperability Baseline Survey* (Dec. 2006), *at* http://www.safecomprogram.gov/NR/rdonlyres/40E2381C-5D30-4C9C-AB81-9CBC2A478028/0/2006NationalInteroperabilityBaselineSurvey.pdf (last visited Mar. 9, 2007).

- 43 percent of the survey's respondents have no funding or only limited funding for interoperability; 37 percent of the respondents said they have some funding allocated, but that it does not meet their needs. Only seven percent reported that they had enough funding to meet their emergency communications needs.
- Only 20 percent of respondents have strategic plans to ensure interoperability across disciplines, and 19 percent have plans to ensure interoperability across jurisdictions. For state-local interoperability, that proportion falls to 16 percent.
- About half of all agencies either do not use Standard of Operating Procedures (SOPs) or rely on informal SOPs to support interoperable communications.

On January 3, 2007, the Department released the findings of the Tactical Interoperability Communications Initiative (TICP), which assessed the interoperable communications capabilities of 75 jurisdictions based on live exercises and the coordination of different levels of government. The TICP study found that, while there was strong cooperation in the field among first responders, there was a lack of multi-jurisdictional planning and long-term investment.

III. THE PRESIDENT'S BUDGET

Pursuant to the 21st Century Emergency Communications Act, which was enacted as part of the Post-Katrina Emergency Management Reform Act of 2006 (P.L. 109-295), the President's budget reflects the consolidation of the Department's emergency communications responsibilities in the Office of Emergency Communications (OEC). This new office will integrate the SAFECOM Program, the Department's Integrated Wireless Network responsibilities, and the Interoperable Communications Technical Assistance Program. The President's fiscal year 2008 budget requests $35.7 million for the OEC, which includes provisions for eighteen full-time employees. The OEC will be responsible for ensuring the operability and interoperability of emergency communication systems and networks. However, the Department has failed to meet the statutory deadline of February 1, 2007 to submit a report to Congress detailing the resources and staff needed to establish the OEC.

IV. AREAS FOR IMPROVEMENT

Improved emergency communications would be achieved more quickly if the Department would fully implement the Congressional mandates outlined in the Department of Homeland Security Appropriation's Act of fiscal year 2007 with a sense of urgency.

Specifically, the Department should move quickly to establish the Office of Emergency Communications to support, promote, monitor, and promulgate operable and interoperable communication capabilities, consolidating various offices across the Federal government. The Department should also work diligently to complete a National Emergency Communications Strategy by October 4, 2007. Moreover, the Department needs to identify ways to expedite the adoption of consensus standards for emergency communications equipment and recommend both short and long-term solutions to overcoming obstacles to achieving nationwide interoperability and operability.

The Department should conduct a second assessment as a follow-up to the National Interoperability Baseline released in December 2006. The results of such a survey would provide a comparable quantitative assessment of public safety's interoperable communications capabilities that would hopefully demonstrate relative improvement to the original baseline.

In addition, the Department should move quickly to establish the Emergency Communications Center to act as a clearinghouse for the Federal government's efforts to achieve nationwide interoperability and ensure cooperation among the relevant departments and agencies in implementing the goals of the emergency communications strategy. The Department must also take steps to ensure that recipients of homeland security grants are coordinating and operating consistent with the goals and recommendations of the National Emergency Communications Plan.

Congress should authorize the funding necessary for the Department to establish a stand alone interoperability grant program so that State and local governments do not have to decide between securing infrastructure and improving emergency communication capabilities for their first responders. Finally, the Department should work with the Department of Commerce to administer the Public Safety Interoperable Communications Grant Program established in the Deficit Reduction Act of 2006, (P.L. 109-171).

AVIATION SECURITY GRADE: C

I. STATEMENT OF PROBLEM HISTORICALLY

The nineteen hijackers who carried out the terrorist attacks on September 11, 2001 exposed known weaknesses in aviation security. Until that fateful day, America's civil aviation security system was designed to prevent a hijacking. Since the attacks of September 11th, Congress and the Administration have taken significant steps to encourage the American people that it is safe to fly again, including federalizing aviation security. The Transportation Security Administration (TSA) was created to address gaps in our transportation security. Following the attacks, TSA's most pressing tasks included: federalizing the screeners workforce, increasing airports' baggage screening capability to detect explosives, and developing and implementing a training program for screeners to reinforce explosive detection.

TSA struggled to recruit, screen and hire up to 60,000 Federal screeners. As a result, TSA contracted a company called NCS Pearson to conduct this effort. However, TSA failed to employ proper control mechanisms and the NCS Pearson contract, capped at $104 million, quickly ballooned to $741 million. A subsequent audit of this contract uncovered improprieties and almost $300 million in deficient or unsubstantiated billing.[40]

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. Between November 2001 and September 2004, about 93 percent of TSA's budget was dedicated to meeting the equipment challenge.[41] 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" ETDs and the minivan-sized EDS machines so that they were not integrated with airport baggage conveyor systems—usually in temporary locations in airport lobbies. Some of these interim lobby solutions resulted in operational inefficiencies, some of which led to a need for more screeners versus configurations using EDS machines correctly integrated with baggage conveyer systems.[42]

TSA identified nine accomplishments in its aviation security program for fiscal year 2006. One accomplishment was the rapid response to developing training curricula to detect the liquid explosive threat similar to the threat used in London.

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

[41] GOVERNMENT ACCOUNTABILITY OFFICE, *TRANSPORTATION SECURITY: Systematic Planning Needed to Optimize Resources*, GAO-05-357T (Feb. 15, 2005) (Statement of Cathleen A. Berrick before the Senate Committee on Commerce, Science, and Transportation), at 9.

[42] *Id.* at 8-9. The Transportation Security Administration often refers to this approach to aviation security as a "system of systems" or a "layered approach." *Id.*

TSA trained its 43,000 security officers to recognize and respond to the threat of liquid explosives and Improvised Explosive Devices (IED), as well as training Transportation Screening Officers (TSO) at all airports to address this newly identified threat. Since November 2005, over 46,542 TSOs have received intensive classroom training, and some 36,886 TSOs have received online training to reinforce agency explosive detection capabilities.

Despite the billions of dollars Congress has appropriated for aviation security since September 11th, the achievements of TSA are scant compared to their failures. The American people have the right to expect and demand more.

II. STATE OF AVIATION SECURITY

Significant gaps in aviation security have been brought to TSA's attention by Congress, the GAO, the Department's Inspector General, and the National Commission on Terrorist Attacks on the United States (9/11 Commission). Among the areas warranting greater attention are the risks of sabotage by airport workers, terrorists being allowed to board a U.S.-bound aircraft before being checked against the terrorist watch list, attacks emanating from the air cargo hold, and explosive devices at checkpoints.

The Continuing Threat of Sabotage by Airport Workers

Although millions of passengers, pilots, and flight crews are subject to checkpoint screening, tens of thousands of airport caterers, cleaners, mechanics, employees at airport restaurants and shops, gate agents, and baggage handlers are allowed to bypass security checkpoints and, through the use of their airport identification/access card, gain access to nominally secured and sterile airport areas, including the aircraft themselves. The thought that an airport worker might exploit this gap in aviation security to plant an incendiary device or other weapon is not far-fetched. Indeed, al Qaeda has tried it before. In 1995, Philippine authorities uncovered "Operation Bojinka," a plot developed by Ramzi Yousef, the architect of the 1993 World Trade Center bombing, to detonate explosives on eleven commercial air carriers in a synchronized manner. A dry run of the attack was attempted on a Tokyo-bound Philippine Airlines flight, where a small bomb—a contact lens solution bottle containing nitroglycerin—was detonated under seat 27F.[43] In the subsequent prosecution, U.S. authorities estimated that 4,000 passengers would have died had the plot to bomb all eleven planes been successful.[44] In the wake of this event, however, TSA has not taken the appropriate steps to close this airport security gap that could facilitate a "sleeper" attack in which an airport worker could exploit the trust and access inherent in his position to launch a terrorist attack.

[43] Matthew Brzezinski, *Bust and Boom*, WASHINGTON POST, Dec. 30, 2001, at W9.

[44] Plane Terror Suspects Convicted on All Counts, CNN (September 5, 1996), available at http://www.cnn.com/US/9609/05/terror.trial/index.html (last visited Mar. 9, 2007)

In the absence of checkpoint screening protocols for airport workers, controlling access to secure areas through stringent identification requirements and a secure badge program, including biometrics, is of critical importance. Shortly after its creation in November 2001, TSA announced the new Transportation Worker Identification Card (TWIC) Program whose goal was to, not only fulfill the statutory requirements of the Maritime Transportation Security Act of 2002 creating a credentialing program for maritime workers by August 2004, but to also create a system for transportation workers in all other modes, including aviation. The TWIC program has been viewed as a way to provide unescorted access to secure areas of transportation infrastructure for the more than 12 million persons working in the transportation sector. Programmatic delays, however, have plagued the development of this integrated, credential-based, identity management program.

In August 2004, TSA missed the deadline for deployment of a TWIC program in the maritime sector. In December 2004, GAO reported that "…each delay in TSA's program to develop the card postpones enhancements to port security…."[45] The same can certainly be said for aviation security, insofar as deployment of the TWIC in the maritime environment is a precursor to implementation for airport workers. In response to questioning about delays in the TWIC program, Michael P. Jackson, the then-nominee for Deputy Secretary 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."[46] In January 2007, TSA promulgated the final rule for TWIC and published it in the Federal Register. The rule, which should be effective in April 2007, would provide the regulatory framework to conduct background checks and issue biometric-based ID cards to maritime workers. TSA expects to enroll people into the program over an eighteen-month period beginning in March 2007; however, there are many who question if TWIC will be operational in the proposed time frame.

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

At present, the Department requires air carriers to transmit full manifests of U.S. bound flights to U.S. Customs and Border Protection (CBP) within 15 minutes after departure. 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 the airport of origin or to another unexpected en route destination. According to this protocol, six wide-body 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. Susan Ginsburg, former

[45] GOVERNMENT ACCOUNTABILITY OFFICE*, Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (December 2004) at 17-18.

[46] *Confirmation Hearing of Michael P. Jackson: Hearing Before the Senate Committee on Homeland Security and Governmental Affairs*, 109th Cong. (Mar. 7, 2005) (statement of the Honorable Michael P. Jackson).

Senior Counsel of the 9/11 Commission, argues that one of the key possibilities for improving aviation security is "[i]nvesting in the ability to track individuals *en route*."[47] Moreover, technology exists to fully automate the pre-screening of passengers and to restrict the issuance of boarding passes until a passenger's name is checked against the consolidated terrorist watch lists. Indeed, Australia has had such a system in place since the Sydney Olympics in 2000.

The Department failed to tighten its pre-screening program to ensure that all U.S.-bound passengers are checked before departure. It has also been slow to implement the Immigration Security Initiative, since renamed the "Immigration Advisory Program." This Program deploys CBP inspectors to foreign airports with high volume U.S.-bound traffic to share critical information to prevent travelers identified as security threats, and others deemed inadmissible, from continuing on to the United States.[48]

The Air Cargo Security Risk

Screening the 23 billion pounds of air cargo annually entering the United States is also necessary to keep America secure. In recent years, TSA has increased the number of air cargo inspectors and canine teams. At TSA's request, the Office of Science and Technology within the Department, is undertaking research and development of technologies and systems that could be utilized in an air cargo environment. Yet, TSA has not moved forward to issue a final air cargo rule, as required under section 4053 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458). The deadline was August 14, 2005. TSA's approach to securing air cargo is predicated on air carriers and freight forwarders verifying known shippers and conducting their own screening and physical inspection. GAO recently reported that there are a number of structural weaknesses in TSA's plans to create a centralized Known Shipper Database, and that a number of exemptions granted to known shippers for screening air cargo may "create potential vulnerabilities in the air cargo security system."[49]

The Threat of an Explosive Device at the Checkpoint

One of the principal aviation recommendations of the 9/11 Commission was to improve airline screening checkpoints' ability to detect explosives. In fact, the 9/11 Discourse Project is comprised of a number of former 9/11 Commissioners, recently gave TSA a "C" for its progress on this critical security recommendation. The 9/11 Discourse Project not only urged Congress to fund the development of advanced screening technology, but stated that "TSA needs to move as expeditiously as possible with the appropriate installation of explosive detection trace portals at more of the

[47] Susan Ginsburg, *Countering Terrorist Mobility: Shaping an Operational Strategy*, MIGRATION POLICY INSTITUTE (February 2006) at 5.

[48] Pub.L. No. 108-458 § 7206, 7210.

[49] GOVERNMENT ACCOUNTABILITY OFFICE, *Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security*, GAO-06-76 (October 2005) at 6.

nation's commercial airports."[50] If the goal of a suicide bomber is to inflict mass casualties at the security checkpoint itself, then it is worth noting that TSA has made progress in reducing wait times at our nation's airports, decreasing the number of backups and the possibility of injury or death resulting from a bomb detonation at the checkpoint. However, if a suicide bomber's target is the aircraft, the technology at airport checkpoints is inadequate. Most of the screening equipment cannot detect plastic explosives concealed beneath passengers' clothing, nor does it have the ability to detect liquid explosives. Just as TSA has made improvements in on-board aircraft defenses through such efforts as increasing the presence of Federal Air Marshals, hardening cockpit doors, and arming some pilots, it should also focus on eliminating the vulnerabilities of airport screening systems.

Communications Regarding Aviation Terrorist Threats

Operationally, TSA continues to struggle to establish timely and effective communications concerning internal threats. The Department's Inspector General found that information about potential security violations, threats, and criminal activity was not always reviewed and forwarded in a timely manner within TSA.[51] This finding came two years after TSA failed to act on 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 conceal box cutters and other prohibited items on six different Southwest flights.

