September 2008

Report Prepared by the Majority Staffs of the Committee on Homeland Security and Committee on Foreign Affairs

Wasted Lessons of 9/11:

How the Bush Administration Has Ignored the Law and Squandered Its Opportunities to Make our Country Safer

EXECUTIVE SUMMARY

On September 11, 2001, this country suffered the most devastating terrorist attacks ever experienced on our soil. The series of coordinated attacks, perpetrated by 19 hijackers affiliated with al Qaida, killed 3,000 people, inflicted hundreds of millions of dollars of economic damage, brought commercial aviation to a standstill, and opened the eyes of the American people to the threat of terrorism as never before.

To establish how the perpetrators were able to execute their deadly plot, Congress chartered the independent, bipartisan National Commission on Terrorist Attacks Upon the United States (9/11 Commission). In addition to providing a full account of the circumstances surrounding the attacks, Congress directed the 9/11 Commission to develop recommendations for corrective measures that could be taken to prevent future acts of terrorism.[1] On July 22, 2004, the 9/11 Commission issued its final report, which included 41 wide-ranging recommendations to help prevent future terrorist attacks. Many of these proposals were put in place in 2004 with the passage of the Intelligence Reform and Terrorism Prevention Act[2], which brought about the most significant reorganization of the intelligence community since 1947. Among the key provisions of that law was the establishment of a Director of National Intelligence to oversee the intelligence community and the creation of a National Counterterrorism Center to analyze domestic and international threats, share that information, and integrate activities to ensure unity of effort against terrorism.

Yet, a year after it was issued, the lead authors of the 9/11 Commission Report, Governor Thomas H. Kean and Representative Lee H. Hamilton, asked "[a]s a result of these and other reforms, are we safe? We are safer – no terrorist attacks have occurred inside the United States since 9/11 – but we are not as safe as we need to be. . . . [T]here is so much more to be done. . . . Many obvious steps that the American people assume have been completed, have not been. . . . Some of these failures are shocking."[3] The 9/11 Commission concluded that "the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management."[4]

Determined to fill the gaps left by the Bush Administration and the Republican-controlled Congress, and to provide the American people the security they deserve, the House of Representatives under the new Democratic leadership passed H.R. 1, the "Implementing the 9/11 Commission Recommendations Act of 2007" within the first 100 hours of the 110th Congress. This comprehensive homeland security legislation included provisions to strengthen the nation's security against terrorism by requiring screening of all cargo placed on passenger aircraft; securing mass transit, rail and bus systems; assuring the scanning of all U.S.-bound maritime cargo; distributing homeland security grants based on risk; creating a dedicated grant program to improve interoperable radio communications; creating a coordinator for U.S. non-proliferation programs and improving international cooperation for interdiction of weapons of mass destruction; developing better mechanisms for modernizing education in Muslim communities and Muslim-majority countries, and creating a new forum for reform-minded members of those countries; formulating coherent strategies for key countries; establishing a common

coalition approach on the treatment of detainees; and putting resources into making democratic reform an international effort, rather than a unilaterally U.S. one.

When President George W. Bush signed H.R. 1 into law on August 3, 2007 without any limiting statement, it seemed that the unfulfilled security recommendations of the 9/11 Commission would finally be implemented. To ensure that they were, over the past year the Majority staffs of the Committees on Homeland Security and Foreign Affairs have conducted extensive oversight to answer the question, ***How is the Bush Administration doing on fulfilling the requirements of the "Implementing the 9/11 Commission Recommendations Act of 2007" (P.L. 110-53)?*** The Majority staffs of the two Committees prepared this report to summarize their findings. While the Majority staffs of the Committees found that the Bush Administration has taken some steps to carry out the provisions of the Act, this report focuses on the Administration's performance with respect to key statutory requirements in the following areas: (1) aviation security; (2) rail and public transportation security; (3) port security; (4) border security; (5) information sharing; (6) privacy and civil liberties; (7) emergency response; (8) biosurveillance; (9) private sector preparedness; and (10) national security. In each of the 25 individual assessments in this report, a status update is provided on the Bush Administration's performance on these key provisions. The table below sets forth the status of the key provisions identified in the report and help explain why the report is entitled "WASTED LESSONS OF 9/11: HOW THE BUSH ADMINISTRATION HAS IGNORED THE LAW AND SQUANDERED ITS OPPORTUNITIES TO MAKE OUR COUNTRY SAFER."

PROVISION OF P.L. 110-53	STATUS UPDATE
Aviation Security: Advanced Passenger Prescreening System (Sec. 1605)	Plan transmitted but little progress on the program
Aviation Security: Screening of Air Cargo Aboard Passenger Aircraft (Sec. 1602)	Missed opportunities
Aviation Security: General Aviation Security (Sec. 1617)	Failure to take action
Rail & Public Transportation Security: National Strategy for Public Transportation Security (Sec. 1404) and Security Assessments and Plans (Sec. 1405)	Incomplete, putting public transportation at risk
Rail & Public Transportation Security: Public Transportation Security Training Program (Sec. 1408), Railroad Security Training Program (Sec. 1517), and Over-the-Road Bus Security Training Program. (Sec. 1534)	Missed opportunities
Rail & Public Transportation Security: Railroad Transportation Security Risk Assessment and National Strategy (Sec. 1511)	Incomplete; limited progress
Port Security: Maritime Cargo Security (Sec. 1701)	No progress
Border Security: Modernizing the Visa Waiver Program (Sec. 711)	Initial steps taken but significant implementation challenges remain

Information Sharing: Department of Homeland Security State, Local, and Regional Fusion Center Program (Sec. 511)	Failure to take action
Information Sharing: Homeland Security Grants For Intelligence Analysts (Sec. 101)	Acted in a manner inconsistent with the intent of the provision
Privacy and Civil Liberties: Federal Agency Data Mining Reporting Act of 2007 (Sec. 804)	Some progress but required reports have not been submitted
Emergency Response: Interoperable Emergency Communications Grant Program (Sec. 301)	Delivery of key plan late; risks delays in grants
Emergency Response: Credentialing and Typing (Sec. 408)	No progress
Biosurveillance: National Biosurveillance Integration Center (Sec. 1101)	Initial steps taken but little progress
Private Sector Preparedness: Private Sector Preparedness (Sec. 901).	Limited progress
Private Sector Preparedness: National Asset Database (Sec. 1001)	Some progress but little use of the National Asset Database
National Security: Interdicting Weapons of Mass Destruction (Sec. 1821)	Failure to take action
National Security: Coordinating U.S. Nonproliferation Programs (Sec. 1841)	Failure to take action
National Security: International Muslim Youth Opportunity Fund (Sec. 2012)	Failure to take action
National Security: Establishment of a Middle East Foundation (Sec. 2021)	Missed opportunities
National Security: United States Policy Towards Detainees (Sec. 2033)	Progress is slow and uncertain
National Security: Strategy For the United States Relationship with Pakistan (Sec. 2042)	Lack of comprehensive strategy yields disastrous results
National Security: Strategy for the United States Relationship with Afghanistan (Sec. 2041)	Still diverted from the crisis in Afghanistan
National Security: United States Policy Towards Saudi Arabia (Sec. 2043)	Progress is slow and uncertain
National Security: Advancing Democracy Around The World (Title XXI)	Key elements unmet

As this report demonstrates, the Bush Administration has not delivered on myriad critical homeland and national security mandates set forth in the "Implementing the 9/11 Commission Recommendations Act of 2007" (P.L. 110-53). Democratic Members of the Committees are alarmed that the Bush Administration has not made more progress on implementing these key provisions. Without them, the Administration has failed to provide the American people the security they expect and deserve. This report is intended as a wake-up call to the Bush Administration. In the short time left in office, the President should redouble his efforts to make America more secure by acting expeditiously to make progress as identified in this report. Fulfilling the unfinished

business of the 9/11 Commission will most certainly be a major focus of President Bush's successor, as many of the statutory requirements are to be met in stages, with the final implementation deadlines occurring during the Administration of 44th President. However, for the next President to succeed in implementing this critical law, this President needs to deliver on the commitment he made on August 3, 2007 and fulfill the statutory requirements of this major homeland security law.

TABLE OF CONTENTS

SEC. 1605: ADVANCED PASSENGER SCREENING SYSTEM

Statutory Requirement

Section 1605 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) requires the Department of Homeland Security (DHS) to develop a strategic plan to test and implement advanced passenger prescreening system for all flights into or out of the United States. The strategic plan for DHS to shift the responsibility for checking passengers against the terrorist watch list from air carriers to DHS was due December 3, 2007.

Status Update: PLAN TRANSMITTED BUT LITTLE PROGRESS ON THE PROGRAM

While the strategic plan was submitted to Congress in December 2007, Secure Flight, the program, announced in August of 2004 as the platform for DHS to conduct watch list checks, is years behind schedule. DHS initially projected the Secure Flight system would be tested and verified in an operational environment by July 15, 2005[9] but today, because of repeated delays, the agency expect to fully assume the watch list matching function from air carriers in fiscal year 2010.[10] The December 2007 strategic plan, though it did provide some information on scheduling and testing, lacked essential risk management information and failed to provide the specificity that Congress needs to closely monitor whether progress is being achieved.

Interestingly, on April 15, 2008, a Committee on Homeland Security subcommittee held a hearing where Members of the subcommittee were told that – notwithstanding the lack of deliverables on this $200 million program – the Transportation Security Administration (TSA) was optimistic about approaching the final planning stages for implementation of Secure Flight by the start of 2009.[11] Given that TSA has not begun testing Secure Flight in an operational environment, it is difficult to believe that Secure Flight will be in operation in a matter of months.

National Significance

One of the most critical recommendations in aviation security made by the 9/11 Commission addressed the operational management of intelligence information.[12] Since the inception of DHS, Congress has repeatedly stated that operational management of intelligence information be strengthened at DHS. Such programs include TSA's Secure Flight Initiative, which would collect passenger information and match the data against watch lists to better identify suspected terrorists attempting to board commercial aircraft, while facilitating legitimate passenger air travel and protecting the privacy rights of individuals.

The 9/11 Commission recommended that the passenger watchlist screening function "be performed by the TSA, and it should utilize the larger set of watchlists

maintained by the federal government. Air carriers should be required to supply the information needed to test and implement this new system."[13] Secure Flight has been touted as a program resolve problems with improper passenger identification against the terrorist watchlist, and ensure that the Federal government – and not the private sector – takes the lead in administering this critical screening activity. TSA has stated that Secure Flight will remove inconsistencies caused by the various methods used by air carriers to match passenger information against the watchlist, reduce and possibly eliminate misidentifications, and alleviate the frustrations of passengers without compromising security. However, the Government Accountability Office (GAO) testified before the Committee on Homeland Security that TSA has not fully addressed program management issues, nor has TSA implemented a risk management plan for Secure Flight.[14] GAO also commented that TSA lacks a comprehensive testing strategy and recommended that TSA ensure that information security requirements be fully implemented in the system. These recommendations addressed the need to incorporate end-to-end testing requirements in the program and to incorporate a test and evaluation master plan for Secure Flight. Additionally, GAO recommended that TSA incorporate best practices into the development of Secure Flight program cost and schedule estimates. These programmatic recommendations would ensure that DHS timeline is feasible.

Section 1605 was included in P.L. 110-53 in an effort to bring about progress on improving passenger prescreening. While the report required under Section 1605 was transmitted, actual progress on Secure Flight implementation remains elusive.

SEC. 1602: SCREENING OF AIR CARGO ABOARD PASSENGER AIRCRAFT

Statutory Requirement

Section 1602 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) requires the Department of Homeland Security (DHS) to screen 100 percent of cargo transported on passenger planes in the United States by foreign and domestic air carriers within three years. Under the law, the Transportation Security Administration (TSA) must screen at least 50 percent of all cargo transported by passenger planes in the United States by February 3, 2009 and all cargo aboard passenger aircraft by August 3, 2010. In recognition of the tight timeline, the law grants TSA the authority to issue an interim final rule on air cargo and bypass the standard lengthy rulemaking process.

Status Update: MISSED OPPORTUNITIES

Though the first deadline for the 100% air cargo mandate is not until February 3, 2009, recent testimony before the Committee on Homeland Security makes it clear that there has been little progress on this critical homeland security mandate.[15] For the better part of a year, TSA has been developing the Certified Cargo Screening Program (CCSP), a new program to screen air cargo earlier in the supply chain-- well before the cargo is loaded on a plane for shipment. However, TSA only commenced a pilot program to test CCSP this past August, a full year after enactment of P.L. 110-53. At the Committee on

Homeland Security hearing, stakeholders representing airline pilots and flight attendants testified that they have not been consulted by TSA since completion of the conceptual plan for CCSP in May of 2008. Furthermore, certain industry stakeholders, such as air carriers and air freight forwarders, claim that, beyond a short list of technology items that have been approved for screening in the program, there has been no guidance or best practices issued on how to screen cargo within the CCSP.

General provisions requiring the screening of all mail and cargo carried aboard passenger aircraft have been in law since the passage of the Aviation Transportation Security Act of 2002 (P.L. 107-71) and Congress has appropriated over $500 million to DHS to specifically address air cargo security during fiscal years 2003 through 2008[16] Given that TSA has been working on this program long before the enactment of P.L. 110-53, failure to meet the first deadline of 50% screening of air cargo by February 3, 2009 would be unacceptable.

National Significance

On December 28, 1988, Pan Am Flight 103 –traveling from London Heathrow International Airport to New York John F. Kennedy International Airport—exploded over Lockerbie, Scotland. Subsequent investigations concluded that the blast was triggered by explosives hidden in checked luggage. The attack on Pan Am Flight 103 resulted in the deaths of 259 passengers and crew as well as 11 residents of Lockerbie.

