

Report on the Status of 9/11 Commission Recommendations

Part I: Homeland Security, Emergency Preparedness and Response

RECOMMENDATION	STATUS	NEXT STEPS
----------------	--------	------------

EMERGENCY PREPAREDNESS AND RESPONSE

Provide adequate radio spectrum for first responders	Minimal Progress	Congress
Establish a unified Incident Command System	Minimal Progress	Local, State, Federal
Allocate homeland security funds based on risk and vulnerability	Minimal Progress	Congress
National critical infrastructure risks and vulnerabilities assessment	Unsatisfactory	Executive
Private sector preparedness	Minimal Progress	Private Sector

TRANSPORTATION SECURITY

National Strategy for Transportation Security	Unsatisfactory	Executive
Improve airline passenger pre-screening	Unsatisfactory	Executive
Improve airline screening checkpoints to detect explosives	Minimal Progress	Executive & Congress
Checked bag and cargo screening	Minimal Progress	Executive & Congress

BORDER SECURITY

Better terrorist travel intelligence	Some Progress	Executive
Comprehensive screening system, including borders and transportation	Minimal Progress	Executive
Biometric entry-exit screening system	Some Progress	Executive & Congress
International collaboration on borders and document security	Unsatisfactory	Executive & Congress
Standardize secure identifications	Some Progress	Executive, States

Emergency Preparedness and Response

PROVIDE ADEQUATE RADIO SPECTRUM FOR FIRST RESPONDERS

“Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, DC, should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.” (p. 397)

Grade: **MINIMAL PROGRESS**

What has happened: Legislation to provide radio spectrum for first responders has been introduced in the House and Senate. The National Association of Broadcasters has announced that it will not oppose pending legislation to reallocate a portion of the analog broadcast spectrum to first responders.

Why this is still important: On 9/11, inadequate radio spectrum hindered first responder communications. New spectrum is needed to facilitate interoperable communications between responder agencies; to allow effective radio communications during large-scale responses to major disasters; and to allow emergency response agencies to deploy next-generation communications technologies.

How to fix it: Pending legislation before Congress would compel the return of the analog broadcast spectrum and its reallocation, including for public safety purposes, on various dates. Congress should use the “reconciliation” process, or another legislative vehicle, to mandate this reallocation by the earliest possible date.

ESTABLISH A UNIFIED INCIDENT COMMAND SYSTEM

“Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. ... In the future, the Department of Homeland Security should consider making funding contingent on aggressive and realistic training in accordance with ICS and unified command procedures.” (p. 397)

Grade: **MINIMAL PROGRESS**

What has happened: Many fire and police departments and state and local authorities are already well versed in using the ICS—others are being trained in it. Hurricane Katrina demonstrates a major failure: the absence of unified command.

Why this is still important: In the event of terrorist attack or natural disaster, clear lines of command and control for responding authorities are essential to minimize civilian and responder casualties.

How to fix it: The Department of Homeland Security set the deadline for full Incident Command System compliance “to the maximum extent possible” as October 1, 2004. The hard deadline for full compliance as a condition for federal preparedness funds is October 1, 2006. This date must not slip. All jurisdictions must train and exercise the Incident Command System as it applies to them.

ALLOCATE HOMELAND SECURITY FUNDS BASED ON RISK AND VULNERABILITY

“Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. Washington, D.C., and New York City are certainly at the top of any such list. We understand the contention that every state and city needs to have some minimum infrastructure for emergency response. But federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks and vulnerabilities that merit additional support. Congress should not use this money as a pork barrel.” (p. 396)

Grade: **MINIMAL PROGRESS**

What has happened: Congress has considered, but has not yet sent to the President, legislation to overhaul the homeland security grant program.

Why this is still important: Preventing terrorist attacks is a matter of national security. Federal resources are scarce in proportion to the number of potential targets. Congress and the Administration must set priorities based on the risk, vulnerability, and consequences of an attack on a given site.