Additionally, the responsibilities of Federal Security Directors (FSDs), TSA's top officials at airports, are not clear in the airport environment, especially relative to those of the Federal Bureau of Investigation and other Federal and State authorities, during an aviation emergency. A GAO report found that "TSA's primary document outlining the 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."[52] The survey data that GAO has collected from FSDs suggest that the lack of clarity on appropriate action by different officials during security incidents "could result in conflict, confusion, and increased response time."[53]

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget requests $4.95 billion for aviation security, a $221.3 million increase over the fiscal year 2007 level. Most of the increase is for the new Travel Document Checkers (TDC) Program which would provide an additional layer of security to deter and detect individuals attempting to board an

[50] 9/11 DISCLOSURE PROJECT, *Final Report on 9/11 Commission Recommendations* (December 5, 2005) at 1, *at* http://www.9-11pdp.org/press/2005-12-05_report.pdf (last visited Mar. 9, 2007).
[51] DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, *Transportation Security Administration's Revised Security Procedures (Unclassified Summary)*, OIG-05-51, (Sept. 2005).
[52] GOVERNMENT ACCOUNTABILITY OFFICE, *Transportation Security Administration: More Clarity on the Authority of Federal Security Directors Is Needed*, GAO-05-935, 36 (Sept. 2005).
[53] *Id.* at 3.

aircraft with fraudulent documents. However, the benefits will not be known for some time.

TSA's air cargo operations budget is proposed to be funded at $55.8 million - a small increase over fiscal year 2007 level most of which is for cost of living increases. Most of this increase is significantly less than what was authorized for air cargo security under the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458). The President's fiscal year 2008 budget request will not provide TSA with the resources to increase the number of cargo inspectors over the currently authorized level of 300, deploy explosive detection equipment, or the additional technology to needed to improve air cargo screening and inspections.

IV. AREAS FOR IMPROVEMENT

To close the major security gaps, the Department must do the following:

1) Put systems in place to restrict unescorted access to secured and sterile areas of the airport or to screen airport workers;

2) Deploy an automated system to pre-screen U.S.-bound passengers before their flights depart;

3) Eliminate known shipper exemptions to the screening of air cargo; and,

4) Develop a multi-layered approach to cargo security where "known shippers" are verified and elevated risk cargo is identified and screened.

PORT SECURITY GRADE: C-/D+

I. STATEMENT OF PROBLEM HISTORICALLY:

America's ports are the gateway to the global economy. The Nation's economic prosperity rests on the ability of tens of thousands of containers arriving unimpeded at United States ports to support the "just-in-time" delivery system. For example, over 12,000 containers arrive at the Port of Los Angeles/Long Beach every day.[54] More than $100 billion worth of cargo moves through the Port of Long Beach every year - creating jobs and generating tax revenues.[55] The Nation's ports also serve as points of departure for United States exports. According to the American Association of Port Authorities, about two-thirds of all the country's wheat and wheat flour, one-third of soybean and rice production and almost two-fifths of the Nation's cotton production is exported via Unites States' ports.[56]

Globalization has 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 encourages efficiency. As a result, the port system cannot afford disruptions or delays. For example, a 2002 simulation of a lockout at West Coast ports estimated the cost to the American economy to be $5 billion per day.[57] Likewise, the economic impact of Hurricanes Katrina and Rita was felt immediately at the gas pumps when oil tankers could not enter the ports of New Orleans and Houston. All experts agree that the efficiency at the ports and economic consequences of disruptions of port operations make them attractive terrorist targets.

Terrorist groups have already targeted ports and vessels to carry out attacks, including:

- The hijacking of the cruise ship Achille Lauro in1985;
- The attack on the USS Cole in 2000; and,
- The attack of the French oil tanker Limburg in 2001.

Since the attacks on September 11th, Congress has taken steps to improve port security by passing the Maritime Transportation Security Act (MTSA) of 2002 and the Security and Accountability for Every (SAFE) Port Act of 2006. MTSA requires the development of facility and vessel security plans, the issuance of Transportation

[54] 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 (last visited Mar. 9, 2007); *see also* WASHINGTON STATE DEPARTMENT OF TRANSPORTATION, *Washington Ferries: History*, *at* http://www.wsdot.wa.gov/ferries/your_wsf/index.cfm?fuseaction=our_history (last visited Mar. 9, 2007).

[55] THE PORT OF LONG BEACH, *Economic Impacts*, *at* http://www.polb.com/about/overview/economics.asp (last visited Mar. 9, 2007).

[56] AMERICAN ASSOCIATION OF PORT AUTHORITIES, *U.S Port Industry, at* http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1022&navItemNumber=901 (last visited Mar. 9, 2007).

[57] Mark Gerencser, Jim Weinberg, and Don Vincent, *Port Security War Game: Implications for U.S. Supply Chains*, BOOZ-ALLEN-HAMILTON (Feb. 2003), at 5, *at* http://extfile.bah.com/livelink/livelink/128648/?func=doc.Fetch&nodeid=128648 (last visited Mar. 9, 2007).

Worker Identification Credentials (TWIC), the creation of Coast Guard security teams and a grant program to assist ports with security costs. The SAFE Port Act mandates that the Department issue the TWIC regulation by January 1, 2007; calls for the creation of a long-range vessel tracking system by April 1, 2007; establishes port security training and exercise programs; requires the scanning for radiation of all containers entering the United States through the 22 largest volume ports by December 31, 2007; proposes the development of a strategic plan to enhance the security of the international supply chain; directs the development of protocols for the resumption of trade; and, authorizes an integrated scanning system pilot at foreign ports to scan all containers destined for the United States. In addition, the SAFE Port Act codifies into law the Customs-Trade Partnership Against Terrorism Program (C-TPAT) and the Container Security Initiative (CSI) Program.

II. THE STATE OF PORT SECURITY:

Coast Guard

In October 2003, the Coast Guard, which is responsible for port security, issued security regulations for the Nation's 361 ports that requires the hiring of security officers and the installation of barriers and surveillance systems.[58] All of the Nation's port facilities complied with the regulations as of July 1, 2004. The Coast Guard has established maritime security teams to board high-risk vessels and screens all incoming vessels to determine if the vessels' crew or cargo pose a terrorist risk. Also, the Coast Guard developed maritime security conditions that require port facilities to increase the screening of cargo and people entering the ports. The Coast Guard has also increased security patrols in the harbors.

The Coast Guard undertook an effort to replace its aging fleet of ships and aircraft that are currently patrolling the shores. In November 2006, the Coast Guard christened the Coast Guard cutter *Bertholf* which is both the first new high endurance cutter built in more than 35 years, and first national security cutter in its Deepwater acquisition program. The cutter was designed to satisfy the Coast Guard's multi-mission responsibilities in homeland security, national defense, marine safety and environmental protection.

The Deepwater Program, however, is beset with problems. The Department's Inspector General released a report that was critical of the Coast Guard's legend-class national security cutter (NSC).[59] The NSC was designed to be the flagship of the U.S. Coast Guard's fleet, capable of executing the most challenging maritime security missions. The Inspector General determined that "the National Security Cutter, as designed and constructed, would not meet the performance specifications described in the original Deepwater contract."[60] The report also concluded that "the National

[58] Implementation of National Maritime Security Initiatives, 68 Fed. Reg. § 60, 448, (Oct. 22, 2003).

[59] DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, *Acquisition of the National Security Cutter*, OIG-07-23, (Jan. 2007) at http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-23_Jan07.pdf (last visited Mar. 9, 2007).

[60] *Id* at 1.

Security Cutter's design and performance deficiencies are fundamentally the result of the Coast Guard's failure to exercise technical oversight over the design and construction of its Deepwater assets."[61] Finally, the Inspector General "encountered resistance" from the Coast Guard and the contractor in its efforts to evaluate the structural design and performance issues associated with the cutter.[62]

The Coast Guard has had problems recently with other vessels. In December 2006, the Coast Guard announced the drydocking of the entire fleet of 123-foot cutters, which were lengthened and retrofitted with new computer and navigation systems extending service until the next generation of patrol boats came on line.[63] Unfortunately, the ships were drydocked because they were not seaworthy in heavy seas. In an effort to minimize operational impact, the Coast Guard has had to double-crew existing 110 foot cutters to minimize the operational impact.

The Department's Inspector General released a report concerning whistleblower allegations made against the 123-foot Coast Guard cutter program.[64] Among the Inspector General's findings is the fact that the contractor did not install low smoke cabling aboard the 123-foot cutter, which was required as an effort to eliminate the polyvinyl chloride jacket encasing the cables, which is responsible for producing toxic fumes and dense smoke during shipboard fire.[65] Additionally, the contractor installed C4ISR topside equipment aboard both the 123-foot cutters and prosecutors that was not tested to ensure compliance with specific environmental performance requirements outlined in the Deepwater contract.[66]

The Coast Guard is working with the Transportation Security Administration (TSA) to roll-out the TWIC program which was originally required in 2002. The TWIC program lingered in the Department due to numerous bureaucratic reasons. In February 2007, TSA announced that the TWIC program will roll-out in the Port of Wilmington, Delaware.[67] The Department has not yet finalized the deployment plan for the rest of the ports.

Customs and Border Protection

In response to the need to secure the supply chain while ensuring the flow of goods, the Department is working with the private sector to initiate a series of programs designed to target high-risk vessels, enhance container screening, 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 the responsibility of

[61] *Id.*

[62] *Id* at 2.

[63] Email from Homeland Security official to House Committee on Homeland Security (Committee) staff member (Nov. 28, 2006, 8:54 EST) (on file with Committee).

[64] DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, *110'/123' Maritime Patrol Boat Modernization Project*, OIG-07-27 (Feb. 2007), *at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-27_Feb07.pdf (last visited Mar. 9, 2007).

[65] *Id* at 2.

[66] *Id.*

[67] Email from Homeland Security official to House Homeland Security Committee (Committee) staff member, (Feb. 9, 2006, 18:02 EST) (on file with Committee).

securing the cargo established a screening system, the Automatic Targeting System (ATS), which assesses the risk of incoming cargo. ATS determines if the information listed on the manifest contains anomalies that would indicate illegal goods smuggled inside a container. In November 2006, the Inspector General released an audit on the ATS program.[68] The audit found that CBP did not make use of other sources of intelligence that was available.[69] Additionally, the Inspector General found that additional guidance for inspection of shipments with elevated ATS scores was needed.[70] The report also concluded that during secondary level inspections, non-intrusive inspection imagery was not always available to CBP officers.[71]

CBP created the Container Security Initiative (CSI), whereby their inspectors are deployed to fifty foreign seaports to inspect high-risk containers before they are shipped to the United States. There is also the Customs Trade Partnership Against Terrorism (C-TPAT) program which 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 is less likely to be inspected when it arrives in the United States. CBP, in conjunction with the Department of Homeland Security's Domestic Nuclear Detection Office, is also deploying radiation portal monitors at seaports which can screen containers for nuclear or radiological weapons. The Department has not, however, released a report required by the SAFE Port Act concerning the strategy for radiation portal monitor deployment at the 22 largest volume ports.

The SAFE Port Act of 2006 also required the establishment of an integrated scanning system pilot at three foreign ports – the Secure Freight Initiative – to better assess the risk of inbound containers. The Department of Homeland Security and the Department of Energy announced the first phase of the Secure Freight Initiative in December 2006.[72] The initial phase involved the deployment of a combination of existing technology and proven nuclear detection devices to six foreign ports: Port Qasim, Pakistan; Puerto Cortes, Honduras; Southampton, United Kingdom; Port Salalah, Oman; Port of Singapore; and the Gamman Terminal at Port Busan, Korea.

The House of Representatives, unhappy with the limited maritime cargo provisions in the SAFE Port Act, passed H.R. 1, the "Implementing the 9/11 Commission Recommendations Act of 2007" on January 9, 2007 which requires one-hundred percent scanning of all containers. The purpose of the provision was to provide CBP an opportunity to build upon the lessons learned under the Secure Freight Initiative.

[68] DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary)*, OIG 07-09 (Nov. 2006), *at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-09_Nov06.pdf (last visited Mar. 9, 2007).

[69] Coast Guard and Maritime Transportation Act of 2004, Pub.L. 108-293, § 809(g), 118 Stat. 1062.

[70] OIG 07-09, *supra* note 67, at 3.

[71] *Id.*

[72] DEPARTMENT OF HOMELAND SECURITY, *Press Release: DHS and DOE Launch Secure Freight Initiative*, (Dec. 7, 2006), *at* http://www.dhs.gov/xnews/releases/pr_1165520867989.shtm (last visited Mar. 9, 2007).

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget requests $8.726 billion for the Coast Guard, an increase of $99.4 million over the fiscal year 2007 enacted level. The proposed budget also requests $788.1 million to complete the Integrated Deepwater System (IDS) acquisition which represents a decrease of $356 million from the fiscal year 2007 enacted level.

The President's fiscal year 2008 budget proposal continues to limit the Department's progress in port security. The SAFE Port Act of 2006 authorized the appropriation of $400 million for port security grants for fiscal years 2007-2011. The President, however, only requested $210 million for port security grants for fiscal year 2008.

For several years, the Department has been criticized for its grant distribution process. Congress attempted to fix this problem in the Department of Homeland Security Appropriations Act for fiscal year 2007 by requiring the Department to release the grant application guidance within 75 days of enactment. [73] As in the past, the Department did not meet this deadline and released the guidance several weeks late.

IV. AREAS FOR IMPROVEMENT:

The Department should take concerted steps to follow the recommendations laid out by the Inspector General concerning the two recent Deepwater-related audits. The National Security Cutter and the other Deepwater assets must be fully operational in all environmental conditions.

The Department would benefit from critical decision making based on rational, underlying key decisions associated with design, construction, and implementation of all assets. Also, the decisions should be formally documented and approved by senior management.

Similarly, the Department should follow the Inspector General's recommendations on the ATS program. Specifically, the CBP should (1) review the use of intelligence from available resources; (2) review security clearances; (3) improve port performance evaluation procedures; (4) refine policies and procedures for identifying and reviewing high-risk shipments; and, (5) ensure that inspection imagery is provided to officers conducting secondary level inspections.

The Department's grant distribution system must also be improved. For the past five years, delays by the Department processing paperwork has lead to delays in funds distribution, and thus, delays in ports making security improvements. The President's budget should also match the authorization of appropriations in the SAFE Port Act.

[73] Pub. L. 109-295.

The Department has not met several deadlines specified in the SAFE Port Act. Congress specifically added deadlines to the legislation as means to ensure that the Department takes the necessary steps to improve port security. The Department must finalize the Radiation Portal Monitor report. It must also meet the April 1, 2007 deadline for developing and implementing a long-range automated vessel tracking system for all vessels in United States waters that are equipped with the Global Maritime Distress and Safety System or equivalent satellite technology. Coast Guard officials have informed our staff that the Coast Guard will not meet this deadline. The Coast Guard's inability to meet this deadline is of concern for the Committee.