There is evidence of interest within al Qaida to disrupt aviation through a cargo-based attack. In fact, according to the 9/11 Commission, in the fall of 2000, Zacarias Moussaoui, one of the chief architects of the September 11th attacks, was sent to Malaysia for flight training but when he did not find a school he liked he "worked instead on other terrorist schemes, such as buying four tons of ammonium nitrate for bombs to be planted on cargo planes flying to the United States."[17] The 9/11 Commission concluded that "major vulnerabilities still exist in cargo"[18] and recommended that "TSA also needs to intensify its efforts to identify, track, and appropriately screen potentially dangerous cargo in both the aviation and maritime sectors."[19]

A report released by the Center for American Progress released in May 2007 highlighted the efforts and plotting by terrorists to plant explosives in air cargo shipped to the United States. The report specifically highlights that:

> "At a recent hearing at Guantanamo, Khalid Sheikh Muhammad took responsibility for the so called Bojinka plot, a plan to use terrorists posing as passengers to blow up a dozen 747s simultaneously in 1995. Less well known is what the 9/11 mastermind's nephew, Ramzi Yousef (and the operational director of Bojinka), did when this first plot was foiled. He tried twice to place bombs in cargo shipments on airliners bound for the United States before he was arrested."[20]

SEC. 1617: GENERAL AVIATION SECURITY

Statutory Requirement

Section 1617 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs the Transportation Security Administration (TSA) to develop a standardized threat and vulnerability assessment program for general aviation (GA) airports. A GA airport is defined as any airport that is not a commercial airport. Section 1617 also requires TSA to conduct such assessments on a "risk-managed basis" at GA airports. Six months following the implementation of such program, TSA is required to initiate and complete a study of the feasibility of a program to provide grants to operators of GA airports to upgrade GA airport security projects. The first step in the GA security provision—the development and implementation of a standardized threat and vulnerability assessment program for GA—was due August 3, 2008.

Status Update: FAILURE TO TAKE ACTION

TSA missed the August 3, 2008 deadline. TSA admitted its failure to meet the deadline in a letter to the Committee on Homeland Security.[21] According to TSA, it is working with industry stakeholders, such as the National Association of State Aviation Officials and National Air Transportation Association, to develop a survey that will be sent to the GA membership later this year. TSA stated that the survey is a precursor to the overdue standardized threat and vulnerability assessment program.

National Significance

The 9/11 Commission found that "major vulnerabilities" still exist in general aviation.[22] The vulnerabilities present in the GA sector should have hit close to home when, in the fall of 1994, a small aircraft flown by an individual with a history of mental illness targeted the White House and wrecked the stolen single-engine aircraft on the South Lawn.[23] Then, four months after the attacks of September 11, 2001, a student pilot crashed a small single-engine aircraft into a skyscraper in downtown Tampa, Florida.[24] Although the student pilot acted alone and had no known connections with terrorist groups, he had previously expressed support for the 9/11 terrorist attacks on Americans. Concerns were also raised in October of 2005, when a 22-year old male stole a Cessna Citation VII business jet from the St. Augustine, Florida airport.[25] The aircraft was used for "late-night joyride" and landed safely at Briscoe Field near Atlanta Georgia. These incidents highlight the evolving vulnerabilities that TSA must address to assure that GA airports and aircraft are properly secured.

Congress acknowledged the unique security challenges posed by GA assets and infrastructure, and instituted the recommendation of the 9/11 Commission in Section 1617 of P.L. 110-53. In this provision, the standardized threat and vulnerability assessment program was intended to require TSA to adopt a risk-based approach to assess the threats and vulnerabilities of GA airports. Key elements that could be tailored to a facility, based on risk, include surveillance and monitoring of airports and aircraft; vetting of aircraft pilots and airport workers, and proper access controls to facilities and aircraft. As a consequence, this program would provide much needed security grants to the operators of GA airports, and other infrastructure, to upgrade their security projects.

SEC. 1404: NATIONAL STRATEGY FOR PUBLIC TRANSPORTATION SECURITY AND SEC. 1405: SECURITY ASSESSMENTS AND PLANS

Statutory Requirement

Section 1404 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs the Department of Homeland Security (DHS) to develop and implement a modal plan for public transportation-- the National Strategy for Public Transportation Security.[26] It also requires DHS to establish guidelines that minimize security threats to public transportation systems and maximize the abilities of public transportation systems to mitigate damages resulting from a terrorist attack or other major incident. Section 1404 requires DHS to consult with relevant stakeholders and include in the National Strategy a description of the prioritized goals, objectives, and schedules as well as the roles, responsibilities, and authorities of Federal, State, and local agencies, tribal governments, and appropriate stakeholders. Additionally, the National Strategy must include the identification of gaps and unnecessary overlaps in the roles, responsibilities, and authorities of Federal agencies; a plan to address such gaps and overlaps; and a process for coordinating existing or future security strategies and plans. Under Section 1404, the deadline for developing and implementing the National Strategy for Public Transportation Security was May 3, 2008.

Section 1405 of P.L. 110-53 requires the Federal Transit Administrator to submit all public transportation security assessments and other relevant information to DHS. It also requires DHS to review these assessments and conduct additional assessments, as necessary, to ensure that all high-risk public transportation agencies are fully assessed. The provision also directs DHS to conduct security assessments, based on a representative sample, to determine the specific needs of local bus-only public transportation systems and systems that receive formula grants for non-urbanized areas. It also requires DHS to make these representative assessments available for use by similarly situated systems and requires operators of high-risk public transportation systems to develop a comprehensive security plan. In addition, Section 1405 establishes plan and review requirements and generally prohibits DHS from requiring an operator to develop a plan if it does not receive Federal homeland security funding.

Status Update: INCOMPLETE, PUTTING PUBLIC TRANSPORTATION AT RISK

DHS missed the May 3, 2008 deadline but, according to the Transportation Security Administration (TSA), the first draft of the National Strategy will be available for comment this fall.[27] TSA has stated that, because the National Strategy required under Section 1404 covers much of the same issues as the mass transit annex of the

Transportation Sector-Specific Plan under the National Infrastructure Protection Plan,[28] progress on this requirement will be expeditious.

Section 1405 of the provision required the assessments and plans for public transportation to be submitted 30 days after the enactment of P.L. 110-53. This requirement has not been met.

National Significance

Over the past decade, mass transit systems all over the world have proven to be popular targets for acts of terrorism, including those perpetrated by al Qaida. Since 2001, multiple attacks have resulted in the deaths and injuries of hundreds of innocent people. Forty people were killed in a bomb attack by Chechyan terrorists on the Moscow subway in 2004. That same year, ten explosions hit four Madrid commuter trains at the height of rush hour. In July 2005, four explosions ripped through the London Underground, claiming the lives of 56 people and seriously injuring hundreds more. A year later, a series of seven bomb blasts hit a suburban railway in Mumbai, India, resulting in hundreds of casualties. Most recently, in July 2008, two buses were bombed in Kunming, the capital of China's Yunnan province, resulting in several deaths and multiple injuries.

The 9/11 Commission recognized the terrorist threat to rail and mass transit, saying that "[w]hile commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime or surface transportation. Initiatives to secure shipping containers have just begun. Surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible and extensive."[29]

The need to bring rail and mass transit security in line with modern security threats is clear. A crucial first step toward accomplishing this important goal is the development and implementation of a National Strategy for Public Transportation Security. Conducting security assessments and developing security plans for public transportation systems are also critical steps toward accomplishing this important mission. It is vital that DHS fulfill its responsibilities under P.L. 110-53 in order to enhance the abilities of public transportation systems to anticipate and prepare for acts of terrorism and other emergency situations.

SEC. 1408: PUBLIC TRANSPORTATION SECURITY TRAINING PROGRAM; SEC. 1517: RAILROAD SECURITY TRAINING PROGRAM; AND SEC. 1534: OVER-THE-ROAD BUS SECURITY TRAINING PROGRAM

STATUTORY REQUIREMENT

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) included provisions to significantly enhance the detection, preparedness and response capabilities of frontline workers on public transportation, rail, and over-the-road bus systems. Three Sections of P.L. 110-53 mandate that the Department of Homeland Security (DHS) issue regulations for security training programs for employees of the three modes. Under Section 1408 of P.L. 110-53, the deadline for issuance of interim final regulations "for a public transportation security training program to prepare public transportation employees, including frontline employees, for potential security threats and conditions" was Nov. 3, 2007 and the deadline for final regulations was Aug. 3, 2008. Similar requirements were outlined in Sections 1517 and 1534 for regulations to ensure training for railroad and over-the-road bus frontline employees that address potential security threats and conditions. These regulations were due by February 4, 2008.

Status Update: MISSED OPPORTUNITIES

To date, DHS has not issued notice of proposed rulemakings, interim final regulations, or final regulations for training of any of the transportation employees, as required under the law.

National Significance

Everyday, more than 11.3 million passengers in 35 metropolitan areas and 22 States use some form of commuter rail or mass transit system and these numbers continue to rise. In fact, ridership of rail to public transportation has increased over the past months as the public copes with increases in gas prices.[3031] These systems typically provide regional service between a central city and adjacent suburbs. They are the life-line for daily commuters in many communities and are essential to the health of the Nation's economy. The task of securing these modes and training the frontline employees grows in importance as the traveling public increases its dependence on these systems in a time of rising energy costs. The Bush Administration has failed to establish baseline training for frontline transportation workers, a prerequisite to enhancing the security of passengers that utilize public transportation.

The men and women who operate and work on our Nation's buses, public transit, and rail systems are best situated to detect an attack on these critical systems and are the likely first responders if an attack occurs. According to a study by the Volpe Center, "probably the most significant factor in determining whether a transportation employee

makes a helpful or harmful decision during an emergency is training. Trained and alert transportation professionals can make the difference between success and disaster."[32] Likewise, Rafi Ron, former Director of Security at Tel-Aviv's Ben-Gurion International Airport, testified before Congress that "training provides the skills and confidence…to employees who are present at every point in the system. No one is in a better position to recognize irregularities on the ground than the people who regularly work there."[33]

James Little, the International President of the Transport Workers Union of America, AFL-CIO, who represents many bus, subway, and rail workers, testified before Congress in February 2007 that:

> "Reports of threats, suspicious activities and potential problems are usually communicated to frontline workers by passengers. And oftentimes frontline workers themselves discover the suspicious activity or threat. Thus, it is essential that these "eyes on the scene" receive full and proper training in how to handle these threats and activities with a specific protocol of action to follow."[34]

Yet, prior to enactment of P.L. 110-53, the Transportation Security Administration (TSA) did not require mass transit, rail, or bus systems to provide training for their employees and, as a result, workers were not adequately being trained to deal with security matters. While the National Transit Institute and Federal Transit Administration's training has reached some of the transit employee workforce, the fact remains that only a fraction of employees have been trained.

Recognizing the unique challenges of securing public transportation systems and that "[n]o single security measure is foolproof," the 9/11 Commission stated that "the TSA must have multiple layers of security in place to defeat the more plausible and dangerous forms of attack against public transportation."[35] The security training required under Sections 1408, 1517, and 1534 are essential to establishing a layered system of security. Asking the public and the workforce to remain vigilant is not enough. TSA and DHS must fulfill the mandate and issue training regulations for frontline transportation workers.

SEC. 1511: RAILROAD TRANSPORTATION SECURITY RISK ASSESSMENT AND NATIONAL STRATEGY

Statutory Requirement

Section 1511 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs the Department of Homeland Security (DHS) to establish a taskforce to complete a nationwide risk assessment of railroad carriers that includes an assessment of public and private operational recovery plans, accounts for actions taken by public and private entities to address identified rail security issues, and identifies the level of integration of such actions.

This provision also requires DHS to develop and implement the National Strategy for Railroad Transportation Security. The National Strategy must include (1) prioritized goals, actions, and schedules for improving the security of rail infrastructure and facilities, information systems, and other areas posing significant rail-related risks to public safety and interstate commerce; (2) deployment of equipment and personnel to detect security threats; (3) training railroad employees in terrorism prevention, preparedness, passenger evacuation, and response activities; (4) identification of the immediate and long-term costs of measures that may be required to address those risks; and (5) identification of public and private sector sources to fund such measures. In addition, Section 1511 requires the National Strategy to include a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, government-sponsored entities, tribal governments, and appropriate stakeholders. DHS is also required to report to Congress on the assessment and the Strategy, as well as provide an estimate of the cost to implement the Strategy on an annual basis.

Under the law, the nationwide risk assessment was to be completed by February 3, 2008 and the deadline for development and implementation of the National Strategy for Railroad Transportation Security was May 3, 2008.

Status Update: INCOMPLETE; LIMITED PROGRESS

The nationwide risk assessment was not completed by February 3, 2008 and the National Strategy for Railroad Transportation Security was not developed and implemented by May 3, 2008. Instead, on May 9, 2008, the Transportation Security Administration wrote to the Committee on Homeland Security that "the Department has already completed much of the groundwork that will serve as a basis for the national strategy"[36] and that it intends to build upon the existing Freight Rail Modal Plan – which is part of the Transportation Sector-Specific Plan under the National Infrastructure Protection Plan[37] – to meet the requirements for the National Strategy.

National Significance

Freight rail is a vital cog in the infrastructure of our economy. For instance, rail is the preferred mode of transportation for 40 percent of all intercity freight and 67 percent of the coal used by electric utilities to produce power. Railroads also provide critical support to the Department of Defense (DOD) by making more than 30,000 miles of rail line available for the movement of DOD shipments. At the same time, rail transportation has several unique features making it inherently vulnerable to attack. Both freight and passenger rail networks traverse dense, urban landscapes that may offer multiple attack points and easy escape as well as vast rural stretches that are difficult to patrol and secure.