How to fix it: The administration’s FY 2006 budget proposal was a positive step forward. Congress should now act to ensure that all federal homeland security assistance is allocated based on an assessment of risk and vulnerability—not as general revenue sharing. The House has overwhelmingly passed a very good bipartisan bill; the Senate has passed a reform amendment as well. The two bodies should come together and produce a bill for the President’s signature that distributes dollars based on risk. This can and should happen before the end of the First Session of the 109th Congress.

NATIONAL CRITICAL INFRASTRUCTURE RISKS AND VULNERABILITIES ASSESSMENT

“The Department of Homeland Security and its oversight committees should regularly assess the types of threats the country faces to determine (a) the adequacy of the government’s plans—and the progress against those plans—to protect America’s critical infrastructure and (b) the readiness of the government to respond to the threats that the United States might face.” (p. 428)

Grade: **UNSATISFACTORY**

What has happened: The Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458) required DHS to issue a report by June 15, 2005, assessing the risks and vulnerabilities of the nation’s critical infrastructure. This report has not yet been released.

Why this is still important: Regular national assessments of threat, vulnerability, and preparedness will ensure that government efforts are making measurable progress in reducing the overall terrorist threat.

How to fix it: DHS should produce the report required by PL 108-458 as soon as possible, and demonstrate its capability to regularly review and modify the assessment to reflect the changing threat environment and state of readiness.

PRIVATE SECTOR PREPAREDNESS

“We endorse the American National Standards Institute’s recommended standard for private preparedness...and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company’s compliance with the ANSI standard in assessing its insurability and creditworthiness.” (p. 398)

Grade: **MINIMAL PROGRESS**

What has happened: In a May 2005 speech to private sector representatives, Secretary Chertoff correctly noted that preparedness is not solely a government responsibility. The insurance and credit-rating industries are beginning to incorporate national preparedness standards into their underwriting and risk-analysis criteria. Leaders in the legal profession are beginning to evaluate the National Preparedness Standard as a “legal standard of care.” Still, awareness of the Standard throughout the corporate sector is low.

Why this is still important: The terrorists have repeatedly targeted private sector assets. In another attack and in any natural disaster, private-sector employees will likely again be on the front lines. As the 9/11 Commission Report showed, employees of enterprises that institutionalize a high level of emergency preparedness are far more likely to survive in a disaster.

How to fix it: Corporate leaders should take the lead in encouraging all American businesses, especially those in high-risk areas, or who own critical national infrastructure, to incorporate National Preparedness Standards into their business practices. DHS should make private-sector preparedness a higher priority. The insurance and credit-rating industries should incorporate the National Preparedness Standard into their evaluations.

Transportation Security

NATIONAL STRATEGY FOR TRANSPORTATION SECURITY

“The U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (federal, state, regional, and local), and to private stakeholders.” (p. 391)

Grade: UNSATISFACTORY

What has happened: The Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458) required DHS to prepare a National Strategy for Transportation Security, due April 1, 2005.

Why this is still important: With limited resources available for transportation security, resources must be allocated according to rational, risk-based priorities. Without a comprehensive assessment of the security needs of the nation’s transportation system, this will be impossible.

How to fix it: DHS must produce this report as soon as possible, and maintain a capability to review and modify the assessment to reflect the changing threat environment and state of transportation security.

IMPROVE AIRLINE PASSENGER PRE-SCREENING

“Improved use of ‘no-fly’ and ‘automatic selectee’ lists should not be delayed while the argument about a successor to CAPPs continues. This screening function should 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.” (p. 393)

Grade: UNSATISFACTORY

What has happened: Contrary to the Commission recommendation, the TSA test program is combining watchlist screening with the use of commercial databases to verify passenger identities, which has produced controversy over privacy issues. This has delayed completion of the testing phase. TSA now hopes to begin operation of the new system in late 2005 or early 2006.

Why this is still important: With the airlines still responsible for implementing the “no fly” and “automatic selectee” lists, the names of many known or suspected terrorists are still not being included on these lists, making airline passengers less secure than they should be.

How to fix it: As recommended by the Commission and mandated by PL 108-458, TSA should focus its priority attention on taking over implementation of passenger pre-screening so that all names on the consolidated terrorist watch list are utilized.