Lastly, the Department must meet the TWIC deadlines. In particular, the Department should work closely with industry, including non-profit employee labor organizations, to ensure that this program is rolled out correctly and on-time. The slightest mistake by the Department could create significant problems for all involved.

SURFACE TRANSPORTATION SECURITY GRADE: C

I. STATEMENT OF PROBLEM HISTORICALLY

The Transportation Security Administration (TSA) was created to oversee the nation's efforts to secure all modes of transportation. Historically, the agency's roots and expertise lie in aviation, as TSA was spun off from the Federal Aviation Administration (FAA). This singular focus continues even after numerous terrorist attacks on rail and mass transit systems in other countries have dramatically revealed the vulnerability of these systems. 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. The next month, 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 trains at outlying stations, deployed their device-laden packages, 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, four attacks were attempted on London's transit system in which only one person was injured, but the system—and to a great extent the entire city—was crippled for hours. A year later on July 11, 2006, explosions rippled through a commuter train in Mumbai, India, killing 165 and injuring 400. Most recently, on February 19, 2007, a train headed for Pakistan burst into flames after explosions outside New Delhi, India. At least 68 people were killed in what is considered an attempt to undermine relations between India and Pakistan.

These devastating attacks demonstrate that terrorists view non-aviation transportation modes as attractive targets, and they should serve as a wake-up call for the mass transit, commuter rail, inter-urban rail, and highway systems in this country. While TSA and the Coast Guard have focused on securing aviation and maritime security, no entity has focused needed attention on land-based surface transportation. Thought TSA has primary responsibility, it has not mandated the creation of security plans, risk assessments, or training for land-based surface transportation.

II. THE STATE OF SURFACE TRANSPORTATION SECURITY TODAY

Best Standards, Guidance, and Regulations

TSA has not issued a full array of best standards, guidance, or regulations regarding security programs for mass transit, rail, or highway transportation owners and operators. Rather, these industries have begun developing these plans on their own initiative. As the agency responsible for ensuring security of *all* modes, TSA should be taking a lead role, and there are indications that it may do so in the future.

Risk Assessments and Duplication of Effort

TSA has conducted risk assessments, but too often it duplicates those already conducted by the Federal Transit Administration or by the Department's 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.[74] This reported duplication of effort has led to questions about what the various agencies within the Department are doing with the information it collects; 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 the attacks on September 11th, 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 in the industry.[75]

Security Directives

In response to the terrorist attack in Madrid, TSA issued two Security Directives (SDs) on May 20, 2004.[76] The Administration developed these SDs without public comment, and GAO is currently examining the legal basis under which they were issued.[77] These were the only SDs that TSA has issued for mass transit and rail security, despite the fact that the agency has issued eighty SDs for aviation security.[78]

Surface Inspectors

TSA has 43,000 aviation screeners.[79] In contrast, there are only 100 land-based surface inspectors.[80] The inspectors are responsible for ensuring the security of the thousands of miles of railroad tracks and mass transit lines that crisscross the Nation' cities and States. TSA must devote more personnel to non-aviation security if it wants to prevent surface transportation from becoming the weak link in the national transportation system. The Administration must also develop regulations and security directives that can be enforced.

Training and Exercises

[74] GOVERNMENT ACCOUNTABILITY OFFICE, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO 05-851, (Sep. 2005), at 4.

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

[76] These SDs are classified as Sensitive Security Information. Individuals wishing to attain copies should contact TSA.

[77] GOVERNMENT ACCOUNTABILITY OFFICE, *supra* note 2, at 36.

[78] E-mail from Transportation Security Administration to House Committee on Homeland Security staff member (Feb. 23, 2006) (on file with Committee staff).

[79] These screeners have recently been reclassified as Transportation Security Officers. DEPARTMENT OF HOMELAND SECURITY, 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 (last visited Mar. 9, 2007).

[80] 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. 108-334, 118 Stat. § 1298 (2004). The Conference Report accompanying the public law contains specific information about the inspectors. H.R. Conf. Rep. 108-774 (2004).

Despite the recent wave of attacks, TSA has not yet mandated security training for the men and women who operate the trains, subways, and trucks that carry millions of people and many tons of cargo each day. In contrast, security training is properly mandated for the maritime sector.[81] The International Brotherhood of Teamsters, in a fall 2005 report, called for mandatory training for all rail employees.[82] TSA has taken some small steps. It has contracted with the National Transit Institute[83] to develop training for passenger and freight rail employees.[84] In addition, TSA Administrator Kip 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. However, TSA has not yet consulted labor organizations on these issues.[85]

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 Mayor Michael Bloomberg announced that the city, in response to a credible terrorist threat, would be taking additional security measures to protect its subway system. The Department's officials told the press that the threat was not credible.[86]

Research and Development

The Department and TSA have failed to adequately address mass transit and rail research and development (R&D). Possible R&D projects could include efforts to reduce vulnerability of passenger trains, stations, and equipment including developing technology to screen passengers; testing new emergency response and recovery techniques and technologies; improving freight railroad technologies; and enhancing security for transportation of hazardous materials by railroad. When the Department was established, TSA retained the R&D budget and controlled the R&D program including work at the Transportation Security Laboratory (TSL) in Atlantic City, New Jersey. TSA's R&D emphasis remains on aviation security. In fiscal year 2007, the Department's R&D functions, including TSA R&D, were consolidated into the Science and Technology Directorate. There has been little to no progress despite TSA and S&T

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

[82] 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 (last visited Mar. 9, 2007).

[83] The National Transit Institute is a private organization housed at Rutgers, the State University of New Jersey, and is funded by a Federal Transit Administration grant.

[84] E-mail from Transportation Security Administration to House Committee on Homeland Security staff member (Feb. 24, 2006) (on file with Committee staff).

[85] Amalgamated Transit Union, *ATU Action Weekly Update* (Feb. 21, 2006), *at* http://www.unionvoice.org/atuaction/notice-description.tcl?newsletter_id=1551241 (last visited Mar. 9, 2007).

[86] 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*, Los Angeles Times Oct. 8, 2005, at 14.

efforts to establish a meaningful R&D program addressing non-aviation transportation areas.

Hazardous Material

The vulnerability of hazardous material has been of particular interest to several cities in the country that want to ban the trans-shipment of certain hazardous materials. In their fall 2005 report the International Brotherhood of Teamsters highlighted the security gap that exists with regard to the movement of hazardous materials.[87] In December 2006, both TSA and the Department of Transportation issued proposed rules addressing the transport of hazardous materials. While both proposed rules represent advances in tracking and routing hazardous cargo, neither goes far enough to address the public's concerns regarding the transport of hazardous shipments through densely populated urban areas. The proposed rules still leave far too much flexibility to carriers in securing dangerous shipments.

Surge Capacity

In December 2005, TSA piloted a surge capacity initiative designed to enhance security in non-aviation modes of transportation. The surge capacity was piloted in Los Angeles, Houston, Atlanta, Washington, DC, Philadelphia, and Baltimore.[88] They have sponsored Visible Intermodal Protection and Response (VIPR) Teams to conduct more exercises in 2007. This pilot initiative was controversial. According to Representative Allyson Schwartz (D-PA), 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.[89]

High Turnover

Finally, TSA has suffered from a high level of personnel turnover in the past four years. More than twelve thousand individuals let the agency in fiscal year 2004. In fiscal year 2005, the trend continued as an additional 12,232 departed.[90] TSA Administrator Hawley is the fourth person to lead the agency in four years. The turnover at all levels of the agency has resulted in a lack of continuity, constant upheaval, and minimal progress in the improvement of land-based surface transportation security.

III. PRESIDENT'S BUDGET

[87] INTERNATIONAL BROTHERHOOD OF TEAMSTERS, *supra* note 81.

[88] DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, *Press Release* (Dec. 13, 2005) (on file with Committee staff).

[89] Leslie Miller, *Undercover Air Marshals to Expand Work Beyond Airplanes to Trains, Buses*, ASSOCIATED PRESS, Dec. 15, 2005, *at* http://www.foxnews.com/story/0,2933,178642,00.html (last visited Mar. 9, 2007).

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

The President's budget request for fiscal year 2008 only allocates $41.4 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, it eliminates rail and transit security grants and intercity bus grants, which were funded at $144 million and $9.6 million, respectively, in fiscal year 2006. Instead of providing more direct funding, the Administration has again proposed to consolidate all critical infrastructure funding under the Targeted Infrastructure Protection Program (TIPP). This will force land-based surface transportation entities to compete against each other and with other critical infrastructure, such as ports. Moreover, the $600 million proposed for the TIPP 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.[91]

IV. AREAS FOR IMPROVEMENT

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 over five years since 9/11. TSA cannot continue to delay this important step.

TSA, working with its partners, must ensure that all surface transportation security issues—budgets, grants, vulnerability assessments, R&D, and outreach—are better coordinated and directly relate to the National Strategy for Transportation Security. If these systems are to make adequate security enhancements, it is important that TSA develop, implement and execute long term plans which include a dedicated and sufficient funding stream for land-based surface transportation grants and initiatives.

The development of security standards for land-based surface transportation security is another important benchmark the Department has yet to reach. TSA should develop security standards for these modes reflecting the best practices of these industries. 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 acceptable methodologies. These assessments should be protected and shared, as appropriate. In addition, TSA should work with fellow agencies to minimize the number of assessments completed for each individual asset. Perhaps most important, TSA should improve outreach, communication, and

[91] 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 (last visited Mar. 9, 2007) (nonprofit international association of more than 1,600 transportation related entities).

sharing of information with State and local officials, and with the private sector, including industry and labor organizations. The Department's partners should know who is in charge and who they should contact if and when a transportation security incident occurs.

CRITICAL INFRASTRUCTURE GRADE: INCOMPLETE

I. STATEMENT OF PROBLEM HISTORICALLY

The private sector owns and operates more than 85 percent of the critical infrastructure in the United States. On May 8, 1998, President Bill Clinton, recognizing the vulnerability of this infrastructure, issued Presidential Decision Directive 63 with the intent to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures."[92]

Eight years later, the security of the Nation's critical infrastructure remains a problem. In the Homeland Security Act of 2002, 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."[93] In December 2003, President George W. Bush issued Homeland Security Presidential Directive-7 (HSPD-7) making the Secretary "responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure."[94] Until recently, the Secretary failed to comply with the Presidential Directives and much remains undone.

II. STATE OF CRITICAL INFRASTRUCTURE PROTECTION TODAY

Critical infrastructure includes our drinking water, the food we eat, the fuel we use to drive our cars, and the subways that we use to get to work. This infrastructure is vital to our everyday lives.

The President proclaimed progress when the Department issued the completed National Infrastructure Protection Plan (NIPP) in June 2006 and another iteration of the National Asset Database (NADB) pursuant to HSPD-7.[95] The NIPP was released one and one-half years after the President's December 2004 deadline. The Department was working on the plan when terrorists bombed the London metro system and Hurricane Katrina struck the Gulf coast.

There also remains some confusion about the purpose and use of the NADB since the Department, Congress, and the public have different views about how the database should be used and for what purpose.[96] Also, Congress is still waiting for the

[92] THE WHITE HOUSE, *Presidential Decision Directive-63, Critical Infrastructure Protection*, (May 22, 1998) *at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (last visited Mar. 9, 2007).

[93] Homeland Security Act of 2002, Pub. L. 107-296, § 201(d)(5), 116 Stat. 2135 (2002). Under this Section, the Assistant Secretary for Infrastructure Protection and Information Analysis was responsible for completing this task. Id.

[94] THE WHITE HOUSE, *Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection*, (Dec. 17, 2003), *at* http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html (last visited Mar. 9, 2007).

[95] *Id.*

[96] *See* John Moteff, *Critical Infrastructure: The National Asset Database*, CONGRESSIONAL RESEARCH SERVICE, CRS RL33648, (updated January 10, 2007).

Department to issue sector specific coordinating plans which are to govern how the various sectors will coordinate in response to an emergency.

On February 9, 15, and March 2, 2007, the Department informed the Committee that the sector specific plans for the seventeen industry sectors described in HSPD-7 and required under the NIPP were completed by December 31, 2006. However, the sector specific plans have yet to be furnished to the Committee or Congress. As of the date of issuance of this report card, the Committee still does not know the content of the sector plans or if they are consistent across all sectors. The Committee has requested that the Government Accountability Office inquire about the sector plans and review several of them.

When the Department issued the National Asset Database that effectively catalogues critical infrastructure in the U.S., the database contained some 77,000 critical and non-critical assets such as shopping malls, local banks, and extraneous items such as a popcorn factory. There have been many critics of the database, including the Department's Inspector General who issued a report and recommendations, one of which provided for regular verification of the entries in the database. The Homeland Security Committee in its *Fiscal Year 2007 Department of Homeland Security Authorization Bill* adopted an amendment sponsored by Rep. Lowey (D-NY) that would have provided for routine verification of database entries and require, among other things, that the Department confer with the States before conducting a data collection. A similar provision was included in the *Implementing the 9/11 Commission Recommendations Act of 2007,* H.R.1, in the 110th Congress.

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget provides for an increase for infrastructure protection, specifically in the areas of chemical site security. The Department is also proposing to rename the Preparedness Directorate into the National Protection and Program Directorate (NPPD). The reorganization of the Preparedness Directorate into the NPPD is designed to strengthen national risk management efforts for critical infrastructure and define and synchronize the Department's efforts to address coordination and planning across the public and private sectors. According to the Department, this new reorganization is supposed to provide a more focused approach to protecting the Nation's critical infrastructure, cyber security, emergency communications, and security measures for persons traveling through ports of entry. Within the NPPD, there will a reorganized Office of Infrastructure Protection.

IV. AREAS FOR IMPROVEMENT

The Department must make every effort to ensure that the proposed Office of Infrastructure Protection has the resources to allow it to accomplish its mission and establish the goals of the NIPP. The Department also needs to continue to work on the National Asset Database and identify specific improvements. Finally, the Department must complete and share the sector specific plans required under the NIPP with Congress.