Ensuring that rail passenger facilities are secure is particularly challenging given that their open architecture and the also rapid and easy movement of patrons in and out of facilities and on and off trains. The 2004 terrorist bombings in Madrid, thought to be the work of al Qaida sympathizers, ranks among the most sophisticated rail attacks with its near simultaneous detonation of 10 charges on four trains. In terms of overall casualties, however, it ranks second to an August 2001 attack by Angolan separatist rebels who used

a combination of remote-detonated explosives and directed gunfire to kill 252 rail passengers.

The 9/11 Commission acknowledged that "surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible and extensive" but, nonetheless, "[d]espite congressional deadlines, the TSA has developed neither an integrated strategic plan for the transportation sector nor specific plans for the various modes-air, sea, and ground."[38] The railroad industry cannot continue to operate without a nationwide security strategy, safeguarding rail infrastructure, passengers and commercial cargo from the threats of terrorism. The implementation of a strategy by DHS would vastly improve the prioritization of threats, the preservation of vital assets, and create an efficient method of the allocation of resources. Moreover, without a national strategy, frontline employees of railroad carriers will be ill-equipped and untrained in terrorism prevention, preparedness, passenger evacuation, and response activities. The security of the railroad industry and its passengers ought to be a priority for the Bush Administration.

SEC. 1701: MARITIME CARGO SECURITY

Statutory Requirement

Section 1701 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) mandates that, by July 1, 2012, no maritime container bound for the United States enter a U.S. port unless it was scanned by nonintrusive imaging equipment and radiation detection equipment before it was loaded. The provision's incremental five year approach enables the Department of Homeland Security (DHS) to build upon the lessons learned from the Secure Freight Initiative pilot.[39]

Status Update: NO PROGRESS

Over the past year, DHS has not acted in a manner that is likely to result in the fulfillment the mandate established in Section 1701 – instead, it has actively campaigned against them. Three months after the enactment of P.L. 110-53, DHS Secretary Michael Chertoff told other maritime representatives that the 100 % mandate "would be the end of our ports."[40] In June of this year, DHS signaled its intended non-compliance with the mandate wit the announcement that it would focus its resources on "high risk trade corridors" instead of dedicating resources to protect all maritime cargo containers.[41] Last week, Secretary Chertoff compared to mandate to "old Soviet style heavy regulation" and stated that "it is simply impossible for the federal government . . . to take on the responsibility."[42]

National Significance

Today, 95 percent of all imports are transported in shipping containers that move through international waters but less than five percent of these containers are scanned to determine whether a nuclear device, a so-called "dirty bomb," or another terrorist threat is present. This lack of scanning creates an opportunity for terrorists to exploit. For instance, a nuclear explosion at the Port of Long Beach could potentially kill sixty thousand people instantly and expose one hundred and fifty thousand more to hazardous levels of radioactive water and sediment.[43] The early cost of this potential tragedy could exceed $1 trillion and would devastate the United States supply chain as the ports of Long Beach and Los Angeles handle thirty percent of United States shipping imports.[44]

Terrorists have repeatedly demonstrated that airplanes, trains, and subways are not the only targets. The 9/11 Commission revealed that al Qaida operatives "were involved during 1998 and 1999 in preparing to attack a ship off the coast of Yemen with a boatload of explosives. They had originally targeted a commercial vessel, specifically an oil tanker, but [Osama] Bin Ladin urged them to look for a U.S. warship instead. In January 2000, their team had attempted to attack a warship in the port of Aden, but the attempt failed when the suicide boat sank. More than nine months later, on October 12, 2000, [the] operatives in a small boat laden with explosives attacked a U.S. Navy

destroyer, the USS Cole. The blast ripped a hole in the side of the USS Cole, killing 17 members of the ship's crew and wounding at least 40."[45] A few years later, on February 27, 2004, a bomb exploded on the Superferry 14 while it was transiting off the Philippine coast. One hundred and sixteen innocents died that day.

Terrorists target vulnerabilities. P.L. 110-53 recognizes this reality and requires DHS to build on the Secure Freight Initiative pilot and work towards assuring that within five years all cargo that arrives at United States ports is scanned. It is vital to our Nation's security that all maritime containers arriving at United States ports are scanned. Limiting scanning to so-called "high risk trade corridors" puts ports outside of this designation at risk. Logically, terrorists will focus their attention on corridors that are not scrutinized.

It is worth noting that Congress has repeatedly requested a definition for "high risk trade corridor" but DHS has failed to provide an answer.[46] Conceivably, the term could mean a port, a country, or even a region. This lack of clarity creates confusion for our trading partners as to whether the 100 percent scanning mandate will be fulfilled. Moreover, for those ports that find themselves in a high risk trade corridor, the significance of that designation in the eyes of shippers is unknown. Shippers may choose to avoid ports in high risk trade corridors if they presume that the scanning will cause delays in the movement of their cargo – therein, significantly and negatively impacting the global supply chain. Requiring all United States-bound maritime cargo to undergo the same scrutiny—as set forth in P.L. 110-53— will create a baseline of security thereby closing existing gaps and improving security for everyone.

SEC. 711: MODERNIZING THE VISA WAIVER PROGRAM

Statutory Requirement

Section 711 of the Implementing the Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) requires the Department of Homeland Security (DHS), in conjunction with the State Department, to implement several critical security enhancements to the Visa Waiver Program (VWP)[47], while providing for the program's limited expansion.

Specifically, this provision requires the development and implementation of an electronic system for travel authorization (ESTA) under which a traveler from a VWP country would provide biographical information electronically, in advance of travel, necessary to determine whether the individual is eligible to travel to the United States.

Section 711 also requires DHS to establish, within one year of the date of enactment of P.L. 110-53, an exit system that records the departure of each VWP traveler who leaves the United States by air. The system must check the traveler's biometric information against relevant watchlists and immigration databases and match the traveler's biometric information against passenger manifest data to ensure that the traveler has departed the United States.

In addition, this provision requires all VWP countries to enter into agreements with the United States to facilitate repatriation of its citizens, report information on theft or loss of passports, and share information about whether a national of that country traveling to the United States represents a threat to our nation's security.

Once ESTA is fully operational and an air exit system is in place that can verify the departure of not less than 97 percent of foreign nationals leaving the United States by air, Section 711 requires DHS to certify to Congress that those mandates have been fulfilled. After such certification is made and the required security agreements are in place, Section 711 permits DHS, in consultation with the State Department, to adjust the nonimmigrant visa refusal rate requirement of the program from three percent to up ten percent.[48] Furthermore, DHS and the State Department would be permitted to establish an acceptable visa overstay rate, in lieu of the three percent nonimmigrant visa refusal rate, for admitting countries into the program.

While the air exit system need not be biometric initially, if a biometric system is not implemented by June 30, 2009, DHS waiver authority that was based upon the 97 percent accuracy certification will be suspended until a biometric exit system is fully operational.

Status Update: INITIAL STEPS TAKEN BUT SIGNIFICANT IMPLEMENTATION CHALLENGES REMAIN

Election System for Travel Authorization (ESTA)

On June 3, 2008, DHS released an Interim Final Rule (IFR) for ESTA.[49] ESTA is an Internet-based system intended to make the VWP more secure by enabling DHS to determine, prior to an individual boarding a flight to the United States, whether the individual is eligible to travel under the VWP or whether he or she poses any security, law enforcement, or immigration control-related risks. ESTA is intended to provide an almost immediate determination of eligibility for travel under the VWP.

Under the ESTA program, a VWP traveler logs on to the program's website and provides the same biographical and eligibility information as is currently conveyed on the paper I-94W form when a traveler arrives at a United States land, air, or maritime border. Possible responses include: Authorization Approved, Travel Not Authorized, or Authorization Pending. An approved ESTA travel authorization is: (1) valid for up to two years or until the traveler's passport expires, whichever comes first; (2) valid for multiple entries into the United States; and (3) not a guarantee of admissibility to the United States at a port of entry. ESTA approval only authorizes a VWP traveler to board a flight to the United States; Customs and Border Protection (CBP) officers make admissibility determinations at the ports of entry. The ESTA web-based system became available for voluntary applications on August 1, 2008, and DHS currently expects ESTA to be implemented as a mandatory program on January 12, 2009.[50]

There are several concerns with the manner in which DHS is implementing the ESTA program. In the interest of time, DHS chose to issue an IFR, thereby bypassing the standard notice and comment rulemaking procedure, where feedback is officially received from stakeholders such as VWP countries, airlines, travel agents, and the traveling public. Though DHS is not required to do outreach to these key stakeholders in the IFR process, it is critical that such feedback is solicited, received, and integrated into the program. Without the appropriate outreach and education, achieving the desired level of compliance will be difficult.

Second, to date, DHS has only put forth plans to make ESTA available via the Internet. That means that travelers who lack Internet access will have to rely on a travel agent, friend, or family member to fill out their ESTA application or find another means of accessing the Internet to apply for their ESTA. While the majority of VWP travelers have access to the Internet, the absence of an alternative for those without Internet access could affect traveler compliance with the program in some cases.

Third, until October 15, ESTA will only be available in English, despite the fact that the VWP spans 27 countries and includes travelers who speak a number of languages other than English.[51] Though the ESTA web-based system is supposed to be made available in several languages prior to the mandatory compliance deadline, the fact that the system is currently available only in English will limit program participation and familiarization during the voluntary period.

Finally, it is unclear whether DHS, in conjunction with the State Department, has adequately studied what effect ESTA refusals or travelers electing not to seek an ESTA and instead apply for a visa might have on visa demand and resources at U.S. embassies and consulates overseas. The Government Accountability Office (GAO) recently reported that neither DHS nor the State Department has estimated how these factors might affect visa demand, though State has said that if one percent to three percent of current VWP travelers came to embassies in VWP countries for visas it may greatly increase visa demand at some locations, which could disrupt visa operations significantly.[52]

Air Exit System

US-VISIT is expected to be the vehicle through which DHS attempts to meet the biometric entry and exit matching requirements of Section 711. While DHS has established the biometric *entry* portion of US-VISIT, it has yet to implement an operational biometric *exit* system. Starting in January 2004, a kiosk-based US-VISIT exit system was piloted at 12 airports and two seaports, but DHS terminated the pilot in May 2007. GAO was critical of the pilot and found low compliance rates, poor planning, and inadequate evaluations.[53]

To meet the requirements of Section 711, in April 2008, DHS issued a Notice for Proposed Rulemaking (NPRM) for a new US-VISIT air exit system. The NPRM discussed a number of alternatives, including the use of a kiosk system. However, DHS identified as its preferred option an untested approach—one that requires airlines to collect travelers' biometrics.

There are several serious concerns with the proposed approach. First, by requiring airlines to collect travelers' biometric information, DHS is delegating its border security and immigration responsibilities to the private sector. Border security and immigration control are a Federal government function, and abdicating these responsibilities to the private sector sets a bad precedent.

Second, DHS' preferred option raises serious concerns about the security of extremely sensitive traveler data. While airlines and other private sector entities already collect passengers' biographic information, the collection and transmission of individuals' biometrics is particularly sensitive. Since the United States government is requiring the collection of this biometric data, it should take responsibility for its security.

Third, testimony before the Committee on Homeland Security from private sector travel industry stakeholders indicates that DHS is proceeding with this plan without adequate involvement from airline, airport, and other travel industry stakeholders. If DHS expects the airlines and travel industry to take on the responsibility for collecting biometrics, it must do a better job of engaging them going forward and ensuring that they institute systems to protect passenger biometric data from misuse.

DHS is expected to publish a final rule for US-VISIT air exit by the end of this calendar year in an effort to ensure that the additional authority granted to the Secretary of

Homeland Security to bring additional countries into the VWP does not suspend on June 30, 2009.

National Significance

For most countries, temporary foreign visitors for business or pleasure must obtain a visa from State Department at a consular post abroad before coming to the United States. Personal interviews are generally required and consular officers screen visa applicants against various databases to determine whether an individual is admissible to our country.

The VWP enables eligible nationals of participating countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. Only limited checks are conducted on travelers under the VWP prior to their departure for the United States. Instead, prior to the traveler's arrival, an electronic passenger manifest is sent from the airline to DHS and is checked against security databases. Approximately 15 million visitors from 27 VWP countries arrived in the United States during Fiscal Year 2006.[54]

Since the attacks of September 11, 2001, concerns have been raised about the ability of terrorists to enter the United States through the VWP. For example, the "Shoe Bomber" Richard Reid, a British citizen, attempted to enter the country under the VWP, and convicted al-Qaeda member Zacarias Moussaoui, a French national, came to the United States through the VWP. Because of these concerns, some have even called for the elimination or suspension of the VWP. The scope of the VWP and the associated potential security vulnerabilities make the security enhancements mandated by P.L. 110-53 all the more significant.

A chief vulnerability of the VWP program is that it paints all travelers from a particular VWP country with the same brush. Successful implementation of ESTA under Section 711 would allow DHS to make individualized assessments about whether a VWP traveler poses a threat before departing for the United States. Therefore, such a system would help prevent terrorists, criminals, and immigration violators from exploiting the VWP. It is imperative that DHS implement the ESTA program to ensure traveler compliance, while still welcoming and even facilitating legitimate travel to the United States.

For both VWP travelers and those who travel to the United States on visas, an acknowledged weakness of the current border security management systems is the failure to identify visa overstays. Of the 12 terrorists who were illegally in the United States when they committed crimes between 1993 and 2001, seven were visa overstays, including four of the 9/11 terrorists.[55] Because there was no entry-exit system in place, there was no systematic way for the United States government to track whether these individuals had departed the United States in accordance with the law. In response, the 9/11 Commission concluded that "completing a biometrics-based entry-exit system is an essential investment in our national security."[56]

Having an exit system in place at airports is an important part of enhancing the security of the VWP because it will allow us to track the arrival and departure from the United States of visitors who travel by air and enter the country without visas. That will permit DHS and Federal law enforcement to ascertain more readily whether an individual of interest is still in the United States or has departed the country. It will also allow the United States government to make a more accurate assessment of overstay rates from various countries, rather than continuing to rely on models and estimates.