IMPROVE AIRLINE SCREENING CHECKPOINTS TO DETECT EXPLOSIVES

“The TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. As a start, each individual selected for special screening should be screened for explosives. Further, the TSA should conduct a human factors study, a method often used in the private sector, to understand problems in screener performance and set attainable objectives for individual screeners and for the checkpoints where screening takes place.” (p. 393)

Grade: MINIMAL PROGRESS

What has happened: The Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458) required DHS to develop and deploy effective checkpoint explosives and WMD detection equipment, to screen all selectees and their carry-on property for explosives, and to report to Congress within 180 days on the results of any human factors study it has conducted. TSA has deployed explosives trace detection devices at all airports to examine selectees’ carry-on items, and installed explosives detection trace portals (“puffers”) at 17 airports (with seven more airports due for installation in the near future) to scrutinize the persons of selectees. After the suicide bombing of Russian commercial aircraft in August 2004, TSA stepped up the use of “pat-down” searches for explosives, but after privacy-related protests it took steps to reduce the intrusiveness of these searches. While TSA has indicated that human factors analysis is being carried out at a Research & Development facility in Atlantic City and elsewhere, it has not yet submitted to Congress the report required by statute.

Why this is still important: Following improvements in on-board defenses against suicide hijacking, explosives currently represent the major security threat to passenger aviation.

How to fix it: Congress needs to provide the funding for, and TSA needs to move as expeditiously as possible with, the installation of explosives detection trace portals at more of the nation’s 441 commercial airports, while both continue to support the development of more advanced screening technology. Furthermore, until such time as the trace portals, or more effective successors, are fully deployed, TSA must utilize other means (including the canine teams and “pat-down” searches) to insure that selectees are searched for explosives, no matter what airport they fly from.

CHECKED BAG AND CARGO SCREENING

“More attention and resources should be directed to reducing or mitigating the threat posed by explosives in vessels’ cargo holds. The TSA should expedite the installation of advanced (in-line) baggage screening equipment. Because the aviation industry will derive substantial benefits from this deployment, it should pay a fair share of the costs. The TSA should require that every passenger aircraft carrying cargo must deploy at least one hardened container to carry any suspect cargo. TSA also needs to intensify its efforts to identify, track, and appropriately screen potentially dangerous cargo in both the aviation and maritime sectors.” (p. 393)

Grade: MINIMAL PROGRESS

What has happened: The Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458) incorporated the Commission’s recommendations for deployment of “in-line” screening equipment, converted the hardened container requirement into a pilot program, and established a detailed program for air cargo security. In response, TSA does not appear to have expedited its plans for in-line installation, with just nine operational systems and eight more under construction as of mid-2005. There has been little progress on the hardened container pilot project. The agency’s air cargo security efforts have centered on a slow-moving regulatory proceeding. Efforts by the Department of Homeland Security’s Custom and Border Protection (CBP) division have improved upon the pre-9/11 state of maritime cargo security, yet these programs have received relatively little funding. The Government Accountability Office, among others, has documented continuing problems in each of them.

Why this is still important: Deployment of in-line explosives detection equipment has been shown to improve security and to significantly reduce operational costs. Air and maritime cargo continue to be very vulnerable to terrorist attack.

How to fix it: The main impediment to improved checked bag and cargo security is inadequate funding. If the Congress and the administration believe these to be priorities, they must determine the costs and specify how they will pay for these improvements.

Border Security

BETTER TERRORIST TRAVEL INTELLIGENCE

“The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.” (9/11 Report, p. 385)

Grade: SOME PROGRESS

What has happened: The National Counterterrorism Center, the Human Smuggling and Trafficking Center, and representatives of multiple government agencies are jointly developing the first terrorist travel strategy. They are taking steps to integrate terrorist travel intelligence into border operations.

Why this is still important: As terrorists move across international borders to meet, train, and carry out their operations, they make themselves vulnerable to detection and interdiction. Targeting terrorist travel can help detect terrorists and help prevent attacks.