INFORMATION SHARING Grade: C

With State, Local and Tribal Law Enforcement

I. STATEMENT OF PROBLEM HISTORICALLY

In its pivotal report detailing the Federal government's failure to prevent the September 11, 2001 terrorist attacks, the National Commission on Terrorists Attacks Upon the United States (9/11 Commission) cited a "lack of imagination" as a primary reason why officials were unable to connect the data dots and take action. As noted by the Commission, a secure homeland depends on the State, local, and tribal law enforcement officers in our communities. These individuals are the people best positioned not only to observe criminal and other activity that might be the first sign of a terrorist plot, but also to help thwart attacks before they happen. Indeed, the evidence shows that terrorism financing, planning, logistics, and travel know no jurisdictional boundaries and involve a wide array of American communities whether urban, suburban, or rural. Accordingly, providing police and sheriffs' officers with the information and intelligence resources they need to make sense of what they encounter on the ground every day—and to share their observations and concerns with the Federal Intelligence Community (IC) in response—would be a giant leap toward making the homeland more secure. Almost six years after the September 11th attacks, imagination appears to be on the march, although real progress in addressing the fundamental obstacles to better information sharing is only now beginning. Simply stated, the Federal government has historically done a poor job of reaching out to "first preventers" and finding out how best it can help.

As Congress recognized in the Homeland Security Act of 2002, police and sheriffs' officers observe activities and conditions in the course of their day-to-day work that may be indicators of emerging terrorist plots.[97] Accordingly, they need access to "homeland security information" to help prevent attacks.[98] Nevertheless, Federal policymakers have failed to develop policies and procedures for converting highly classified intelligence into an unclassified or "less classified" format that the IC can share rapidly with those officers. Likewise, they have failed to create a mechanism by which those same officers can effectively share information from the field with the IC.

To effectively address these problems, one must look not only to the Department of Homeland Security but also to other agencies working the problem throughout the Federal government. Congress originally planned to locate a centralized, collaborative intelligence analysis and integration center at the Department through its Information Analysis and Infrastructure Protection Directorate (IAIP). This unit's intended purpose was to collect, analyze, and disseminate intelligence information about terrorist threats to State, local, and tribal authorities—including law enforcement.[99] In early 2003, however, IAIP ceded most of these functions to the Terrorist Threat

[97] Homeland Security Act of 2002, *supra* note 91, at § 891(b)(2), (4).
[98] *Id.*
[99] *Id.* § 201.

Integration Center (TTIC)[100] which was subsequently folded in short order into the National Counterterrorism Center (NCTC).[101] Today, the NCTC serves as the primary fusion center for all terrorism intelligence analysis and integration—a development that has left the Department with a hobbled intelligence function for over a year.

However, during his Second Stage Review testimony before Congress on July 13, 2005, Secretary Chertoff set a new course—announcing the creation of a Chief Intelligence Officer (CINT) to head what he called an "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.[102] The Secretary explained that I&A would serve as the primary connection between the Department and the IC as well as a primary source of information for the Department's State, local, and private sector partners.[103]

Among the key goals identified by Chief Intelligence Officer Charles E. Allen 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 IC.[104] Nevertheless, Mr. Allen 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 to disseminate intelligence information more promptly.[105] He admitted that the Department, the FBI, and others could do "a better job" of sharing information with State, local, and tribal authorities.[106] 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 various intelligence units, including Customs & Border Protection (CBP), Immigration & Customs Enforcement (ICE), and the Transportation Security Administration (TSA). His intention is to

[100] THE WHITE HOUSE, *Press Release: Fact Sheet: Strengthening Intelligence to Better Protect America* (Jan. 28, 2003), *at* http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html (last visited Mar. 9, 2007).

[101] THE WHITE HOUSE, *Press Release: Reforming and Strengthening Intelligence Services,* Sep. 8, 2004, *at* http://www.fas.org/irp/news/2004/09/wh090804.html (last visited Mar. 9, 2007); THE WHITE HOUSE, *Press Release: Fact Sheet, Making America Safer by Strengthening Our Intelligence Abilities*, Aug. 2, 2004, *at* http://www.fas.org/irp/news/2004/08/wh080204-fact.html (last visited Mar. 9, 2007).

[102] DEPARTMENT OF HOMELAND SECURITY, *Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security*, July 13, 2005, *at* http://www.dhs.gov/xnews/releases/press_release_0703.shtm (last visited Mar. 9, 2007).

[103] *Id.*

[104] *Written Statement to the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment*, 109th Cong.(Oct. 19, 2005) (statement by Charles Allen, Chief Intelligence Officer, Department of Homeland Security).

[105] *Second Stage Review: Hearing on the Role of the Chief Intelligence Officer Before the House Committee on Homeland Security*, 109th Cong. (July 13, 2005) (statement of Charles Allen, Department of Homeland Security).

[106] *Id.*

create unique intelligence products that would benefit both the IC and the Department's partners at the state, local, and tribal levels of government.[107]

Mr. Allen testified repeatedly during the 109th Congress that he did not believe he needed additional budgetary authority to attain his goals. Instead, he pointed to the Department's Management Directive 8110, which "establishes the Assistant Secretary for Intelligence and Analysis as the Chief Intelligence Officer (CINT)" for the Department, "and establishes the authorities" of the CINT "to effectively integrate and manage the Department's Intelligence programs."[108] Mr. Allen stated publicly that he believed that the authorities afforded him under the Management Directive would allow him to drive a common intelligence mission at the Department. Moreover, during recent testimony before the Senate Mr. Allen stated, "I don't know that I require things like direct budget authority, but I do believe that we have to synchronize our overall intelligence within the department, and I think we're well on our way to doing that."[109]

Even with these assurances, it has not been at all clear that Mr. Allen or I&A have the capability to assess what intelligence information would be of most use to law enforcement officers. Historically, most intelligence analysis conducted by the IC has been destined for high-level Federal policymakers—not for first preventers in the field. Without some input from the people on the frontlines, 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, has observed.[110] "If law enforcement officers are deluged with intelligence reports, the information overload will have the same outcome as not sharing information at all."[111] Carter added, "If officers are deleting intelligence products without reading them, then the effect is the same as if it had never been disseminated."[112] Similarly, Peter A. Modafferi, Chief of Detectives of the Rockland County, New York, District Attorney's Office, 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 IC.[113] "We, jointly, have to develop not only policies but also an implementation plan that will bring all law enforcement into

[107] *Id.*

[108] *See* DEPARTMENT OF HOMELAND SECURITY, *Management Directive 8110*, Jan. 30, 2006, *at* http://www.fas.org/irp/agency/dhs/md8110.pdf (last visited Mar. 9, 2007).

[109] *Intelligence Reform -- FBI and Homeland Security: Hearing Before the Senate Select Committee on Intelligence*, 110th Cong. (Jan. 25, 2007) (statement of Charles Allen, Chief Intelligence Officer, Department of Homeland Security).

[110] *See* David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement* Agencies, Nov. 2004 at 62, *at* http://www.cops.usdoj.gov/mime/open.pdf?Item=1439 (last visited Mar. 9, 2007).

[111] *Id.*

[112] *Id.*

[113] Telephone Interview with Peter A. Modafferi, Chief of Detectives, Rockland County, New York District Attorney's Office (Nov. 16, 2005).

the intelligence process," he stated.[114] "The biggest issue and obstacle to achieving this is not technology but history and culture."[115]

II. THE STATE OF INFORMATION SHARING

To address the needs of the Department's key law enforcement customers, Mr. Allen announced on February 14, 2007, that he supported the participation of State, local, and tribal representatives in the newly established Interagency Threat Assessment and Coordination Group (ITACG) at the NCTC.[116] The ITACG—which the Program Manager of the Information Sharing Environment (ISE), Ambassador Ted McNamara, proposed as part of his ISE Implementation Plan (the "Plan") in November 2006—"will engage in collaborative decision-making to ensure timely and effective production, integration, vetting, sanitization, and communication of terrorism information that cuts across multiple agencies to inform and empower State, local, and tribal partners."[117] The potential benefits for vertical information sharing are dramatic. "A primary purpose of the ITACG," the Plan continues, "will be to ensure that classified and unclassified intelligence produced by Federal organizations within the intelligence, law enforcement, and homeland security communities is fused, validated, deconflicted, and approved for dissemination in a concise and, where possible, unclassified format."[118] Under the leadership of Mr. Allen, the ITACG therefore holds tremendous promise for facilitating the production of accurate, actionable, and timely intelligence products that police and sheriffs' officers nationwide need to help prevent terrorist attacks. Notably, Mr. Allen's ITACG announcement comes on the heels of the Secretary's recent revelation that I&A will host State, local, and tribal law enforcement officers in Washington, D.C. at a similar information sharing fellows program situated within the Department itself.[119]

By putting its customers first, I&A appears to be moving in the right direction. Involving law enforcement at the start of the ITACG and as an essential part of its own homeland security fellows program will help the Department learn valuable lessons about (1) what kinds of information and intelligence are of interest to officers working in urban, suburban, and rural communities across America; (2) how to format that information and intelligence in a way that is useful to officers on the beat; and (3) which agencies and departments should receive particular threat warnings to target intelligence most productively. If done right, these initiatives could go a long way

[114] *Id.*

[115] *Id.*

[116] *The President's Proposed FY2008 Budget for the Department of Homeland Security: The Office of Intelligence and Analysis: Hearing Before the Subcommittee on Intelligence, Information Sharing & Terrorism Risk Assessment, House Committee on Homeland Security Committee*, 110th Cong. (Feb. 14, 2007) (Statement of Charles E. Allen, Assistant Secretary for Information Analysis, Department of Homeland Security).

[117] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Information Sharing Environment Implementation Plan* Nov. 2006 at 29, *at* http://www.ise.gov/docs/ise-impplan-200611.pdf (last visited Mar. 9, 2007).

[118] *Id.*

[119] DEPARTMENT OF HOMELAND SECURITY, *Remarks by the Secretary of Homeland Security Michael Chertoff at the International Association of Chiefs of Police Annual Conference*, Oct. 16, 2006, at http://www.dhs.gov/xnews/speeches/sp_1161184338115.shtm (last visited Mar. 9, 2007).

toward making the homeland safer by making State, local, and tribal law enforcement officers key partners from the outset.

In January of 2007 Mr. Allen provided an assessment of I&A's strategic development to date.[120] Among other things, he highlighted his office's progress in (1) developing its intelligence collection management and open source capabilities; (2) streamlining information of intelligence value; (3) improving the exploitation of information gathered through the Department's exercise of its law enforcement and regulatory responsibilities; (4) training intelligence professionals to recognize information of intelligence value; (5) integrating existing information collection capabilities; and (6) developing a robust analytic focus in the areas of border security; chemical, biological, radiological, and nuclear attack; critical infrastructure; and extremism/radicalization.[121] At the same time, Mr. Allen conceded, "We are still in the 'building' mode—we have yet to develop the required expertise and experience to fully implement our mission."[122] He added that I&A's current needs include a more integrated intelligence effort particularly with the Department's operating components, as well as a more integrated effort with its State, local, tribal, and private sector partners.[123] Toward that end, Mr. Allen has identified five key priorities that are now advancing:

First, he has as an overarching goal of integrating the intelligence units of the Department components to (1) create a unified intelligence culture; (2) improve the reporting of intelligence information from the Department's operating components and providing actionable, relevant analysis back to them; and (3) improve the flow of intelligence information both horizontally within the Department and vertically with its partners at the State, local, and tribal levels, and in the private sector.[124] Specifically, Mr. Allen wants to transform I&A into an entity that can support an all-hazards approach to homeland security by bringing intelligence closer to operations.[125] In so doing, he hopes to provide our nation's leaders with the best possible understanding of threats to inform their decision-making in terms of policy, spending, and response to crisis.[126]

Second, Mr. Allen has established a State and Local Fusion Center Program, which is placing Department intelligence professionals in State and local fusion centers.[127] These officers are working with their partner homeland security and law

[120] Allen, *supra* note 9.
[121] *Id.* at 4-5.
[122] *Id.* at 6.
[123] *Id.*
[124] Allen, s*upra* note 9, at 2-3; *See supra* note 16, at 3.
[125] *Id.*
[126] *Id.*
[127] *Id.* at 9. Fusion centers have been defined as "…effective and efficient mechanism[s] to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources." *See* UNITED STATES DEPARTMENT OF JUSTICE, Bureau of Justice Assistance and Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World*, July 25, 2005 at 3, *at* http://it.ojp.gov/documents/fusion_center_guidelines.pdf (last visited Mar. 9, 2007). While the 43 fusion

enforcement intelligence professionals in the fusion centers to share information, to collaborate in its analysis, and to identify information of intelligence value.[128] The goal is better reporting of valuable information—both between and among fusion centers and with the IC.[129] To date, the Department has deployed twelve officers to 12 fusion centers around the country.[130] According to his recent testimony before the Senate Select Committee on Intelligence, Mr. Allen plans to continue his "aggressive" schedule to deploy up to 35 additional officers by the end of fiscal year 2008 and is currently conducting assessments to determine which centers have the greatest need.[131]

Third, Mr. Allen wants to improve the Department's border security intelligence capabilities and ability to secure the border.[132] Accordingly, he has been pursuing a Campaign for Border Security since the fall of 2005 which, by most reports, is still in the formative stages. Indeed, he stated during his recent Senate testimony that he is still "building" a strong border security strategic intelligence analysis capability within I&A.[133] He reported that a unit designed to create threat assessments and other intelligence products to help guide the activities of the Department's Border Enforcement Security Task Forces has only recently gotten underway,[134] and added that he is "aggressively" sharing his office's border intelligence product by using I&A's State and local fusion center officers to reach out to fusion centers in border States.[135]

Fourth, Mr. Allen is leading an effort within the IC to develop a "Homeland WMD[136] Intelligence Strategy" that will outline the unique aspects of the WMD threat, along with the "goals and actions" needed for I&A to meet this challenge.[137] He wants I&A to collect and analyze non-traditional sources of information, along with traditional intelligence, to detect indicators of the transfer of knowledge, expertise, and materials among individuals with the WMD knowledge and experience, known terrorist organizations, and other criminal or extremist groups.[138] Critical to this "building" effort, he stated, is "developing the homeland intelligence tradecraft through the recruitment and training of a first-class WMD intelligence cadre."[139]

centers that exist today are each unique, their memberships typically include State, local, and tribal law enforcement authorities; State entities responsible for the protection of public health and infrastructure; private sector owners of critical infrastructure; and Federal law enforcement and homeland security personnel, among others. *See* Alice Lipowicz, *To Be or Not to Tell*, Washington Technology, July 24, 2006, *at* http://www.washingtontechnology.com/news/21_14/federal/28981-1.html (last visited Mar. 9, 2007); Joe Trella, *State Intelligence Fusion Centers: Recent State Actions, National Governor's Association Center for Best Practices*, July 7, 2005, *at* http://www.nga.org/Files/pdf/0509FUSION.PDF (last visited Mar. 9, 2007).