In short, establishment of this biometric system will implement a 9/11 Commission recommendation to enhance our nation's border security and immigration enforcement. Therefore, it is essential that DHS work with the airlines, airports, and other travel industry partners to implement an effective, efficient, secure US-VISIT entry-exit system at airports as soon as possible, with minimal disruption to the travel process.

SEC. 511: DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL AND REGIONAL FUSION CENTER INITIATIVE

Statutory Requirement

Section 511 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) mandates the Department of Homeland Security (DHS) to issue a concept of operations for DHS State, Local, and Regional Information Fusion Center Initiative. The law requires the concept of operations to, "include a clear articulation of the purposes, goals, and specific objectives for which the program is being developed; identify stakeholders in the program and provide an assessment of their needs; contain a developed set of quantitative instruments (including surveys and expert interviews) to assess the extent to which stakeholders believe their needs are being met; and include a privacy and civil liberties impact assessment". The law requires DHS to issue the concept of operations, with an initial privacy and civil liberties impact assessment within 90 days or by November 1, 2007. A more comprehensive privacy and civil liberties impact assessment tracking the Initiative's progress was due by August 3, 2008.[57]

Status Update: FAILURE TO TAKE ACTION

To date, DHS has not produced a concept of operations for the State, Local, and Regional Information Fusion Center Initiative, including the initial privacy and civil liberties impact assessment, which was due on November 1, 2007.[58] Moreover, DHS has not released the comprehensive privacy and civil liberties impact assessment that was due on August 3, 2008.[59]

NATIONAL SIGNIFICANCE

The ability of State, local, and tribal law enforcement officers – America's "first preventers" – to partner effectively with the Federal government to address terrorism and other homeland security threats is reliant on the sharing of homeland security information. To address gaps in information sharing by the Federal government and enhance the exchange of information among agencies, State and local governments have established fusion centers. A fusion center has been defined as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[60] The potential value of fusion centers is clear: by integrating the various streams of information and intelligence from Federal, State, local, and tribal sources, as well as the private sector, a more accurate picture of risks to people, economic infrastructure and communities can be developed and translated into protective action. While fusion centers hold tremendous promise, there must be vigilance to assure that the counter-terrorism and intelligence activities undertaken at fusion centers do not run afoul of the United States Constitution.

Under P.L. 110-53, DHS is directed to actively engage fusion centers and, through its Office of Intelligence and Analysis (I&A), partner with these centers. To date, I&A has stationed over 20 officers at fusion centers nationwide. This field presence allows the centers to access DHS information sharing systems – including the Homeland Security Data Network (HSDN), a Secret-level network through which classified intelligence products are to be shared. It also allows fusion centers direct access 24 hours a day, seven days a week to I&A's Intelligence Watch and Warning Division, which answers requests for information from deployed DHS personnel and provides access to current classified threat information through daily intelligence briefings. I&A analysts in Washington, D.C., are likewise in daily contact with fusion centers to field queries on the latest threat information.

Notably, I&A has been promoting an internal analytical effort to support the provision of threat warning and intelligence assessments to fusion centers. For example, it prepares classified threat papers for each State and territory in order to help DHS understand the unique threat environment each State and territory faces.[61] I&A also produces the Chief Intelligence Officer (CINT) Notes that communicate information and analysis on emergent issues, domestic or international, to DHS' State, local, and tribal partners. Despite these positive developments, a recent I&A-commissioned survey of six fusion centers shows that DHS is not consistently generating intelligence products that make America more secure. Among other things, the study concluded that:

- State and local fusion centers [SLFC] leaders "do not believe that the raw reporting and finished intelligence they currently receive from DHS fully meets their mission-critical needs. The intelligence provided is not sufficiently focused on their unique requirements and the substantive issues that dominate the daily work of their fusion center personnel."[62]

- Support to the Secretary [of Homeland Security] and other senior officials "still sometimes dominate[s] decision-making in I&A about what to produce and how to produce it. As a result, DHS has not yet put in place a structured intelligence process that balances the needs of the multiple customers [at the State, local, and tribal levels]."[63]

- Although the deployment of I&A officers to fusion centers has improved SLFC leaders' understanding of DHS, the leaders "remained generally skeptical of how essential DHS support was for fulfilling their mission."[64]

For the State, Local, and Regional Fusion Center Initiative to succeed, DHS must – as required under P.L. 110-53 – complete a concept of operations that articulates the purposes, goals, and specific objectives of the program in accordance with common guidelines for fusion centers operations; assesses the information needs of State, local, and tribal stakeholders; and establishes mechanisms to evaluate how well those needs are being met. This blueprint will help promote more accurate, actionable, and timely flows of homeland security information that will help police and sheriffs' officers and other non-Federal homeland security leaders nationwide in their shared mission of making their communities safer.

Central to this effort is the Section 511 requirement that a Border Intelligence Fusion Center Program be included in the concept of operations to provide DHS with a more robust "border intelligence" capability – one that improves its ability to interdict terrorists, weapons of mass destruction, and related contraband at America's land and maritime borders. This program is key to helping DHS make better use of its resources, and obtaining better situational awareness of terrorist threats at or involving those borders, through more effective partnerships with State, local, and tribal law enforcement officers in border jurisdictions. With better border intelligence, law enforcement in those communities can act as a "force multipliers" and help prevent the next attack. Toward that end, I&A should also include in the concept of operations – in accordance with Section 101 – its plan to ensure that the Federal Emergency Management Agency (FEMA) provides rural and other underrepresented communities at risk of terrorism with an opportunity to participate in fusion center grant funding.

DHS has also been unable to provide either of the privacy and civil liberties impact assessments required under Section 511 that are critical for fusion center guidance and future success. In recent months, the American Civil Liberties Union (ACLU) has identified a host of potential dangers with fusion centers that pose a direct threat to the Constitution.[65] The Electronic Privacy Information Center (EPIC), in turn, warns that the effort by DHS to create a network of fusion centers, "'inculcates DHS with enormous domestic surveillance powers and evokes comparisons with the publicly condemned domestic surveillance program of COINTELPRO,' the 1960s program by the FBI aimed at destroying groups on the American political left."[66] The CATO Institute has echoed these findings, warning that without a guarantee that traditional Justice Department guidelines on infiltrating domestic groups could be enforced at fusion centers, "the slippery slope to spying on political dissidents – as the FBI's COINTELPRO did before such guidelines – is inevitable."[67]

Accordingly, the mandated privacy and civil liberties impact assessments for the State, Local, and Regional Fusion Center Initiative – which will describe how DHS should partner with fusion centers in a way that preserves privacy and civil liberties – are critical to the Initiative's success. Specifically, the assessments will describe what best practices should be adopted, what safeguards should be in place, and how compliance with the law will be assessed over time. These assessments, moreover, will include details on how the privacy and civil liberties training programs required for staff at all fusion centers receiving DHS funding – described in Sections 101 and 511 of P.L. 110-53 – are being developed and implemented across the country. This training is essential for promoting a "culture of constitutionality" in the fusion center environment. Without these assessments, DHS will lack the direction it needs to promote information sharing within legal boundaries – putting the long-term viability of fusion centers, and public support for them, at grave risk.

SEC. 101: HOMELAND SECURITY GRANT PROGRAM (HOMELAND SECURITY GRANTS FOR INTELLIGENCE ANALYSTS)

Statutory Requirement

Section 101 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) states that "not more than 50 percent of the amount awarded to a grant recipient under Section 2003 [Urban Area Security Initiative (UASI)] or 2004 [State Homeland Security Grant Program (SHSGP)] in any fiscal year may be used to pay for personnel including overtime and backfill costs, in support of the permitted uses under subsection (a)." That section permits the use of such funds for "establishing, enhancing, and staffing with appropriately qualified personnel State, local, and regional fusion centers that comply with the guidelines established under Section 210A(i)" and "paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts."

Status Update: ACTED IN A MANNER INCONSISTENT WITH THE INTENT OF THE PROVISION

The Federal Emergency Management Agency (FEMA) issued Homeland Security Grant Program guidance earlier this year that limited the amount a grant recipient could spend on fusion center personnel costs under both UASI and SHSGP to 25 percent of the total grant award – expressly ignoring the 50 percent cap prescribed under P.L. 110-53.[68] At the same time, FEMA limited the period that this Federal funding could be used to pay the salary and benefits for specific intelligence analysts to just two years.[69] Making matters worse, FEMA stated that a grant recipient's failure to sustain those analyst positions, *at its own cost*, after the two-year deadline "will result in disqualification of grantees from hiring analysts with Federal funds in future program years." In short, FEMA required States and localities to make an upfront commitment to pay 100 percent of the sustainment costs for intelligence analysts after two years – or lose all Federal funding for new analyst positions going forward.[70] Although FEMA subsequently amended its grant guidance to extend the Federal funding time limit from two to three years, it continues to require grant recipients to commit to keeping existing intelligence analysts positions on the books, and to picking up the entire tab for them, after the third year of Federal funding has passed.[71]

In response to the failure by DHS to administer the program as Congress intended, the House on July 29, 2008, approved legislation (H.R. 6098) to give States and localities the discretion to hire and retain the staff they need to keep their communities safe without the arbitrary financial caps and time restrictions. The bill clarifies a commitment to sustainment as promised in both P.L. 110-53 and the President's own information sharing strategy.

National Significance

State and local grant recipients need the flexibility to use Department of Homeland Security (DHS) funding to hire, train, and ***retain*** new and existing intelligence analysts, including contractors, engaged in the terrorism prevention mission at fusion centers. FEMA's arbitrary funding caps – and time limitation on use of funds – has had the absurd result of forcing some States and localities to fire analysts after two years just to continue qualifying for DHS funding. While a third year of funding would otherwise be welcomed by many communities, some are choosing to forego SHSGP or UASI funding for intelligence analysts altogether because they cannot predict whether State legislatures will agree to pay 100 percent of the cost in the future. Equally troubling is the fact that the FEMA grant guidance undermines the stringent privacy and civil liberties training requirements that are the centerpiece of P.L. 110-53. By forcing some States and localities to discharge staff every two years or discouraging them from hiring intelligence analysts in the first place, DHS is effectively preventing a "culture of constitutionality" from taking root at fusion centers, which is nonsensical.

The stationing of police, first responders, intelligence analysts, and public health experts side-by-side at fusion centers allows personal relationships to be built and information sharing to happen. "On the whole, fusion centers play a decisive role," said Ambassador Thomas McNamara, Program Manager for the Information Sharing Environment.[72] "They strengthen the nation's ability to protect communities from future attacks."[73] Fusion centers accordingly are not just State and local assets; they are national assets that can play a central role in the country's homeland security effort. Sustainment funding to keep the fusion center effort going is not about building new facilities or buying new equipment, but on the contrary, it is about helping State, local, and tribal authorities hire and retain qualified intelligence analysts.[74] This is a significant challenge. Backlogs in the security clearance process for new employees are well documented and training for new personnel can take many months. As a result, fusion center leaders often rely on contractors as they endeavor to build up their respective workforces. How effectively they do so – given severe fiscal constraints at the State and local levels – is a matter of ongoing and increasing concern.

Section 101 of P.L. 110-53 addresses this challenge by including a 50 percent ceiling on personnel costs for intelligence analysts and other staff. The President's National Strategy for Information Sharing, released several months after P.L. 110-53 was enacted, likewise emphasizes the need to sustain baseline capabilities and operations of fusion centers through financial and other means, describing the commitment as a "national priority."[75] DHS' short-sighted grant guidance simply ignores the central homeland security role that both Congress and White House policy have identified for fusion centers.[76] DHS likewise misses the mark when it comes to Constitutional protections. For fusion centers to be effective they must not only have adequate resources but also rigorous privacy and civil liberties protections built into their procedures and activities. Without these safeguards, the public will rightly become wary of or even outright opposed to them. That is why P.L. 110-53 requires, in Sections 101 and 511, that fusion center personnel undergo necessary training to ensure that the intelligence work they do complies with the law. By forcing some States and localities to fire staff every two years in order to access Federal funds, however, DHS is effectively preventing a "culture of constitutionality" from taking root. Privacy and civil liberties best practices accordingly have no time to develop and abuses will inevitably result.

SEC. 804: FEDERAL AGENCY DATA MINING REPORT ACT OF 2007

Statutory Requirement

Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) requires Federal agencies to report to Congress annually on the development and use of pattern-based data mining programs. This type of data mining is capable of reviewing and analyzing millions of public and private records of Americans in search of patterns of terrorist or criminal activity. Additionally, this provision modifies the Federal definition of "data mining" to include activities in which the Federal government is the source of the data thereby broadening the amount of information that is to be included in annual data mining reports that Federal agencies must transmit to Congress. Section 804 also requires agencies to include an assessment of the actual or likely impact on the privacy and civil liberties of individuals of data mining actions taken by each agency. Under this provision, each report must include details regarding the data mining project, including a description of the technology and data to be used; a discussion of the plans and goals for using the technology, when it will be deployed, and an assessment of the expected efficacy of the data mining project; a privacy impact assessment; an analysis of the relevant laws and regulations that would govern the project; and a discussion of policies, procedures and guidelines that are in place or plan to be developed in order to protect the privacy and due process rights of individuals and ensure that only accurate and complete information is collected, reviewed, gathered, analyzed or used to guard against harmful consequences or potential inaccuracies.

P.L. 110-53 requires each agency involved in data mining activities to submit a report to Congress that encompasses the new definition and includes a privacy and civil liberties assessment no later than 180 days after the enactment or January 30, 2008.