How to fix it: The U.S. government must develop and implement a long-term terrorist travel strategy, comparable to the multi-faceted strategies currently directed at terrorist finance and terrorist communications. Completing a terrorist travel strategy (and report) in December 2005 is the first major benchmark. What to look for: Progress in implementing a program to screen travel documents for terrorist indicators.

COMPREHENSIVE SCREENING SYSTEM

“The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with systemwide goals in mind.” (p. 387)

Grade: MINIMAL PROGRESS

What has happened: Presidential Homeland Security Directive 11 (August 27, 2004), announced a new U.S. policy to “implement a coordinated and comprehensive approach to terrorist-related screening—in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure -- that supports homeland security, at home and abroad.” A working group developed an implementation plan, and Secretary Chertoff has announced the establishment of a new Screening Coordination Office at DHS.

Why this is still important: Having too many different biometric standards, travel facilitation systems, credentialing systems, and screening requirements hampers the development of information crucial for stopping terrorists from entering the country. It is also expensive and inefficient. A coordinating body should raise standards, facilitate information-sharing, and survey systems for potential problems.

How to fix it: The Screening Coordination Office should set standards and break down bureaucratic stovepipes that prevent the match-up of information. Goals need to be set and implemented for resolving differences in biometric systems, traveler systems, and credentialing and identification standards.

BIOMETRIC ENTRY-EXIT SCREENING SYSTEM

“The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers. It should be integrated with the system that provides benefits to foreigners seeking to stay in the United States.” (p. 389)

Grade: **SOME PROGRESS**

What has happened: The US-VISIT system is running at 115 airports and 15 seaports, and is performing secondary screening at the 50 busiest land borders. A plan exists to equip all land borders by the end of the year, though it is not likely to be completed on time. The exit component of the system has not been widely deployed. The numerous border screening systems operated by DHS, including US-VISIT, are not yet interoperable.

Why this is still important: It is imperative for national security that the government knows who is coming into our country, can effectively verify identities, establishes how long people are here, and when they leave.

How to fix it: Continuing to build this system, developing and deploying the exit component of US-VISIT, and making entry-exit and immigration benefits systems interoperable, should remain top priorities for DHS.

INTERNATIONAL COLLABORATION ON BORDERS AND DOCUMENT SECURITY

“We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long-term through extensive international cooperation.” (p. 390)

Grade: **UNSATISFACTORY**

What has happened: Terrorist watchlists—the most basic tool of border control—need to be shared. More information should be shared with a greater number of allies. The U.S. is not moving to include fingerprints in passports and therefore is not taking a leadership role in passport security.

Why this is still important: The U.S. government does not have complete information on terrorist identities; much information is held by foreign governments. U.S. security will be greatly strengthened by access to this information and the help of other governments in interdicting terrorist travel. If terrorists are to enter, prepare for and carry out operations in the United States, they need travel documents. International collaboration on document standards and security is needed to ensure that foreign travelers’ documents are legitimate and secure, and to keep out suspected terrorists.

How to fix it: Watchlist sharing must be a higher priority, and it needs a systematic diplomatic effort. Congress should make fingerprints in passports a priority.

STANDARDIZE SECURE IDENTIFICATIONS

“The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses.” (p. 390)

Grade: **SOME PROGRESS**

What has happened: The Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458) started a regulatory process to establish standards for state-issued ID’s acceptable for federal purposes. The REAL ID Act (PL 109-13) superseded this regulatory process and established these standards by statute. The fragmented and insecure system of birth certificate issuance has not yet been addressed. The Intelligence Reform Act requires the administration to issue new standards by December 2005.

Why this is still important: Birth certificate security is critical to preventing fraud in the acquisition of U.S. passports and other identification, such as drivers' licenses. Drivers' license issuance affects terrorist mobility and presents an opportunity to screen terrorists.

How to fix it: Congress will need to monitor states' compliance with the REAL ID Act. Congress should insist on the issuance of new birth certificate standards by December 2005, as required by PL 108-458.

###