[128] Allen, *supra* note 9.

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] Allen, *supra* note 9*,* at 10

[133] *Id.* at 10-11.

[134] *Id.* at 10.

[135] *Id.* at 11.

[136] Weapons of Mass Destruction

[137] Allen, *supra* note 9, at 11.

[138] *Id.*

[139] *Id.* at 12.

Fifth, as previously mentioned, Mr. Allen has made clear that one of his key priorities is integrating the intelligence units of the Department components. Among other things, this will require a common information sharing system allowing those components to more adequately share information within the Department.

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 to avoid public disclosure of I&A's classified budget and personnel numbers. For fiscal year 2008, the President's budget request for Analysis and Operations is $314.6 million, a five percent increase over the enacted fiscal year 2007 level. For fiscal year 2008, the combined full-time employee request is for 518 staff positions, a 9 percent increase fiscal year 2007 level. Notably, the entire Analysis and Operations budget request accounts for only 1 percent of the President's entire Department of Homeland Security budget request for fiscal year 2008. The modest increases that the President proposes for fiscal year 2008 may complicate Mr. Allen's plans for making I&A the rigorous intelligence shop he envisions.

IV. AREAS FOR IMPROVEMENT

The Department-led ITACG initiative and the Department's separate information sharing fellows program are both steps in the right direction, but the devil is in the details. Although Mr. Allen has committed to including State, local, and tribal representatives as part of the ITACG, he has not yet provided any details about how best to embed them at the NCTC or who he plans to convene as part of a proposed panel to ascertain their information sharing needs. Mr. Allen should provide that information to Congress and to the State, local, and tribal law enforcement community without delay and should provide an implementation plan with key development benchmarks. The Secretary and Mr. Allen should do the same for the Department-based information sharing fellows program. Once both initiatives are underway, the Department should provide regular progress reports to the relevant Congressional committees to ensure that they are guided by a clearly defined mission and have adequate funding to complete their critical work.

Mr. Allen's five I&A priorities—while equally promising—present even greater challenges given the modest budget increases to the Analysis and Operations account proposed by the Administration for fiscal year 2008. The apparent leveling off of funding is troubling given Mr. Allen's still unfulfilled goals, including program integration of the Department's numerous intelligence units; fully funding, staffing, and rolling out I&A's State and Local Fusion Center Program; developing a robust border intelligence capability; and protecting the homeland from a WMD attack. All of these initiatives are in critical stages of their development and need a robust funding stream to make America safer. Indeed, good intelligence is the cornerstone of good policymaking. By knowing what the threats are, where we are vulnerable, and the consequences of not acting, the Congress, the Department of Homeland Security, and other Executive Branch agencies alike can ascertain what resources to expend where.

By shortchanging the Analysis and Operations account, however, the Administration has tied one hand behind America's back in its fight against its terrorist antagonists. Mr. Allen should set priorities among his mission goals and level with Congress about his office's true needs so it can authorize and appropriate funding accordingly.

Finally, the slow progress of program integration in the Department remains a serious challenge. Although Department Management Directive 8110 may have gotten Mr. Allen halfway toward his goal in this area, it appears that the authorities he has been provided—which include limited input into the component budget process—falls short of what he needs. Time is of the essence. The Department, including Mr. Allen and the various heads of its intelligence components, should form an integration task force clarifying what authorities are needed to create the common intelligence culture and mission that both the Secretary and Mr. Allen have described to Congress and the American people, take appropriate action at the Department level to make that culture and mission a reality, and make recommendations to Congress about what legislative authorities may be needed to drive needed change in this area.

SCIENCE AND TECHNOLOGY GRADE: C+

I. STATEMENT OF PROBLEM HISTORICALLY

The Science and Technology (S&T) Directorate spent much of 2006 on the defensive, as Congress and the press criticized the unit for its failures in technology production, leadership, and budget justification. An August 2006 article in the *Washington Post* stated that the organization was "hobbled by poor leadership, weak financial management and inadequate technology," adding that S&T "struggled with turnover, reorganizations and raids on its budget."[140] Concerned about a lack of transparent strategic planning, inadequate budget justification detail, systemic deficiencies in financial and accounting controls, and poor response to the needs of customers, Congressional appropriators expressed their frustration with the Directorate's production by slashing the FY 2007 budget and withholding funds until performance measures can be reached.[141] As a general matter, many—both in and out of Congress—have lost confidence in the ability of the S&T Directorate to fulfill its statutory responsibilities.

Against this backdrop, retired Navy Rear Admiral Jay M. Cohen became the Department's second Under Secretary for Science and Technology Directorate on August 10, 2006.

II. STATE OF SCIENCE AND TECHNOLOGY TODAY

Since August 2006, Under Secretary Cohen has made significant strides towards improvement. Focused on making "a change in organizational culture" to make the S&T Directorate "a model service organization focused on its customers," the Under Secretary spent his first six months reorganizing the Directorate. [142] He created six major divisions: (1) Explosives (Transportation Security Program and Counter-MANPADS); (2) Chemical/Biological Programs; (3) Command, Control, and Interoperability (including interoperability and cybersecurity); (4) Borders/Maritime; (5) Human Factors (psychology of terrorism); and (6) Infrastructure/Geophysical (critical infrastructure protection). He also created two additional divisions – Research and Transition. The six major divisions have matrixes to their staff representatives from the Research and Transition divisions; each Director of Research will report to a new Division Director of Research, while each Director of Transition will report to a new Division Director of Transition.

[140] Spencer S. Hsu, *DHS Terror Research Agency Struggling*, WASHINGTON POST , Aug. 20, 2006.
[141] S. REP. NO. 109-273, *Department of Homeland Security Appropriations Bill* (2007). "The Committee is extremely disappointed with the manner in which S&T is being managed within the Department of Homeland Security. Despite the efforts of the Acting head of S&T, this component is a rudderless ship without a clear way to get back on course. The Committee directs the Secretary to immediately develop a 5-year research plan, including performance measures, which reflect DHS's research and funding priorities, and brief the Committee no later than 60 days after the date of enactment of this act. Developing and implementing this 5-year plan is the only way S&T will be successful."
[142] Testimony of Jay M. Cohen, Under Secretary for Science and Technology, Department of Homeland Security, before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Emergency Preparedness, Science, and Technology (Sep. 7, 2006)

Under Secretary Cohen wants to change the way the S&T Directorate interacts with the rest of the Department. Under Cohen's organizational structure, the S&T Directorate serves its consumers, the people and organizations that make use of the technologies and capabilities that the Directorate develops or adapts to secure the homeland.

The S&T Directorate has two main consumers of its research, development, testing, and evaluation ("RDT&E") process, (1) customers and (2) end-users. The Directorate's customers are the Department's other components, such as the Transportation Security Administration, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement. The Directorate's end-users are the "boots on the ground," first responders and others who use homeland security technology in the field. In establishing its research and development priorities, the S&T Directorate needs to solicit feedback and input from both its customers and end-users on a continual basis.

This innovative organizational model is still very new, and time will tell if the Integrated Project Teams created by the Under Secretary will work. For the time being, there exists a great deal of confidence in his ability to turn the Directorate into an effective branch of the Department.

Some observers question whether the S&T Directorate's staff can adequately manage and monitor research and development projects and the associated contracts that are generated. This deficiency, it is said, has led to the Directorate's inability to produce the technological advances required to improve contemporary technology to meet the needs of the Department's operations. The shortfall in establishing effective program management and controls may explain why the Directorate has not been able to spend its allocated budget in recent years.

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget requests $799 million for the S&T Directorate, a decrease of $49 million from the enacted fiscal year 2007 amount.[143] This represents a troubling trend for research and development spending at the Department. Without additional investments in homeland security research, development, testing, and evaluation, it is hard to imagine that the Department will continue to make significant progress in these critical areas.

Several program cuts are particularly troubling. There is great concern about the budget for cybersecurity research and development. In fiscal year 2007, the President proposed a budget of $22.7 million for cybersecurity; this year that request fell to $14.8 million. This is disturbing given the release of several reports by the President's Information Technology Advisory Council (February 2005) and the Interagency Working Group on Cyber Security and Information Assurance (April 2006)

[143] *Supra* note 6.

calling for a higher investment in Federal cybersecurity R&D. The President also proposed a cut for University Programs, from $48.5 million in fiscal year 2007 to $38.7 million in fiscal year 2008. The Department claims that the budget cut is justified because they are instituting an across-the-board reduction to the level of effort at all Centers of Excellence and in the number of Scholars and Fellows.

Several areas of the President's budget warrant positive mention. The President's fiscal year budget requested almost $6 million more than last year's request for the Human Factors program, which promises to produce social and behavioral research that will enhance passenger screening methods consistent with the Bill of Rights. Similarly, the BioWatch program was so successful it was transferred out of the S&T Directorate and into the Office of Health Affairs when research and development concepts were transformed into operational programs.

IV. AREAS FOR IMPROVEMENT

There are several areas for improvement in fiscal year 2008. Part of leading an organization is to provide clear statements of principles, priorities, and vision. Unfortunately, in spite of its mandate in the Homeland Security Act, neither the national policy nor the strategic plan for the S&T Directorate has been produced.[144] The strategic plan will reportedly be ready at the end of March 2007, but there are questions about whether specific items will be included. There is no date for the issue of the national policy.[145]

Financial reporting will remain an area for improvement. In November 2005, the Department's independent financial auditors reported that during fiscal year 2005 S&T had financial reporting deficiencies that included "serious difficulties maintaining accurate financial records related to obligations and disbursements."[146] In a review of the President's fiscal year 2007 budget request, the Government Accountability Office (GAO) found that S&T was unable to provide breakdowns of funds it obligated to private and public sector facilities.[147] This led to a significant cut in S&T funding during the fiscal year 2007 budget cycle. S&T must continue to develop a mature business model, involving financial management system accountability and prudent project management including performance metrics.

The recently released OPM (Office of Personnel Management) Survey ranked the Department at or near the bottom in four major personnel categories, including

[144] The Homeland Security Act, *supra* note 93. The Act requires the Secretary to produce both a strategic plan for S&T and a national policy on homeland security research and development. Id.

[145] *Understanding the Budget and Strategic Agenda of the Science and Technology Directorate: Hearing Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology*, 110th Cong. (Feb. 14, 2007) (Testimony of Jay M. Cohen, Under Secretary for Science and Technology, Department of Homeland Security).

[146] DEPARTMENT OF HOMELAND SECURITY, *Performance and Accountability Report Fiscal Year 2005*, Nov. 15, 2005.

[147] GOVERNMENT ACCOUNTABILITY OFFICE, *Department of Homeland Security, Science and Technology Directorate, Fiscal Year 2007*, letter to House Appropriations Committee (on file with House Homeland Security Committee staff).

performance and job satisfaction. During a February 14, 2007 hearing, Under Secretary Cohen told the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology that he will provide a plan to strengthen workforce recruitment and retention, improve the institutional knowledge base, and improve management control issues (with regard to ethics and Intergovernmental Personnel Act deployments).[148]

Finally, the Under Secretary must become a strong intra-department coordinator for determining the R&D needs and performance of the various Department divisions. He should be included in the chain of acquisition authority throughout the Department, to ensure consistency throughout all intra-departmental R&D activities. Under Secretary Cohen's Integrated Project Team (IPT) process may address some of these issues, but there is certainly room for improvement over the 2006 performance. More important, the Under Secretary must improve the relationship between the Department and the Department of Energy laboratories, often strained in the past because of inadequate communication and a lack well-defined roles.

[148] *See* Cohen, *supra* note 144.

THE STATE OF BIOSECURITY GRADE: B-

I. STATEMENT OF PROBLEM HISTORICALLY

A bioterrorist attack or pandemic outbreak in the United States could have devastating consequences. A bioterrorism incident or a naturally occurring biological event, such as a SARS or avian influenza pandemic, could be indistinguishable in the early stages. Because of this, the Nation's biodefense should be constructed using an all-hazards approach. Unfortunately, as with the current situation in first responder grants and other areas of disaster response, the Nation has adopted an approach that treats terrorist acts differently from accidents or natural disasters. The immediate response on September 11th would have been the same whether the planes that struck the Twin Towers and the Pentagon had been made to do so intentionally or by accident. The same view should be applied to a biological event.

Examining the preparedness for what most experts believe is an impending influenza pandemic should not only inform the Nation of its preparedness for that event, but should also give the Nation an idea of its preparedness for a bioterrorist attack. If the Nation cannot prepare for a pandemic that could infect a large number of people with little warning, then the Nation will definitely be caught unprepared for a biological attack coming without warning.

II. STATE OF BIO SECURITY TODAY

The biodefense capabilities of the United States 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. Although some progress has been made in the past year, these systems are not adequately developed. The National Biosurveillance Integration System (NBIS) is intended to provide situational awareness by integrating environmental, epidemiological, group-behavioral, and other data streams that combine to form indicators of disease outbreaks. The NBIS, which had begun but subsequently stalled in the Infrastructure Protection Directorate at the Department, has been moved to the new Office of Health Affairs where it has been given a high priority.

The United States still needs to enhance international cooperation to conduct biosurveillance. Disease outbreaks and other health-related activities in some countries remain beyond the view of the Federal government. For example, although the H5N1 strain of avian influenza has been infecting humans since 1997, China was able to temporarily hide the level of its outbreaks from the United States and the international community.[149]

[149] Tiaji Salaam-Blyther and Emma Chanlett-Avery, *US & International Responses to Avian Flu – Issues for Congress*, CONGRESSIONAL RESEARCH SERVICE, CRS RL 33219, January 11, 2006, (noting international

BioWatch, the environmental monitoring program operated in over 30 cities across the Nation by the Department in partnership with the Laboratory Response Network (LRN), has had difficulties in recent years. A recent report by the Department's Inspector General found that serious problems existed in the handling of laboratory samples, including:

- improper transfer of exposed filters at 84% of the labs;
- improper decontamination of chain-of-custody bags at 74% of the labs;
- procedural errors in field-to-lab transfer of samples at 65% of sites,
- improper quality control at 53% of the labs;
- improper storage of filters during transport in 42% of BioWatch sites, and,
- improper sample management at 32% of labs.[150]

The Inspector General's report notes that the problems have been corrected; however, the existence of such widespread problems signals the need for aggressive oversight to ensure program integrity.