Status Update: SOME PROGRESS BUT REQUIRED REPORTS HAVE NOT BEEN SUBMITTED

One month prior to the enactment of P.L 110-53, the Department of Homeland Security (DHS) issued its 2007 report on data mining that provided a review of DHS data mining activities.[77] The report, however, did not include new information required under P.L. 110-53 including the activities where the Federal government was the source of the data. According to the time frame set forth in Section 804, DHS was required to provide the new information on data mining by January 30, 2008. However, it did not. Instead, on February 11, 2008, DHS issued a four-page "letter report" that acknowledged the new definition contained in Section 804 and identified DHS activities that met the criteria of the new definition. However, it failed to communicate what new information was garnered about DHS' data mining activities through its new template.[78] Moreover, the

document did not include required information regarding the privacy and civil liberty impact of the stated DHS activities.

To the credit of DHS, prior to the enactment of P.L. 110-53, they had satisfied the previously mandated data mining report requirement by issuing consecutive reports in July 2006 [79]and July 2007,[80] but it has not yet released its report for 2008 which, was due by July 2008 under the Federal Agency Data Mining Reporting Act of 2007. If DHS contends the due date was changed pursuant to P.L. 110-53, at the very least the information provided in the February 11, 2008 letter report should have included a more thorough analysis of data mining activities to prevent a gap in knowledge in this important area of concern. By any measure, the information that should have been received is overdue. Given the myriad issues involving data mining activities, the neglect by DHS of its reporting requirement is extremely troublesome.

National Significance

The Federal government should be able to use information that is lawfully at its disposal to ferret out criminal and terrorist activity. However, the American public should be advised of Federal government programs that sift through millions, if not billions, of records containing individual personal information and the measures that are in place to confine these activities. While data mining can generate useful homeland security and law enforcement information, it also raises considerable legal issues and implications; including, data quality, interoperability of data mining software and databases, mission creep, and privacy.[81] The reporting requirements in Section 804 bring needed transparency to the data mining activities of Federal agencies. Failure to fulfill these requirements not only results in a lack of transparency but places well-intended, effective homeland security programs at risk. After all, DHS has a documented record of spending millions of dollars on programs that were ultimately cancelled or discontinued because of fundamental privacy and civil liberties concerns. Among DHS data mining programs that have met this fate are MATRIX,[82] CAPPS II[83] and ADVISE.[84] Providing Congress with timely, annual reports on data mining activities allows Congress to exercise oversight and determine the validity of these programs on a regular basis to assure that no agency goes forward with a multi-million dollar program that will ultimately be discontinued once it becomes known that the fundamental privacy and civil liberties of the American public have been violated or put at risk.

SEC. 301: INTEROPERABLE EMERGENCY COMMUNICATIONS GRANT PROGRAM

Statutory Requirement

Section 301 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) established the first-ever, stand alone emergency communications grant program at the Department of Homeland Security (DHS). P.L. 110-53 authorized the Interoperable Emergency Communications Grant Program (IECGP) at $1.6 billion over five years. In an effort to improve accountability and ensure that expenditures enhance interoperability, the law specifically states, "The Secretary [of Homeland Security] may ***not*** award a grant under this section before the date on which the Secretary completes and submits to Congress the National Emergency Communications Plan required under section 1802." Issuance of the National Emergency Communications Plan (NECP) is one of the primary responsibilities of DHS' Director of the Office of Emergency Communications (OEC) and was due to Congress in April 2008 the Post Katrina Emergency Management Reform Act of 2006.[85]

Status Update: DELIVERY OF KEY PLAN LATE; RISK DELAYS IN GRANTS

Recognizing the importance of interoperable communications[86], P.L. 110-53 established a dedicated program to help State and local jurisdictions achieve interoperable emergency communications. IECGP is intended to enhance and improve interoperable emergency communications at all levels of government by supporting State and local efforts to implement Statewide Communication Interoperability Plans (SCIPs). In order to receive grant funds, States must have their statewide plans approved by the OEC. The SCIPs help ensure coordination among first responders and other government officials and also identify gaps in communications capabilities. In turn, the capability gaps identified in the SCIPs are to be used to inform the NECP.

The NECP was released by DHS on July 31, 2008, three months after the statutory deadline. It proposed three goals to achieve a baseline of interoperable communications for Federal, State, local and tribal authorities:

- By 2010, 90% of all Urban Areas Security Initiative (UASI) participants can demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.
- By 2011, 75% of non-UASI jurisdictions can demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.

- By 2013, 75% all jurisdictions can demonstrate response-level emergency communications within three hours of a significant event, as outlined DHS' national planning scenarios.

The NECP stresses the importance of governance, planning, technology, training and exercises, and disaster communications capabilities based on the findings from the 56 SCIPS, the National Communications Capabilities Report (NCCR), the National Response Framework (NRF), the National Incident Management System, the National Preparedness Guidelines, the Target Capabilities List and the Interoperability Baseline Survey by SAFECOM's Executive Committee and the Emergency Response Council – all of which reflect the perspectives of over 200 practitioners from across the country.

However, essential information on how the Federal government currently responds to emergencies in all States, and how they communicate with State officials and other jurisdictions needs more clarification in the NECP. Specifically, the NECP does not detail how the Emergency Communications Preparedness Center – established to further interagency efforts to promote emergency communications nationwide – will work to advance interoperable communications in a cooperative manner.

The delay in issuance of the NECP has significantly reduced the review period of the grants by DHS. Congress appropriated $50 million for IECGP in FY 2008.[87] Grant guidance and application materials were not issued until June 20, 2008. Under the grant guidance's, States would have until July 21st to apply for IECGP grants, allocation announcements would be made by August 1st, and distributions would be made to qualified States in September. DHS is expected to announce the IECGP awards before September 30, 2008.

National Significance

The inability of first responders to communicate during emergencies persists despite high-profile events such as the bombing of the Alfred P. Murrah building in Oklahoma City, the September 11th attacks on the World Trade Center, and Hurricanes Katrina and Rita in 2005. In 2002, the National Task Force on Interoperability (NTFI) identified five key challenges to interoperability: (1)Incompatible and aging communications equipment; (2) Limited and fragmented funding since 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 constrains, complicate the implementation of long-term projects needed to achieve full interoperability; (4) Lack of coordination and cooperation since agencies are reluctant to give up management and control of their communication systems; and (5) Limited and fragmented radio communications spectrum since public safety must compete with other interested party to secure access to limited spectrum.

The 9/11 Commission recommended that Federal funding for interoperable communications be given "high priority by Congress," explaining that there is "strong evidence that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem."[88] The Homeland Security Grant Program has awarded approximately $9.5 billion in grants

since 2003 to help State and local authorities strengthen their preparedness and response capabilities for a terrorist attack or other catastrophic event. Of this amount, approximately $2.9 billion has been spent on interoperable communications, making it the single largest use of grant funds.[89]

Over the years, interoperability expenditures have mostly focused on the equipment purchases. The IECGP was authorized to provide resources for essential interoperability needs that have traditionally not been funded but are critical to the development of an effective system. For FY 2008, the IECGP grant guidance identifies two major funding priorities: (1) leadership and governance and (2) common planning and operational protocols, and emergency responder skills and capabilities.[90] The challenges to achieving interoperable communications were confirmed by DHS 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."[91] When discussing emergency communication capabilities, Dr. David Boyd of DHS testified before Congress that "operability must be in place for interoperability to be possible."[92]

During Hurricane Katrina, the entire communications infrastructure on the Mississippi Gulf Coast was destroyed and thirty-eight 9-1-1 call centers collapsed.[93] DHS 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."[94] The IECGP grants must be provided in accordance with the NECP to assure baseline capabilities for operability and interoperability, thus advancing emergency communications capabilities on a National level.

SEC. 408: CREDENTIALING AND TYPING (OF INCIDENT MANAGEMENT PERSONNEL)

Statutory Requirement

Under Section 408 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), the Federal Emergency Management Agency (FEMA) is required to provide standards and written guidance to each Federal agency that has responsibilities under the National Response Plan (NRP), as well as State, local and tribal governments. The purpose of the standards and written guidance is to aid with credentialing and typing incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster. FEMA is also required, under Section 408, to provide expertise and technical assistance to aid Federal, State, local and tribal entities that need assistance with credentialing and typing incident management personnel.

Under the law, the credentialing and typing standards and written guidance were to be transmitted no later than 1 year after the date of enactment of P.L. 110-53 or August

3, 2008. Each Federal agency with responsibilities under the NRP, in turn, is required to ensure that the appropriate incident management personnel and resources likely to be needed to respond to a disaster, man-made or natural, are credentialed and typed not later than six months after receiving the standards.

Status Update: NO PROGRESS

To date, FEMA has not issued standards and written guidance on credentialing emergency personnel, as required by law. At a June 27, 2008 briefing with Committee on Homeland Security staff, FEMA indicated the detailed written guidance and technical assistance would be provided to State, local, and tribal governments to facilitate credentialing by August 2008.

It is worth noting that FEMA has been working on this issue for some time. In 2005, the National Incident Management System (NIMS) Integration Center (NIC), within FEMA, initiated development of a national credentialing system to enhance the ability of Federal, State, local and tribal governments to identify and dispatch appropriately qualified emergency responders from other jurisdictions when needed. As outlined, the system, entitled the National Emergency Responder Credentialing System would set forth minimum professional qualifications, certifications, training and education requirements for specific emergency response functional positions.[95] By July 2007, FEMA testified before a Committee on Homeland Security subcommittee that it was establishing a working group for developing and integrating credentialing requirements and programs.[96]

National Significance

The 9/11 Commission noted that "the 'first' first responders on 9/11, as in most catastrophes, were private sector civilians."[97] It is, therefore, critical that there be standards and a system in place to allow incident managers to verify identities of responders who appear at the scene of a disaster. At the same time, private-sector workers, such as telecommunications employees, need to have emergency access to disaster scenes to enable them to recover, repair, and reconstitute critical communications infrastructure.

Access to a qualified pool of emergency personnel was a major problem in both Louisiana and Mississippi during Hurricane Katrina. In the immediate aftermath of Katrina, health professionals wanted to volunteer their time and services to the affected region, a contractor was hired to individually verify the credentials of the 34,000 individuals who volunteered in the weeks after Katrina.[98] If a system had been in place where individuals who volunteer to respond to a disaster had credentials that were easily verifiable, this time-consuming, expensive verification process could have been avoided.

SEC. 1101: NATIONAL BIOSURVEILLANCE INTEGRATION CENTER

Statutory Requirement

Section 1101 of the Implementing Recommendations of the 9/11 Commission Act of 2007(P.L. 110-53) established the National Biosurveillance Integration Center (NBIC) in statute and required the Department of Homeland Security (DHS) to ensure that NBIC has the ability to "rapidly identify, characterize, localize, and track a biological event of national concern" - in as close to real-time as possible - that presents a risk to the population, economy, or infrastructure of the United States. Section 1101 requires NBIC to operate by "integrating and analyzing data relating to human health, animal, plant, food and environmental monitoring systems…disseminate alerts and other information to Member Agencies…oversee development and operation of the National Biosurveillance Integration System." The Act requires the NBIC to be "fully operational" by September 30, 2008.

Status Update: INITIAL STEPS TAKEN BUT LITTLE PROGRESS

According to NBIC, to ensure the integration of biosurveillance information, the Center should have representatives of twelve Federal agencies: DHS, the Department of Commerce (DOC), the Department of Defense (DOD), the Environmental Protection Agency (EPA), the Department of Health and Human Services (HHS), the Department of the Interior (DOI), the Department of Justice (DOJ), the Department of State (DOS), the Department of Transportation (DOT), the U.S. Postal Service (USPS), and the Veteran's Administration (VA), as well as state, local, private sector, and international entities. [99]

Prior to enactment of P.L. 110-53, DHS had Memoranda of Understanding (MOUs) with five different Federal agencies reflecting high-level agreements to participate.[100] In its February 2008 interim report delivered to Congress,[101] as required by P.L. 110-53, DHS could only report that these five pre-existing MOUs were in place. One additional MOU was just signed in August of 2008, bringing the total to 6. The new MOU was the first to be signed since February 2007.

For NBIC to ever become "fully operational," MOUs must be signed with the remaining six Federal agencies. All 12 MOUs must be followed by detailed Interagency Agreements (IAAs) that specifically detail what support including manpower and data feeds would be supplied to NBIC. There would also need to be agreements with each of the agencies on information governance as well as Interagency Security Agreements (ISAs) that detail the cybersecurity measures needed for data linkages between the agencies. Finally detailees from the other agencies, paid for by NBIC, must be provided. At present, only one IAA has been signed with HHS, no ISAs are signed, and only one agency, HHS/CDC, has supplied a detailee to NBIC. In practical terms, this means that

Federal agencies are not sharing data with NBIC, and currently the only data feeding into NBIC is open source information taken from the Internet, news reports, and other media. NBIC is hopeful that it can get agreements on ISAs with the remaining five Departments with which it has an MOU but the track record to date indicates that this goal is not realistic.

National Significance

Well before the attacks of September 11, 2001, there was awareness of the need to protect against biological threats. In fact, the 9/11 Commission recalled that President Bush, speaking before the Naval Academy in 1998, announced "we will undertake a concerted effort to prevent the spread and use of biological weapons and to protect our people in the event these terrible weapons are ever unleashed by a rogue state, a terrorist group, or an international criminal organization."[102]

Biosurveillance, through an effective NBIC, is an important component of a national effort to protect the United States from biological attacks by terrorist and naturally occurring disease outbreaks, by providing early detection and situational awareness of disease incidents, in the human population, in animals, and in food. For any disease outbreak, early detection offers the opportunity for early response, which can limit the spread, intensity, and duration of an outbreak. Situational awareness allows disease tracking and source determination. It also affords decision-makers the opportunity to determine the best response options and focus resources most effectively, and in extreme cases conduct appropriate and effective isolation or quarantine. In the case of an overseas outbreak, early situational awareness can provide important "lead time" to prevent disease from spreading to the United States or allow preventive measures to be deployed to protect the population. Such a capability could have helped stop the Severe Acute Respiratory Syndrome (SARS) outbreak of 2003 from spreading to North America or swiftly trace the source of the salmonella outbreak in the United States in 2008. NBIC was authorized to ensure that the United States has this important capability.

In broader terms, effective biosurveillance requires rapid and trusted information exchange between all levels of government: Federal, state, local, and tribal, as well as private sector stakeholders and international partners. The "Spanish Flu" epidemic of 1918-1920 killed 675,000 Americans and more than 20 million people around the world. It is estimated that a similar epidemic of a human-transmissible of influenza, which most experts consider "inevitable," could produce nearly 1.8 million deaths in the United States, and up to 300 million deaths worldwide.[103] An effective biosurveillance system could greatly reduce such consequences if implemented effectively. The lack of progress in establishing critical agreements and securing necessary resources for the NBIC represents a major failure of the Bush Administration. Looking ahead, a sense of urgency must be applied to getting NBIC to "fully operational" status as quickly as possible.

SEC. 901: PRIVATE SECTOR PREPAREDNESS (AND ACCREDITATION AND CERTIFICATION PROGRAM)

Statutory Requirement

Section 901 of the Implementing Recommendations of the 9/11 Commission Act (P.L. 110-53) requires the Department of Homeland Security (DHS) to create a Voluntary Private Sector Preparedness Accreditation and Certification Program. The provision requires DHS to work with different private sector entities, such as the Sector Coordinating Councils,[104] to develop and promote a program to certify the preparedness, emergency management and security of private sector entities that voluntarily choose to seek certification under the program. In addition, DHS is required to provide Congress with a report detailing any action taken to implement the Voluntary Private Sector Preparedness Accreditation and Certification Program, including a discussion of the separate methods of classification and certification for small business concerns. The Act requires submission of the report to Congress by March 3, 2008.

Status Update: LIMITED PROGRESS

Six months have passed since the Section 901 deadline and DHS has yet to submit to Congress the required report on the Voluntary Private Sector Preparedness Accreditation and Certification Program. The intent of Congress in requesting this report was to give DHS a chance to demonstrate its progress and accomplishments with respect to the Voluntary Private Sector Preparedness Accreditation and Certification Program. Unfortunately, it has failed to take advantage of this opportunity. DHS has provided two briefings to the Committee on Homeland Security about its work to develop this accreditation and certification program, yet a detailed and comprehensive description of DHS' activities has not been produced in accordance with P.L. 110-53.

With respect to encouraging the development of voluntary preparedness standards in the private sector, DHS' progress has been dismal. One of the requirements in this provision was to encourage DHS to consult with representatives of appropriate organizations, such as the Sector Coordinating Councils, to develop these preparedness standards. Briefings by DHS to the Committee on Homeland Security revealed it has done little outreach to these organizations and councils, which include over 1,000 private sector entities.[105] These councils include companies that have demonstrated a willingness and desire to partner on preparedness yet DHS has failed to effectively access this wide, promising network.

As required by P.L. 110-53, DHS has appointed a "Designated Officer"—the Administrator of the Federal Emergency Management Agency to work with the Assistant Secretary for Infrastructure Protection and the Under Secretary for Science and Technology. Although compliant with the law, this selection is quizzical given that the

Assistant Secretary for Infrastructure Protection has the most coordinated outreach to vital elements of the private sector.

Although DHS was past due in its requirement to enter into an agreement with a qualified entity to manage the accreditation process and oversee the certification process, it complied and signed a "potentially three-year agreement with American National Standards Institute-American Society for Quality National Accreditation Board to develop and implement an accreditation and certification program."[106]

National Significance

The 9/11 Commission asserted that "[t]he mandate of the [Department] does not end with government; [it] is also responsible for working with the private sector to ensure preparedness."[107] In addition, the 9/11 Commission endorsed the American National Standards Institute's recommended standards for private preparedness.[108] The 9/11 Commission also encouraged the "insurance and credit-rating industries to look closely at a company's compliance with the ANSI standard in assessing its insurability and creditworthiness."[109]

Congress has continuously advocated engaging the private sector in preparedness efforts, as it is essential to the success and viability of homeland security for this Nation. Accordingly, 85 percent of the Nation's critical infrastructure is owned and operated by the private sector. Regrettably, DHS has not demonstrated a real, tangible progress in ensuring private entities are engaging in security efforts. The Voluntary Private Sector Preparedness Accreditation and Certification Program could be utilized more effectively to promote security efforts by DHS. It is unfortunate that the Bush Administration has been sluggish in rolling out this program and lackluster in engaging with the very entities that will be asked to voluntarily comply. This program should be market oriented and not compulsory, and acquiring the insight of private companies is essential for its success.

SEC. 1001: NATIONAL ASSET DATABASE

Statutory Requirement

Section 1001 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) codified the National Asset Database in statute and required the Department of Homeland Security (DHS) to "use the database…in the development and implementation of Department plans and programs." In addition, Section 1001 required that a report on the status of the database be submitted to Congress no later than 180 days after the date of enactment of P.L. 110-53. DHS was also required to provide to Congress a prioritized list of critical infrastructure within 180 days of enactment.

The deadline for submission of the report and the prioritized list of critical infrastructure was February 3, 2008.

Status Update: SOME PROGRESS BUT LITTLE USE OF THE NATIONAL ASSET DATABASE

Since the National Asset Database was established and authorized in law by P.L. 110-53, DHS has failed to "use the database…in the development and implementation of Department plans and programs."[110] Despite the Congressional mandate, the National Asset Database does not inform any decision making by DHS. DHS continues to use other warehouses, databases, and catalogues for its critical infrastructure planning—all of which are outside congressional mandates and requirements.

In disregard of reporting requirements, DHS has failed to provide Congress with a report on the database. DHS has, however, briefed the Committee on Homeland Security on its programs, lists, and warehouses. Notwithstanding these briefings, DHS is nearly a year overdue with this report. DHS provided Congress with the list of prioritized critical infrastructure and, thus, fulfilled that requirement of Section 1001.

National Significance

The United States is interconnected by a vast network of infrastructure. Therefore, it is imperative that we attempt to secure and protect those assets that are deemed critical and most at risk of being attacked by terrorists. After all, al Qaida has repeatedly pledged to cripple the underpinnings of our economy and our civil institutions. The threat from terrorism was exacerbated by the events during and following Hurricane Katrina when it became clear that a great deal of critical infrastructure—modes of mass transit, utilities, and more—did not properly plan for such a disaster. DHS ought to focus on securing and protecting those assets that, if incapacitated, would impact our economy, governance, and ability to respond to a disaster. The National Asset Database was intended to assist DHS in locating and securing these assets.

The rationale for codifying the National Asset Database was twofold. First, it was an attempt to rectify the concerns about the quality of assets tracked by DHS, after it was made public that popcorn factories and other facilities with dubious national significance were deemed critical infrastructure.[111] By developing a clear and delineated process in P.L. 110-53, Congress was attempting to ensure that the assets were, indeed, critical lest monies and other resources were diverted to undeserving assets. Second, the National Asset Database was codified so that Congress could clearly articulate that it wanted the newly defined database to inform the decision-making of DHS in securing critical infrastructure.

Since its inception, however, this intent and consultation has not materialized. Instead, the National Asset Database soon housed information about assets that were not threatened nor critical because states and localities had the mistaken belief that the more assets that they had in the National Asset Database, the more funding they would receive from DHS. The Bush Administration did nothing to dispel this myth. It is clear that the National Asset Database includes a great deal of irrelevant assets and that it is not coordinating inputs properly from diverse stakeholders. Congress attempted to rectify these problems in Section 1001 in order to ensure the database was driven by risk-based resource allocation and, yet, the Bush Administration has failed to meet the intent of this congressional mandate.

SEC. 1821: INTERDICTING WEAPONS OF MASS DESTRUCTION

Statutory Requirement

Section 1821 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53) provides that the President should strengthen and formalize the Proliferation Security Initiative (PSI), the United States' primary program to interdict and seize illicit shipments of dangerous materials and equipment to support Weapons of Mass Destruction programs by rogue nations and terrorist groups. It provides that the President improve the planning, funding and coordination of the PSI.

Status Update: FAILURE TO TAKE ACTION

The President has failed to take any of the actions recommended in P.L. 110-53. Specifically, the President has not issued a directive to agencies and departments to establish clear PSI authorities, responsibilities, and structures; identify in annual budget requests funds for PSI activities, and to provide the necessary resources to achieve more efficient and effective performance of United States PSI-related activities.

National Significance

Without clear guidance and coordination, the PSI cannot realize its full potential. Like a ship with no charts and no navigation, it is in danger of steaming in circles, relegated to the status of a political demonstration project rather than an effective multilateral WMD interdiction force. The President's knee-jerk resistance to formalizing and structuring any multilateral initiative – even within the U.S. government - risks undermining the PSI.

SEC. 1841: COORDINATING U.S. NONPROLIFERATION PROGRAMS

Statutory Requirement

Section 1841 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53) established an office of the Coordinator for the Prevention of Weapons of Mass Destruction Proliferation and Terrorism. The Coordinator was required to formulate a comprehensive and well-coordinated United States strategy and policies for preventing weapons of mass destruction (WMD) proliferation and terrorism; lead inter-agency coordination of United States efforts to implement the strategy and policies relating to preventing WMD proliferation and terrorism; conduct oversight and evaluation of accelerated and strengthened implementation of initiatives and programs to prevent WMD proliferation and terrorism; and to oversee the development of a

comprehensive and coordinated budget for programs and initiatives to prevent WMD proliferation and terrorism.

Status Update: FAILURE TO TAKE ACTION

The President has failed to appoint a Coordinator to ensure that the United States and its allies are fully protected against terrorist attacks using nuclear, chemical, biological or radiological weapons, despite the clear mandate of P.L. 110-53.

National Significance

There is no individual in the Executive Branch fully in charge of the disparate and largely-uncoordinated programs and activities of the United States to prevent such terrorist attacks; no one to "connect all the dots" to bring all these programs and activities into a more coherent campaign; no one to foresee and ensure that there are no dangerous gaps in United States efforts that terrorist groups could exploit.

SEC. 2012: INTERNATIONAL MUSLIM YOUTH OPPORTUNITY FUND

Statutory Requirement

Under Section 2012 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53), the President is authorized to establish an International Muslim Youth Opportunity Fund to provide assistance to enhance modern educational programs in the Islamic World; for training and exchange programs for teachers, administrators, and students; to target primary and secondary students; and to develop youth professionals, as well as other types of assistance such as the translation of foreign books, newspapers, reference guides, and other reading materials into local languages and the construction and equipping of modern community and university libraries.

Status Update: FAILURE TO TAKE ACTION

While the Bush Administration has devoted additional resources to education in the Muslim world, the Bush Administration has not established the International Muslim Youth Opportunity Fund nor has it submitted a report on implementation of this section.

National Significance

The United Nation's 2003 Arab Human Development Report stated that the quantitative expansion of education in the Muslim world remains incomplete and that high rates of illiteracy, especially among women, persist. The UN report also cited the decline in quality as the most significant challenge in the educational arena in Arab countries. In addition, many factors in Arab countries adversely affect teachers' capabilities, such as low salaries, which force educators in Arab countries to take on other jobs that consume their energy and cut into the time they can devote to caring for their students; lack of facilities; poorly designed curricula; indifferent quality of teacher

training; and overcrowded classes. Educational attainments in the Muslim world – from literacy rates to mathematical and science achievements – are well below global standards. It is estimated that there are 65 million illiterate adult Arabs, and two-thirds of them are women. While educational enrollment for Arab countries rose from 31 million in 1980 to approximately 56 million in 1995, 10 million Arab children between the ages of 6 and 15 are currently not in school. Even though women's access to education has tripled in Arab countries since 1970, illiteracy in the Arab region affects women disproportionately; and women make up two-thirds of illiterate adults, mostly in rural areas.

Researchers argue that curricula taught in Arab countries seem to encourage submission, obedience, subordination and compliance, rather than free critical thinking, making populations more receptive propaganda by our enemies, and many educational systems in Muslim countries widen the gap between rich and poor with poor children receive grossly inadequate schooling. Increased assistance to modernize education in the Muslim world is critical to furthering United States interests in the region.

SEC. 2021: ESTABLISHMENT OF A MIDDLE EAST FOUNDATION

Statutory Requirement

Section 2021 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53) provides that the Secretary of State "is authorized to designate an appropriate private, nonprofit organization that is organized or incorporated under the laws of the United States or of a State as the Middle East Foundation." The purposes of this foundation are to support the expansion of civil society, protections for internationally recognized human rights, independent media, and other aspects of civil society. In particular, Section 2021(c) provides that the Foundation may make a grant to an institution of higher learning in the Middle East to establish a Center for Public Policy "for the purpose of permitting scholars and professionals from the countries of the broader Middle East region and from other countries, including the United States, to carry out research, training programs, and other activities to inform public policymaking in the broader Middle East region and to promote broad economic, social, and political reform for the people of the broader Middle East region."

Status Update: MISSED OPPORTUNITIES

While the Secretary has designated the Foundation for the Future, based in Amman, Jordan, as the "Middle East Foundation (MEF)," it has made a total of 25 grants and has failed to establish the Center for Public Policy.

National Significance

Section 2021 envisioned the Center as a magnet for "scholars and professionals" from throughout the broader Middle East and elsewhere, which clearly would encourage cross-fertilization of ideas and policy-promotion techniques. This much-needed center could promote indigenous networking and reinforcing of reform-minded leaders throughout the region. The failure to develop the Center may well undermine the ability

of reforms in countries throughout the region to help develop pluralistic and open societies that are so important to improving the well being of people in the regions.