Biological countermeasures are needed to protect and mitigate the effects of a biological incident. Project BioShield (Pub. L. 108-276) is the primary Federal program for developing biological countermeasures.[151] Unfortunately, it has not lived up to expectations. To date, Project BioShield has only awarded contracts for immunizing against or treating anthrax, botulinum toxin, and radiological sicknesses,[152] even though the Centers for Disease Control and Prevention has listed over thirty "select agents" of concern.[153] The real bottleneck in the process seems to be the Department of Health and Human Services, which in December vacated their largest contract for a next-generation anthrax vaccine.[154]

The first step in the BioShield process requires the completion of Material Threat Determinations (MTD). The Department of Homeland Security has successfully completed fourteen MTDs, up from only five one year ago. [155] Serious questions remain, however, regarding preparedness for a bioterrorist attack and which Federal

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).

[150] DEPARTMENT OF HOMELAND SECURITY OFFICE OF INSPECTOR GENERAL, *"DHS' Management of BioWatch Program,"* OIG-07-22, Jan. 2007.

[151] Frank Gottron, *Project BioShield,* CONGRESSIONAL RESEARCH SERVICE, CR RS 21507 (updated Jan. 22, 2007) *at* http://www.congress.gov/erp/rs/pdf/RS21507.pdf (last visited Mar. 9, 2007).

[152] DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF RESEARCH AND DEVELOPMENT COORDINATION, *Project BioShield Related Procurement Projects*, at http://www.hhs.gov/ophep/bioshield/PBPrcrtPrjct.htm (last visited Mar. 9, 2007).

[153] CENTERS FOR DISEASE CONTROL AND PREVENTION, *Agents, Diseases, and Other Threats, at* http://www.bt.cdc.gov/agent/ (last visited Mar. 9, 2007).

[154] Renae Merle, *Anthrax Vaccine Contract Voided, Thwarting Administration*, WASHINGTON POST, December 20, 2006, at A1.

[155] Information from DEPARTMENT OF HOMELAND SECURITY OFFICE OF LEGISLATIVE AFFAIRS (on file with House Homeland Security Committee).

department is in charge in the event of such an attack or a pandemic outbreak. The Bush Administration released its National Strategy for Pandemic Influenza in November 2005.[156] In May 2006, the Administration released the Implementation Plan for the National Strategy. [157] Nevertheless, it is not clear how the plans will be executed if an actual pandemic occurs. For example, a very small-scale, one-day pandemic influenza exercise recently conducted by the Centers for Disease Control and Prevention had to be aborted half-way through because of bad weather.[158]

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget request essentially represents flat funding for most biodefense programs within the Department. 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 in fiscal year 2006 to $8.2 million in fiscal year 2007. The President's fiscal year 2008 budget request is essentially flat at $8 million.[159] Without more funds, the NBIS will not be adequately prepared to monitor patterns of illness for an attack or outbreak in the United States.

The President's fiscal year 2008 budget is essentially flat regarding the BioWatch program as well.[160] Last year the program resided entirely within the Department's Science and Technology Directorate (S&T), but the operational components were transferred to the newly created Office of Health Affairs (OHA). OHA will be headed by the Chief Medical Officer, who is responsible for ensuring completion of all Departmental Project BioShield activities and serves as the Department's point person for avian influenza preparedness. Yet, this unit only received a total of $5 million and fifteen full-time employees. The President's fiscal year 2008 budget request is $118 million and forty-nine full-time employees, of which $84 million is committed to BioWatch operations.[161]

The National Strategy on Pandemic Influenza proposed $7.1 billion to prepare for avian flu, 85% of which is focused on vaccines and antivirals that the United States does not have the capacity to produce. Only $251 million is proposed to "detect and contain outbreaks" and $644 million "to ensure that all levels of government are prepared to respond to a pandemic outbreak."[162]

[156] THE WHITE HOUSE, *National Strategy for Pandemic Influenza,* Nov. 2005, *at* http://www.whitehouse.gov/homeland/nspi.pdf (last visited Mar. 9, 2007).

[157] THE WHITE HOUSE*, National Strategy for Pandemic Influenza Implementation Plan*, May 2006, *at* http://www.whitehouse.gov/homeland/nspi_implementation.pdf (last visited Mar. 9, 2007).

[158] David Brown, In Drill, CDC Practices For Influenza Pandemic, *Washington Post*, Feb. 4, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/02/03/AR2007020301120.html (last visited Mar. 9, 2007).

[159] DEPARTMENT OF HOMELAND SECURITY OFFICE OF HEALTH AFFAIRS, *Summary of FY 2008 Budget*, 2007.

[160] DEPARTMENT OF HOMELAND SECURITY, *supra* note 25.

[161] *Id.*

[162] THE WHITE HOUSE*, Implementation of the National Strategy for Pandemic Influenza: Six-Month Status Report, at* http://www.whitehouse.gov/infocus/pandemicflu/ (last visited Mar. 9, 2007).

To date, emergency supplemental appropriations have provided $6.1 billion in additional funding.[163] The President's fiscal year 2008 budget requests $1.19 billion. If enacted, this amount would overshoot the original proposed $7.1 billion by $200 million.[164]

IV. AREAS FOR IMPROVEMENT

First, a robust biointelligence and biosurveillance capability must continue to 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 capability in this area. The NBIS is designed to fuse many of these sources of information, but it needs more support to succeed. In addition, BioWatch, an important data stream for NBIS, must be closely monitored to ensure smooth operation and to stop a resurgence of previous problems.

Second, Project BioShield, created to promote development of vaccines and other medical countermeasures, must be either improved or replaced with a program that will achieve this objective. The cancellation of the largest BioShield contract after the company invested $175 million of its own funds will probably result in the collapse of the company, and does not bode well for the future of the program.[165]

[163] $3.8 billion of this funding came in the Department of Defense, Emergency Supplemental Appropriations to Address Hurricanes in the Gulf of Mexico, and Pandemic Influenza Act of 2006 (Pub. L. 109-141), while $2.3 billion came in the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Hurricane Recovery, 2006 (Pub. L. 109-234). *See* Sarah A. Lister, *Pandemic Influenza: Appropriations for Public Health Prepardness and Response*, CONGRESSIONAL RESEARCH SERVICE, CRS Report RS22576 (updated February 20, 2007) *at* http://www.congress.gov/erp/rs/pdf/RS22576.pdf (last visited Mar. 9, 2007).

[164] *Id.*

[165] *Id.* at 6.

CHEMICAL PLANT SECURITY GRADE: B-

I. STATEMENT OF PROBLEM HISTORICALLY

Until this year, the Department did not have any authority to ensure that chemical plants, or any critical infrastructure sector for that matter, had adequate security. Although chemical plants constitute "critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being,"[166] prior Congresses did not respond to numerous demonstrations of need.

In October 2002, then-Department of Homeland Security Secretary Tom Ridge and then-Environmental Protection Agency Administrator Christie Todd Whitman declared in a joint letter to the *Washington Post* that "[v]oluntary efforts alone are not sufficient to provide the level of assurance Americans deserve."[167]

In November 2003, the television show *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."[168]

In April 2005, during his appearance before the House Committee on Homeland Security, Secretary Chertoff stated "I know, for example, 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 in order to make sure we get to where we need to get."[169]

In the fall of 2006, Congress finally responded by granting the Department authority to regulate security at chemical facilities. After failing to pass comprehensive chemical facility legislation[170], Congress instead attached an amendment to the Homeland Security Appropriations Act for fiscal year 2007[171] directing the Department

[166] THE WHITE HOUSE, *Homeland Security Presidential Directive 7*, December 17, 2003, *at* http://www.fas.org/irp/offdocs/nspd/hspd-7.html (last visited Mar. 9, 2007).
[167] James V. Grimaldi, *Fearing Litigation, EPA Treads Lightly with Chemical Industry, Despite Terror Threat*, WASHINGTON POST, Mar. 24, 2003.
[168] *60 Minutes*, (CBS television broadcast, Nov. 14, 2003).
[169] *The Department of Homeland Security: Promoting Risk-Based Prioritization and Management: Hearing Before the House Committee on Homeland Security*, 109th Cong. (Apr. 13, 2005) (statement by Michael Chertoff, Secretary, Department of Homeland Security).
[170] The Chemical Facility Anti-Terrorism Act of 2006, H.R. 5695, 109th Cong. (2006).
[171] Homeland Security Appropriations Act, *supra* note 5, at § 550.

to develop interim final regulations for chemical facility security to be completed within six months of enactment.

II. STATE OF CHEMICAL PLANT SECURITY TODAY

The overall state of chemical plant vulnerability is high, given the relatively low level of security in place today. There are some facilities that are voluntarily doing an excellent job with their security practices. Others have simply not increased their security enough to prevent or adequately mitigate a terrorist attack. As chemical plant security specialist Sal DePasquale stated in testimony before the House Committee on Homeland Security in June of 2005, "[s]urely 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. Indeed, the most sophisticated and costly camera systems can not stop an armed assailant and may produce little more than material for use on the 11 o'clock news."[172]

The Government Accountability Office (GAO) agrees with Mr. DePasquale. In testimony before the Senate Committee on Homeland Security and Governmental Affairs in April 2005, John Stevenson, Director of Natural Resources and Environment at the GAO stated that, "[a]bout 1,100 facilities participate in a voluntary industry effort in which they assess vulnerabilities, develop security plans, and undergo third party verification that the facilities implemented the identified physical security enhancements. The extent to which the remaining facilities are addressing security is unclear and the extent of chemical facilities' security preparedness is unknown."[173]

The Department has taken positive steps to ensure chemical plant security. For example, the development of analytical metrics to properly categorize the risk posed by any specific plant has been a great improvement. The use of the Risk Assessment Methodology for Critical Asset Protection has allowed the quantification of threat, vulnerability, and consequence factors to be taken into account in a rational and systematic way.

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget requests $15 million for Chemical Site Security Office, up from $10 million in fiscal year 2007.[174] The office is tasked with implementing and enforcing the regulations the Department will promulgate in April 2007. With over 10,000 facilities to regulate and only seventeen full-time employees for the office, the task is daunting. The Office plans to tackle first the very highest risk

[172] *Preventing Terrorist Attacks on America's Chemical Plants: Hearing Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity*, House Committee on Homeland Security, 109th Cong (June 15, 2005) (statement of Sal DePasquale).

[173] John B. Stephesnon, *HOMELAND SECURITY: Federal and Industry Are Addressing Security Issues at Chemical Facilities, but Additional Action is Needed*, GOVERNMENT ACCOUNTABILITY OFFICE, GAO-05-631T (Apr. 27, 2005).

[174] DEPARTMENT OF HOMELAND SECURITY, *supra* note 59.

facilities, numbering less than 20. More funding and more personnel will be needed in future years if the mission of securing all chemical facilities is to be successful.

Assistant Secretary for Infrastructure Protection Bob Stephan reaffirmed the need for increased future funding in an interview last year with *Congressional Quarterly*. "Right now, we don't have a robust enough office to deal with chemical security as a regulatory process inside my shop, so the $10 million would support the…first year's worth of activity to support the rulemaking that's going to be necessary…Business writ large has made a lot of improvements, but the progress has not necessarily been even across the board," Stephan said. "We have to take care of that," he added.[175]

IV. AREAS FOR IMPROVEMENT

Grave concerns remain regarding the specifics of the proposed rulemaking, which was open for public comment until February 7, 2007. The most glaring problem was the assertion that the Federal law should preempt state laws if they "conflict with, hinder, pose an obstacle to or frustrate the purposes of the [federal] regulations."[176] In addition, the proposed regulation would unnecessarily create a new class of protected information; does not promote chemical facility employee protection or involvement; does not promote the use of safer technologies that would inherently lower the consequences of an attack on or accident at a chemical facility, and other problems.

Many in Congress, including Members of the Committee on Homeland Security and the Committee on Energy and Commerce, have submitted comments asking the Department to address the issues before the interim final regulation is promulgated on April 7, 2007. The proposed regulations have a three-year sunset provision.

[175] Benton Ives-Halperin, *DHS Budget Request May Portend New Authority Over Chemical Security*, CONGRESSIONAL QUARTERLY – HOMELAND SECURITY, Feb. 22, 2006, *at* http://homeland.cq.com/hs/display.do?docid=2054309&amp;sourcetype=31&amp;binderName=news-all (last visited Mar. 9, 2007).

[176] Department of Homeland Security Chemical Facility Anti-Terrorism Standards, 71 Fed. Reg. 78275 – 78332 (Dec. 28, 2006).

DOMESTIC NUCLEAR DETECTION OFFICE GRADE: B

I. STATEMENT OF PROBLEM HISTORICALLY

It is widely agreed that the number one threat facing the nation is a nuclear attack. Although the likelihood that a terrorist group could successfully carry out such an attack is low, the consequences would be so catastrophic that defending against this threat is a top priority of the Department.

The Domestic Nuclear Detection Office (DNDO) is responsible for detecting and reporting efforts to import or transport nuclear or radiological materials into or within the United States. DNDO was originally one of the portfolios within the Department's Science and Technology (S&T) Directorate. After the Department's Second Stage Review, the decision was made to move DNDO out of S&T and execute programs as a stand-alone office.

The President's fiscal year 2007 budget request reflected this desired change in organization. Congress agreed and the DNDO was authorized as part of the SAFE Ports Act of 2006.[177]

II. STATE OF DNDO TODAY

The DNDO has moved aggressively to procure and deploy technologies to detect radiological and special nuclear materials, mostly at the Nation's ports of entry. As of February 2007, Radiation Portal Monitors (RPM) were scanning one-hundred percent of all United States mail, eighty-nine percent of all cargo entering through the Nation's seaports, ninety-six percent of cargo at the Southern border and ninety-one percent at the Northern border, with expected increases to ninety-seven percent at seaports and ninety-nine percent at the Southern border by the end of fiscal year 2007. To date, roughly 1,000 RPMs have been deployed. Future deployments designed to scan one-hundred percent of all conveyances will require an additional 1,500 – 2,000 units over a deployment schedule through fiscal year 2013. Rail crossings and airports have yet to be addressed.[178]

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget request is $561.9 million, up from the fiscal year 2007 enacted level of $481 million.[179] Additional funding is requested for the Securing the Cities Initiative ($30 million), a pilot program for radiological and nuclear "defense in depth" to be carried out in New York City, and $47 million for Next-

[177] Pub. L. 109-347.

[178] DOMESTIC NUCLEAR DETECTION OFFICE, *FY2008 Budget: Briefing to House Homeland Security Committee Staff*, Feb. 21, 2007.

[179] DEPARTMENT OF HOMELAND SECURITY, *supra* note 59.

Generation Research and Development to deploy new technologies, including the Advanced Spectroscopic Portal Monitors (ASP).[180]

IV. AREAS FOR IMPROVEMENT

There has been an aggressive pace with which DNDO has deployed radiation detection technologies as well as the good working relationships they have forged with Customs and Border Protection and the Department of Energy. Serious questions linger, however, regarding DNDO's cost-benefit analysis of ASP systems. In October 2006, GAO sent a letter to the Chairmen of the House and Senate Appropriations Committee critical of the methods used by DNDO in their cost-benefit analysis of ASP. [181] The anomalies included incorrect performance indicators such as false negative rates as well as inflated cost estimates of traditional "plastic" RPMs.

In addition, as the information sharing chapter of this report card indicates, it appears there is a possible overlapping of functions between the Office Intelligence and Analysis (OIA) and DNDO. The DNDO funds a Joint Analysis Center (FY 2008 $9.2M) whose program objectives include, "[e]nhanc[ing] the sharing of nuclear detection information to Federal, State, and local authorities, and the Intelligence Community (NCTC, DHS/OIA, FBI)."[182]

Through oversight, Congress will be in a better place to assess if cooperation is effective among DNDO and other entities; examine the possibilities of aggressive deployment of detection technologies; and, determine whether proper internal procedures are being installed to ensure that the right technologies are deployed.

[180] *Id.*
[181] Gene Aloise, *Combating Nuclear Smuggling: DHS's Cost-Benefit Analysis to Support the Purchase of New Radiation Detection Portal Monitors Was Not Based on Available Performance Data and Did Not Fully Evaluate All the Monitors' Costs and Benefits,* GOVERNMENT ACCOUNTABILITY OFFICE, GAO-07-133R (October 17, 2006).
[182] DOMESTIC NUCLEAR DETECTION OFFICE, *supra* note 76.

MANAGEMENT AND ORGANIZATION GRADE: INCOMPLETE

I. STATEMENT OF PROBLEM HISTORICALLY

The Directorate for Management plays a pivotal role in the functioning of the Department. It is responsible for:

- Budget;
- Appropriations;
- Expenditure of funds;
- Accounting and finance;
- Procurement;
- Human resources and personnel;
- Information technology systems;
- Facilities, property, equipment, and other material resources; and,
- Identification and tracking of performance measurements relating to the responsibilities of the Department.

The Directorate defines its mission as "ensuring that the Department's more than 170,000 employees have well-defined responsibilities and that managers and their employees have effective means of communicating with one another, with other governmental and nongovernmental bodies, and with the public they serve." The Under Secretary for Management has direct authority over the Department's six chief operating officers, who reside in the Directorate:

- Chief Administrative Services Officer;
- Chief Financial Officer;
- Chief Human Capital Officer;
- Chief Information Officer;
- Chief Procurement Officer; and,
- Chief Security Officer.

The current Under Secretary for Management, Paul Schneider, was sworn in on January 3, 2007. Prior to his arrival, the Directorate for Management under the leadership of Under Secretary Janet Hale, who reportedly ruled with a heavy hand, tightly controlling access to the Secretary. The Chief Operating Officers reportedly received limited support from Ms. Hale's office in their efforts to resolve problems and had a difficult time raising their concerns to the Secretary or Deputy Secretary. The resulting impact is that progress on core Departmental functions remains hindered.

In the face of these problems, the Committee's bipartisan fiscal year 2007 authorization bill included a provision that would have eliminated the position of Under Secretary for Management, establishing the Chief Operating Officers as direct reports to the Secretary. This provision was intended to mirror Secretary Chertoff's Second Stage Review (2SR) reforms, which dissolved the Border and Transportation Directorate and gave component heads direct access to the Secretary. The bill also included a provision to give the Chief Operating Officers direct authority over their respective counterparts in component agencies.

II. THE STATE OF MANAGEMENT AND ORGANIZATION

There was bad news waiting for Under Secretary Schneider when he first arrived at the Department. In December 2006, the Department's Inspector General issued a report entitled *Major Management Challenges Facing the Department of Homeland Security*. Several areas within the Directorate's jurisdiction were among the challenges identified, including financial management, acquisition and contract management, and information technology. In January 2007, the Government Accountability Office (GAO) issued its *High Risk Series—an Update* report. GAO first designated the establishment and transformation of the Department as a high risk area in January 2003. In the 2007 update, though the GAO found that the Department had made some progress in its transformation, management, and program challenge, it still identified numerous management challenges. These included the failure to submit a corrective action plan to address issues previously raised by the GAO, the lack of a department-wide financial system capable of generating reliable data, the continuing failure to receive a clean audit opinion, inadequate oversight of major procurement programs, and understaffed procurement offices. [183]

More bad news came in late January in the form of the Office of Personnel Management's (OPM) 2006 Federal Human Capital Survey. The Department came in last or nearly last in every category. It had the lowest score of any Federal agency or department in terms of "job satisfaction" and "results-oriented performance culture." It also received rock-bottom scores for "talent management" (third from last) and "leadership and knowledge management" (second from last).

The "incomplete" grade in this area is a reflection of the recent turnover at the top of the Directorate. But for the recent change in leadership, the Department would have received a failing grade, as the Directorate for Management has failed to fulfill its responsibilities to date.

III. PRESIDENT'S BUDGET

Many of the problems of this Directorate cannot be solved by additional resources alone, as the root cause historically rested with poor leadership. However, the President's budget did add some needed funds in the procurement section of this report. Specifically, the President's fiscal year 2008 budget requests $120 million for the relocation and consolidation of Departmental facilities in the National Capital Region to the St. Elizabeth's Hospital site. While there is support for the goal of consolidating Department functions, there is also concern about the potential cost for this effort and that the Department might view a consolidated headquarters as a panacea for its dangerously low morale and its integration difficulties. A headquarters

[183] GOVERNMENT ACCOUNTABILITY OFFICE, *High Risk Series—an Update*, GAO-07-310 (Jan. 2007) at 52.

that is physically consolidated should not be mistaken for a Department that is philosophically united.

IV. AREAS FOR IMPROVEMENT

There is general consensus that Under Secretary Schneider can assist the Directorate, and the Department, to change course. In his short time in office, Under Secretary Schneider has quickly identified many of the significant problems at the Directorate, and has been candid in discussing them with the Committee on Homeland Security. Under Secretary Schneider recognized that the Department sorely lacks experienced procurement and contract management staff, and has expressed his deep concern over the recent OPM job satisfaction survey. As the Directorate enters its third month under Under Secretary Schneider's leadership, it is time to move from identifying problems to offering concrete solutions.

EMPLOYEE MORALE GRADE: F

I. STATEMENT OF PROBLEM HISTORICALLY

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. Congress, at the Administration's urging, sought to create a flexible and modernized personnel system which could meet the mission needs of the Department, while preserving principles of fundamental merit.

Since its creation, the Department has failed to demonstrate that it is capable of creating a fair and flexible system. In its annual survey, the Office of Personnel Management (OPM) found that Department consistently ranked among the lowest cabinet departments and independent agencies in employee morale. OPM asks questions it finds reflective of four indices: leadership and knowledge management, a results-oriented performance culture, talent management, and job satisfaction. In the 2004 survey, the Department was *last* of all federal agencies for employee satisfaction. An abysmal 3% of Department employees felt that personnel decisions were based on merit, while only 4% felt that creativity and innovation were rewarded.

Two years later, nothing changed: the Department was 36th in job satisfaction and results-oriented performance culture as well as 35th on leadership and knowledge management and 33rd on talent management. Forty-three percent of the Department's employees said they have insufficient resources to do their jobs. Forty-one percent said they do not get enough information from management—a particularly important matter when it comes to protecting the nation. When it comes to top-down leadership, the numbers are equally bad: 47% said their leaders fail to generate high levels of motivation, while 43% disagreed that awards are based on how well employees do their jobs. A workforce that continues to suffer from low morale is not likely to deliver peak performance.

While employed by the Department's component legacy agencies, pay, promotion, and benefits were governed by the time-tested federal civil service system. Needing to start from scratch, DHS proposed a system of its own called MaxHR. In August and October of 2005, the United States District Court for the District of Columbia struck down the system, finding it violated collective bargaining rights and other employee protections. The D.C. Circuit affirmed this decision in June 2006, declaring the that Department's scheme "defies common sense," is "bizarre," and does not "ensure collective bargaining."

Despite the court's ruling, the Department has now implemented a program that blends MaxHR components with other problematic standards for measuring employee success. The new program is entitled the "Human Capital Operations Plan" (HCOP). Among other issues, the phrase "human capital" presents significant challenges. The new plan consists of five goals:

- Hire and retain a talented and diverse workforce;
- Create a Department-wide culture of performance;

- Create high-quality learning and development programs;
- Implement Department-wide integrated leadership system; and,
- Be a model of human capital service excellence.

Although the stated goals of HCOP are seemingly admirable, MaxHR sets out to accomplish the top three goals of the new plan. In fact, a Department-produced document states, “the operational plan [HCOP] encompasses all MaxHR initiatives and more.”

THE DIVERSITY CHALLENGE CONTINUES

Adding to low employee morale is the Department’s ongoing diversity challenge. The Department has not moved to enhance minority representation in any measurable manner. Minority employees account for a thirty-seven percent of the total employee population. By February 2006, the Department had increased the number of employees by 6,030, but non-minority employees accounted for 5,098 or an astoundingly high *ninety-nine percent* of this group. Indeed, because of the increase in the total employee population, the overall percentage of minority representation decreased. The table below details the February 2006 ethnic racial and gender division of employees.

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

II. AREAS FOR IMPROVEMENT

The security of our homeland is at risk when the employees charged with protecting it have low morale and the Department is unable to attract and retain a talented and professional workforce. The Department should do several things, all of which were recommendations in the Committee report card last year.

First, in attempting to re-make the federal civil service system through MaxHR/HCOP, the Department should retain many of the system’s time-tested features. Especially important are 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.

Second, and of particular importance to employee morale, the Department must ensure that hiring and promotions are not only *conducted* in a fair manner, but are *perceived* as fair.

Third, the Department must immediately institute mechanisms to recognize employee contributions and achievement. Given the Department's congressionally-authorized flexibility in the personnel arena, it has the opportunity to implement a novel approach to recognize and award front line and other non-supervisory employees. One approach would be to place a moratorium on monetary awards or bonuses for all employees in the upper echelons of management and the Senior Executive Service, reserving those awards for front-line and non-supervisory employees to demonstrate that everyone's work is appreciated and valued.

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

PROCUREMENT GRADE: C-

I. STATEMENT OF PROBLEM HISTORICALLY

Since its inception, the Department has had problems with its procurement operations. As part of the merger process, the Department winnowed down the procurement operations of twenty-two distinct entities to eight. Seven of these serve separate units within the Department while one office, Office of Procurement Operations, serves the headquarters and the units that lack independent acquisitions capacity. [184]

There are many pieces to a successful procurement, including but not limited to defining requirements, developing a request for proposals, evaluating offers, selecting an award recipient, and managing the contract. Program management efforts should start at the beginning of the acquisition process in order to have successful procurement. Three key measures for successful procurement are: cost, performance/meeting requirements, and schedule. Unfortunately, the Department's track record in all three is poor.

Indeed, the Department's oversight and management of basic procurement processes has been weak. Historically, both the Government Accountability Office (GAO) and the Department's Inspector General have expressed significant concerns about the manner in which procurement practices are implemented. Below are but a few examples of problems with the Department's procurement that have both hurt the agency and often resulted in a waste of taxpayer dollars:

- **Deepwater -** The Deepwater program was designed to modernize the Coast Guard's fleet. A recent report by the Department's Inspector General determined that "the National Security Cutter, as designed and constructed, would not meet the performance specifications described in the original Deepwater contract." It went on to state the problems were "fundamentally the result of the Coast Guard's failure to exercise technical oversight over the design and construction of its Deepwater assets." In addition, Inspector General Skinner found that "since the Deepwater contract was signed in June 2002, the combined cost of National Security Cutters 1 and 2 has increased from $517 million to approximately $775 million." This estimate *does not* include costs to correct the structural design deficiencies, labor and materials costs related to Hurricane Katrina, or the ultimate cost of a $302 million Request for Equitable Adjustment that the Coast Guard is negotiating.

- **ISIS** - The Integrated Surveillance Intelligence System (ISIS) purpose was supposed to use technology to upgrade cameras and sensor capabilities - as a force multiplier to secure the Nation's borders. ISIS was originally an

[184] 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).

Immigration and Naturalization Service (Border Patrol) program which transitioned to the Department. The GAO, the General Services Administration's Inspector General and the Department of Homeland Security raised serious concerns about the vision and strategy in executing this technology-based border security program and the ability of the Department's procurement operations to implement such a program. In the end, the Department spent approximately $429 million before terminating the flawed program.

- **eMerge2** -The Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency project (eMerge2) began in 2003 with the intent to integrate the financial, budget, asset control and grant activities of the Department's legacy agencies. The Department estimated that it would cost about $100 million and would be completed by 2006. 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. At the time the decision was made to abandon eMerge2, the Department had spent approximately $10 million.

II. STATE OF PROCUREMENT AT DHS

Although significant procurement problems remain, the Department did make some progress in the past year. For example, the Department involved the Inspector General early in the SBI*net* procurement process. By inviting early oversight and suggestions for improvements, the Department demonstrated that it has learned some lessons from its earlier failures. To be clear, the success of SBI*net* is by no means guaranteed, but the process changes in the SBI*net* procurement are noteworthy. The Department should continue to follow this proactive model in the future.

Reviews in the past year by the GAO and the Department's Inspector General have generally not been favorable. Among other things, GAO found that the Coast Guard needs to improve the management and oversight of its Rescue 21 program;[185] that TSA explosive detection systems maintenance contracts needed better oversight;[186] that the Department needs to improve its interagency contracting;[187] and that the Department's weak control over the use of purchase cards left it exposed to waste, fraud, and abuse.[188] For its part, the Inspector General found that the Department needs to improve its management of automated procurement systems,[189] and that, as a

[185] GOVERNMENT ACCOUNTABILITY OFFICE, *United States Coast Guard: Improvements Needed in Management and Oversight of Rescue System Acquisition*, GAO 06-623 (May 2006).

[186] GOVERNMENT ACCOUNTABILITY OFFICE, *Transportation Security Administration: Oversight of Explosive Detection Systems Maintenance Contracts Can Be Strengthened*, GAO 06-795 (July 2006).

[187] GOVERNMENT ACCOUNTABILITY OFFICE, *Interagency Contracting: Improved Guidance, Planning, and Oversight Would Enable the Department of Homeland Security to Address Risks*, GAO 06-996 (Sep. 2006).

[188] GOVERNMENT ACCOUNTABILITY OFFICE, *Purchase Cards: Weaknesses Leave DHS Highly Vulnerable to Fraudulent, Improper, and Abusive Activity*,GAO 06-1117 (Sep. 2006).

[189] DEPARTMENT OF HOMELAND SECURITY INSPECTOR GENERAL, *DHS' Management of Automated Procurement Systems Needs Improvement,* OIG 06-46 (July 2006).

general proposition, it "needs to improve its major acquisitions planning, operational requirements definition, and implementation oversight."[190]

III. PRESIDENT'S BUDGET

The President's fiscal year 2008 budget request includes $4.5 million for the Management Directorate's department-wide training of acquisition staff and $5.1 million to expand the Acquisition Workforce Intern Program. The additional training funds will reportedly allow procurement staff to take approximately three training courses during the year and is a good step towards improving the workforce.

The funds for the Acquisition Workforce Intern Program should assist with the hiring of sixty to seventy interns. The proposed expansion of the internship program is a good sign, and is consistent with recommendations the Committee made in the 109th. That investment should assist the Department in developing a home-grown cadre of contracting professionals. Although promising, this proposal does not address the immediate and pressing needs in the procurement area.

IV. AREAS OF IMPROVEMENT

Significant work remains to transform the Department's procurement operations into one integrated function. An important first step would be to provide the Department's Chief Procurement Officer (CPO) with the authority to set and enforce standards and guidelines for the seven procurement offices still located in component agencies. Currently the CPO does not have direct authority over the purchasing decisions or processes used throughout the Department. Instead, four years after the Department was created, 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 from across the Department. Setting policy by committee is simply not efficient, and can too often result in policies that are better at pleasing everyone than at solving problems.

Additionally, the Department needs to significantly increase its procurement workforce. It simply cannot function without an adequate number of well-trained employees. There are two parts to this crisis – first, the immediate shortages, and second, the need to develop a cadre of procurement professionals. While the increase in the Acquisition Workforce Intern Program is a good step towards addressing the second, long term problem, the Department has yet to identify a plan to address the first, more immediate need. Until the Department can develop and successfully implement that plan, it will be hard-pressed to improve much upon its current state of affairs.

[190] An Overview of Issues and Challenges Facing the Department of Homeland Security: Hearing Before House Homeland Security Committee, 110th Cong. (Feb. 7, 2007) (Testimony of Richard Skinner, Inspector General, Department of Homeland Security).

OFFICE OF CIVIL RIGHTS AND CIVIL LIBERTIES GRADE: C

I. STATEMENT OF PROBLEM HISTORICALLY

Following the September 11 terrorist attacks, Americans witnessed widespread reports of racial profiling, the Presidential authorization of warrantless searches, and the enactment of laws that came under attack by civil rights and civil liberties organizations. The Department was created in the midst of this environment and it was clear that any polices and programs aimed at securing the Nation had to take into consideration the civil rights and liberties of American citizens. The primary purpose of the Civil Rights and Civil Liberties (CRCL) Office is to ensure that the constitutional rights and liberties that define our democratic society are preserved. Like the Department's Chief Privacy Officer, the Civil Rights and Civil Liberties Officer was statutorily created and is unique. The fact that the office was established illustrates Congress' intent to make certain that in our attempt to secure the Nation, civil rights and civil liberties are not violated. Congress mandated that the Civil Rights and Civil Liberties Officer play a vital role in the formation of policies from their inception through their development. The purpose of the CRCL Office is not to simply investigate whether civil rights or civil liberties violations have occurred; rather, it should sit "at the table" during policy formation. The CRCL Office is also unique in that it houses the Department's Equal Employment Opportunity program, thus granting it both external and internal responsibilities.

II. THE CURRENT STATE OF AFFAIRS

The CRCL Office has numerous programs and training opportunities in place that could be beneficial to the Department's components. However, many of the components have been resistant to fully utilizing CRCL's services. For instance, while the office has developed several civil rights and civil liberties trainings, the Department has made many of these voluntary. The CRCL office has, as a result, resorted to using posters, pamphlets, and brochures to spread their message throughout the Department.

Moreover, despite the fact that the Civil Rights and Civil Liberties Officer is appointed by the President and answers only to the Secretary, this office has flown under the radar at the Department and in Congress as well. The current officer, Daniel Sutherland, has testified before Congress once on March 14, 2007, even though he was appointed in 2003 and has served as the Department's only Civil Rights Civil Liberties Officer. The Office has also not filed its annual report to Congress, as required by statute, since 2004. Despite these shortcomings, the CRCL office has made strides in the areas of outreach to Arab American and Muslim American communities, participation in inter-agency working groups and holding frequent and open public dialogues with advocacy organizations to discuss the Department's policies as they relate to civil rights and civil liberties.

III. THE PRESIDENT'S BUDGET REQUEST

The President's fiscal year 2008 budget request for the Office of Civil Rights and Civil Liberties is $13.7 million, which is an increase of $722,000.00 over the enacted fiscal year 2007 amount.

IV. AREAS FOR IMPROVEMENT

The Secretary should direct all Department components to cooperate fully with the CRCL Office. Additionally, the Office of Civil Rights and Civil Liberties must release its annual reports to Congress on a timely basis. Its failure to do so results in a lack of transparency for Congress and the American public. The CRCL Office must also exercise more oversight regarding the Department's internal equal employment policies to achieve more diversity in the Department's workforce.

The CRCL Office is required by statute to coordinate with the Privacy Officer to ensure that "civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner."[191] Although the two offices serve on several working groups together, the level of integration between the two offices is minimal and both offices would benefit from an increased level of interaction.

[191] *See generally* 6 U.S.C. § 345(a)(5)(A).

CHIEF PRIVACY OFFICER GRADE: B-

I. STATEMENT OF PROBLEM HISTORICALLY

The Department's Chief Privacy Officer was established pursuant to Section 222 of the Homeland Security Act of 2002. The stated mission of the Chief Privacy Officer (CPO) is to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while achieving the mission of the Department. The CPO is unique within the structure of the federal government insofar as it is a statutory position that is intended to be involved at all levels of the Department's activities – from policy formation to its implementation. Congress created this position to ensure that the Department protects the privacy of American citizens. However, in a recent study released by the Ponemon Institute entitled *2007 Privacy Trust Study of the United States Government*,[192] out of the seventy-four Federal government agencies presented in the survey, the Department ranked third to last with an alarming privacy trust score of only twenty-two percent. Moreover, when the scores for the last three years were averaged, the Department ranked in last place.[193] The purpose of the study was to ascertain the level of confidence Americans have in Federal government agencies that collect and use the public's personal information. While there have been some strides made by the Chief Privacy Officer, these results show that the general public's confidence and trust in the Department's handling of privacy matters remains abysmally low.

The office itself has been beset with constant turnover. From the period of 2004 through 2006, three different individuals have served as Chief Privacy Officer.[194] As a result, employees working within the Privacy Office and others within the Department that rely on its guidance and expertise have had to constantly adjust to new leadership. This has led to erratic privacy policies and a lack of consistency throughout the entire Department in complying with the Privacy Act of 1974. Also, several high-profile homeland security projects have been terminated or drastically reduced following public uproars related to privacy concerns. Among these are:

- **Automated Targeting System** - The Department's Customs and Border Protection Program (CBP) announced in November 2006 through a Notice published in the Federal Register,[195] that it had been operating a passenger screening program called the Automated Targeting System (ATS), which it touted as the most advanced targeting system in the world. This announcement was met with a public outcry because the program had been operating without first publishing the Privacy Act Notice, as required by law. Pursuant to ATS, the Department maintained an individual's personally identifiable information,

[192] The Ponemen Institute, *2007 Privacy Trust Study of the United States Government,* February 15, 2007.
[193] *Id.* at 8.
[194] Nuala O'Conner became the Department's first Chief Privacy Officer in April 2003 and resigned from that post in September 2005. She was then replaced by Maureen Cooney who remained in the position from 2005 to July 2006. Hugo Tuefull, III was appointed as the current Chief Privacy Officer in July 2006.
[195] Department of Homeland Security, *Notice of Privacy Act system of records*, 71 Fed. Reg. 64543 (Nov. 2, 2006).

which included a numerical calculation of the passenger's risk assessment for a period of up to forty years.

The Privacy Office prepared a Privacy Impact Analysis[196] of the Department which resulted in a finding that the potential number of Department personnel with access to the system created a privacy risk, yet the Privacy Office ultimately concluded that ATS did not raise any serious privacy concerns. Many disagreed with this assessment and expressed their concerns via public comments filed with the Department. Based on the content of the comments received, including those filed by Chairman of the Committee on Homeland Security, Bennie G. Thompson, CBP has not reissued a new Notice and the public still awaits a determination by CBP regarding whether the Notice will be modified. The privacy issues raised by the comments might have been avoided had the Chief Privacy Officer exercised oversight over this program from the start, as envisioned by the statute.

- **Secure Flight -** The Privacy Office conducted a review of the Transportation Security Administration's (TSA) Secure Flight, an airline passenger prescreening program.[197] Although TSA had properly published a Privacy Act Notice, in its report released in December 2006, the Privacy Office found that "the disparity between what TSA proposed to do [in the Notice] and what it actually did in the testing program resulted in significant privacy concerns being raised about the information collected …as well as the Secure Flight Program."[198] Once again, the Chief Privacy Officer missed an opportunity to embed himself at every stage of the development and implementation process, resulting in another public disaster.

- **MATRIX** - The Privacy Office also released a report on the Department's Multi-state Anti-Terrorism Information Exchange Program (MATRIX) in December 2006.[199] The MATRIX project was a collaborative effort involving public, private, and non-profit entities designed to promote information sharing within the state law enforcement community. The Privacy Office found that the MATRIX project "failed to consider and adopt comprehensive privacy protections from the beginning."[200] The report further stated that "[t]he project lacked a privacy policy that clearly articulated the project's purpose, how it would use personal information, the types of information contained, and the security and

[196] DEPARTMENT OF HOMELAND SECURITY, *Privacy Impact Assessment for the Automated Targeting System*, Nov. 22, 2006, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf (last visited Mar. 9, 2007).

[197] *See* DEPARTMENT OF HOMELAND SECURITY, *Secure Flight Report, DHS Privacy Office Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations,* Dec. 2006, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-secure-flight-122006.pdf (last visited Mar. 9, 2007).

[198] *Id.* at 14.

[199] *See* DEPARTMENT OF HOMELAND SECURITY, *MATRIX Report, DHS Privacy Office Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project,* Dec. 2006, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-matrix-122006.pdf (last visited Mar. 9, 2007).

[200] *Id.* at 2.

auditing protections governing the project."[201] In this situation, the Chief Privacy Officer's analysis highlighted the major privacy-related flaws rooted in the program from the start. However, the Department had been involved in the MATRIX program for three years prior to the report being released.

As indicated by the failure of these programs, the Department continues to be challenged by the need to embed privacy measures into a program from its inception. In doing so, the public's confidence in the Department remains low. This resulted in wasted funds, time and effort.

II. THE CURRENT STATE OF AFFAIRS

The Privacy Office operated under the leadership of two separate Chief Privacy Officers in 2006. To the Privacy Office's credit, it produced four reports in 2006 and thirty-nine Privacy Impact Assessments. These reports pointed out both the success and challenges presented in Department programs and policies. Of major concern, however, was the Privacy Office's lack of timeliness in producing its annual report to Congress. The Department is required by law to provide an annual report to Congress, however it did not produce this report in 2004 or 2005. In late 2006, it released a report which covered its activities from July 2004 to July 2006. In neglecting to file this report, it ignored its statutory requirement to advise Congress on the "activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters."

There is also major concern regarding the Privacy Office's involvement at the outset of the policymaking process. As indicated by the privacy-related problems in the programs stated above, every Department component must be made fully aware of the importance of including the Privacy Office in the process from the very beginning. It is also incumbent upon the Privacy Office to insert itself into the process.

Despite these shortcomings, one area of achievement has been the work of the Department's Data Privacy and Integrity Advisory Committee created by former Chief Privacy Officer Nuala O'Conner. On March 7, 2006, the Committee released its Framework for Privacy Analysis of Programs, Technologies and Applications. The document contained a useful framework, which if applied to future Department programs, will go a long way in alleviating many privacy concerns.

III. THE PRESIDENT'S BUDGET REQUEST

The President's fiscal year 2008 budget request for the Office of Privacy is $5.1 million, which is an increase of $676,000.00 over the enacted fiscal year 2007 amount.

IV. AREAS FOR IMPROVEMENT

Privacy Office

[201] *Id.*

To be fully effective, the Chief Privacy Officer must have enhanced authorities to conduct investigations into privacy complaints. In January 2007, the House of Representatives passed H.R. 1, which included the Privacy Officer With Enhanced Rights (POWER) Act. The passage of these provisions is a step in the right direction as it relates to providing the Privacy Office with the tools needed to fulfill its obligations.

Although the Privacy Office released numerous reports related to Department programs, its commitment to release its annual report to Congress in a timely fashion is vital. In the future, this report should be released each year, as required by law.

- END -