SEC. 2033: UNITED STATES POLICY TOWARD DETAINEES

Statutory Requirement

Section 2033 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53) provides that the Secretary of State should "continue to build on the Secretary's efforts to engage United States allies to develop a common coalition approach, in compliance with Common Article 3 of the Geneva Conventions and other applicable legal principles, toward the detention and humane treatment of individuals detained during Operation Iraqi Freedom, Operation Enduring Freedom, or in connection with United States counterterrorist operations."

Status Update: PROGRESS IS SLOW AND UNCERTAIN

Despite continued efforts to explain its position abroad and to discuss these issues with like minded countries, there remain fundamental disagreements regarding how the law of war applies to foreign terrorist organizations and how to treat detainees of such organizations and others detained during Operation Iraqi Freedom and Operation Enduring Freedom. As the State Department's report on this matter admits, despite progress on this issue, "there continue to be important differences between the United States and its allies on detention-related issues." Efforts to forge consensus at meetings even with countries that have shown some understanding of the United States position have failed to achieve consensus on these important issues. Finally, the Administration's approach continues to be rejected by the U.S Supreme Court itself, as in the case of Boumedienne vs. Bush, 553 U.S. ___ (2008), where the Supreme Court rejected the suspension of habeas corpus in the Military Commissions Act, drafted by the Republican majority in the 109th Congress in cooperation with the White House. This continued uncertainty of the legality of the United States system undermines the ability to achieve a common approach with our allies.

National Significance

The failure to reach a consensus with our allies on the treatment of detainees and the Bush Administration's continued effort to breach legal frontiers long honored by past Presidents continues to damage the United States image abroad and reduce respect internationally for the rule of law and, with profound consequences. It undermines public support for United States efforts to combat terrorism, invites our enemies to mistreat our own forces, makes it harder for other governments to cooperate with the United States, and severely impacts the ability of the United States to exercise moral leadership on other issues relating to human rights and democracy. It further helps our enemies recruit foot soldiers in their efforts to attack us further, makes it more difficult to operate with other countries in Afghanistan, and provides a justification for other countries to abuse their own citizens in their self-declared "war on terror" All of these effects severely hams United States national security interests around the globe and puts United States troops at risk.

SEC. 2042: STRATEGY FOR THE UNITED STATES RELATIONSHIP WITH PAKISTAN

Statutory Requirement

Section 2042 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53) lists several publicly-stated goals of the Government of Pakistan and national interests of the United States that are in close agreement and states "increased commitment on the part of the Government of the United States in regard to working with all elements of Pakistan society in helping to achieve the correlative goals…" Under Section 2042, the President is required to submit a report no later than 90 days after the date of enactment "that describes the long-term strategy of the United States to engage with the Government of Pakistan…"

Section 2042 also places a limitation on certain types of assistance and the provision of export licenses for fiscal year 2008 until the President provides a determination that "the Government of Pakistan (A) is committed to eliminating from Pakistani territory any organization such as the Taliban, al Qaeda, or any successor, engaged in military, insurgent, or terrorist activities in Afghanistan; (B) is undertaking a comprehensive military, legal, economic, and political campaign to achieving the goal described in subparagraph (A); and (C) is currently making demonstrated, significant, and sustained progress toward eliminating support or safe haven for terrorists."

Status Update: LACK OF COMPREHENSIVE STRATEGY YIELDS DISASTROUS RESULTS

To date, the President has not been able to implement an effective strategy towards achieving United States national security goals with respect to Pakistan. United States national security interests in combating terrorist activities in Pakistan have been sacrificed for unyielding support for a military dictator. The strategy that the President did submit pursuant to Section 2042 read as a white paper on the importance of the United States-Pakistan relationship and a justification for continued support for the current regime rather than a comprehensive strategy paper. In addition, the President was quick to provide the determination necessary in Section 2042(d) to avoid the assistance limitations for FY 2008, despite the clear lack of progress towards eliminating support for safe haven for terrorists.

National Significance

As Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen stated that the tribal areas of Pakistan are the likely source of the next attack on the United States. Therefore, working with Pakistan to eliminate the safe havens being provided to terrorist elements in these tribal areas is of paramount importance to United States national security interests. Unfortunately, however, the Bush Administration has relied solely upon the credibility of the Pakistani military, whose will and capability to fight in the tribal areas is questionable at best. This can be clearly seen in the Pakistani military's efforts to strike truce deals with militants in the tribal areas, leaving them to more freely

conduct cross-border attacks against United States and NATO troops in Afghanistan. Instead of working to support the democratic institutions of Pakistan after 9/11, the Bush Administration decided to provide unrelenting support for President Musharraf, which has fomented a new wave anti-American sentiment despite the large amounts of assistance that the United States provides to Pakistan. The continuing lack of a long-term, comprehensive strategy has made the new leadership in Pakistan question our long-term commitment to the region, which has severely undermined Pakistani counter-terrorism cooperation.

SEC. 2041: STRATEGY FOR THE UNITED STATES RELATIONSHIP WITH AFGHANISTAN

Statutory Requirement

Under Section 2041 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53), the President is required "to make increased efforts to (A) dramatically improve the capability and effectiveness of United States and international police trainers, mentors, and police personnel for police training programs in Afghanistan, as well as develop a pre-training screening program; (B) increase the numbers of such trainers, mentors, and personnel only if such increase is determined to improve the performance and capabilities of the Afghanistan civil security forces; and (C) assist the Government of Afghanistan, in conjunction with the Afghanistan civil security forces and their leadership, in addressing the corruption crisis that is threatening to undermine Afghanistan's future." A report on United States efforts to fulfill these requirements was due 180 days after the date of enactment (Feb. 3, 2008) and every 6 months thereafter until September 30, 2010.

Status Update: STILL DIVERTED FROM THE CRISIS IN AFGHANISTAN

United States efforts to increase security in Afghanistan are still woefully inadequate, hobbled by the crippling drain of United States military and financial resources in Iraq. To date, the President has not submitted this report as required under the law.

National Significance

As is stated by Section 2041, "a democratic, stable, and prosperous Afghanistan is vital to the national security of the United States and to combating international terrorism." A key component of providing stability in Afghanistan is to have a functioning police force that can provide security and law enforcement. Of the many challenges Afghanistan faces, the areas in which an effective police force can provide relief include cracking down on rampant corruption, leading efforts of interdiction and eradication for counter-narcotics, and supporting counter-insurgency operations. However, without a professionally trained police force, effective enforcement measures and the provisions of rule of law could be sacrificed. In order to evaluate United States efforts of providing proper training and support for the Afghan police, it is essential to track the progress of our efforts, which is why Congress mandated the report required in

Section 2041. By failing to provide this report (or any other set of comprehensive metrics associated with United States assistance for police training), there is little confidence that we are putting forward the necessary resources or making the best of use of the resources that are being utilized towards this worthy objective.

SEC. 2043: UNITED STATES POLICY TOWARDS SAUDI ARABIA

Statutory Requirement

Section 2043 of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53) provided that it is the policy of the United States "(1) to engage with the Government of Saudi Arabia to openly confront the issue of terrorism, as well as other problematic issues such as the lack of political freedoms; (2) to enhance counterterrorism cooperation with the Government of Saudi Arabia; and (3) to support the efforts of the Government of Saudi Arabia to make political, economic, and social reforms, including greater religious freedom, throughout the country."

Status Update: PROGRESS HAS BEEN SLOW AND UNCERTAIN

Progress with Saudi Arabia on areas of concern to the United States remain slow and halting. On counter-terrorism (including cooperation with the United States), there appears to be meaningful progress. However, Saudi measures to control the flow of funds abroad for extremist purposes are far from adequate – "virtually zero," as one United States Government official privately described these efforts to me. An agency conceived to control these funds – the Saudi National Charities Committee for Relief and Charity Work Abroad – was announced in 2004, but has not yet been set up. Saudi political reform proceeds with minute steps taken at a snail's pace; minority religious rights remain non-existent; and textbook/educational reform has been limited. On two key areas of diplomatic interest to the United States – support for the Iraqi regime and for Palestinian Authority (PA) President Mahmoud Abbas – Saudi Arabia again has done virtually nothing. Its financial support for the PA remains generally at the same level it has been since 2002 (roughly $90 million per year) with occasional, and limited, supplements. Despite promises over the years, it has provided no financial backing for the new Palestinian security forces. Despite occasional encouraging statements, Riyadh has not offered the new Iraqi regime meaningful debt relief, nor has it a designated an ambassador to Baghdad.

National Significance

Saudi Arabia is a critical partner in the Middle East that also has been a major source of terrorist activity and terrorist financing. Without further progress by Saudi Arabia in increased openness, religious moderation, modernization of their educational system and stemming the flow of terrorist financing, many United States goals in the region cannot be accomplished, and United States national security will be at risk.

Similarly, Saudi Arabia's failure to fully support the Palestinian Authority and provide meaningful support for the new regime in Iraq is undermining efforts on these two critical issues.

TITLE XXI: ADVANCING DEMOCRACY AROUND THE WORLD

Statutory Requirement

Under Title XXI of the Implementing Recommendations of the 9/11 Act of 2007 (P.L. 110-53), the Secretary of State was required to establish new democracy liaison officer positions around the world to work regionally and with international organizations to promote democracy, create new strategies for the most difficult countries, advance the work of an Advisory Committee on Democracy Promotion and enhance its publicly available website, provide for greater training in Democracy and Human Rights and increase the incentives for employees to carry out democracy and human rights activities, increase cooperation with other countries, and working on increased funding and improved mechanisms for democracy assistance.

Status Update: KEY ELEMENTS UNMET

Central provisions of P.L. 110-53 such as appointment of democracy liaison officers to regional organizations, dedicated human rights and democracy training, increased incentives such as a State Department-wide award on democracy, and establishment of United States website to provide resources to democracy and human rights activists, all remain unmet at this time.

National Significance

United States efforts to promote democracy and human rights, often on a unilateral basis without consultation with our friends and allies, has led to failures or setback in the Middle East and elsewhere. A more focused effort to coordinate with our allies, to improve the capacity of our diplomats to learn what works and doesn't work and to enhance the ability of those in the State Department committed to this crucial work to do this responsibly is critical to learning from our mistakes and promoting United States values abroad more effectively and more responsibly. Absent implementation of these key elements, democracy and human rights activists will continue to be isolated, promotion of democracy and protection of human rights will remain a backwater at the State Department and we can expect continued failures of fledgling democracies in the future.

ENDNOTES

[1] P.L. 107-306.
[2] P.L. 108-458.
[3] http://www.9-11pdp.org/press/2005-12-05_statement.pdf
[4] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 339.
[9] United States. Government Accountability Office. *AVIATION SECURITY: Secure Flight Development and Testing Under Way, but Risks Should be Managed as System is Further Developed*, GAO-05-356, March 2005,pg. 26.
[10] United States. Government Accountability Office. *TRANSPORTATION SECURITY: Efforts to Strengthen Aviation and Surface Transportation Security Continue to Progress, but More Work Remains*, GAO-08-651T, 15 April 2008, pg. 8.
[11] United States. Cong. House. Committee on Homeland Security. *Moving Beyond the First Five Years: How can the Transportation Security Administration ensure that it will continue to enhance security for all modes of transportation?* 15 April. 2008. 110th Cong., 2nd sess.
[12] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004.
[13] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004, pg 393.
[14] United States. Cong. House. Committee on Homeland Security. *Moving Beyond the First Five Years: How can the Transportation Security Administration ensure that it will continue to enhance security for all modes of transportation?* 15 April. 2008. 110th Cong., 2nd sess.
[15] United States. Cong. House. Committee on Homeland Security. *The Next Step in Aviation Security—Cargo Security: Is DHS Implementing the Requirements of the 9/11 Law Effectively?* 15 July 2008. 110th Congress, 2d sess.
[16] Congressional Research Service. *Aviation Security: Background and Policy Options for Screening and Securing Air Cargo*, 25 February 2008, pg 41.
[17] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004, pg 225.
[18] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 392.
[19] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 393.
[20] Crowly, P.J. & Bruce Butterworth. "Keeping Bombs Off Planes: Securing Air Cargo, Aviation Security Soft Underbelly". *Center for American Progress*, May 2007, available at http://www.americanprogress.org/issues/2007/05/air_cargo.html. Last accessed on 05 September 2008.
[21] United States. Cong. House. Hawley, Kip. Letter to Chairman Thompson and the House Committee on Homeland Security re Section 1617 of P.L. 110-53, 21 August 2008. 110th Cong. 2nd sess..
[22] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004, pg. 391.
[23] "Crash at the White House: The Pilot." *The New York Times*, 13 September 1994, p. 20.
[24] Chachere, Vickie. "Police: Student pilot who crashed Cessna into Florida building inspired by bin Laden." *Associated Press Newswires*, 7 January 2002.
[25] Morris, Mike. "Buford Man, 22, Accused of Stealing Jet." *The Atlanta Journal-Constitution*, 12 October 2005.
[26] The National Strategy is to be based upon previous and ongoing security assessments conducted by the Department of Homeland Security and the Department of Transportation.
[27] United States. Cong. House Briefing with Committee on Homeland Security Staff, 26 August 2008. 110th Cong. 2nd sess.
[28] United States Department of Homeland Security. *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan* , May 2007, available at http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf. Last accessed on 05 September 2008.

[29] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 391.
[30] "Amtrak Ridership Flying High: Soaring Sales for the Heartland Flyer Train," *Amtrak News Release*, 18 August 2008, available at http://www.amtrak.com/servlet/ContentServer?pagename=Amtrak/am2Copy/News_Release_Page&c=am2Copy&cid=1178294200218&ssid=180. Last accessed on 05 September 2008.
[31] "Metrorail breaks its all-time monthly ridership record," *WMATA Press Release*, 7 August 2008, available at http://www.wmata.com/about/MET_NEWS/PressReleaseDetail.cfm?ReleaseID=2223. Last accessed on 05 September 2008.
[32]Murray, Lynn, Ed. "Mitigating the Consequences of Accidents," *The Volpe Journal 2005: Transportation and Safety, Volpe National Transportation Systems Center*, 2005. available at : http://www.volpe.dot.gov/infosrc/journal/2005/mitigate.html#top. Last accessed 28 August 2008.
[33] United States. Cong. House. Subcommittee on Transportation Security and Infrastructure Protection of the Committee on Homeland Security, *Testimony submitted by James C. Little*, 13 February 2007, 110th Cong. 1st sess..
[34] United States. Cong. Senate. Committee on Homeland Security and Governmental Affairs, *Testimony submitted by Rafi Ron*, 21 September 2005, 109th Cong. 1st sess..
[35] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 392.
[36] United States. Cong. House. Hawley, Kip. Letter to Chairman Thompson and the House Committee on Homeland Security re Section 1511 of P.L. 110-53, 09 May 2008. 110th Cong. 2nd sess.
[37] United States Department of Homeland Security. *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan* , May 2007, available at http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf. Last accessed on 05 September 2008.
[38] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 391.
[39] The Secure Freight Initiative Pilot was required by Section 231 of the Security and Accountability for Every (SAFE) Port Act of 2006.
[40] Secretary of Homeland Security Michael Chertoff. Press release. "Remarks by Homeland Security Secretary Michael Chertoff at the Eighth Annual U.S. Customs and Border Protection 2007 Trade Symposium" 15 November 2007, available at http://www.dhs.gov/xnews/speeches/sp_1195225858995.shtm. Last accessed on 05 September 2008 .
[41] United States. Customs and Border Protection. *Report to Congress on Integrated Scanning System Pilots (Security and Accountability for Every Port Act of 2006, Section 231)*. 12, June 2008.
[42] Secretary of Homeland Security Michael Chertoff. Press release. "Remarks by Homeland Security Secretary Michael Chertoff at Brookings on the Nation's Critical Infrastructure, 5 September 2008, available at http://www.dhs.gov/xnews/speeches/sp_1220876790967.shtm. Last accessed on 05 September 2008.
[43] Meade, Charles & Roger C. Molander. "Considering the Effects of a Catastrophic Terrorist Attack" *RAND Corp*. 2006, available at http://www.rand.org/pubs/technical_reports/2006/RAND_TR391.pdf. Last accessed on 05 September 2008.
[44] Id.
[45] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 190.
[46] Staffers from the House Committee on Homeland Security requested a definition during a meeting with Department of Homeland Security officials on June 12, 2008. Staffers followed up this request at subsequent meetings. On August 5, 2008, Chairman Thompson from the House Committee on Homeland Security sent a letter to Secretary Chertoff requesting a definition. The Secretary has failed to respond to the Chairman's request.
[47] The VWP allows nationals from certain countries to enter the United States as temporary visitors for business or pleasure without first obtaining a visa from a U.S. consulate abroad. The VWP constitutes one of a few exceptions under the Immigration and Nationality Act in which foreign nationals are admitted into the United States without a valid visa.
[48] A visa is refused or denied if an applicant cannot establish his or her eligibility to enter the United States, either because the application does not meet the requirements of an established visa category or because there are grounds for ineligibility based on other aspects of the case. A visa refusal is the formal denial of a

nonimmigrant visa application by a U.S. consular officer acting pursuant to the Immigration and Nationality Act. Currently, a nation's visa refusal rate is used to determine whether it is eligible to participate in the VWP.

[49] Federal Register Vol. 73, No. 111, 9 June 2008, available at: http://www.cbp.gov/linkhandler/cgov/travel/id_visa/esta/visa_waiver_changes.ctt/visa_waiver_changes.pdf . Last accessed on 05 September 2008.

[50] United States Customs and Border Protection. *Visa Waiver Program Traveler: Introducing the Electronic System for Travel Authorization*, June 2008, available at http://www.cbp.gov/linkhandler/cgov/travel/id_visa/esta/esta_tear_sheet.ctt/esta_tear_sheet.pdf. Last accessed on 05 September 2008.

[51] United States Customs and Border Protection. *Frequently Asked Questions About ESTA.* August 2008, available at: http://www.cbp.gov/xp/cgov/travel/id_visa/esta/esta_faq.xml. Last accessed on 05 September 2008.

[52] United States. Government Accountability Office. *Border Security: State Department Should Plan for Potentially Significant Staffing and Facilities Shortfalls Caused by Changes in the Visa Waiver Program*, GAO-08-623, 22 May 2008.

[53] United States. Government Accountability Office. *Prospects for Biometric US-VISIT Exit Capability Remain Unclear*, GAO-07-1044T, 28 June 2007.

[54] United States Department of Homeland Security. *Privacy Impact Assessment for the Electronic System for Travel Authorization (ESTA)*. 02 June 2008, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_esta.pdf. Last accessed on 05 September 2008.

[55] United States. Cong. House. Subcommittee on Oversight and Investigations of the Committee on International Relations, *Visa Overstays: Can We Bar the Terrorist Door?* 109th Congress.

[56] 9/11 Commission. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. 2004.

[57] P.L. 110-53 § 511(d).

[58] Id.; staff notes from staff briefings with representatives from Office of the Under Secretary for Intelligence and Analysis (Feb. 8, 2008; March 14, 2008; April 11, 2008; May 9, 2008; June 27, 2008; Aug. 8, 2008).

[59] P.L. 110-53 § 511(d).

[60] United States Department of Justice and Department of Homeland Security. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* August 2006, available at http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf. Last accessed on 05 September 2008.

[61] These reports are prepared by I&A's "Critical Infrastructure Threat Assessment" Division.

[62] "Enhancing DHS Information Support to State and Local Fusion Centers: Results of the Chief Intelligence Officer's Pilot Project and Next Steps", *CENTRA Technology, Inc.*, 20 February 2008.

[63] Id.

[64] Id. at 13.

[65] Among the potential dangers identified by the ACLU are ambiguous lines of authority that could lead to fusion center "policy shopping" when applying Federal, State or local law as a part of their analysis work; abuse by private sector players at fusion centers; military participation at fusion centers that could lead to violations of *Posse Comitatus*; data mining activity that could threaten privacy; and excessive secrecy and a lack of transparency in the fusion center process itself. See, German, Michael & Jay Stanley. "What's Wrong With Fusion Centers?" *American Civil Liberties Union* December 2007 at 9-21; "ACLU Says Fusion Centers Remain Problematic", *States News Service*, 17 April 2008; Bain, Ben, "A New Threat, a New Institution: the Fusion Center", *FCW.com*, 18 February 18, 2008.

[66] Shorrock, Tim. "America Under Surveillance," *Salon.com*, 09 August 2007); Bain, Ben. "Confusion Over Fusion Centers", *FCW.com*, 08 October 2007. (EPIC criticizing lack of fusion center guidance and transparency).

[67] Harper, Jim. "Fusion Centers: Leave 'Em to the States," *CATO Institute*, 13 March 2007.

[68] United States Department of Homeland Security. *Fiscal Year 2008 Homeland Security Grant Program*, 2008, available at http://www.fema.gov/pdf/government/grant/hsgp/fy08_hsgp_guide.pdf. Last access on 05 September 2008.

[69] Id.

[70] Id.

[71] United States Department of Homeland Security. Grant *Programs Directorate Information Bulletin No. 288*, 25 April 2008, available at http://www.ojp.usdoj.gov/odp/docs/info288.pdf. Last accessed on 05 September 2008.
[72] Office of the Director of National Intelligence. "Second National Fusion Center Conference Held to Foster Greater Collaboration." Press Release. 20 March 2008, available at http://www.dhs.gov/xnews/releases/pr_1206047160541.shtm. Last accessed on 05 August 2008.
[73] Id.
[74]Congressional Research Service. *Fusion Centers: Issues and Options for Congress*, 06 July 2007 at CRS-44 (describing "sustainment funding" as "funding which is provided annually, on a sustained basis, to fusion centers to support personnel costs and information connectivity, among other functions").
[75] President George W. Bush, *National Strategy for Information Sharing* Oct. 2007, available at http://www.whitehouse.gov/nsc/infosharing/index.html. Last accessed on 05 September 2008.
[76] Jason Hancock, "Iowa's Intelligence Fusion Center Connects the Dots," *Iowa Independent*, 29 July 2008; available at http://iowaindependent.com/2983/iowas-intelligence-fusion-center-connects-the-dots; Ben Bain, "Funding Worries Fusion Center Officials," *FCW.com*, 21 April 2008, available at http://www.fcw.com/online/news/152306-1.html; Eileen Sullivan, "Intel Centers Losing Anti-Terror Focus," *Associated Press*, 20 (November 2007), available at http://www.foxnews.com/wires/2007Nov29/0,4670,IntelligenceCenters,00.html; Bruce Finley, "Funding for Colorado Intel Center May Die," *DenverPost.com*, 13 August 2006), available at http://www.denverpost.com/nationworld/ci_4175196. All last accessed on 05 September 2008.
[77] United States Department of Homeland Security. *Data Mining Report: DHS Privacy Office Response to House Report 109-669* 06 July 2007.
[78] United States Department of Homeland Security. *Letter Report Pursuant to Section 804 of the Implementing Recommendations of the 9/11 Commissions Act of 2007*, 11 February 2008.
[79] United States Department of Homeland Security. *Data Mining Report: DHS Privacy Office Response to House Report 108-774*, 26 July 2006.
[80] *Id*, note 1.
[81] Congressional Research Service. *Data Mining and Homeland Security: An Overview*, 03 April 2008.
[82] The Multistate Anti-Terrorism Information Exchange Pilot Project (MATRIX), was cancelled in April 2005 after the Department expended $8 million because "the MATRIX pilot project lost public support because it failed to consider and adopt comprehensive privacy protections from the beginning." *See* United States Department of Homeland Security. *DHS Report to the Public Regarding the Multistate Anti-terrorism Information Exchange Pilot Project*, December 2006.
[83] In August 2004, the Department cancelled the $100 million Computer Assisted Passenger Prescreening System II (CAPPS II) program because issues regarding privacy concerns were unresolved. See United States Government Accountability Office, *Aviation Security: Computer-Assisted Prescreening System Faces Significant Implementation Challenges*, GAO-04-385, February 2004.
[84] The Analysis, Dissemination, Visualization, Insight and Semantic Enhancement program, otherwise known as ADVISE, funded and managed by the Department of Homeland Security Science and Technology Directorate (S&T), cost the Department $42 million prior to being canceled due to privacy concerns. *See* United States Department of Homeland Security, Office of Inspector General. *ADVISE Could Support Intelligence More Effectively*, OIG-07-56, June 2007.
[85] Section 1802 of the Post-Katrina Emergency Management Reform Act of 2006 (P.L. 110-295).
[86] 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." See, P.L. 108-458 § 7303(g)(1).
[87] P.L. 110-161
[88] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 397.
[89] Figures provided by the Department of Homeland Security – current as of July 9, 2008.
[90]National Protection and Programs Directorate, Office of Emergency Communications, and the Federal Emergency Management Agency, Grant Programs Directorate. *Interoperable Emergency Communications Grant Program: Program Guidance and Application Kit,* 18 June 2008, pg 2.

[91] United States Department of Justice, Office of State and Local Government Coordination Preparedness. *ICTAP Interoperable Communications Equipment Survey*, July 2005, available *at* www.ojp.usdoj.gov/odp/docs/ICTAPJuly05Bulletin_att.pdf . Last accessed 09 March 2007.
[92]United States. Cong. House. Subcommittee on Telecommunications of the Committee on Energy and Commerce *Protecting Homeland Security: A Status Report on Interoperability Between Public Safety Communications Systems.* 23 June 2004 108th Cong.
[93] United States House of Representatives Report 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, available at http://www.gpoaccess.gov/serialset/creports/katrina.html. Last accessed on 05 September 2008.
[94] *International Association of Fire Fighters Legislative Conference*, Mar. 21, 2006 (Remarks by Michael Chertoff, Secretary, Department of Homeland Security).
[95] United States Federal Emergency Management Agency. *Resource Management: Credentialing*, 07 June 2007, available at http://www.fema.gov/emergency/nims/rm/credentialing.htm. Last accessed on 05 September 2008.

[96] United States. Cong. House. Subcommittee on Emergency Communications, Preparedness, and Response of the Committee on Homeland Security,: *Leveraging the Private Sector to Strengthen Emergency Preparedness and Response*, 19 July 2007 110th Cong, 1st Sess.
[97] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg. 317
[98]United States Senate Report 109-322, 375. *Hurricane Katrina, A Nation Still Unprepared: Special Report of the Committee on Homeland Security and Governmental Affairs.*2006, Pg 417.
[99] United States Department of Homeland Security: *National Biosurveillance Integration System and the National Biosurveillance Integration Center*. Brief for House Homeland Security Staff, June 2008.
[100] MOUs are in place with the following Federal agencies: USDA, HHS, DOT, DOD, and DOI.
[101] United States Department of Homeland Security: *Interim Report on the Status of the Operations at The National Biosurveillance Integration Center (NBIC)*, February 2008.
[102] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 102.
[103] Dr. Michael Osterholm, University of Minnesota School of Public Health, presentation to House Members and Staff, 18 October 2005.
[104] United States Department of Homeland Security. *Critical Infrastructure Sector Partnership*, 01 May 2008, available at http://www.dhs.gov/xprevprot/partnerships/editorial_0206.shtm. Last accessed on 05 September 2008.
[105]United States Department of Homeland Security, *Voluntary Private Sector Preparedness Accreditation and Certification Program* Briefing to Congress, 30 May 2008.
[106] *Id*.
[107] 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. 2004. pg 397-398.
[108] *Id*. at 398.
[109] *Id*.
[110] P.L. 110-53.
[111] Congressional Research Service. *Critical Infrastructure: The National Asset Database*. 17 August 2007.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK