9/11 Commission Recommendations: Implementation Status

/name redacted/
Specialist in International Security

December 4, 2006

Congressional Research Service
7-....
www.crs.gov
RL33742

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

This report provides a review of the 9/11 Commission recommendations and the status of their implementation at the end of the 109th Congress. The discussions herein are organized on the basis of policy themes that are at the core of the 9/11 Commission's recommendations, rather than through a review of each numbered item set out in the Commission's final report. The analysis was produced by a large team of CRS Specialists, analysts, and attorneys who are responsible for the wide variety of policy areas covered by the 9/11 Commission in its work. The authors of the varied segments of this report are identified in footnotes. Each section of the report summarizes the pertinent elements of the 9/11 Commission's recommendation relevant to the section's policy theme. Then a review is made of responses made by the Congress to implement, in whole or in part, the given recommendation. Where appropriate, notice is taken of Executive branch actions regarding the policy matter. A detailed table of contents provides the reader with a guide to each of the policy themes discussed. Footnotes in each section of the report provide references to more detailed information on particular topics related to each policy theme.

This report will only be updated if circumstances warrant.

Contents

Introduction 1
Strengthening the Intelligence Function 1
Commission Concerns and Recommendations 1
Congressional Responses 1
Intelligence Oversight: Congressional Options 2
Commission Concerns and Recommendations 2
Congressional Responses 3
Improving Transitions Between Administrations 4
Commission Concerns and Recommendations 4
Congressional Responses 5
Enacted Provisions 5
Related Potential Congressional Concerns for the 110th 8
Afghanistan and Terrorism 9
Commission Concerns and Recommendations 9
Congressional Responses 10
Future Considerations 11
Pakistan and Terrorism 11
Commission Concerns and Recommendations 11
Congressional Responses 12
Foreign Assistance 12
Coalition Support Funds 13
Saudi Arabia and Terrorism 13
Commission Concerns and Recommendations 13
Congressional Responses 14
Provisions Enacted 14
Related Options Also Considered 15
Terrorism: Its Global Dimensions 15
Commission Concerns and Recommendations 15
Congressional Responses 16
Legislation Enacted 16
Policy Concerns Not Addressed or Postponed 16
Islam and U.S. Policy 17
Commission Concerns and Recommendations 17
Congressional Responses 17
Policy Concerns Not Addressed 18
Radical Islam in Europe 18
Islam in Politics 19
Terrorism: U.S. Policy Instruments 19
Commission Concerns and Recommendations 19
Congressional Responses 19
Public Diplomacy, Education and Exchange Programs 20
Commission Concerns and Recommendations 20
Congressional Response 20
Terrorist Financing 22

Commission Concerns and Recommendations....22
Congressional Responses....23
U.S. Military Forces and the War on Terrorism....24
Commission Concerns and Recommendations....24
Congressional Responses....25
Relevant Provisions Enacted by Congress....25
Policy Concerns Not Addressed....25
Options Considered by the 109th Congress....25
Weapons of Mass Destruction: Proliferation Security and Threat Reduction....26
Commission Concerns and Recommendations....26
Congressional Responses....26
Border Security and Immigration....27
Terrorist Travel....27
Commission Concerns and Recommendations....27
Congressional Response....28
Terrorist Screening and Watch Lists....29
Commission Concerns and Recommendations....29
Congressional Response....29
Related Administrative Response....29
Biometric Screening System and Data Systems Integration....31
Commission Concerns and Recommendations....31
Congressional Responses....31
Standards for Identification Documents....32
Commission Concerns and Recommendations....32
Congressional Response....32
Other Immigration Concerns....33
Commission Concerns....33
Congressional Response....33
Transportation Security....35
Aviation Security....35
Commission Concerns and Recommendations....35
Congressional Response....36
Policy Concerns Not Addressed In Enacted Legislation....40
Port and Maritime Security....41
Commission Concerns and Recommendations....41
Congressional Response....41
Surface Transportation Security....43
Commission Concerns and Recommendations....43
Status of Implementation of the Recommendations....43
Critical Infrastructure Security....44
Commission Concerns and Recommendations....44
Congressional Responses....45
Emergency Preparedness and Response and the 9/11 Commission....46
Commission Concerns and Recommendations....46
Congressional Responses....47
Department of Defense and the 9/11 Commission....49
Commission Concerns and Recommendations....49
Congressional Responses....50

Homeland Security Oversight: Congressional Options 50
Commission Concerns and Recommendations 50
Congressional Responses 50
Civil Liberties and Government Information Policies and Practices 51
Driver's Licenses, Personal Identification Cards, Birth Certificates, and Social Security Numbers 51
Commission Concerns and Recommendations 51
Congressional Responses 51
Future Considerations 53
Protection of Civil Liberties 54
Commission Concerns and Recommendations 54
Congressional Responses 55
Balancing Security and Information Sharing 57
Commission Concerns and Recommendations 57
Congressional and Administrative Responses 57
DHS Reorganization Related to Information Sharing 61

Contacts

Author Contact Information 62

Introduction

This report provides a review of the 9/11 Commission recommendations and the status of their implementation at the end of the 109th Congress. It is intended to provide a structured road map to this end. The discussions herein are organized on the basis of policy themes that are at the core of the 9/11 Commission's recommendations, rather than a review of every numbered item set out in the Commission's final report. The analysis was produced by a large team of CRS Specialists, analysts, and attorneys who are responsible for the wide variety of policy areas covered by the 9/11 Commission in its work. The authors of the varied segments of this report are identified in footnotes. Each section of the report summarizes the pertinent elements of the 9/11 Commission's recommendations relevant to that section's policy theme. Then a review is made of responses made by the Congress to implement, in whole or in part, the given recommendation. Where appropriate, notice is taken of executive branch actions regarding the policy matter. A detailed table of contents provides the reader with a guide to each of the policy themes discussed. Footnotes in each section of the report provide references to more detailed information on particular topics related to each policy theme.

Strengthening the Intelligence Function[1]

Commission Concerns and Recommendations

The 9/11 Commission concluded that the organization of the U.S. Intelligence Community had contributed to a failure to develop a management strategy to counter Islamic terrorism. The Commission recommended a major reordering of the Intelligence Community to enable a single official to manage the entire national intelligence effort and oversee the agencies that contribute to it. The Commission also recommended the establishment of national intelligence centers, including a National Counterterrorism Center (NCTC), to correlate and analyze information from all sources on particular topics.

A principal recommendation of the Commission was the creation of the position of Director of National Intelligence (DNI), separate from the Director of the Central Intelligence Agency (CIA), who would have major statutory authorities over the Intelligence Community's 16 agencies, including the preparation of budgets, systems acquisition, and the setting of personnel policies and standards for information use throughout the Intelligence Community. The DNI would also be the principal intelligence advisor to the President and would prepare national intelligence estimates.

Congressional Responses

Congress responded to many of the recommendations of the 9/11 Commission by passing the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), hailed by some as the most important intelligence legislation since the National Security Act of 1947. The Act established a DNI (along with a separate Director of the CIA) and provided him with additional

[1] Prepared by Richard A. Best, Jr., Specialist in National Defense, Foreign Affairs, Defense and Trade Division.

authorities beyond those that the former Director of Central Intelligence (DCI) had over all intelligence agencies. The DNI possesses substantial authorities to prepare the national intelligence budget and the expenditure of funds appropriated for the national intelligence effort. The DNI also is charged with establishing priorities for collection and analysis; and managing intelligence centers composed of analysts from various intelligence and law enforcement agencies.

Questions involving the DCI's budgetary authorities were debated at length during consideration of the legislation. The management and oversight authorities proposed by the 9/11 Commission and reflected in some versions of intelligence reform legislation appeared to some Members as complicating, undermining, or replacing the authorities of the Secretary of Defense over intelligence agencies in the Defense Department (in particular, the National Security Agency, National Reconnaissance Office, and National Geospatial-Intelligence Agency, that are also integral components of DOD's warfighting capabilities). The agreement reflected in the final legislation provides the DNI with authority to "develop and determine an annual consolidated National Intelligence Program budget," along with authorities to manage appropriations, transfer or reprogram funds (within strict limitations), transfer a limited number of personnel annually, and establish common information technology standards. At the same time, the Act called for the President to issue guidelines to ensure that the authorities granted to the DNI are implemented "in a manner that respects and does not abrogate the statutory responsibilities" of other departments including DOD. Some observers have suggested that the legislation has not definitively resolved the question of the DNI's responsibilities for the Defense agencies in particular, and have argued that further legislative changes may be required and/or that an effective solution will depend on the ability of the DNI and the Secretary of Defense to work in close coordination.

To a large extent P.L. 108-458 adopted the recommendations of the 9/11 Commission regarding the organization of the Intelligence Community but it did not centralize management of the Intelligence Community to the extent that at least some on the 9/11 Commission would have preferred. As a result there remains a potential that the national intelligence agencies within the Department of Defense may be subject to conflicting guidance from the Secretary of Defense and the DNI. Thus far, however, there has been little public controversy regarding the budgets of intelligence agencies since the enactment of P.L. 108-458.

Intelligence Oversight: Congressional Options[2]

Commission Concerns and Recommendations

The 9/11 Commission stated that congressional oversight for intelligence and counter-terrorism is "dysfunctional." Commission members suggested two basic alternatives for strengthening and improving Congress's oversight of these policy domains. The two recommendations were: (1) to create either a joint committee on intelligence modeled after the former Joint Committee on Atomic Energy; or (2) establish a committee in each chamber that has the authority to both authorize and appropriate for intelligence agencies and activities. In addition, the commission suggested that an intelligence committee should have a subcommittee specifically dedicated to oversight; the panel should have subpoena authority; majority party representation on the

[2] Prepared by (name redacted), Senior Specialist in the Legislative Process, Government and Finance Division.

panel should exceed the minority by only one member; a member from each of these panels—Armed Services, Judiciary, Foreign Affairs, and the Defense Appropriations Subcommittee—should serve on an intelligence committee; Members who serve on an intelligence committee should not be subject to term limits; the staff of an intelligence committee should be nonpartisan and serve the entire committee; and the size of an intelligence committee should range from seven to nine members.

Congressional Responses

The House and Senate did not create a joint intelligence committee, nor did either chamber consolidate authorizing and appropriating responsibility for the intelligence community in a single committee. On the other hand, the two chambers followed some but not all of the commission's other recommendations.

In the House, the Permanent Select Intelligence Committee for the 109th Congress has an oversight subcommittee, subpoena authority, and members who serve also on the Defense Appropriations Subcommittee and the Armed Services, Judiciary, and International Relations Committees. The House panel's ratio of majority to minority party members does not, however, track the commission's recommendation. The House Permanent Select Intelligence Committee's size is larger than nine; its members are subject to tenure limitations with exceptions for the chair and ranking minority member; and it has a partisan staff model.

In October 2004, the Senate adopted S.Res. 445, which made a number of changes affecting oversight of the intelligence community. Some of the recommendations in S.Res. 445 parallel the commission's ideas, while others are new proposals agreed to by the Senate. The ideas in S.Res. 445 that affect the Select Intelligence Committee, and which generally emulate the commission's proposals, are these: an oversight subcommittee; subpoena authority; a one-seat margin for the majority party; a two-seat representation on the panel from each of these committees: Appropriations, Armed Services, Foreign Relations, and Judiciary; moreover, Intelligence members are not subject to term limits. On the other hand, the Select Intelligence Committee employs a partisan staff model and its size is larger than nine members.

S.Res. 445 made a number of other changes affecting the Select Intelligence Committee. These include granting the Majority Leader formal authority to name the chairman, and the Minority Leader the vice chairman, of the panel; authorizing the chair and vice chair of the Intelligence panel to name, respectively, the chair and vice chair of any subcommittee; assigning to the panel jurisdiction over civilian nominations to advice-and-consent positions within the intelligence community; permitting each Intelligence member to appoint a staff aide to the committee (subject to appropriate security clearances); allocating committee staff resources between the parties on a 60/40 ratio, excluding staff designees appointed by individual Senators; expanding current requirements that the Intelligence Committee report periodically to the Senate on its findings and to require such reports quarterly; elevating the Select Intelligence Committee to a category "A" assignment status; obligating the panel to consult with the Majority Leader and Minority Leader about the disclosure of classified information given to the committee by the executive branch; and reducing what are called "on demand sequential referrals" from 30 days to 10 days.

S.Res. 445 recommended that the Committee on Appropriations "shall reorganize into 13 subcommittees as soon as possible after the convening of the 109th Congress." The Senate Committee on Appropriations did not establish its customary 13 subcommittees. Bicameral discussions at the start of the 109th Congress involving, among others, the majority party leaders and the respective House and Senate Appropriations chairs, led to a downsizing and reshuffling of Appropriations subcommittees and jurisdictions.

In mid-February 2005, the House panel established 10 subcommittees, eliminating three (District of Columbia, Legislative Branch, and VA-HUD). A few weeks later the Senate Appropriations Committee created 12 subcommittees. The panel retained its District of Columbia and Legislative Branch subcommittees, but, like the House, it eliminated its VA-HUD subcommittee and transferred its jurisdiction to other Appropriations subcommittees. One goal of revamping the organizational structure of the two Appropriations Committees is to minimize the need for end-of-year appropriations measures.

The recommendation in S.Res. 445 for an Appropriations Subcommittee on Intelligence was not acted upon by the Committee on Appropriations during the 109th Congress. The Resolution stated that the proposed Intelligence subcommittee "shall have jurisdiction over funding for intelligence matters, as determined by the Senate Committee on Appropriations." A Senate Appropriations member indicated that it would be difficult to create a subcommittee with a classified budget. The 9/11 Commission recommended public disclosure of the nation's budget for intelligence, which has not been agreed to by the Congress.[3]

Improving Transitions Between Administrations[4]

Commission Concerns and Recommendations

The *9/11 Commission Report*[5] included a general recommendation that appointments to key national security positions at the time of presidential transitions occur more quickly. The goal of the 9/11 Commission's recommended changes was to "minimize as much as possible the disruption of national security policymaking" and maintain national security continuity when a new President comes into office. The recommendation addressed the commission's concern about the length of time a new Administration takes to install key national security personnel. The commission noted, in particular, the abbreviated transition period resulting from the delayed resolution of the 2000 presidential race. The report stated, "Given that a presidential election in the United States brings wholesale change in personnel, this loss of time hampered the new administration in identifying, recruiting, clearing, and obtaining Senate confirmation of key appointees."[6] As a result, the commission reported, "the new administration did not have its

[3] For further information generally, see CRS Report RS21955, *S.Res. 445: Senate Committee Reorganization for Homeland Security and Intelligence Matters*, by (name redacted) and (name redacted). For historical background on the public disclosure issue, see CRS Report 94-261, *Intelligence Spending: Public Disclosure Issues*, by (name redacted) and (name redacted).

[4] Prepared by (name redacted), Analyst in American National Government, and (name redacted), Specialist in American National Government, Government and Finance Division.

[5] U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), p. 422.

[6] *9/11 Commission Report*, p. 198.

deputy cabinet officers in place until the spring of 2001, and the critical subcabinet officials were not confirmed until the summer—if then. In other words, the new administration—like others before it—did not have its team on the job until at least six months after it took office."[7]

In line with its overall recommendation, the commission called for seven specific changes, six of which are related to presidential appointments and transitions. Two of these proposed changes are related to the national security clearance process during transitions. First, the commission recommended starting the security clearance process for prospective appointees to national security positions immediately after the presidential election. It also proposed that, prior to the election, each presidential candidate provide to the FBI "the names of selected members" of his or her prospective transition team to facilitate quicker security clearances following the election.

Three additional recommendations would modify the nomination and Senate consideration processes for certain national security positions. First, the report proposed that all nominations to positions on the "national security team"[8] be submitted to the Senate by the President-elect no later than the date of his or her inauguration. Furthermore, the commission called for the Senate to "adopt special rules requiring hearings and votes to confirm or reject national security nominees within 30 days of their submission." The final recommended change to the appointment process would be the elimination of advice and consent requirements for any "national security team" members below Level III of the Executive Schedule.

The commission also suggested that, beginning immediately after the election, the transition include a prompt and thorough written national security information exchange between the outgoing and incoming Administrations.

In addition to these six changes, the commission called for centralization of the security clearance process in one agency, including providing and maintaining security clearances and ensuring uniform standards.[9]

Congressional Responses

Enacted Provisions

The Intelligence Reform and Terrorism Prevention Act of 2004 (hereafter the "Intelligence Reform Act")[10] included several provisions that responded to commission concerns and recommendations. The legislation amended the Presidential Transition Act of 1963 to (1) recommend submission by the President-elect to the agency with national security clearance functions of the "names of candidates for high level national security positions through the level of undersecretary" of agencies and departments, as soon as possible after the presidential election; (2) require the responsible agency or agencies to carry out background investigations of these candidates for high-level national security positions "as expeditiously as possible ... before the date of the inauguration"; and (3) authorize "relevant outgoing executive branch officials" to prepare a "detailed classified, compartmented summary ... of specific operational threats to

[7] *9/11 Commission Report*, p. 422.

[8] The phrase "national security team" was not defined in the report.

[9] *9/11 Commission Report*, p. 422.

[10] P.L. 108-458, 118 Stat. 3638.

national security; major military or covert operations; and pending decisions on possible uses of military force," which would be provided to the President-elect and Vice President-elect as soon as possible after the general election.[11]

Just as the Intelligence Reform Act seeks to facilitate more rapid security clearances for top national security position candidates, it also does so for transition team members. It allows each major party presidential candidate to submit, before the general election, security clearance requests for "prospective transition team members who will have a need for access to classified information" in the course of their work. The law directs that resulting investigations and eligibility determinations be completed, as much as possible, by the day after the general election.[12]

The Intelligence Reform Act also expresses "the sense of the Senate" about a timetable for submission and consideration of high-level national security nominations during transitions. Under this timetable, nominations to such positions should be submitted by the President-elect to the Senate by Inauguration Day, and Senate consideration of all such nominations should be completed within 30 days of submission.[13] Because most presidential appointees are subject to a limited "vetting" process and not a full-scale security clearance investigation and adjudication, these changes may have a significant impact on the duration and difficulty of the confirmation process. A personnel security clearance investigation, for instance, is normally more exhaustive and longer than the usual "vetting" process for potential nominees. A background investigation for access to the highest clearance level—Top Secret with access to Sensitive Compartmented Information—may take a year. That is because the process requires a full field investigation, including interviews with former colleagues and employers, neighbors, friends, and acquaintances, along with checks of databases from law enforcement entities, financial services, and, to a degree, medical services.

The Intelligence Reform Act also made government-wide changes to the national security clearance process that are designed to consolidate and streamline this function. Concerns have long existed over the substantial backlog, delays, and time consumed in initial background investigations and subsequent re-investigations associated with gaining access to classified national security information. These problems have been exacerbated by the increased number of personnel requiring access to classified information and the growth of materials being classified or being classified at higher levels; both of these changes, in turn, have been driven by the expanding programs in national and homeland security. Other reasons for seeking improvements in the clearance process, especially the background investigations, are (1) the lack of reciprocity among agencies, so that one federal agency may not accept the findings of investigations previously conducted for another federal agency; and (2) questions about the capacity of existing agencies to handle the increased workload (or overload) in light of its size and recent growth.[14]

[11] P.L. 108-458, Sec. 7601(a).

[12] P.L. 108-458, Sec. 7601(c).

[13] P.L. 108-458, Sec. 7601(b).

[14] U.S. House Committee on Government Reform, *What's the Hold Up? A Review of Security Clearance Backlog and Reciprocity Issues Plaguing Today's Government and Private Sector Workforce*, hearings, 108th Congress, 2nd sess. (Washington: GPO, 2004). At the same time, the Department of Defense transferred the background investigation function and related personnel to the Office of Personnel Management, which now handles about 90% of all federal background investigations.

The Intelligence Reform Act required the President to designate a single executive entity to oversee and develop uniform standards and policies for access to classified information and to designate other investigative agencies, if appropriate, for national security and efficiency purposes.[15] The statute further stipulated that reciprocity should be the rule among agencies for clearances at the same level and the legislation established a national database to track clearances. The head of the entity charged with overseeing the process is to evaluate and report to Congress on the use of available technology in clearance investigations and adjudications, as well as to consult with Congress and adjudicative agencies in developing a plan, within five years, to reduce the length of the clearance process.

The first step along this new path was undertaken during the 109th Congress, with the Office of Personnel Management (OPM) designated as the lead agency in conducting security clearance background checks under the guidance and oversight of the Deputy Director of OMB. Certain deadlines and a reciprocity requirement among agencies have also been established to speed up the process and make it less costly and more efficient. Setting this in motion was an executive order issued by President George W. Bush, designed to strengthen and speed up processes to determine eligibility for access to classified national security information.[16] In the order, the President called upon the Director of the Office of Management and Budget (OMB) to develop the policy for meeting the following goals: "To the extent consistent with safeguarding the security of the United States and protecting classified national security information from unauthorized disclosure, agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal."[17]

The Intelligence Reform Act also contained appointment process-related provisions[18] that were not specifically recommended by the 9/11 Commission. These included provisions that (1) require a report from the Office of Government Ethics (OGE) regarding potential improvements

[15] P.L. 108-458, Title III, Sec. 3001(c).

[16] Executive Order 13381, "Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information," issued by President George W. Bush, June 27, 2005, 70 *Federal Register* 37953, June 30, 2005.

[17] Ibid., Sec. 1. In developing the plan, the OMB Deputy Director was required to consult with the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, as well as the Director of the Office of Personnel Management (OPM) and the Director of National Intelligence (DNI). The OMB Director issued guidelines and instructions to the heads of agencies to ensure such goals. A separate section covers Sensitive Compartmented Information, that information generated by way of intelligence sources and methods, and special access programs pertaining to intelligence activities, including special activities or covert operations. The Deputy Director for Management at OMB has been delegated responsibility for carrying out the order. Along with this, specialized areas of responsibility have been assigned to the Directors of OPM and of National Intelligence as well as to the Assistant to the President for National Security Affairs. The particulars of the plan and its production are covered in several executive reports, testimony before Congress, and a Government Accountability Office (GAO) report. See U.S. Office of Management and Budget, *Report on the Status of Executive Branch Efforts to Improve the Security Clearance Process Required under Title III of P.L. 108-458* (Washington: OMB, 2006), and *Plan for Improving the Personnel Security Clearance Process* (Washington: OMB, 2005); and Kathy L. Dillaman, Associate Director, Federal Investigative Services Division, OPM, testimony on *Human Capital Issues and Security Clearance Procedures*, before the Subcommittee on Management, Integration, and Oversight, House Committee on Homeland Security, May 18, 2006. GAO, however, has found continuing weaknesses in this area; see U.S. Government Accountability Office, *DOD Personnel Clearances: Additional OMB Actions Are Needed to Improve the Security Clearance Process*, GAO-06-1070 (Washington: GAO, 2006).

[18] P.L. 108-458, Sec. 8403.

to the financial disclosure process for executive branch employees;[19] (2) direct the Office of Personnel Management (OPM) to transmit an electronic record "on Presidentially appointed positions," with specified contents, to each major party presidential candidate soon after his or her nomination, and to make such a record available to any other presidential candidate after this; (3) direct each agency head to submit an advice and consent position reduction plan, with specified contents, to the President, the Senate Committee on Governmental Affairs (as of the 109th Congress, the Senate Committee on Homeland Security and Governmental Affairs), and the House Committee on Government Reform;[20] and (4) require the Director of OGE, in consultation with the Attorney General, to "conduct a comprehensive review of conflict of interest laws relating to Federal employment," with specified contents and recipients.[21]

Although the Intelligence Reform Act addressed each of the recommendations in this section of the *9/11 Report*, its provisions were generally not identical to the commission's recommended actions. For example, whereas the commission recommended that the "Senate should not require confirmation of [national security] executive appointees below Executive Level 3," the statute requires agencies to submit advice and consent position reduction plans to the President and congressional committees.

Related Potential Congressional Concerns for the 110th

The presidential transition process changes called for by the 9/11 Commission and provided for in the Intelligence Reform Act are arguably more critical to national security continuity at the time of a transition between Presidents than between the first and second terms of a two-term President. Nonetheless, some top-level national security positions changed hands at the beginning of the second George W. Bush Administration, and Congress may elect to conduct oversight, during the 110th Congress, on the implementation of the modifications to the presidential transition process. Congress might also elect to conduct oversight regarding provisions that would be implemented during the run-up to the 2008 presidential election.

Changes to the national security clearance process under the Intelligence Reform Act extend beyond the presidential transition and presidential appointment processes. Some changes are designed to modernize the national security clearance process, by adding new formal requirements (e.g., for reciprocity among agencies) and by consolidating the process under a single entity, the Office of Personnel Management, with guidance and supervision under the Deputy Director of the Office of Management and Budget. The implementation of these and other new developments might become the subjects of congressional oversight, to determine whether the changes are proceeding as expected, whether their goals are being met, whether legislative intent is being followed, what the implementation costs are, and what other modifications might be necessary.

[19] OGE submitted this report on March 17, 2005. It is available at http://www.usoge.gov/pages/forms_pubs_otherdocs/fpo_files/reports_plans/rpogc_fin_dis_03_05.pdf.

[20] At the end of the 109th Congress, staffers for both of the congressional committees indicated that only a few agencies had submitted the required PAS position reduction plans.

[21] OGE submitted this report in Jan. 2006. It is available at http://www.usoge.gov/pages/forms_pubs_otherdocs/fpo_files/reports_plans/rpt_title18.pdf.

Several provisions of the law reflect ongoing concern among some Members of Congress about the length and complexity of the presidential appointment process. The last several Congresses have seen efforts to develop consensus, inter alia, on streamlining executive branch financial disclosure requirements; reducing the number of positions requiring Senate confirmation for appointment; and simplifying conflict of interest laws and decriminalizing conflict of interest. With the submission of reports to Congress concerning these topics, required by the Intelligence Reform Act, discussions regarding possible changes may be renewed during the 110th Congress.

Congress might elect to revisit provisions contained in earlier versions of the intelligence legislation that were not included in the enacted law. These include proposed changes to provisions of the Federal Vacancies Reform Act of 1998 that would make it easier for the President to make long-term temporary appointments to advice and consent positions during presidential transitions.[22]

Other appointments-related issues could be of interest in the 110th Congress. For example, it is possible that the Senate may attempt to change its floor procedures concerning nominations. In addition, issues related to recess appointments may come to the fore. At times, for instance, the President's use of his recess appointment power has been seen as circumventing the Senate confirmation process and has proven controversial.

Afghanistan and Terrorism[23]

Commission Concerns and Recommendations

The 9/11 Commission Report (p. 370) praised the U.S. efforts in Afghanistan to that date, but emphasized the need for a sustained, long-term commitment by the United States and the international community to Afghanistan's stability and security,[24] in order to prevent Afghanistan from "again becom[ing] a sanctuary for international crime and terrorism." The Commission was far-reaching in its recommendations, calling for greater peacekeeping participation by international forces, particularly NATO; stepped up counter-narcotics activities, disarmament of regional militias, and efforts to promote rule of law; and follow through on funding pledges with increased flexibility in allocating money for relief and reconstruction.[25]

Most of the recommendations had already formed major pillars of Administration policy on post-Taliban Afghanistan, and these efforts accelerated after the release of the 9/11 report. Key milestones in the U.S. stabilization effort were the October 9, 2004 presidential election, in which interim leader Hamid Karzai was elected, and the September 18, 2005 elections for a 249 seat lower house of parliament, and subsequent selections to a 102-seat upper house.

[22] See 108th Cong., H.R. 10, § 5042.

[23] Prepared by (name redacted), Specialist in Middle Eastern Affairs, Foreign Affairs, Defense, and Trade Division.

[24] For further information on U.S. efforts to stabilize Afghanistan, see CRS Report RL30588, *Afghanistan: Post-Taliban Governance, Security, and U.S. Policy*, by (name redacted).

[25] See The 9/11 Commission Report, Section 12.2, Recommendation No. 3.

The Commission recommendation for increased NATO participation in Afghanistan peacekeeping has, by most accounts, been implemented. As of October 5, 2005, NATO now has overall control of peacekeeping operations throughout Afghanistan, including the volatile and violent south and east of the country. NATO's force in Afghanistan now numbers about 31,000, including about 11,250 U.S. forces. NATO countries run 13 of the 25 total "provincial reconstruction teams" (PRTs)—regional civilian-military enclaves intended to promote security and reconstruction.

The United States, Afghanistan, and the international community have also had significant success over the past few years in disarming regional militiamen—a "disarmament, demobilization, and reintegration program (DDR), run jointly by the United Nations, Japan, and the United States, resulted in the disarmament of 63,000 private militiamen by the June 2005 close-out of the program, according to U.S. and U.N. officials. A follow-on program, called Disarmament of Illegal Armed Groups (DIAG) is currently in the process of attempting to disband several hundred illegal militia groups around Afghanistan, although progress is said to be slow.

Counter-narcotics programs, on the other hand, have not been as successful. U.N. officials estimate that a record opium poppy crop was produced in Afghanistan during the 2005-2006 season that supplied 92% of the world's illicit opium and reversed a slight reduction that occurred from 2004-2005. U.S., Afghan, and international officials have cited the cultivation and trafficking as a serious strategic threat to U.S.-led efforts to stabilize and reconstruct Afghanistan.

Congressional Responses

The 108th and 109th Congresses have acted to implement at least some of the Commission's recommendations. The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) contained a subtitle called "The Afghanistan Freedom Support Act Amendments of 2004." The subtitle mandated the appointment of a U.S. coordinator of policy on Afghanistan in order to streamline and instill greater flexibility and inter-agency cooperation in the administration of U.S. programs in Afghanistan. The subtitle also required additional Administration reports to Congress on progress in reconstruction. In addition, the subtitle contained "sense of Congress" provisions recommending more rapid disarmament of private militias; expansion of the NATO-led peacekeeping force; and new initiatives to combat narcotics trafficking. The subtitle did not specify dollar amounts for U.S. aid to Afghanistan for FY2005 and FY2006, authorizing instead "such sums as may be necessary for each of the fiscal years 2005 and 2006."

In appropriations legislation, the 108th and 109th Congresses have sought to address the need for reconstruction funds. For FY2005, a total of $4.3 billion was appropriated for programs in Afghanistan, from a regular foreign aid appropriation (P.L. 108-447) and a supplemental (P.L. 109-13). Of those funds, about $1.6 billion was earmarked to equip and train the Afghan National Army (ANA) and Afghan National Policy (ANP). Slightly less was appropriated for FY2006—a total of about $3.05 billion in a regular appropriation (P.L. 109-102) and a supplemental (P.L. 109-234). The FY2006 funds include a total of about $2 billion to train and equip the ANA and the ANP. As noted above, building up the ANA is a key recommendation of the September 11 Commission so that the central government can extend its writ and services throughout Afghanistan.

Future Considerations

For FY2007, some funding for Afghanistan awaits congressional action. The Administration requested $1.1 billion for civilian reconstruction programs, including counter-narcotics, and congressional action on these funds has not been completed to date, although both House and Senate versions fund roughly the total amounts requested. The FY2007 Defense appropriation (P.L. 109-289) provides $1.5 billion to train and equip the ANA and ANP and provides $100 million for Defense Department counter-narcotics support activities for Afghanistan. Some experts believe that the upsurge in Taliban opposition violence during 2006 is a product of popular frustration at the slow pace of reconstruction, particularly in southern Afghanistan, and several experts believe the remedy for this is accelerated reconstruction.

Pakistan and Terrorism[26]

Commission Concerns and Recommendations

The 9/11 Commission Report emphasizes that the mounting of large-scale international terrorist attacks appears to require sanctuaries in which terrorist groups can plan and operate with impunity. In addition to identifying Pakistan as a principal transit country for the 9/11 hijackers and naming the western regions of the country as one of six "actual or potential terrorist sanctuaries" worldwide, the report warns that Pakistan's "vast unpoliced regions" remain attractive to extremist groups. The first recommendation of the Commissioners is identification and prioritization of terrorist sanctuaries and the development of a realistic strategy for denying them to terrorists.

In its country-specific discussion, *The 9/11 Commission Report* further claims that—even after acknowledging problems in U.S.-Pakistan relations and President Musharraf's role in them—"Musharraf's government is the best hope for stability in Pakistan and Afghanistan." It recommends that the United States make a long-term commitment to provide comprehensive support for Islamabad so long as Pakistan itself is committed to combating extremism and to a policy of "enlightened moderation." Specifically, the Commission urges sustaining U.S. assistance to Pakistan at "current scale" with programs that extend from military aid to support for better education.[27] A November 2005 follow-on report by Commissioners gave a "C" grade to U.S. efforts to support Pakistan's anti-extremism policies and warned that the country "remains a sanctuary and training ground for terrorists."

[26] Prepared by (name redacted), Specialist in Asian Affairs, Foreign Affairs, Defense, and Trade Division. See also CRS Report RL33498, *Pakistan-U.S. Relations*, CRS Report RL32259, *Terrorism in South Asia*, CRS Report RL32615, *Pakistan's Domestic Political Developments*, and CRS Report RS22009, *Education Reform in Pakistan*, all by (name redacted); and CRS Report RL32745, *Pakistan's Nuclear Proliferation Activities and the Recommendations of the 9/11 Commission: U.S. Policy Constraints and Options*, by (name redacted), (name re dacted), and (name redacted).

[27] See Sections 12.1 and 12.2 (p. 361-374) of *The 9/11 Commission Report*. The concept of "enlightened moderation," as expounded by Musharraf himself, is a direct response to a growing world perception that Islam is linked to fundamentalism, and thus to extremism, and thus to terrorism. It is a strategy meant to both shun the militancy that is rooted in "political injustice, denial, and deprivation," and to bring "socioeconomic uplift" in the Muslim world. Musharraf has called upon Muslims to "adopt a path of moderation and a conciliatory approach to fight the common belief that Islam is a religion of militancy in conflict with modernization, democracy, and secularism" (Pervez Musharraf, "A Plea for Enlightened Moderation," *Washington Post*, June 1, 2004).

The issue of a long-term U.S. commitment to supporting Pakistan is key for many analysts, as past experiences have engendered Pakistani skepticism regarding the strategic (as opposed to tactical) reliability of the United States as an ally. Many Bush Administration officials, Members of Congress, and independent analysts remain concerned about the continued existence in Pakistan of terrorist groups and their supporters, evidence that Pakistan has been the source of significant "onward" proliferation of nuclear weapons materials and technologies to third parties, and continuing human rights abuses, including perceived nondemocratic practices, by the military-dominated government in Islamabad.

Congressional Responses

In passing the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), the 108th Congress broadly endorsed the Pakistan-specific 9/11 Commission recommendations. Section 7103 of the bill, entitled "United States Commitment to the Future of Pakistan," called for U.S. aid to Pakistan to be sustained at a minimum of FY2005 levels and required the President to report to Congress a description of a long-term U.S. strategy to engage with and support Pakistan. It further extended the President's authority to waive coup-related sanctions on Pakistan through FY2006, allowing continued U.S. military and economic assistance to Pakistan despite the 1999 overthrow of an elected government in Islamabad.

Foreign Assistance

In June 2003, President Bush vowed to work with Congress on establishing a five-year, $3 billion aid package for Pakistan. Annual installments of $600 million each began in FY2005 and are split evenly between military and economic aid. The Foreign Operations FY2005 Appropriations bill (P.L. 108-447) established a new base program of $300 million for military assistance for Pakistan. When additional funds for development assistance, law enforcement, and other programs are included, the aid allocation for FY2005 was about $688 million. Significant increases in economic support, along with relief funding in response to Pakistan's devastating October 2005 earthquake, may bring the FY2006 total to around $874 million. The Bush Administration's FY2007 request calls for another $739 million in aid to Pakistan, although the House Appropriations Committee (H.Rept. 109-486) recommended reducing that amount by $150 million (ostensibly for domestic budgetary reasons unrelated to Pakistan-U.S. relations). In S.Rept. 109-277, the Senate Appropriations Committee called for redirecting some of the requested FY2007 U.S. economic aid to Pakistan toward development and democracy promotion programs there (House and Senate committees have issued separate concerns about "the slow pace of the democratic development of Pakistan").

In the five years since September 2001, Pakistan has received nearly $1.5 billion in direct U.S. security-related assistance (Foreign Military Financing totaling $970 million plus about $516 million for other programs). Congress has taken no action to block major U.S. arms sales to Pakistan during this period, including the multi-billion dollar sale of F-16 combat aircraft currently in process.[28] Programs overseen by USAID in Pakistan include those aimed at

[28] Other major government-to-government arms sales and grants in recent years have included C-130 military transport aircraft, P-3C Orion maritime patrol aircraft, AH-1F Cobra attack helicopters, F-16 combat aircraft, surveillance radars, air traffic control systems, military radio systems, Harpoon anti-ship missiles, Phalanx guns, and TOW anti-armor missiles. Other pending sales include Sidewinder air-to-air missiles and self-propelled howitzers.

strengthening that country's democratic institutions and civil society, reforming the education sector, alleviating poverty, improving health, and bolstering macroeconomic stability while stimulating economic growth. Such efforts have been funded with some $2 billion since September 2001 (Economic Support Funds of nearly $1.7 billion plus $288 million for other programs). Congress also has eased Islamabad's foreign debt burden by authorizing Pakistan to use $388 million in economic support to cancel about $1.5 billion in concessional debt to the U.S. government.

Coalition Support Funds

In addition to the foreign assistance discussed above, Congress has appropriated billions of dollars to reimburse Islamabad for its support of U.S.-led counterterrorism operations (Pakistan has since 2002 been undertaking military operations along its border with Afghanistan). As of December 2006, a total of $6.65 billion had been appropriated for FY2002-FY2007 Defense Department spending for coalition support payments to "Pakistan, Jordan, and other key cooperating nations." Pentagon documents indicate that disbursements to Islamabad—averaging about $66 million per month—account for the majority of these funds. This amount is roughly equal to one-fifth of Pakistan's total military expenditures. The Defense Department Appropriations Act, 2007 (P.L. 109-289) allows that up to $900 million in Pentagon funds be used for FY2007 reimbursements.

Saudi Arabia and Terrorism[29]

Commission Concerns and Recommendations

The September 11, 2001 attacks kindled criticism within the United States of alleged official Saudi involvement in terrorism or of Saudi laxity in acting against terrorist groups. Some critics believe that Saudi domestic and foreign policies have created a climate that may have contributed to terrorist acts by Islamic radicals. Critics, for example, have cited reports that the Saudi government permitted or encouraged fund raising by allegedly charitable institutions with links to Al-Qaeda. Saudi leaders maintain that they are working to suppress terrorism, which they say is aimed even more at the Saudi regime than at the United States. The U.S. State Department acknowledges a more proactive Saudi stance against terrorist groups since terrorist attacks on Saudi Arabia in 2003.

In its July 2004 report, the 9/11 Commission described Saudi Arabia as having been "a problematic ally in combating Islamic extremism." The report took note of long-standing cooperative relations between the U.S. and Saudi governments and acknowledged the integral role of charitable donations in the Islamic religion. At the same time, the report noted a lack of oversight mechanisms to monitor charitable spending in Saudi Arabia, misunderstandings between the United States and Saudi Arabia at the popular level, and recent reform measures adopted by the Saudi Government. In its recommendations, the Commission states that the United States and Saudi Arabia must confront openly the problems in their relationship and "determine if they can build a relationship that both sides are prepared to publicly defend—a relationship about

[29] Prepared by (name redacted), Specialist in Middle East Affairs, and (name redacted), Analyst in Middle East Affairs, Foreign Affairs, Defense, and Trade Division.

more than oil." The report went on to urge a "shared commitment" to political and economic reform" in Saudi Arabia and a "shared interest in greater tolerance and cultural respect," as a means of fighting violent extremists.[30] In late 2005, U.S. and Saudi officials initiated a "strategic dialogue" to expand cooperation in six key areas: counterterrorism, military affairs, energy, business, education and human development, and consular affairs.

Congressional Responses

Provisions Enacted

Relevant sections of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) capture many of the concerns reflected in the 9/11 Commission report regarding Saudi Arabia. Section 7105(a) contains findings which review problems in the bilateral relationship but note improvements in counter-terrorism cooperation between the two countries since mid-2003. Section 7105(b) expresses the sense of Congress that "there should be a more robust dialogue between the people and Government of the United States and the people and Government of Saudi Arabia." Section 7120(b) required the President to submit to Congress within 180 days a strategy for collaboration with Saudi Arabia, as part of a larger report on U.S. government activities to implement the provisions of this act. The strategy paper was to include steps to institutionalize U.S.-Saudi relationships, intelligence and security cooperation, ways to increase Saudi contributions to peace and stability in the Middle East, political and economic reform, ways to promote tolerance and diversity in Saudi Arabia, and ways to diminish support from Saudi sources to extremist groups. The Administration transmitted the classified report to designated congressional committees on September 7, 2005.[31]

Though not directly addressed as an issue in the 9/11 Commission Report, some Members of Congress have criticized the U.S. military assistance program of $20-25,000 per year under the International Military Education and Training (IMET) program because of what they perceive to be the failure of Saudi authorities to suppress terrorist activity and incitement. House amendments to the Foreign Operations Appropriations Acts for FY2005 (incorporated as Division D of the FY2005 Consolidated Appropriations Act, P.L. 108-447, December 8, 2004) and FY2006 [P.L. 109-102] banned U.S. aid to Saudi Arabia. However, Senate versions of both bills did not include such bans, and presidential national security waiver authority was included in the final versions of both pieces of legislation. President Bush exercised his waiver authority in FY2005, but did not issue a waiver for FY2006 funds because, according to State Department officials, FY2006 funds appropriated for use in Saudi Arabia were not obligated. On June 9, 2006, the House adopted H.Amdt. 997 to the Foreign Operations Appropriations Act for FY2007 (H.R. 5522) by 312-97 (Roll no. 244); the amendment prohibits U.S. assistance to Saudi Arabia and contains no presidential waiver provision. H.R. 5522 passed the House on June 9; the Senate has not passed its version as of November 20.

[30] For additional information, see CRS Report RL33533, *Saudi Arabia: Background and U.S. Relations* and CRS Report RL32499, *Saudi Arabia: Terrorist Financing Issues*, both by (name redacted).

[31] House Committee on International Relations, Survey of Activities, Week of September 6, 2005: Letter Transmitting Report—September 7, 2005, CLASSIFIED, Department of State, pursuant to Sec. 7120 of the Intelligence Reform and Terrorism Prevention Act, 2004 (P.L. 108-458); Ex. Comm. 3684.

Related Options Also Considered

Congressional concerns continue during the 109th Congress over the role of Saudi Arabia in the war against terrorism, with particular emphasis on encouraging Saudi leaders to heighten their efforts against terrorist financing. H.R. 2037/S. 1171, the Saudi Arabia Accountability Act of 2005, is similar to the Saudi Arabia Accountability Act proposed but not enacted in the 108th Congress (H.R. 3643/S. 1888). Like the earlier bills, the 109th proposal would prohibit export or issuance of an export license to Saudi Arabia for any U.S. defense articles or defense services on the U.S. munitions list or dual use items and would restrict travel of Saudi diplomats in the United States. S. 12, the Targeting Terrorists More Effectively Act of 2005, introduced on January 24, 2005, contains sections on Saudi Arabia including:

- A statement of U.S. policy to work with the Saudi government to curtail terrorist financing through a variety of methods.
- Findings that Saudi Arabia has an uneven record in fighting terrorism, especially with regard to terrorist financing, support for radical *madrasas* (schools), and lack of political outlets for its citizens; and that the Saudi government must undertake political and economic reforms.
- A requirement for the President to submit a report to designated congressional committees containing a long-term strategy for U.S.-Saudi engagement and for effective prevention of terrorist financing.[32]

H.R. 2037, S. 1171, and S. 12 remained in committee and had not passed as of November 30, 2006.

Terrorism: Its Global Dimensions[33]

(Denying Sanctuary and Building a Coalition)

Commission Concerns and Recommendations

The 9/11 Commission Report emphasizes the global nature of the terrorist threat. It is portrayed as a threat that is motivated by religion. It is a threat consisting of a stateless network of terrorists. This threat with global dimensions is also characterized as a radical ideological movement in the Islamic world, inspired in part by al Qaeda. The Commission advocates attacking terrorist organizations as a strategy and tactic for responding to the threat. It recommends that the United States identify and prioritize terrorist sanctuaries, working with allies, and developing a realistic strategy to keep terrorists insecure and on the run. As specific examples, it refers to Pakistan, Afghanistan, and Saudi Arabia, but also identifies broader regions: the Arabian Peninsula; Horn of Africa; Southeast Asia; West Africa; and European cities. The National Strategy for Combating Terrorism, released by the Bush Administration in September 2006, places strong emphasis on closing down terrorist sanctuaries.

[32] Section 7120 of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458)—required the President to submit a strategy as part of a larger reporting requirement within 180 rather than 90 days, as explained above.

[33] Prepared by Raphael Perl, Specialist in International Affairs, Foreign Affairs, Defense, and Trade Division.

A second Commission recommendation relating to the global dimensions of terrorism centers on turning a national strategy into a coalition strategy. To this end, the Commission recommends that the United States engage other nations in developing a comprehensive coalition strategy against Islamist terrorism. Included here are joint strategies for targeting terrorist travel and a common strategy to deal with sanctuaries.

The National Strategy for Combating Terrorism, released by the Bush Administration in September 2006, also places strong emphasis on promoting international cooperation in the global fight against terrorism.

Congressional Responses

Legislation Enacted

Many congressional decisions related to measures designed to respond to the global terrorist threat are expected to be manifested through the appropriations process. Title VII, of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, section 7102, mirrors Commission recommendations by expressing a Sense of the Congress that it should be the policy of the United States to identify terrorist sanctuaries, work with allies, and develop a strategy to prevent terrorists from using foreign countries as sanctuaries. It also requires a report from the President to Congress on terrorist sanctuaries and what is being done to eliminate them. H.R. 4942, (109th Congress, Second Session), the Promoting Antiterrorism Capabilities through International Cooperation Act, would establish an office within DHS to promote international anti-terrorism cooperation.

Policy Concerns Not Addressed or Postponed

The issue of creating a coalition is arguably, a matter best suited for diplomats and not legislators. Notwithstanding, an office within DHS charged with promoting anti-terror cooperation could arguably do much to enhance such cooperation. However, the need for such cooperation, as envisioned by the 9/11 Commission, goes well beyond the jurisdictional domain of DHS. In this regard, creation of a joint congressional/executive branch commission to look at the overall issue of promoting international anti-terror cooperation—similar in structure to the National Commission on terrorism may warrant consideration.

Arguably also, physical sanctuaries are declining in overall importance to terrorist groups which are becoming increasingly decentralized both geographically and in terms of organizational hierarchy. This might warrant congressional consideration of the pro's and con's of including the issue of use by terrorists of virtual sanctuaries in any required reports to Congress on the issue of terrorist sanctuaries.

Islam and U.S. Policy[34]

Commission Concerns and Recommendations

Since the September 11, 2001, terrorist attacks, many experts have stated that the fight against terrorism cannot be won using force alone; it must be accompanied by long term policies that address development and reform issues in Arab and Muslim-majority countries and by a sophisticated public diplomacy effort that seeks to counter anti-American views commonly found in these countries. The 9/11 Commission Report's recommendations on tempering extremism in the Middle East and elsewhere echoed these sentiments. According to the report, "A comprehensive U.S. strategy to counter terrorism should include economic policies that encourage development, more open societies, and opportunities for people to improve the lives of their families and to enhance prospects for their children's future."

The 9/11 Commission Report also stressed that while U.S. public diplomacy, trade and cultural exchange, and international assistance programs are necessary, ultimately, it is our policies in the region that fuel anger and resentment. According to the report, "Right or wrong, it is simply a fact that American policy regarding the Israeli-Palestinian conflict and American actions in Iraq are dominant staples of popular commentary across the Arab and Muslim world." Increasingly, public debate over how best to win the "struggle of ideas" in the Arab and Muslim world has shifted away from the "means" (policy instruments) and toward the "ends" (overall direction of U.S. policy). Critics charge that U.S. efforts to highlight its outreach and assistance to Muslim societies has been overtaken by the negative Arab and Muslim reaction to alleged human rights abuses at Abu Ghraib, and Guantanamo Bay. Furthermore, many Arabs and Muslims feel that the United States continues to place its strategic regional interests above those of human rights and democracy by insufficiently protesting alleged abuses committed by friendly regional governments under the guise of the war on terror.

Congressional Responses

Due to the complexity and broad scope of directives laid out by the 9/11 Commission Report, it has been difficult for the U.S. government, including Congress, to address all of the various policy problems and solutions to the challenge of Islamic extremism. P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, is one piece of legislation that addresses many of the 9/11 Commission Reports recommendations. However, P.L. 108-458 only authorized the expansion of existing programs; it did not appropriate new funds. For example, P.L. 108-458 authorized the following steps to expand U.S. public diplomacy efforts with the Muslim world and promote reform and democracy throughout the "broader Middle East:"

- (section 7112) authorized a substantial expansion of U.S. exchange, scholarship, and library programs that benefit people in the Muslim world.

[34] Prepared by (name redacted), Middle East Policy Analyst, Foreign Affairs, Defense, and Trade Division.

- (section 7112) authorized the creation of a pilot program to make grants to United States-sponsored elementary and secondary schools in countries with predominantly Muslim populations for the purpose of providing full or partial merit-based scholarships to students from lower-income and middle-income families of such countries to attend such schools.
- (section 7113) authorized the establishment of an International Youth Opportunity Fund to provide financial assistance for the improvement of public education in the Middle East and other countries of strategic interest with predominantly Muslim populations.
- (section 7115) authorized the Middle East Partnership Initiative (MEPI), an economic assistance program designed to promote reform and democracy in the Arab world. MEPI, which Congress had not previously authorized, has received $284 million since its creation in FY2002.

For fiscal years 2005-2006 and possibly for fiscal year 2007, Congress has used the appropriations process to expand funding for various government sponsored activities such as cultural exchange, democracy promotion in the Arab world, international broadcasting in Arabic and Farsi, and development assistance for education and health. H.R. 5522, the FY2007 Foreign Operations Appropriations bill (passed the House but not the Senate), provides $75 million for MEPI, of which $9 million is for scholarship programs for students from countries with significant Muslim populations at not-for-profit institutions of basic and higher education in the Middle East. H.R. 5522 also recommends $20 million for the promotion of democracy in countries located outside the Middle East region with significant Muslim populations, such as Indonesia. The Senate version of H.R. 5522 also recommends $750,000 for the Center for Middle Eastern-Western Dialogue, an organization whose mission is to provide a forum for ongoing interaction and dialogue between citizens of the United States and Muslim-majority countries on key issues of mutual concern.

Policy Concerns Not Addressed

Radical Islam in Europe

Some critics assert that although poverty-reduction measures and the promotion of liberal reforms are desperately needed in many Arab and Muslim-majority countries, they are not a panacea and that many international terrorists, including some of Al Qaeda's top planners, were Western-educated and middle class residents of European countries. Some terrorism experts suggest that fundamentalist ideologies enjoy the most receptivity among Arab and Muslim migrant communities in Western countries, which face psychological dislocation and alienation in a new and unfamiliar environment.[35]

[35] For more information, see CRS Report RL33166, *Muslims in Europe: Integration in Selected Countries*, coordinated by (name redacted).

Islam in Politics

By calling for political reform and liberalization in the Muslim world, policymakers run the risk of empowering religious opposition parties that may seek to permanently enshrine Islamic religious law in a country's political and social system. Critics of U.S. foreign policy to combat extremism argue that based on their experience with Iran during its 1979 revolution and the subsequent influence of Islamist militant groups elsewhere in the region, the United States and other Western powers are wary of Islamist groups taking power (as Hamas did in 2006) and that Western support for secular autocratic regimes further enhances the credibility of opposition Islamist groups and some radical organizations. Political conditions vary across the Middle East and some Islamic groups are more moderate than others.

Terrorism: U.S. Policy Instruments[36]

Commission Concerns and Recommendations

The report of the 9/11 Commission underlined the importance for the United States of using the full range of policy instruments at its disposal to attack terrorists and their organizations and prevent the continued growth of Islamic terrorism. These policy instruments include not only intelligence, law enforcement, military force (treated elsewhere), but also diplomacy, bilateral support and economic assistance to front-line and failing states, support for democracy and good governance, international education and exchanges, and public diplomacy to engage the struggle of ideas and define and defend U.S. ideals and values (see below).

The Commission called on the United States to offer an example of moral leadership in the world, commit to treating people humanely, abide by the rule of law, and be generous and caring to its neighbors. It argued that the United States must stand for a better future in countries whose governments are repressive, even if they are friendly towards the United States.

Congressional Responses

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) addressed a number of themes in the 9/11 Commission Report. In Sec. 7101, Congress found that long-term success in the war on terrorism would require the use of all elements of national power, in addition to military action, intelligence, covert operations, law enforcement, and homeland defense, also including economic policy, foreign aid, and public diplomacy. The Act stated that the United States must give economic and diplomatic instruments as high a priority as military capabilities. This implied the need for increased funding for foreign affairs programs.

In Sec. 7115, it was the sense of Congress that U.S. strategy to counter terrorism should include economic policies that encourage development, open societies, and opportunities for people. The Act further states that U.S. policy should include lowering of trade barriers for poor countries, as well as promote economic reform and rule of law, especially in Muslim countries.

[36] Prepared by (name redacted), Specialist in International Relations, Foreign Affairs, Defense, and Trade Division.

More concrete Congressional action related to these recommendations was not contained in P.L. 108-458. The Administration's and Congress' response to these recommendations was reflected to some degree in subsequent foreign relations authorizations and the FY2006 and FY2007 State Department and Foreign Operations Appropriations legislation. While the FY2007 appropriations have not yet been enacted, both the President's request and the relevant bills in the House and Senate reflect some of the priorities contained in the recommendations. Funding for diplomacy and foreign aid have been more closely tied to strategic requirements of the war on terrorism. Foreign aid to the "front-line states" in the war has been increased. More generally, economic assistance has been directed to reducing poverty, creating jobs, and improving education as an antidote to terrorist recruitment in impoverished areas. Resources have also been increased for improving America's image through public diplomacy and international broadcasting, as well as for cultural and educational exchange programs. In the FY2007 appropriations the Administration has requested funding to implement its "transformational diplomacy" and "transformational development" initiatives, aimed at revamping U.S. diplomacy and foreign aid policy for the 21st Century.

Public Diplomacy, Education and Exchange Programs[37]

Commission Concerns and Recommendations

Noting that terrorism is a result of resentment by some Muslims because of American engagement in the Muslim world, the 9/11 Commission asserted that public diplomacy is a key tool in the war on terrorism in helping to change attitudes about America. The Commission recommended that the United States, through the use of public diplomacy, convey respect for human dignity, assist in providing education for their children, and offer hope for economic opportunity. The Commission recommended that America more aggressively promote its values and advertise the aid given by the citizens of the United States. The Commission specifically recommended increasing funding for such public diplomacy activities as international broadcasting, exchanges, and overseas library programs, targeting these activities toward the youth.

Congressional Response

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) contained several measures intended to increase U.S. government public diplomacy activities as recommended by the 9/11 Commission. Sense of Congress provisions affirmed that the U.S. government should offer an example of values and respect for human dignity and should work with other governments to provide human dignity, economic opportunity, and tolerance. Furthermore, the United States should promote the ideas of individual freedom, educational opportunity, political participation and tolerance for opposing points of view.

[37] Prepared by (name redacted), Specialist in Foreign Policy and Trade, Foreign Affairs, Defense, and Trade Division.

Other provisions:

- stated that it is United States policy to promote free media and journalistic integrity overseas through public diplomacy programs and required establishing a media network with grants provided to the National Endowment for Democracy (NED) and authorizes such sums as may be necessary to establish the media network.
- required the Secretary of State to make public diplomacy an integral component in U.S. foreign policy and coordinate public diplomacy activities with all agencies as well as the Broadcasting Board of Governors.
- urged the Secretary of State to recruit, hire, train and promote Foreign Service Officers with an emphasis on public diplomacy and foreign languages of Muslim populations.
- declared that the President and Secretary of State should use the weight of the United States to promote public diplomacy in multilateral organizations and shall provide public diplomacy training for Foreign and Civil Service personnel who represent the United States in multilateral organizations.

For the Consolidated Appropriations Act of FY2005 (P.L. 108-447), conferees noted that alarming public opinion polls and media content continue to reveal profound anti-American sentiments and direct the Department of State to submit reports outlining the criteria for measuring performance of expanded public diplomacy efforts. This Act expanded funding for international information programs, cultural exchanges and international broadcasting, particularly in Muslim populations.

The 109th Congress made some gains in meeting the public diplomacy recommendations of the 9/11 Commission largely through the appropriations process. The Foreign Operations, Export Financing, and Related Programs Appropriation, FY2006 (P.L. 109-102) established a new account entitled Democracy Fund. This account is intended to increase effectiveness and oversight of programs that promote democracy, governance, human rights, independent media, and the rule of law globally. Within this new account amounting to $95 million for FY2006 is additional funding for the National Endowment for Democracy (NED), as well as other programs and countries.

Within the State Department appropriation for FY2006 (P.L. 109-108) Congress increased funding for already-established public diplomacy programs, including educational and cultural exchanges, international broadcasting, and regular appropriations for the NED. Additional funding for public diplomacy programs, specifically U.S. broadcasting into Iran, was included in the FY2006 supplemental (P.L. 109-234).

The 109th Congress also considered, but did not pass, Foreign Relations Authorization legislation (H.R. 2601/S. 600) which included measures to authorize grants be extended to the Middle East Broadcasting Networks (MBN), subject to specified limitations and restrictions, such as the Broadcasting Board of Governors (BBG) taking full responsibility for the direction taken by the MBN.

Terrorist Financing[38]

Commission Concerns and Recommendations

The report of the National Commission on Terrorist Attacks Upon the United States (the 9-11 Commission report) sought to refocus the policy debate concerning terrorist financing. The Commission recommended that the Bush Administration shift its focus from seizing terrorist funds to tracking terrorist financial networks in order to gain actionable counter-terrorism intelligence.[39] The Commission also emphasized terrorist organizations' increasing shift to informal methods of money transfer such as *hawala* or *hundi*.[40]

These recommendation have led to an ongoing discussion over the sources and methods used to collect financial intelligence. For example, Congress has investigated efforts by the Department of the Treasury to track international transfers of funds to and from terrorists by accessing information held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[41] SWIFT is a Brussels-based entity that serves as a major hub for international communications among banks and other financial institutions.

Given the experience of the five years since 9/11, legislators and executive branch officials have determined that combating terrorist financing requires effective coordination of many different federal government activities including intelligence gathering, financial regulation, law enforcement, and building international coalitions. Improving the interagency coordination of U.S. counter-terrorist financing efforts remains one of the largest challenges for the U.S. government. According to a 2006 Government Accountability Office report, "the U.S. government lacks an integrated strategy to coordinate the delivery of counter-terrorism financing training and technical assistance to countries it deems vulnerable to terrorist financing."[42] The report recommends, among other things, that the Secretaries of State and the Treasury implement an integrated strategic plan and a Memorandum of Agreement for the delivery of training and technical assistance.

In an effort to focus U.S. counter-terrorist financing efforts, in March 2004, the Department of the Treasury created the Office of Terrorism and Financial Intelligence (TFI). TFI was designed to integrate several offices within Treasury: the Office of Terrorist Financing and Financial Crime (TF/FC), the Office of Foreign Assets Control (OFAC), the Financial Crimes Enforcement Network (FinCEN), the Office of Intelligence and Analysis (OIA), and the Treasury Executive

[38] Prepared by (name redacted), Analyst in International Trade and Finance, Foreign Affairs, Defense and Trade.

[39] According to Commission Chairman Thomas Kean, "Right now we have been spending a lot of energy in the government trying to dry up sources of funding ... , obviously if you can dry up money, you dry it up, but we believe one thing we didn't do effectively is follow the money. That's what we have to do." Quoted in Laura Sullivan, "U.S. Split on Tracing, Freezing Terror Funds," *Baltimore Sun*, Aug. 2, 2004.

[40] See Nikos Passos, "Hawala and Other Informal Value Transfer Systems: How to Regulate Them?" available at http://usinfo.state.gov/eap/Archive_Index/Hawala_and_Other_Informal_Value_Transfer_Systems_How_to_Regulate_Them.html

[41] CRS Report RS22469, *Treasury's Terrorist Finance Program's Access to Information Held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, by (name redacted) and (name redacted).

[42] *Terrorist Financing: Better Strategic Planning Needed to Coordinate U.S. Efforts to Deliver Counter-Terrorism Financing Training and Technical Assistance Abroad*, United States Government Accountability Office, October 2005, GAO 06-19.

Office for Asset Forfeiture (TEOAF). In addition to an Under Secretary, four new senior level positions were created: Assistant and Deputy Assistant Secretaries for Terrorist Financing and Assistant and Deputy Assistant Secretaries for Intelligence and Analysis.

Congressional Responses

Several sections of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) address terrorist financing. The Act made technical corrections to the International Money Laundering Abatement and Anti-Terrorist Financing Act, Title III of the *USA PATRIOT Act* (P.L. 107-56) (Sec. 6202); authorized the Treasury to produce currency, postage stamps, and other security documents for foreign governments subject to certain conditions (Sec. 6301); and reauthorized funds for the biannual money laundering and financial crimes strategy report, the most recent of which was released in 2003 (Sec. 6102).[43] As of November 2006, the expected 2005 national money laundering and financial crimes strategy report has not been released.

The Act authorized funding to improve FinCEN (Sec. 6101). The Act authorized $19 million for improvements related to FinCEN's telecommunications and analytic capacity and authorized $16.5 million for the development of FinCEN's Bank Secrecy Act (BSA) Direct program. In June 2004, Treasury established the BSA Direct Retrieval and Sharing program (BSA R&S). This program was designed to make it easier for law enforcement to access and analyze BSA data and to improve overall data management. Treasury had trouble implementing the BSA R&S program due to problems with its main contractor, Electronic Data Systems. On July 13, 2006, FinCEN halted the program.[44] Robert Werner, FinCEN Director, testified on September 12, 2006 that FinCEN is initiating a "re-planning effort" for the retrieval and sharing component of BSA Direct. No expected completion date has been announced.[45]

The Act required the Secretary of the Treasury to prescribe regulations requiring selected financial institutions to report to FinCEN certain cross-border electronic transmittals of funds (wire-transfers) (Sec. 6302). New regulations must be promulgated by December 2007. Treasury is currently determining the feasibility and impact of these additional reporting requirements.[46]

The Act required the President to submit to Congress a report evaluating and making recommendations on: (1) the effectiveness of efforts and methods to track terrorist financing; (2) ways to improve governmental cooperation; (3) ways to improve the performance of financial institutions; (4) the adequacy of agency coordination and ways to improve that coordination; and (5) recommendations for changes in law and additional resources required to improve this effort (Section 6303). This report was due in September 2005 and has not yet been submitted to Congress.[47]

---

[43] "2003 National Money Laundering Strategy Report," Department of the Treasury, available at http://www.ustreas.gov/offices/enforcement/publications/ml2003.pdf.

[44] *FinCEN Halts BSA Direct Retrieval and Sharing Project*, Treasury Press Release, July 13, 2006, available at http://www.fincen.gov/bsa_direct_nr.html.

[45] Statement of Robert W. Werner, Director, Financial Crimes Enforcement Network United States Department Of The Treasury before The Senate Banking Committee, September 12, 2006, available at http://www.ustreas.gov/press/releases/hp101.htm.

[46] *FinCEN seeks industry input on feasibility of collection of cross-border wire transfer data*, Treasury Press Release, March 10, 2006, available at http://www.fincen.gov/fincennewsrelease03102006.html.

[47] Phone discussion with Treasury Legislative Affairs, November 29, 2006.

The Act requires the Secretary of the Treasury to work with the International Monetary Fund (IMF) to combat terrorist financing and to testify before Congress on the status of implementation of international anti-money laundering and counter-terrorist financing standards by the IMF and other multilateral agencies (Sec. 7703). The IMF is actively involved in establishing anti-money laundering standards and continues to review the anti-money laundering frameworks of IMF member countries.[48]

The Secretary of the Treasury is also required to continue to convene the interagency United States Government Financial Action Task Force (FATF) working group to review and develop U.S. and international anti-money laundering standards (Sec. 7704).[49] The U.S. government is actively involved in FATF operations and has promoted the adoption of international anti-terrorist financing best practices through engagement with and support of a number of FATF-style regional bodies, such as the Middle East and North Africa (MENA) FATF. In March 2006, the Treasury Department established a U.S.-MENA Private Sector Dialogue. A similar dialogue with the Latin American financial community is underway and Treasury is planning to hold an anti-money laundering conference in Latin America in early 2007.[50]

U.S. Military Forces and the War on Terrorism[51]

Commission Concerns and Recommendations

Recommendation 32 of the 9/11 Commission Report states that "the lead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department. There it should be consolidated with the capabilities for training, direction, and execution of such operations already being developed in the Special Operations Command." (Page 415).

The 9-11 Commission's apparent concern appeared to be both performance and cost-based. The report states that the CIA did not sufficiently invest in developing a robust capability to conduct paramilitary operations with U.S. personnel prior to 9/11, and instead relied on improperly trained proxies (foreign personnel under contract) resulting in an unsatisfactory outcome. The report also states that the United States does not have the money or people to build "two separate capabilities for carrying out secret military operations," and suggests that we should "concentrate responsibility and necessary legal authorities in one entity."

[48] "IMF Executive Board Reviews the Quality and Consistency of Assessment Reports for Anti-Money Laundering and Combating the Financing of Terrorism and the Effectiveness of Coordination," *International Monetary Fund Public Information Notice (PIN) No. 06/72*.

[49] The Financial Action Task Force is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. For more information on the Financial Action Task Force, see *Financial Action Task Force Annual Report 2005-2006*,available at http://www.fatf-gafi.org/dataoecd/38/56/37041969.pdf and CRS Report RS21904, *The Financial Action Task Force: An Overview*, by (name redacted).

[50] Testimony of Daniel Glaser, Deputy Assistant Secretary for Terrorist Financing and Financial Crimes before the Senate Committee on Banking, Housing, and Urban Affairs, September 12, 2006, available at http://banking.senate.gov/_files/glaser.pdf.

[51] Prepared by (name redacted), Specialist in National Defense, Foreign Affairs, Defense, and Trade Division.

Congressional Responses

Relevant Provisions Enacted by Congress

Section 1013 of P.L. 108-458 requires the National Intelligence Director, in consultation with the Secretary of Defense and the Director of the Central Intelligence Agency to develop joint procedures to improve the coordination and deconfliction in the planning, execution, and sustainment of operations involving DOD and the CIA. It also requires information exchange between the Secretary of Defense and Director CIA, so that senior operational officials have knowledge of the existence of all ongoing operations. When appropriate, it requires mutual agreement on tactical and strategic objectives.

Policy Concerns Not Addressed

P.L. 108-458 did not address the recommended shift of responsibility for paramilitary operations from the CIA to DOD. Some speculated that this particular issue was too complex and contentious to be included in intelligence reform legislation and that it required further study and analysis. Others suggested that there was no need to shift responsibilities, only to improve coordination and planning between the CIA and DOD which Section 1013 addresses.

Options Considered by the 109th Congress

The 109th Congress did not address this issue legislatively. On November 23, 2004, President Bush issued a letter requiring the Secretary of Defense and the Director of Central Intelligence to review matters relating to Recommendation 32 and submit their advice to him by February 23, 2005. This review directed the examination of all aspects including legal, funding, operational, and supporting infrastructure. A preliminary Pentagon study reportedly concluded that DOD should not take over the paramilitary responsibility from the CIA.[52] In unclassified testimony to the Senate Select Committee on Intelligence in February 2005, the Director of the CIA testified that the CIA and DOD disagreed with the 9-11 Committee's recommendation.[53] In June of 2005 it was reported that the Secretary of Defense and the Director of the Central Intelligence Agency responded to the President, stating that "neither the CIA nor DOD endorses the commission's recommendation on shifting the paramilitary mission or operations."[54] The Administration apparently accepted DOD's and the CIA's recommendation and reportedly rejected the 9-11 Commission's recommendation to shift the responsibility for paramilitary operations to DOD.[55]

[52] Ann Scott Tyson, "Study Urges CIA Not to Cede Paramilitary Functions to Pentagon," *Washington Post,* Feb. 5, 2005, p. 8.

[53] Transcripts, Senate Select Committee on Intelligence, Subject: National Security Threats to the United States, Federal New Service, February 16, 2005, p. 29.

[54] John J. Lumpkin, "Rumsfeld, Goss Oppose DOD Assumption of CIA Paramilitary Covert Operations," *Army Times,* June 29, 2005.

[55] Douglas Jehl, "White House is Said to Reject Panel's Call for a Greater Pentagon Role in Covert Operations," *New York Times,* June 28, 2005.

Weapons of Mass Destruction: Proliferation Security and Threat Reduction[56]

Commission Concerns and Recommendations

In view of intelligence assessments that al-Qaeda has been seeking to acquire weapons of mass destruction for several years, the 9/11 Commission concluded that WMD nonproliferation efforts should be expanded and provided additional resources. Specifically, the Commission recommended: (1) the development of an international legal regime "with universal jurisdiction" to interdict, capture, and prosecute those trafficking in WMD and related technology; (2) the expansion of the Proliferation Security Initiative (PSI) to include Russia, China, and all NATO countries; (3) the expansion of the Cooperative Threat Reduction (CTR) program and the provision of additional financial resources.

Congressional Responses

There has been no congressional initiative regarding the establishment of an international WMD anti-smuggling regime, aside from the continued full funding of the Proliferation Security Initiative (PSI).[57] The Administration has secured the passage of United Nations Resolution 1540 which requires member states to criminalize proliferation, establish export controls over WMD-related technology, and secure WMD-related materiel. The resolution does not provide for enforcement, nor address the establishment of any international anti-smuggling regime.

Members of the 109th Congress introduced several bills and resolutions that called for strengthening and expanding the PSI: S.Con.Res. 36, H.Con.Res. 133, S.Con.Res. 40, H.R. 422, H.R. 665, H.R. 5017/S. 3456, and S. 2566. None, however, was brought to the floor of either chamber. Geographic expansion remains a key issue—particularly how to engage China and India, as well as states in important regions like the Arabian Peninsula. The 110th Congress may consider how intelligence resources are handled. Is intelligence sufficient and are there intelligence-sharing requirements with non-NATO allies? Also, how is PSI coordinated with other federal interdiction-related programs (e.g., export control assistance)? One potential complication for congressional oversight of PSI is the absence of a way to measure PSI's success, relative to past efforts.

The Cooperative Threat Reduction (CTR) program (also known as Nunn-Lugar), which is administered by DOD's Threat Reduction Agency, continues to receive congressional funding support. In the FY2004 National Defense Authorization Act (P.L. 108-176, Sec. 1308), Congress authorized the Bush Administration to spend $50 million of unobligated funds from the Cooperative Threat Reduction Program in states outside the former Soviet Union. As of

[56] Prepared by (name redacted) and (name redacted), Specialists in National Defense, Foreign Affairs, Defense, and Trade Division.

[57] The PSI is an agreement among some nations to cooperate in the detection and interdiction of illicit WMD-related materiel shipments. Currently, sixteen nations are PSI participants. See also CRS Report RS21881, *Proliferation Security Initiative (PSI)*, by (name redacted).

September 2006, the Administration had spent such funds only in Albania ($38.5 million) for the purpose of eliminating chemical weapons stockpiles.

The 109th Congress considered the following legislation that could restrict the provision of CTR assistance to some countries. The State Department's annual foreign operations appropriations bill, the Foreign Operations, Export Financing, and Related Programs Appropriations Act, includes provisions that prohibit assistance to certain countries. Section 507 of the FY2006 foreign operations appropriations bill (P.L. 109-102) states that no funds will be "obligated or expended to finance directly any assistance or reparations to Cuba, Libya, North Korea, Iran, or Syria." The FY2007 bill passed in the House (H.R. 5522) and awaiting passage in the Senate includes the same provision. The Iran Freedom Support Act, introduced in both the House and the Senate (H.R. 282/S. 333), could make supplying CTR assistance to Iran more difficult. The Iran-Libya Sanction Act (P.L. 104-172) has been extended through September 2011, pursuant to the Iran Freedom Support Act (P.L. 109-293). Sudan has been severely limited from receiving U.S. assistance since 1997 by a combination of executive order and U.S. law. These include Executive Order 13067, Section 520 of the Foreign Operations, Export Financing, and Related Programs Appropriations Act, 2006 (P.L. 109-102), the Comprehensive Peace in Sudan Act of 2004 (P.L. 108-497) and The Sudan Peace Act (P.L. 107-245). The 109th also considered legislation that could affect third party states, or any state that could potentially receive CTR assistance, to the extent such states are considered for these initiatives. For example, Section 542 of the FY2006 foreign operations bill (P.L. 109-102) prohibited assistance to countries that provide lethal military equipment to State Sponsors of Terrorism. Other examples include P.L. 109-267 which extended the Iran-Libya Sanctions Act, the Iran Nonproliferation Amendments Act (P.L. 109-112), which added Syria to that Act, and the North Korea Nonproliferation Act of 2006 (S. 3728), which added North Korea to the Iran—Syria Nonproliferation Act.[58]

Border Security and Immigration[59]

Terrorist Travel

Commission Concerns and Recommendations

The 9/11 Commission issued several recommendations that directly pertain to immigration law and policy. These recommendations focused primarily on targeting terrorist travel through an intelligence and security strategy based on reliable identification systems and effective, integrated information-sharing, including the expansion and consolidation of the border-screening systems. More specifically, the 9/11 Commission concluded that targeting travel is at least as powerful a weapon against terrorists as targeting their money, and recommended that the United States combine intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.

[58] See also, CRS Report RL32359, *Globalizing Cooperative Threat Reduction: A Survey of Options*, by (name redacted).

[59] Prepared by (name redacted), Specialist in Immigration Policy, Domestic Social Policy Division.

Congressional Response[60]

The Intelligence Reform and Terrorism Prevention Act (ITRPA) of 2004 (P.L. 108-458) included several provisions aimed at targeting terrorist travel. The Act calls for the accelerated deployment of the biometric entry and exit system to process or contain certain data on aliens and their physical characteristics (see discussion below).[61] It required an in-person consular interview of most applicants for nonimmigrant visas between the ages of 14 and 79, and also required an alien applying for a nonimmigrant visa to completely and accurately respond to any request for information contained in his or her application.[62] The Act also expanded the pre-inspection program that places U.S. immigration inspectors at foreign airports, increasing the number of foreign airports where travelers would be pre-inspected before departure to the United States. Moreover, it required individuals entering the United States (including U.S. citizens and visitors from Canada and other Western Hemisphere countries) to bear a passport or other documents sufficient to denote citizenship and identity.

The Act required improvements in technology and training to assist consular and immigration officers in detecting and combating terrorist travel. It (1) established the Human Smuggling and Trafficking Center, which included an interagency program devoted to countering terrorist travel; (2) required the Secretary of Homeland Security, in consultation with the Director of the National Counter Terrorism Center, to establish a program to oversee DHS's responsibilities with respect to terrorist travel; and (3) established a Visa and Passport Security Program within the Bureau of Diplomatic Security at the Department of State.

In the 109th Congress, the REAL ID Act of 2005 (P.L. 109-13, Division B), among other things, required DHS to: conduct a study on U.S. border security vulnerabilities; establish a pilot program to test ground surveillance technologies on the northern and southern borders to enhance U.S. border security; and implement a plan to improve communications systems and information-sharing between federal, state, local, and tribal agencies on matters relating to border security. DHS was also required to submit reports to Congress regarding its implementation of these requirements.[63] The Secure Fence Act (P.L. 109-367) required DHS to deploy double-layer fencing to 850 miles of the U.S. international border with Mexico.[64]

[60] For further analysis, see CRS Report RL32616, *9/11 Commission: Legislative Action Concerning U.S. Immigration Law and Policy in the 108th Congress*, by (name redacted) and (name redacted).

[61] For background and analysis, see CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, by Lisa M. Seghetti and (name redacted).

[62] For background and analysis, see CRS Report RL31512, *Visa Issuances: Policy, Issues, and Legislation*, by (name redacted).

[63] For further discussion, see CRS Report RL33125, *Immigration Legislation and Issues in the 109th Congress*, by (name redacted) et al. For a legal analysis of the REAL ID Act, see CRS Report RL32754, *Immigration: Analysis of the Major Provisions of the REAL ID Act of 2005*, by (name redacted), (name redacted), and (name redacted).

[64] For more information on border fencing, see CRS Report RL33659, *Border Security: Barriers Along the U.S. International Border*, by (name redacted), Yule Kim, and (name redacted).

Terrorist Screening and Watch Lists[65]

Commission Concerns and Recommendations

The 9/11 Commission concluded that the U.S. intelligence and law enforcement community missed several vital opportunities to watch-list and screen several conspirators involved in the 9/11 terrorist attacks.[66] In addition, the Commission recommended that U.S. border security systems be integrated with other systems to expand the network of screening points to include the nation's transportation system and access to vital facilities.[67] Despite problems with high-profile misidentifications,[68] the Commission also recommended that the controversial "No-Fly" and "Automatic Selectee" lists maintained by the DHS's Transportation Security Administration be improved without delay.[69]

Congressional Response

In the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), Congress included several watch list related airline passenger prescreening provisions that require that airline passengers, among others, be prescreened against the consolidated terrorist watch list database. Another provision requires the Administration to report to Congress on (1) the criteria used to place persons on terrorism-related watch lists, and (2) the privacy and civil liberty implications of the further use of the "No Fly" and "Automatic Selectee" lists. These and other aviation security provisions are described below under "Transportation Security."

Related Administrative Response

Under Homeland Security Presidential Directive 6 (HSPD-6),[70] the Bush Administration elevated and expanded terrorist identification and watch-list functions by establishing a consolidated terrorist watch list database.[71] Undergirding these screening processes is a consolidated Terrorist Screening Database (TSDB), which under HSPD-6 has been established and maintained by the Terrorist Screening Center (TSC)—a multi-agency effort administered by the Federal Bureau of Investigation (FBI). Among other things, the TSC provides support to:

---

[65] Prepared by (name redacted), Specialist in Domestic Security, Domestic Social Policy Division.

[66] National Commission on Terrorist Attacks upon the United States, "Three 9/11 Hijackers: Identification, Watchlisting, and Tracking," Staff Statement no. 2, (Washington, 2004), p. 1.

[67] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, p. 387.

[68] Sara Kehaulani Goo, "Committee Chairman Runs Into Watch-List Problem: Name Similarity Led to Questioning at Anchorage and Seattle Airports, Alaska Congressman Says," *Washington Post*, Sept. 30, 2004, p. A17, and "Hundreds Report Watch-List Trials: Some Ended Hassles at Airports by Making Slight Change to Name," *Washington Post*, Aug. 21, 2004, p. A08.

[69] According to the FBI, the "No Fly" and "Automatic Selectee" lists have been consolidated in the TSDB and the lookout records on those lists are being expanded and improved. U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, "Terrorist Screening Center Consolidates Data for Law Enforcement Needs," *The CJIS LINK*, vol. 7, No. 4, October 2004, pp. 1-2.

[70] The TSC was established under HSPD-6. See, The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, Sept. 16, 2003). Available at http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html.

[71] For further information, see CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by (name redacted).

- the Department of State's Bureau of Consular Affairs by issuing terrorism-related security advisory opinions for visa issuance purposes;
- the Department of Homeland Security's (DHS's) Customs and Border Protection in evaluating potential matches between terrorist lookout records and persons entering the United States at international ports of entry; and
- nearly 750,000 state and local law enforcement officers to whom limited TSDB lookout records have been made available through the National Crime Information Center.

In April 2006, the DHS Privacy Office issued a report assessing the impact of the "No Fly" and "Automatic Selectee" lists on privacy and civil liberties.[72] The report cited concerns about the quality of the information of those lists, as well as the underlying intelligence.[73] The report also noted allegations about profiling on the basis of race, religion, or national origin, but reported that it could not substantiate those allegations.[74]

In regard to the criteria used to place individuals on terrorist watch lists, it is unknown whether the Administration reported to Congress on this matter. Nevertheless, the Privacy Office report stressed that those criteria could not be made public without: (1) comprising intelligence and security, or (2) allowing persons wishing to avoid detection to subvert those lists.[75]

In addition, in late September 2006, the Government Accountability Office (GAO) released a report on efforts to reduce the adverse effects of terrorist watch list screening, outlining measures that DHS and the TSC had taken to reduce and alleviate misidentifications.[76] It also noted that while the total number of misidentifications is unknown, their frequency, which is estimated to be in the tens-of-thousands, remains a serious concern.[77]

[72] U.S. Department of Homeland Security, *DHS Privacy Office Report on Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004,* April 27, 2006, 22 pp.

[73] Ibid., p. 8.

[74] Ibid., p. 9.

[75] Ibid.

[76] U.S. Government Accountability Office, *Terrorism Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, GAO-06-1031, Sept. 2006, p. 55.

[77] Ibid., p. 12.

Biometric Screening System and Data Systems Integration[78]

Commission Concerns and Recommendations

The 9/11 Commission called for the expeditious implementation of "a biometric entry-exit screening system, including a single system for speeding qualified travelers." With respects to biometrics, the 9/11 Commission noted the following: "Biometrics have been introduced into an antiquated computer environment" and that "replacement of these systems and improved biometric systems will be required." The 9/11 Commission also recommended the integration of the various border screening systems with the US-VISIT system, including frequent traveler programs such as NEXUS and the Secure Electronic Network for Travelers' Rapid Inspections (SENTRI).[79]

Congressional Responses[80]

In an effort to implement the 9/11 Commission recommendations, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). Previously, Congress passed legislation that mandated DHS to implement entry and exit controls and integrate immigration-related databases and data systems.

Congress first mandated that the former Immigration and Naturalization Service (INS) implement an automated entry and exit data system that would track the arrival and departure of every alien in §110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA; P.L. 104-208).[81] Several provisions in the Enhanced Border Security and Visa Entry Reform Act (Border Security Act; P.L. 107-173) and the Intelligence Reform and Terrorism Prevention Act of 2004, however, required the immediate implementation of an automated entry and exit data system and called for enhancements in its development, including a requirement that biometric identifiers be used in all visas and other travel documents and that the entry and exit data system be interoperable with other law enforcement and national security databases. Congress, however, first required the entry and exit data system be interoperable with other law enforcement systems in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act; P.L. 107-56). The PATRIOT Act was also the first time Congress required the development and certification of a technology standard that has the capacity to verify the identity of persons applying for a visa or seeking to enter the United States.

[78] Prepared by (name redacted), Analyst in Domestic Security, Domestic Social Policy Division.

[79] Ibid, pp. 388-389.

[80] For further information on the U.S. VISIT program and immigration-related border security measures passed by Congress, see CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, by Lisa M. Seghetti and (name redacted); and CRS Report RL31727, *Border Security: Immigration Issues in the 108th Congress*, by Lisa M. Seghetti.

[81] Subsequent legislation amended §110 of IIRIRA by either changing the scope of categories of aliens who would be subjected to entry and exit controls, or delayed implementation of the system. See the INS Data Management Improvement Act (DMIA; P.L. 106-215); the Visa Waiver Permanent Program Act (VWPPA; P.L. 106-396).

The Intelligence Reform and Terrorism Prevention Act of 2004 called for the Secretary of DHS (Secretary) to develop a plan to accelerate the full implementation of an automated biometric entry and exit data system and to submit a report to Congress on the plan by July 17, 2005. The Act required the entry and exit data system to collect "biometric *exit* data for all categories of individuals who are required to provide biometric entry data."

The Act also required the integration of all databases and data systems that process or contain information on aliens by December 2006. The Act required the integrated data system to be an interoperable component of the entry and exit data system. The Act further required the Secretary to fully implement the interoperable electronic data system as specified in the Border Security Act. In addition to the integration of the entry and exit data system with other databases and data systems, the Act required the Secretary to develop and implement a plan to expedite the processing of registered travelers through a single registered traveler program that can be integrated into the broader automated biometric entry and exit data system.

Standards for Identification Documents[82]

Commission Concerns and Recommendations

The 9/11 Commission recommended that standards should be set "for the issuance of birth certificates and sources of identification, such as drivers licenses." The 9/11 Commission noted that fraudulent documents are " ... no longer just a problem of theft," and that ports of entry are "the last opportunity to ensure that people are who they are ... " Additionally, the 9/11 Commission recommended the elimination of the "Western Hemisphere Exception," whereby U.S. citizens returning from countries in the Western Hemisphere, and some citizens from designated Western Hemisphere nations, are not required to show a passport when entering the United States (but they are required to demonstrate citizenship). In doing so, the 9/11 Commission advocated for ensuring that all individuals presenting themselves for entry into the United States present biometric passports or other identification allowing their identities to be securely verified.

Congressional Response

In the 108th Congress, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required the establishment of new standards aimed at ensuring the integrity for federal use of birth certificates, state-issued driver's licenses and identification cards, and social security cards. States may receive grants to assist them in implementing the proposed birth certificate and driver's license standards.[83] In the 109th Congress, the REAL ID Act of 2005 (P.L. 109-13, Division B) addressed this issue more directly, and while the Act does not directly impose federal standards with respect to states' issuance of driver's licenses and personal identification cards, states nevertheless appear to need to adopt such standards and modify any conflicting

[82] Prepared by (name redacted), Specialist in Immigration Policy, and (name redacted), Analyst in Domestic Security, Domestic Social Policy Division.

[83] For further discussion, see CRS Report RL32722, *Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Driver's Licenses, Social Security Cards, and Birth Certificates*, by (name redacted).

laws or regulations in order for such documents to be recognized by federal agencies for official purposes.[84]

The Intelligence Reform and Terrorism Prevention Act of 2004 also addressed the "Western Hemisphere Exception" by requiring individuals entering the United States (including U.S. citizens and visitors from Canada and other Western Hemisphere countries) to bear a passport or other documents sufficient to denote citizenship and identity as of January 1, 2008. In the 109th Congress, the fiscal year (FY) 2007 DHS Appropriations Act (P.L. 109-295) extended this deadline to the earlier of two dates: June 1, 2009; or no later than three months after the Secretary of Homeland Security and the Secretary of State certify that a series of implementation requirements have been met.[85]

Other Immigration Concerns[86]

Commission Concerns

Reforming the enforcement of immigration law is an underlying theme of the recommendations made by the 9/11 Commission. The 9/11 Commission concluded that the key officials responsible for determining alien admissions (consular officers abroad and immigration inspectors in the United States) were not considered full partners in counterterrorism efforts prior to September 11, 2001, and as a result, opportunities to intercept the September 11 terrorists were missed.[87]

They further recommended that the U.S. border security system be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. In addition, they maintained that the Department of Homeland Security, with proper support from Congress, should complete a biometric entry-exit screening system, including a single system for speeding qualified travelers, as quickly as possible. They also expressed the view that the U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments.[88]

Congressional Response

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) included many immigration-related provisions aimed at addressing broad immigration enforcement concerns raised by the 9/11 Commission. The major features of these immigration-related provisions are summarized below.[89]

---

[84] For a legal analysis of the REAL ID Act, see CRS Report RL32754, *Immigration: Analysis of the Major Provisions of the REAL ID Act of 2005*, by (name redacted), (name redacted), and (name redacted).

[85] For further discussion, see CRS Report RL33125, *Immigration Legislation and Issues in the 109th Congress*, by (name redacted) et al.

[86] Prepared by (name redacted), Specialist in Immigration Policy, Domestic Social Policy Division.

[87] U.S. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, Executive Summary, p. 14, July 2004 (hereafter *The 9/11 Commission Report*).

[88] For a discussion of these recommendations, see *The 9/11 Commission Report*, Chapter 12.4, pp. 383-389, July 2004.

[89] For further analysis, see CRS Report RL32616, *9/11 Commission: Legislative Action Concerning U.S. Immigration Law and Policy in the 108th Congress*, by (name redacted) and (name redacted).

Grounds for Alien Exclusion, Removal, and Relief from Removal

The Intelligence Reform and Terrorism Prevention Act made any alien deportable who has received military training from or on behalf of an organization that, at the time of training, was a designated terrorist organization. It also made the revocation of a nonimmigrant visa by the State Department grounds for removal. The visa revocation, however, is reviewable in a removal proceeding in cases where visa revocation provides the sole ground for removal. The Act made inadmissible and deportable any alien who (1) has ordered, incited, assisted, or participated in conduct that would be considered genocide under U.S. law; (2) committed or participated in an act of torture or an extrajudicial killing; or (3) while serving as a foreign official, was responsible for or directly carried out, at any time, particularly severe violations of religious freedom. The Act also required the Government Accountability Office to conduct a study evaluating the degree that weaknesses in the current U.S. asylum system have been or could be exploited by aliens involved in terrorist-related activity.

Allocation of Additional Resources to Improve Enforcement

The Act authorized the Secretary of State to increase the number of consular officers by 150 per year from FY2006 through FY2009 above the number of such positions for which funds were allotted for the preceding fiscal year. It also increased the numbers of border patrol agents by not less than 2,000, in each year FY2006 through FY2010, and required a number of agents equaling at least 20% of each year's increase in agents to be assigned to the northern border. The Act also increased the number of ICE investigators by not less than 800 in each year FY2006 through FY2010, and required an increase in the number of beds available for immigration detention and removal operations by not less than 8,000 over the same period. Further, the Act established a pilot program to test advanced technologies to improve border security between ports of entry along the northern border of the United States. It also required the Secretary of Homeland Security to submit to the President and Congress a plan for the systematic surveillance of the southwest border of the United States by remotely piloted aircraft, and to implement such plan as a pilot program.

In the 109th Congress, the REAL ID Act required DHS to develop a pilot program to increase the use of ground-surveillance technologies, including video cameras, sensors, and motion-detection technology, to monitor the northern and southwestern borders. The Secure Fence Act (P.L. 109-367) required DHS to deploy double-layer fencing to 850 miles of the U.S. international border with Mexico.[90]

Penalties for Immigration-Related Fraud and Alien Smuggling

The Intelligence Reform and Terrorism Prevention Act increased criminal penalties for alien smuggling in certain circumstances and required the Secretary of Homeland Security to develop an outreach program in the United States and overseas to educate the public about the penalties for illegally bringing in and harboring aliens.

[90] For more information on border fencing, see CRS Report RL33659, *Border Security: Barriers Along the U.S. International Border*, by (name redacted), Yule Kim, and (name redacted).

Transportation Security

Aviation Security[91]

Commission Concerns and Recommendations[92]

The 9/11 Commission expressed concerns over air cargo security, the security of general aviation aircraft, screening of airline passengers and baggage, and access controls at airports. The 9/11 Commission made several specific recommendations to address these concerns.

The 9/11 Commission recommended that improved passenger prescreening not be further delayed by the long-running argument about a successor to the existing computer assisted passenger prescreening (CAPPS) program run by the airlines.[93] The 9/11 Commission recommended that the Transportation Security Administration (TSA) take over the function of prescreening passenger names using the larger set of watchlists maintained by the federal government and that the airlines should be compelled to provide the data needed to test and implement this new prescreening system.

The 9/11 Commission also recommended that the TSA and the Congress give priority attention to improving checkpoint screening for detecting explosives on passengers. It recommended that the TSA also conduct a human factors study to examine screener performance, and establish objectives for screeners and screening checkpoints.

The Commission expressed continued concerns over the screening of checked baggage and cargo. It indicated that the TSA should expedite the installation of advanced in-line baggage screening systems that are integrated with airport baggage processing systems. The Commission noted that, because the aviation industry will derive substantial benefits from this deployment, it should pay a fair share of the associated costs, although the commission did not provide specifics regarding recommended allocation of contributions to pay for in-line explosive detection systems integration.

The Commission recommended that the TSA intensify efforts to identify, track, and screen potentially dangerous cargo in aviation as well as in maritime operations. Additionally, the Commission specifically recommended the deployment of at least one hardened cargo container on every passenger aircraft that also hauls cargo to carry any suspicious shipments.

In addition to these recommendations directly addressing aviation security, the 9/11 Commission also urged establishing risk-based priorities for protecting transportation assets in all modes. It recommended that the TSA select the most practical and cost effective approaches for defending transportation assets and formalize a plan for implementing, budgeting, and funding this effort.

---

[91] Prepared by (name redacted), Specialist in Aviation Safety, Security, and Technology, Resources, Science, and Industry Division.

[92] For more information see CRS Report RL32541, *Aviation Security-Related Findings and Recommendations of the 9/11 Commission*, by (name redacted).

[93] In addition to CAPPS, current prescreening procedures involve checking passenger name records against "automatic-selectee" and "no-fly" lists provided to the airlines by the Transportation Security Administration (TSA).

The 9/11 Commission noted that the plan should assign roles to federal, state, and local authorities, as well as to private stakeholders.

Congressional Response

The 108th Congress passed two major pieces of legislation containing numerous provisions pertaining to aviation security: Vision 100—Century of Aviation Reauthorization Act (P.L. 108-176) and the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458).

Vision 100—Century of Aviation Reauthorization Act

Before the 9/11 Commission had completed its report, several aviation security-related provisions were included in Vision 100—Century of Aviation Reauthorization Act (P.L. 108-176) which was enacted on December 12, 2003. Vision 100:

- established a redress process for pilots, mechanics or other licensed aviation professionals whose certification is denied, suspended, or revoked on the grounds that they pose a risk to aviation security. Vision 100 also requires the Federal Aviation Administration to provide a justification to Congress when establishing an Air Defense Identification Zone (ADIZ) around cities where pilots are required to use special communications and operating procedures to enable air traffic controllers to identify potential security threats.
- modified existing requirements for security training of airline flight and cabin crew members. Under these provisions, the airlines are responsible for providing mandatory basic training in security for crews, while the TSA was to develop and provide a voluntary advanced self-defense training program for crew members.
- required the Department of Homeland Security to study and report to Congress on the effectiveness of the aviation security system, including the air marshal program, hardening of cockpit doors, and security screening of passengers, checked baggage, and cargo. The report was to include recommendations, including legislative recommendations, for improving the effectiveness of aviation security.
- created the Aviation Security Capital Fund. The Act authorizes up to $500 million per year through FY2007 to be appropriated to this fund and requires that the first $250 million in aviation security fee collections be deposited in this fund each year through FY2007. The Act also provided the Under Secretary for Border and Transportation Security with the authority to issue grants to airports for projects to integrate baggage explosive detection systems with baggage conveyer systems; reconfigure terminal baggage areas as needed to install explosive detection systems; deploy explosive detection systems behind the ticket counter, in baggage sorting areas, or in line with baggage handling systems; and for other aviation security-related capital improvement projects. Vision 100 set the federal share of costs for such projects at 90% for large and medium hub airports, and at 95% for all other airports and set guidelines for the allocation of Aviation Security Capital Fund monies for these projects. However, appropriations language (see, for example, P.L. 109-295) has limited the federal share to 75% for large and medium hubs, and 90% for all other airports.

- required the implementation of security programs for air charter operators who use aircraft weighing more than 12,500 pounds maximum takeoff weight.
- required the Government Accountability Office (GAO) to review the proposed CAPPS II passenger prescreening system and prevented the TSA from fully implementing this program until the Under Secretary for Border and Transportation Security certified that a variety of enumerated issues pertaining to civil liberties, privacy, data protection, system security, system performance, and system oversight had been adequately addressed. The TSA has since scrapped the CAPPS II program and is developing an alterative prescreening system called "Secure Flight."
- authorized flight crew members of all-cargo airlines to voluntarily participate in the Federal Flight Deck Officer Program that trains and deputizes armed pilots to guard aircraft cockpits against hostile attacks. Vision 100 also expanded the program to include other flight crew members, such as flight engineers, in addition to pilots.
- requires the promulgation of regulations to ensure the security of foreign and domestic aircraft repair stations. The Act also requires the TSA, in coordination with the FAA, to complete a security review and audit of foreign repair stations that work on air carrier aircraft and components.
- modified the background check requirements for foreign pilots seeking flight training in the United States. The Act transferred the duties of conducting these background checks from the Department of Justice to the DHS. The provisions require flight schools or instructors to provide notification and identification information for individuals seeking training in smaller aircraft, weighing less than 12,500 pounds, and require background checks be completed before training can be initiated in larger aircraft. The legislation authorizes fee collections to offset the costs of conducting these background checks.[94]

The Intelligence Reform and Terrorism Prevention Act of 2004

The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) contains numerous provisions related to aviation security, many directly addressing the concerns and recommendations of the 9/11 Commission. The Act:

- requires the Department of Homeland Security to develop, prepare, implement, and update as needed, a National Strategy for Transportation Security as well as modal-specific security plans including a plan for aviation security. The modal security plan for aviation is to include a threat matrix outlining each threat to the United States civil aviation system and the corresponding layers of security in place to address these threats and a plan for mitigation and reconstitution of the aviation system in the event of a terrorist attack.

[94] For further discussion, see CRS Report RL32498, *Vision 100: Historical Review of the Century of Aviation Reauthorization Act (P.L. 108-176)*, by (name redacted), (name redacted), and (name redacted).

- requires the TSA to issue guidance for the use of biometrics in airport access control systems and establish biometric credential and authentication procedures to identify law enforcement officers authorized to carry firearms aboard passenger aircraft. The Act authorizes $20 million, in addition to any other authorized amounts, for research and development of biometric technologies for aviation security. The Act also authorizes $1 million to establish a center of excellence in biometric technologies.
- required the TSA to begin system testing of an advanced passenger prescreening system by January 1, 2005. Although the Act does not provide a deadline for the completion of testing the prescreening system, it requires the TSA to begin to assume the role of passenger prescreening and checking passenger names against watch lists no later than 180 days after completing that testing. The Act requires the TSA to establish redress and remedy procedures for passengers who are delayed or denied boarding because of being falsely identified or targeted by the system, and requires the TSA to ensure that the number of such false positives is minimized. The Act also requires the TSA to establish an oversight board and implement safeguards to ensure the security and integrity of the system and address and resolve any privacy concerns. The Act also requires that the DHS prescreening of international flights to or from the United States be conducted prior to departure.
- requires that individuals seeking FAA certificates, such as pilots and mechanics, as well as individuals requesting unescorted access to airport secure areas and air operations areas be screened against the consolidated and integrated terrorist watch list. The Act also requires the TSA to establish a process where air charter and leasing companies can voluntarily submit information regarding prospective customers seeking to use aircraft weighing more than 12,500 pounds for prescreening.
- requires the Security Privacy Officer of the Department of Homeland Security to report on the impact of the automatic selectee and no fly lists on privacy and civil liberties and the Director of National Intelligence, in consultation with the Secretary of Homeland Security, the Secretary of State, and the Attorney General, to report on the criteria and standards applied in placing the names of individuals on the consolidated screening watch list.
- directs the DHS to give high priority to developing, testing, improving, and deploying airport checkpoint screening technologies to detect nonmetallic, chemical, biological, and radiological weapons, and explosives on passenger and carry-on items and requires the DHS to create a strategic plan for the deployment and use of explosive detection equipment at airport screening checkpoints. The Act requires the TSA to initiate a pilot program to test advanced airport checkpoint screening systems at five or more airports by March 31, 2005 and authorizes $150 million per year in FY2005 and FY2006 to carry out this pilot. The Act also requires the TSA to carry out and report on a human factors study to better understand problems with screener performance and take such action as may be necessary to improve the job performance of airport screening personnel.
- requires the Federal Air Marshal Service to continue operational initiatives to protect the anonymity of Federal air marshals. The Act also provides for training law enforcement officers authorized to carry firearms on passenger aircraft in

inflight counterterrorism and weapons handling procedures and in the identification of fraudulent identification documents such as passports and visas. The Act also encourages the President to pursue international agreements to allow the maximum deployment of Federal air marshals on international flights, and authorizes the DHS to provide air marshal training to foreign law enforcement personnel.

- authorizes the TSA to take necessary action to expedite the installation and use of in-line baggage screening equipment at airports. The Act further requires the TSA to establish a schedule to expedite this activity and study cost-sharing options among federal, state, and local governments, and the private sector for integrating in-line baggage screening systems. The Act increases the authorization for the aviation security capital fund by authorizing up to $400 million per year through FY2007, in addition to the initial $250 million deposited from aviation security fee collections set forth in Vision 100.
- directs the TSA to study the application of readily available wireless communication technologies to enable cabin crew members to discreetly notify the pilot in the case of a security breach or safety issue occurring in the cabin.
- requires the FAA to begin issuing tamper resistant pilot licences with a photograph of the bearer. The license is to be capable of accommodating a digital photograph, a biometric, or any other unique identifier considered necessary for identification purposes.
- requires the TSA to develop and report to Congress on standards for determining appropriate screener staffing levels at airports that provide necessary levels of security and keep passenger wait times to a minimum. The DHS is also to study the feasibility of integrating operations of the screening workforce and other aviation security-related DHS functions to coordinate these activities and increase their efficiency and effectiveness. The Act also authorizes the expenditure of $100 million for research and development of improved explosive detection systems and directs the TSA to develop a plan and guidelines for implementing these systems.
- required the TSA to prohibit airline passengers from carrying butane lighters and any other objects considered by the TSA to be inappropriate carry-on items.
- directs the President to urgently pursue international treaties to limit the availability, transfer, and proliferation of Man-portable Air Defense Systems (MANPADS), such as shoulder-fired missiles, worldwide. The Act further directs the President to continue to pursue international arrangements for the destruction of excess, obsolete, and illicit MANPADS stockpiles worldwide. The Act requires the President to report on diplomatic efforts to address MANPADS non-proliferation and requires the Secretary of State to provide the Congress with annual briefings on the status of these efforts. The Act also requires the FAA to establish a process for expedited certification of airworthiness and safety for missile defense systems that can be mounted on commercial aircraft. The Act also requires the DHS to provide a report within one year assessing the vulnerability of aircraft to MANPADS attacks and plans for securing airports and aircraft from this threat.

- requires that a pilot program be established to evaluate the use of blast-resistant cargo containers. The Act authorizes $2 million to carry out this pilot program. The Act also authorizes $200 million each year through FY2007 for improved air cargo and airport security related to the transportation of cargo on both passenger aircraft and all-cargo aircraft, and $100 million per year through FY2007 for the research, development, and deployment of technologies to better identify, track, and screen air cargo. The Act establishes a grant program to encourage the development of advanced air cargo security technology. The Act also requires the TSA to issue a final rule regarding its proposed regulations for the security of cargo operations for both passenger and all-cargo aircraft. Finally, the Act requires the DHS, in coordination with the Department of Defense and the FAA, to report on the threats posed by international cargo shipments bound for the United States and provide an analysis of the potential for establishing secure facilities along established international aviation routes for the purposes of diverting and securing aircraft believed to pose a security threat.

In addition to the air-cargo security provisions in the Intelligence Reform and Terrorism Prevention Act of 2004, the Department of Homeland Security Appropriations Act, 2005 (P.L. 108-334, Sec. 513) directs the DHS to research, develop, and procure certified systems to inspect and screen air cargo on passenger aircraft at the earliest date possible and amend security directives and procedures to, at a minimum, triple the percentage of cargo inspected on passenger aircraft.

Policy Concerns Not Addressed In Enacted Legislation

Since several major provisions pertaining to aviation security were enacted during the 108th Congress—many directly reflecting the concerns and recommendations of the 9/11 Commission—there are few policy concerns that have not been addressed to some degree. During the 109th Congress, aviation security legislation directly addressing 9/11 Commission findings and recommendations were not taken up. However, two areas where some may consider that policy concerns have not been adequately addressed through legislation include general aviation security and air cargo security procedures and oversight.

The 9/11 Commission made brief reference to concerns over the security of general aviation operations, however it did not make any formal recommendations to address this concern. During the 108th Congress, legislation on the security of general aviation operations focused on airport and airspace restrictions and examining ways to alleviate what some believed to be unnecessary constraints on certain operations. For example, a provision in Vision 100 required the DHS to develop and implement a security plan allowing general aviation flights to resume at Ronald Reagan Washington National Airport but set no timetable for carrying out this provision. The TSA has now implemented regulations allowing certain general aviation flights, adhering to extensive operational requirements, to operate to and from Ronald Reagan Washington National Airport. In appropriations language, however, temporary flight restrictions over stadiums and other venues during major outdoor sports events were kept in full force and made permanent. Arguably, the legislation pertaining to general aviation security enacted to date has been viewed by many as not being as cohesive and comprehensive as legislation addressing other aviation security concerns.

Some may also argue that comprehensive legislation pertaining to air cargo security operations and oversight and expansion of the known-shipper program have not been adequately addressed. Specifically, comprehensive measures that had been passed by the Senate in the 108th Congress (see S. 165, 108th Congress) were stripped from the final version of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) and replaced by language directing the TSA to issue final rulemaking addressing these issues. This was presumably done because the TSA's regulatory proposals largely reflected the intent of the proposed legislation. However, because Congress did not formally enact several of these specific provisions pertaining to air cargo security operations and oversight, the 110th Congress may be particularly interested in oversight of the TSA's implementation of its air cargo security rules and its air cargo strategic plan to ensure that they meet desired objectives.

Port and Maritime Security[95]

Commission Concerns and Recommendations

The 9/11 Commission was not as specific in making recommendations for non-aviation modes of transportation as it was for aviation.[96] However, one conclusion of the 9/11 Commission is that transportation security resources are not being "allocated to the greatest risks in a cost effective way... Opportunities to do harm are as great, or greater, in maritime or surface transportation [than in aviation]."[97] The 9/11 Commission also reported that deployment of scanning technologies designed to screen containers that can be transported by plane, ship, truck, or rail is still years away.[98]

Under "Strategies for Aviation and Transportation Security," the 9/11 Commission recommended that the federal government 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 Commission recommended that the plan assign roles and missions to the relevant authorities (federal, state, regional, and local) and to private stakeholders. The Commission further noted that perfection is unattainable but that terrorists should perceive that potential targets are defended in order to deter them. It also recommended that Congress set specific dates for the completion of these plans.

Congressional Response

Since September 11, 2001, Congress has enacted two major port and maritime security acts. The Maritime Transportation Security Act of 2002 (MTSA, P.L. 107-295), which was passed by Congress on November 25, 2002, requires ports and vessels to take certain security measures to safeguard their operations and puts the U.S. Coast Guard in charge of enforcing these security

[95] Prepared by (name redacted), Specialist in Transportation, Resources, Science, and Industry Division.

[96] Another commission, The Interagency Commission on Crime and Security in U.S. Seaports, that was established by the Clinton Administration in April 1999 and which reported their findings in the fall of 2000, made 20 specific recommendations for improving port security, most of which have been acted upon since September 11, 2001. This commission's report is available at http://www.securitymanagement.com/library/seaport1200.pdf.

[97] *The 9/11 Commission Report*, p. 391.

[98] Ibid., pp. 391-92.

measures. The SAFE Ports Act (P.L. 109-347), which was passed by Congress on September 30, 2006, requires shippers to take certain security measures to safeguard their cargo from terrorist infiltration and puts U.S. Customs and Border Protection (CBP) in charge of ensuring compliance. Sections 70102 and 70103 of MTSA requires the DHS to prepare a National Maritime Transportation Security Plan and vulnerability assessments of individual marine facilities and vessels. However, these two sections of MTSA did not impose deadlines on DHS in carrying out the prescribed security planning activities. Section 4072 of IRTPA (P.L. 108-458) imposed a deadline of April 1, 2005 for completion of the National Maritime Transportation Security Plan and a deadline of December 31, 2004 for the completion of marine facility and vessel vulnerability assessments. The Administration completed its National Strategy for Maritime Security in September 2005[99] and completed a National Strategy for Transportation Security in August 2006.[100]

The Coast Guard and Maritime Transportation Act of 2004 (P.L. 108-293) was signed into law on August 9, 2004. Title VIII of the Act contains a number of provisions related to maritime security, many of which add specificity to provisions in MTSA. Among other things, the Act requires the DHS to submit a plan to Congress implementing a maritime intelligence system (section 803); it requires the DHS to submit a plan for a maritime security grant program, including recommendations on how funds should be allocated (section 804); it requires the DOT to investigate and examine sensors that are able to track marine containers throughout their supply chain and detect hazardous and radioactive materials within the containers (section 808); it requires the DHS to report on the costs of vessel and container inspections, and a plan for implementing secure systems of transportation, including the need for and feasibility to inspect and monitor intermodal shipping containers within the United States (section 809).

The SAFE Ports Act requires DHS to set up a pilot program at three overseas ports to test the feasibility of scanning all containers bound for the United States at those ports before they are loaded onto a ship. Currently, under the Container Security Initiative (CSI), which is operational at 50 overseas ports accounting for approximately 90% of transatlantic and transpacific containerized cargo, U.S. CBP reviews cargo manifest information at these 50 loading ports to target certain high-risk or unknown-risk containers for closer inspection.[101] At U.S. ports, CBP has thus far deployed 267 Radiation Portal Monitors (RPMs) to scan containers before they leave the port for their final inland U.S. destination.[102] By the end of 2006, CBP expects 75% of containers will be scanned by RPMs and has a goal of scanning 98% by the end of 2008.[103] The SAFE Ports Act authorizes the CSI program and requires DHS to scan all containers for radiation entering the 22 busiest U.S. ports by the end of 2007. In addition, the Act also authorizes the Domestic Nuclear Detection Office within DHS whose primary mission is to further advance and deploy nuclear detection technology. The SAFE Ports Act also modifies the port security grant program from awarding grants in a "fair and equitable" manner to awarding grants based solely on risk.

[99] See http://www.whitehouse.gov/homeland/maritime-security.html#annex.

[100] This document is designated as "Sensitive Security Information."

[101] U.S. CBP, *CSI Fact Sheet*, September 28, 2006.

[102] DHS, *Fact Sheet: Protecting the Homeland Post September 11*, September 11, 2006.

[103] Ibid.

Surface Transportation Security[104]

Commission Concerns and Recommendations

The 9/11 Commission expressed concern that transportation security resources may not be allocated to the greatest risks in a cost-effective way. They noted the government did not have a strategic plan that analyzed assets, risks, and costs and benefits of security measures for the entire transportation system, nor was there a specific security plan for each transportation mode. The Commission recommended that such a strategic plan be prepared to: identify the assets that need protection; set risk-based priorities for defending them; select the most cost-effective ways of protecting those assets; then develop a plan, budget, and funding to implement this strategy, assigning roles and missions to federal, state, regional and local governments and private stakeholders.

Status of Implementation of the Recommendations

The 108th Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), which includes a provision directing the Department of Homeland Security to create a National Strategy for Transportation Security (NSTS). The Act directed that the NSTS should identify national transportation assets, set risk-based priorities for their protection, assign responsibilities for their protection, and recommend appropriate levels and sources of funding for these efforts. The Department of Homeland Security submitted the NSTS, in the form of a classified report, to Congress in the fall of 2005; an update was submitted in the summer of 2006. The initial version of the NSTS was criticized by the original 9/11 Commission members, acting as a private organization called the "9/11 Public Discourse Project," as lacking "the necessary detail to make it an effective management tool."[105] The Government Accountability Office has noted that the use of risk management in homeland security is relatively new, and that addressing risk across different types of infrastructure with multiple parties involved is highly complex.[106]

In June 2006, DHS issued a National Infrastructure Protection Plan (NIPP) which is to serve as a guide to using risk management principles for prioritizing protection efforts within infrastructure sectors (e.g., transportation) and across sectors.[107] The NIPP requires that sector-specific agencies submit plans to DHS by December 2006 identifying critical assets, evaluating the risk to them, and developing measures to protect them.

[104] Prepared by (name redacted), Analyst in Transportation, Resources, Science, and Industry Division.

[105] 9/11 Public Discourse Project, *Final Report on 9/11 Commission Recommendations*, December 5, 2005. Available at http://www.9-11pdp.org/press/2005-12-05_report.pdf (viewed 11/29/2006).

[106] Government Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91, December 15, 2005.

[107] Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07-39, October 16, 2006, p. 2-3.

As for the recommendation that a plan, budget, and funding be provided to implement the NSTS which assigns roles and missions to federal, state, regional and local governments and private stakeholders, the NIPP calls for the sector plans to be developed by councils of federal, state, and regional and local government agencies involved in that sector, along with sector councils made up of private sector stakeholders. The government council for the transportation sector was formed in January 2006, but, alone among the seventeen infrastructure sectors, the transportation sector does not yet have a private sector council.[108]

Congress also began providing funding for grants to transit and rail agencies for security improvements in the annual Department of Homeland Security appropriations bill. Congress provided $150 million in FY2005 and FY2006 and $175 million in FY2007 for this program. As the NSTS had not been completed at the time the grants began, and the risk-based allocation process to implement the NSTS has not been developed, this grant program has operated independently of the NSTS. Several proposals have been introduced in Congress to authorize new multi-billion dollar grant programs to fund security improvements for passenger rail, freight rail, and public transit organizations.

Critical Infrastructure Security[109]

Commission Concerns and Recommendations

The 9/11 Commission expressed its concerns and recommendations regarding critical infrastructure security in three primary areas: transportation security, allocation of assistance to states and localities, and the adequacy of the government's plans, in general, to protect the nation's critical infrastructure. The Commission devoted most of its attention to the transportation infrastructure, and, in particular, aviation security; making relatively specific recommendations in specific areas (e.g., explosive detection). It also recommended that a date specific be set for the Department of Homeland Security to complete its security plans for all transportation modes, as called for in the Aviation and Transportation Security Act (P.L. 107-71). In regard to the allocation of federal assistance, the Commission recommended that the allocation to states and localities be based on an assessment of risks and vulnerabilities and no longer remain a "program for general revenue sharing." While much of the federal assistance to states and localities supports response capabilities, some is also devoted to the protection of critical infrastructure. In the background discussion for its final recommendation, the Commission stated that the Department of Homeland Security (DHS) should identify those elements of the nation's critical infrastructure (beyond just the transportation sector) that need protection and to develop plans to protect them. It recommended that the Department and its oversight committees should regularly assess the types of threats facing the nation's critical infrastructure to determine the adequacy of the government's plans to protect and respond to a terrorist attack on critical infrastructure across all relevant sectors. The rest of this discussion focuses on this last recommendation. A discussion of the first two areas can be found elsewhere in this report under Border and Transportation Security and Emergency Response and Preparedness. Also, a more detailed discussion of the Commission's recommendations related to critical infrastructure protection and the subsequent

[108] Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07-39, October 16, 2006, p. 15.

[109] Prepared by John Moteff, Specialist in Science and Technology Policy, Resources, Science, and Industry Division.

Congressional response in the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) is given in CRS Report RL32531, *Critical Infrastructure Protections: The 9/11 Commission Report and Congressional Response*, by (name redacted).

Congressional Responses

Section 7306 of the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) incorporated similar language to that used by the Commission in its final recommendation. Like the Commission, it noted the responsibilities given the Department by the Homeland Security Act to: a) carry out vulnerability and risk assessments associated with specific threats against the nation's critical infrastructure; b) identify priority protective measures; and c) develop a comprehensive national plan for securing the nation's critical infrastructure. Section 7306 required the Secretary of Homeland Security to report to Congress, within 180 days after enactment (i.e., June 2005), on the progress being made by the Department in assessing the vulnerability and risk associated with the nation's critical infrastructure, and on the adequacy of the government's plans to protect that infrastructure and the readiness of the government to respond to threats. This reporting is to be done in conjunction with the reporting requirements of the Homeland Security Financial Accountability Act (P.L. 108-330). The Homeland Security Financial Accountability Act requires the Department to submit a Performance and Accountability report for each fiscal year. It also amended the requirements for the Future Years Homeland Security Program (i.e., a five year program and planning document required by the Homeland Security Act), which is to be submitted to Congress with, or about the same time as, the Department's annual budget request.

Vulnerability and risk assessments of critical infrastructures began shortly after the terrorist attacks of September 11, 2001. These were primarily conducted by owners/operators of the infrastructure themselves, to varying degrees, sometimes with the assistance of federal agencies, and using a variety of techniques and assumptions. Shortly after the Department of Homeland Security was established, the Department began identifying, on its own, certain critical infrastructure assets or sites as having a high-priority. The Department planned to assess the vulnerability of each of these assets or sites and to assist local law enforcement in developing Buffer Zone Protection Plans. DHS also made itself available to discuss protective strategies with the owners/operators of those sites, on a voluntary basis. DHS keeps the process by which it decides which assets are high-priority relatively secret, stating only that it is based on an initial assessment of vulnerability and the potential consequences associated with a possible attack. The sites or assets themselves are considered classified. However, its initial list of priority assets and sites was met with some criticism.[110]

To meet its responsibility to coordinate a national effort to protect the nation's critical infrastructure, the Department released its long-awaited National Infrastructure Protection Plan in June 2006. The Plan outlines a standardized process by which each critical infrastructure sector is to assess and integrate threat,[111] vulnerability, and consequences, to determine risks and to prioritize actions to reduce those risks. This is to form the basis for Sector Specific Plans for each

[110] According to a DHS Inspector General's report, DHS itself considered its initial priority list unreliable. See, Department of Homeland Security. Office of the Inspector General. *Progress in Developing the National Asset Database*. OIG-06-04. June 2006. p. 16.

[111] Threat information is provided by DHS's Homeland Infrastructure Threat and Risk Analysis Center, which provides an up-to-date set of threat scenarios for each sector.

critical infrastructure sector, which the National Plan expects to be completed by the end of 2006. DHS will use the same process to integrate the Sector Plans in a way that will allow it to identify national priorities, at some yet-to-be-determined date in the future.

The DHS appears to meet its reporting obligations under Section 7306 through its Department of Homeland Security's annual Performance Budget (which implements the current year of the Future Years Program) and the subsequent Performance and Accountability Report published some time after the end of each fiscal year. The Performance Budget and Performance and Accountability Report associate programs, performance measures, and resource allocations with the strategic goals and objectives as laid out in the Department's Strategic Plan. The Department's Strategic Plan, released February 2004, listed 7 goals and a number of objectives under each goal. A number of goals and objectives could be considered relevant to measuring the progress being made in assessing vulnerability and risk and touching upon the adequacy of plans to protect critical infrastructure and preparedness.

For example, in the FY2007 Performance Budget, the Infrastructure Protection Program (listed under Prevention, one of the 7 goals) has two relevant performance measures. One of the performance measures is the percent of high-priority critical infrastructure sites at which a vulnerability assessment has been conducted. The target for this measure in FY2005 was 10%, increasing to 25% for FY2007. According to the FY2007 Performance Budget, DHS stated that vulnerability assessments had been conducted at 14% of the sites. Percentages were not available for FY2006 or FY2007. The other performance measure was the percent of high-priority critical infrastructure sites at which a Buffer Zone Protection Plan had been implemented. The target in FY2005 was 70%. According to the Performance Budget, only 18% of the sites had implemented Buffer Zone Protection Plans. The target for this measure was reduced to 38% for FY2007. The Performance Budget did not mention the actual percentage of sites that had implemented plans after FY2005. Similarly, other programs support other goals and objectives associated with preparedness and anticipating future threats.

Numerous bills have been introduced that address infrastructure security within specific sectors. Some have made it into public law. However, none address the coordination of a national effort across all sectors that characterize the Commission's recommendation.

Emergency Preparedness and Response and the 9/11 Commission[112]

Commission Concerns and Recommendations

The 9/11 Commission report presented distinct descriptions of the emergency response actions taken in New York City and at the Pentagon after the attacks. The report described operational complications in Manhattan that did not occur in Virginia. The Commission found that deficiencies in planning and communications around the World Trade Center towers contributed

[112] Prepared by (name redacted), Specialist in American National Government, Government and Finance Division, with contributions by (name redacted), Analyst in American National Government, Government and Finance Division, and Linda Moore, Analyst in Telecommunications Policy, Resources, Science and Industry Division.

to the deaths of police and fire officials as well as civilians. By comparison, the Commission concluded that emergency response at the Pentagon was "generally effective," largely because the responding agencies used a standard, formalized, incident command system and coordinated communications networks to marshal and coordinate multiple agencies.[113]

The primary emergency preparedness and response concerns identified by the Commission focused on three general deficiencies: the lack of standard command procedures, the lack of a standard communications protocol and standards, and insufficient emergency preparedness steps taken by the private sector. According to the Commission report, the adoption of standardized response procedures, public safety communications standards, and other warning system enhancements, as well as increased emergency preparedness activity in the private sector, would resolve these problems. Accordingly, the Commission recommended that Congress, the Executive Branch, state and local governments, and private sector entities take specified actions.[114]

Recommendations by the Commission regarding the development of standards may be categorized in four areas—(1) encouraging and facilitating the development of open architecture and voluntary standards for interoperable public safety communications and warning systems, (2) the resolution of liability concerns to expedite mutual aid efforts among the states, (3) adoption of a formalized and intergovernmental incident response command system, and (4) the consideration of private sector emergency preparedness standards in assessments of insurability and creditworthiness. Steps to be taken to resolve these gaps rested largely with administrative entities.

The Commission also recommended congressional action in two resource allocation areas—(1) the distribution of federal funding for first responders based on risks and vulnerabilities,[115] and (2) the reallocation of electromagnetic radio spectrum for public safety communications purposes.

Congressional Responses

The 108th Congress acted upon some of the concerns and recommendations of the Commission through enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), hereafter the Intelligence Reform Act. While this legislation addressed some of the issues, Members of Congress left the two resource allocation issues unresolved, one of which (spectrum allocation) was addressed by the 109th Congress.

[113] The Commission noted, however, that liability and indemnification concerns impeded some of the response at the Pentagon and exist throughout the nation. Also of note, the less disastrous results of the Pentagon attack can be explained to a large extent by target and population differences—the jet that struck the Pentagon occurred in a relatively isolated area and directly affected just one building, whereas the jets that destroyed the World Trade Center towers destroyed a significant part of a major metropolitan area. These differences alone meant that the emergency responders in New York City faced a more complex task than those in Virginia.

[114] Four years after the attacks, some of the concerns raised by the Commission in the final report appeared to remain unresolved. Problems identified in the response to Hurricane Katrina (August 2005) indicate that federal and non-federal preparations for catastrophic incidents require further improvement.

[115] For information on proposals in the 108th Congress related to the distribution of federal funds to emergency responders, see CRS Report RL33583, *Homeland Security Grants: FY2003-FY2006 Evolution of Program Guidance and Grant Allocation Methods*, by (name redacted).

Enactments

The Commission's call for the development of standards resulted in the inclusion of several provisions in the Intelligence Reform Act. First, the statute addressed concerns about mutual aid agreements by authorizing federal, state and local officials in the National Capitol Region to enter into mutual aid agreements for emergency response.[116] Specifically, the Act authorizes District of Columbia officials to purchase liability and indemnification insurance or self insure against claims, provides that the laws of the emergency responders' "home" states prevail in litigation actions, and requires the establishment of a program to support emergency management compacts throughout the nation.

With regard to the spectrum allocation issue, the Homeland Security Act (P.L. 107-296) and the Intelligence Reform Act required that the Secretary of the Department of Homeland Security, in consultation with other Administration officials, establish a national strategy for public safety interoperable communications that includes voluntary consensus standards. The Intelligence Reform Act also required that the Secretary establish a program for interoperable communications in high risk urban areas and two pilot projects in high threat urban areas that might serve as national models. In other legislation (the Deficit Reduction Act, P.L. 109-171), Congress addressed the spectrum allocation issue by requiring that the public safety community be given suitable access by February 18, 2009.[117] This legislation also required that the Federal Communications Commission lead a study on spectrum needs for public safety and homeland security. The report was released December 2005; a key conclusion was that it was premature for the FCC to make specific recommendations to increase the amount of spectrum available for public safety.[118]

Despite these congressional actions, DHS has been criticized for insufficient response to the mandates for action expressed in the Intelligence Reform Act. Accordingly, the 109th Congress provided further direction in the "21st Century Emergency Communications Act of 2006" (Subtitle D, Title VI, of P.L. 109-295), by establishing an Office of Emergency Communications within DHS and requiring that the director of the office, among other responsibilities, assist the DHS Secretary in carrying out the program responsibilities required by the Intelligence Reform Act and working with officials of the National Communications System on the establishment of a national response capability.

The emergency preparedness and response concerns raised by the Commission about private sector preparedness standards and adoption of a standardized incident command system resulted in Sense of the Congress provisions in the Intelligence Reform Act that urged administrative action.

---

[116] This text reflects language approved by the Senate. The House language, not approved by conferees, would have authorized all local, state, or federal officials to negotiate mutual aid agreements for emergency assistance. Matters of liability, worker compensation, and judicial review would also have been addressed by the House approved text.

[117] P.L. 109-171, Sec. 3002 (a) (1) (B).

[118] *Report to Congress; on the study to assess short-term and long-term needs for allocations of additional portions of the electromagnetic spectrum for federal, state and local emergency response providers*, Federal Communications Commission, December 19, 2005, at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-262865A1.pdf. Viewed December 27, 2005.

Policy Concerns Not Addressed

Neither the 108th nor the 109th Congresses reached agreement on how to best allocate first responder funding. The Intelligence Reform Act included a Sense of Congress provisions that called for action by the 109th Congress, but, as noted below, legislation was not enacted.

In addition to pressing forward with fundamental policy issues such as standards development and funding, the 110th Congress could explore DHS's response to recently enacted legislation, such as planning and coordination at the state and regional level for emergency communications. Legislation has also required assessments of emergency communications capabilities,[119] including an inventory used by federal departments and agencies that identifies radio frequencies.[120] The requirements for studies on spectrum needs, as stated in the Intelligence Reform and Terrorism Prevention Act, have apparently not met the expectations of the public safety community, which continues to put pressure on Congress for more substantive steps. The 110th Congress could, for example, find itself facing calls to reallocate for public safety use channels at 700 MHz that were designated for auction by the Deficit Reduction Act. There is also interest in creating a structure where spectrum could be shared between the private sector and public safety.

109th Congress Activity

No legislation in the 109th Congress was enacted that modified or altered the distribution method of federal homeland security assistance to states and localities. In the FY2006 and FY2007 DHS appropriations (P.L. 109-90 and P.L. 109-295), Congress continued to require DHS to allocate 0.75% of homeland security funding to states[121], with the remainder of total appropriations to be allocated at the discretion of DHS. In FY2006, DHS allocated the discretionary portions of homeland security grants on the basis of two factors: risk and effectiveness. DHS calculated two kinds of risk: *asset-based risk*, which uses threat values derived from the U.S. intelligence community's assessment of threats to specific critical infrastructure, and *geographic-based risk*, which uses values based on inherent risks associated with geographic areas, taking into account such factors as international borders, terrorism reports and investigations, and population density.[122]

Department of Defense and the 9/11 Commission[123]

Commission Concerns and Recommendations

Aside from ongoing anti-terrorist military operations (see "U.S. Military Forces and the War on Terrorism"), the 9/11 Commission's attention to the Department of Defense was limited to its recommendation that Congress should "regularly assess the strategies and planning" of the new

[119] P.L. 109-295, Title VI, Sec. 671(b), 'Title XVIII, 'Sec. 1803 (a).

[120] P.L. 109-295, Title VI, Sec. 671(b), 'Title XVIII, 'Sec. 1803 (a) (5).

[121] P.L. 107-56, Sec. 1014, (USA PATRIOT Act).

[122] U.S. Department of Homeland Security, Office for Grants and Training, *FY2006 HSGP Fact Sheet: Risk Analysis* (Washington: May 2006), p. 2.

[123] Prepared by (name redacted), Specialist in National Defense, Foreign Affairs, Defense, and Trade Division.

Northern Command (NORTHCOM)which is responsible for coordinating U.S. mainland air and coastal defense. The Commission was particularly concerned that the North American Air Defense Command, a major component of NORTHCOM, expand its focus to include threats from terrorist use of domestic civil aircraft.

Congressional Responses

Congress has not undertaken any special review of Northern Command, aside from routine oversight exercised in its consideration of the FY2007 DOD appropriations legislation. The North American Air Defense Command and the Federal Aviation Agency have integrated their air traffic control system, allowing NORTHCOM to monitor domestic civilian aircraft.[124]

Homeland Security Oversight: Congressional Options[125]

Commission Concerns and Recommendations

The 9/11 Commission proposed that the House and Senate should each have a single authorizing committee responsible for homeland security, as well as one appropriating subcommittee for homeland security. The commission also suggested that the authorizing panel for homeland security should be a standing committee with a nonpartisan staff. A key objective of the commission was to urge the formation in each chamber of a principal panel responsible for oversight and review of the recently-created Department of Homeland Security (DHS). The report of the commission stated there were at least 88 committees and subcommittees of Congress that had some jurisdiction over DHS. Accordingly, the commission suggested some consolidation of committee jurisdiction to minimize turf conflicts and to reduce the number of panels top DHS officials must appear before as witnesses.

Congressional Responses

Each chamber took steps to address jurisdictional issues related to homeland security. At the start of the 108th Congress, the House created a temporary Select Committee on Homeland Security with both legislative and oversight authority for certain homeland security issues. The Senate kept oversight authority for the new department in its Committee on Governmental Affairs. In addition, early in 2003 the House Appropriations Committee created a new Homeland Security Appropriations Subcommittee, while keeping the total number of subcommittees at the panel's traditional 13. The Senate Appropriations Committee followed suit and also established a counterpart subcommittee on homeland security. Later in the 108th Congress, the Senate adopted a homeland security and intelligence committee reorganization plan (S.Res. 445); it renamed the Governmental Affairs Committee the Homeland Security and Governmental Affairs Committee and assigned it limited legislative and oversight authority over DHS. The committee, too, has

[124] For further information, see CRS Report RL34342, *Homeland Security: Roles and Missions for United States Northern Command*, by (name redacted).

[125] Prepared by (name redacted), Senior Specialist in the Legislative Process, Government and Finance Division.

broad oversight jurisdiction under Senate Rule XXV over the "efficiency, economy, and effectiveness of all agencies and departments of the Government," which suggests that the panel could oversee a wide range of Federal entities that have some responsibility for homeland security.

When the 109th Congress began, the House transformed its temporary select panel on homeland security into a standing committee. The new permanent committee was assigned, among other matters, jurisdiction for overall homeland security policy and organizational and administrative aspects of DHS. Further, the new committee was granted broad oversight authority over government-wide homeland security matters. Even with creation of a new committee, oversight of DHS is still spread among six other House authorizing committees: Energy and Commerce, Financial Services, Government Reform, Judiciary, Transportation and Infrastructure, and Ways and Means. "We envision a system of purposeful redundancy," said the House Rules Chairman during January 4, 2005, floor debate. "By that, we mean more than one level of oversight and an atmosphere in which the competition of ideas is encouraged." Both the new House standing committee and the renamed Senate committee use a partisan staff model.

Civil Liberties and Government Information Policies and Practices

Driver's Licenses, Personal Identification Cards, Birth Certificates, and Social Security Numbers[126]

Commission Concerns and Recommendations

The 9/11 Commission's final report recommended that "the federal government should set standards for the issuance of birth certificates, and sources of identification, such as drivers' licenses." Specifically noting the rising problem of identification fraud, the Commission also concluded that "sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists" (p. 390).

Congressional Responses

Drivers Licenses and Personal Identification Cards

Congress's initial response to the Commission's report was to adopt language in the Intelligence Reform and Terrorism Prevention Act of 2004 specifically addressing driver's licenses and personal identification cards.[127] The legislation empowered the Secretary of Transportation, in consultation with the Secretary of Homeland Security, state, and local officials, to set minimum standards for federal acceptance of driver's licences and personal identification cards, including

[126] Prepared by (name redacted), Legislative Attorney, American Law Division.

[127] Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458 §§ 7211-7214, 118 Stat. 3638, 3825-3832 (2004).

anti-tampering and anti-fraud features.[128] These provisions, however, were repealed in May 2005 with the passage of the REAL ID Act of 2005 (REAL ID Act).[129]

The REAL ID Act establishes minimum issuance standards for federal recognition of identification documents.[130] In addition, Section 202(c)(2)(C) establishes a system of temporary licenses and identification cards that can be issued by the states to applicants who can present evidence that they fall into one of six categories.[131] States are also required to adopt procedures and practices to ensure both the security and retention of identity documents. The Department of Homeland Security was delegated the authority to promulgate regulations regarding the implementation of the REAL ID Act as well as the authority to oversee state and local compliance with the Act.

The REAL ID Act contains language requiring that states, if they elect to issue a driver's license or personal identification card that does not conform to the act, use a unique color identifier or design to alert officials that the document is not to be accepted for any official purpose. Moreover, the Act includes a provision requiring the states to maintain a motor vehicle database that, at a minimum, contains all data fields printed on the driver's license or identification card and all motor vehicle driver history, including violations, suspensions, or points.[132]

Pursuant to the REAL ID Act, the Secretary of Homeland Security is authorized to make grants to states and promulgate regulations and standards (in consultation with both the Secretary of Transportation as well as with the states). As of this writing, the regulations required by the statute have not been promulgated. As a result, it is unclear what the current implementation status is of these provisions.

Birth Certificates

The Intelligence Reform and Terrorism Prevention Act of 2004 required the Secretary of Health and Human Services to promulgate, within a year of enactment, minimum standards for birth certificates to be used by federal agencies for official purposes, with the effective date delayed until 2 years after the regulations are issued.[133] The regulations are to require measures "designed

---

[128] *Id.* at § 7212.

[129] Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, P.L. 109-13 Division B, 119 Stat. 231, 302 (2005).

[130] Before a state can issue a driver's license or photo identification card, a state will have to verify with the issuing agency, the issuance, validity and completeness of: (1) a photo identification document or a non-photo document containing both the individual's full legal name and date of birth; (2) date of birth; (3) proof of a social security number (SSN) or verification of the individual's ineligibility for a SSN; and (4) name and address of the individual's principal residence.

[131] Persons are only eligible for temporary driver's licenses or identification cards if evidence is presented that they: (1) have a valid, unexpired non-immigrant visa or non-immigrant visa status for entry into the United States; (2) have a pending or approved application for asylum in the U.S.; (3) have entered into the U.S. in refugee status; (4) have a pending or approved application for temporary protected status in the United States; (5) have approved deferred action status; or (6) have a pending application for adjustment of status to that of an alien lawfully admitted for permanent residence in the United States or conditional permanent resident status in the United States.

[132] For a more complete discussion of the provisions of the REAL ID Act, *see* CRS Report RL32754, *Immigration: Analysis of the Major Provisions of the REAL ID Act of 2005*, by (name redacted), (name redacted), and (name redacted).

[133] Intelligence Reform and Terrorism Prevention Act of 2004, *supra* note 127 at § 7211.

to prevent tampering, counterfeiting, or otherwise duplicating the birth certificate for fraudulent purposes" and to require "proof and verification of identity as a condition of issuance of a birth certificate, with additional security measures for the issuance of a birth certificate for a person who is not the applicant." Concern has been expressed that this provision may have an impact on genealogical and other historical research. The statute also provides for grants to assist the States in conforming to the new standards. As of this writing, the regulations required by the statute have not been promulgated. As a result, it is unclear what the current implementation status is of these provisions.

Social Security Numbers[134]

The Intelligence Reform and Terrorism Prevention Act of 2004 also required the Commissioner of Social Security to implement the following: restrict the issuance of multiple replacement social security cards to any individual to 3 per year and to 10 for the life of the individual, except where there is a minimal opportunity for fraud; create standards for the verification of documents or records submitted to establish eligibility for original or replacement cards; require independent verification of all records provided by applicants for social security numbers other than at birth; and add death and fraud indicators to the verification system for employers, state agencies and others. In addition, an interagency task force to further improve the security of social security cards and numbers is to be created.

The Commissioner was also directed to improve the system of issuing social security cards to newborn children, including (1) the assignment of social security accounts to unnamed children; (2) the issuance of more than one account number to the same child; and (3) other opportunities to obtain a social security account by means of fraud. The Commissioner is to report to Congress on the improvements made to the newborn applicant process and options for ensuring the security of the enumeration at birth process.

Finally, the law expressly prohibits state and local governments from displaying social security numbers on driver's licenses, motor vehicle registrations, or on any other document issued for identification. As of this writing, the regulations required by the statute have not been promulgated. As a result, it is unclear what the current implementation status is of these provisions.

Future Considerations

Much of the recent debate with respect to the REAL ID Act has focused on two issues, implementation costs and privacy concerns. Until the regulations and requirements are published for public comment, however, there remain many unanswered questions and concerns. No new legislation has been proposed to date, although there are many third-party groups that are recommending a variety of options ranging from repeal of the statute to delaying the effective date pending potential implementation issues. With respect to birth certificates and social security numbers, regulation and implementation has been slow to develop, but we are not aware of any introduced legislation targeted to address either of these issues.

[134] *Id.* at § 7213.

Protection of Civil Liberties[135]

Commission Concerns and Recommendations

The final report of the 9/11 Commission recommended that "there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties." (p. 395). This recommendation was the third of three made in a section of the report concerning the protection of civil liberties. In the other two, the commission recommended that (1) the President, in the course of determining the guidelines for information sharing among government agencies and by them with the private sector, "should safeguard the privacy of individuals about whom information is shared";[136] and (2) the "burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted," the report added, "there must be adequate guidelines and oversight to properly confine its use."[137] Read together, these recommendations called for a board to oversee adherence to presidential guidelines on information sharing that safeguard the privacy of individuals about whom information is shared, and adherence to guidelines on the executive's continued use of powers that materially enhance security. The report offered no additional commentary on the composition, structure, or operations of the recommended board. Such a board, however, had been proposed in December 2003 in the fifth and final report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, chaired by former Virginia Governor James S. Gilmore III.[138]

On August 27, 2004, President George W. Bush issued E.O. 13353 establishing the President's Board on Safeguarding Americans' Civil Liberties within the Department of Justice.[139] Chaired by the Deputy Attorney General and composed of at least 19 other senior counsels and leaders largely from within the intelligence and homeland security communities, the board was to advise the President regarding civil liberties policy, gather information and make assessments regarding such policy and its implementation, make recommendations to the President, refer information about possible violations of such policy by a federal official or employee for prompt action, enhance cooperation and coordination among federal departments and agencies in implementing such policy, and undertake other efforts to protect civil liberties as the President might direct.

[135] Prepared by (name redacted), Specialist in American National Government, Government and Finance Division.

[136] Section 892 of the Homeland Security Act of 2002 directs the President to prescribe and implement procedures for sharing relevant and appropriate homeland security information with other federal agencies, as well as state and local government personnel. 116 Stat. 2253; 6 U.S.C. § 482.

[137] U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, pp. 394-395.

[138] U.S. Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *V. Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty* (Arlington, VA: Rand Corporation, 2003), pp. 22-23.

[139] *Federal Register*, vol. 69, Sept. 1, 2004, pp. 53585-53587.

Congressional Responses

When enacting the Intelligence Reform and Terrorism Prevention Act, Congress responded to the commission's recommendations for protecting civil liberties in various regards. Section 1061 created a Privacy and Civil Liberties Oversight Board (PCLOB).[140] Located within the Executive Office of the President, the board consists of a chair, vice chair, and three additional members, all appointed by, and serving at the pleasure of, the President. Nominees for the chair and vice chair positions are subject to Senate approval. While the board does not have subpoena power, it may request the assistance of the Attorney General in obtaining desired information from persons other than federal departments and agencies. It also has broad access to information from federal departments and agencies. On June 10, 2005, the President announced his intention to nominate Carol E. Dinkins to be the chairman of the PCLOB, Alan Charles Raul to be the vice chairman of the board, and Lanny J. Davis, Theodore B. Olsen, and Francis X. Taylor to be members of the panel. Dinkins and Raul were confirmed by the Senate on February 17, 2006. The PCLOB was appropriated $1.5 million for FY2006.[141] Its appropriation for FY2007 has not been finalized.

Section 1062 of the statute expressed "the sense of Congress that each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer." The obligation of the relevant departments and agencies in this regard was less than mandatory. Other arrangements in this regard, however, were subsequently realized (see below).

Section 103D established a Civil Liberties Protection Officer within the office of the newly created Director of National Intelligence (DNI). This official has various responsibilities for civil liberties and privacy protection within the intelligence community. On December 7, 2005, the DNI announced the appointment of Alexander W. Joel as the Civil Liberties Protection Officer.[142]

Section 1016 requires the President to consult with the Privacy and Civil Liberties Oversight Board when issuing guidelines that protect privacy and civil liberties in the development and utilization of an "information sharing environment" (ISE) for the sharing of information about terrorism "in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." The role of the board and sensitivity to protecting privacy and civil liberties in the development of the ISE were reflected in the ISE implementation plan released on November 16, 2006.[143]

On March 15, 2005, Representative Carolyn B. Maloney introduced H.R. 1310, the Protection of Civil Liberties Act, for herself and 23 bipartisan cosponsors. The bill was referred to the Government Reform, Homeland Security, Intelligence, and Judiciary committees. Among other modifications, the legislation, if enacted, would have reconstituted the PCLOB as an independent agency within the executive branch, made all appointments to the board's membership subject to Senate confirmation, and limited the board's partisan composition to not more than three

[140] 118 Stat. 3684.

[141] 119 Stat. 2396.

[142] U.S. Office of the Director of National Intelligence, ODNI Announces Senior Leadership Positions, ODNI New Release No. 7-05 (Washington: Dec. 7, 2005).

[143] U.S. Office of the Director of National Intelligence, Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan* (Washington: Nov. 2006), pp. 21-22, 39, 89-92.

members being from the same political party.[144] As the 109th Congress moved toward final adjournment, the bill remained in committee.

When reporting the Transportation, Treasury and General Government Appropriations Bill, 2005, on September 15, 2004, the Senate Committee on Appropriations indicated that Section 520 of the legislation (S. 2806) "directs each agency to acquire a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy." Section 520 appeared in Title V of the legislation. "Those general provisions that address activities or directives affecting all of the agencies covered in this bill," the committee report explained, "are contained in title V." Thus, the provision appeared to apply only to agencies directly funded by the legislation. "General provisions that are government wide in scope," noted the report, "are contained in title VI of this bill."[145]

Transportation, Treasury and General Government Appropriations were among those which came to be included in the Consolidated Appropriations Act, 2005 (H.R. 4818), and constituted Division H of that legislation.[146] Within that division, Section 522 stated: "Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy," and specified nine particular activities to be undertaken by privacy officers. The section further prescribed privacy and data protection policies and procedures to be established, reviews to be undertaken, and related reports to be made. Located in Title V of the division, the requirements of the section appeared to be applicable only to agencies directly funded by the division. Furthermore, it did not appear that the section created new positions, but, instead, would have the prescribed privacy officer responsibilities assigned to an appropriate individual in an existing position.[147]

Subsequently, a February 11, 2005, memorandum to the heads of the executive departments and agencies from Clay Johnson III, Deputy Director for Management, Office of Management and Budget (OMB), appeared to sweep beyond the Section 522 requirement, and asked recipients, within the next 30 days, "to identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues." Expressing the Administration's commitment "to protecting the information privacy rights of Americans and to ensuring Departments and agencies continue to have effective information privacy management programs in place to carry out this important responsibility," it noted that a Chief Information Officer or "another senior official (at the Assistant Secretary or equivalent level) with agency-wide responsibility for information privacy issues" could be named.[148]

---

[144] See *Congressional Record*, daily edition, vol. 151, Mar. 16, 2005, p. E456.

[145] U.S. Congress, Senate Committee on Appropriations, *Transportation, Treasury and General Government Appropriations Bill, 2005*, S.Rept. 108-342, report to accompany S. 2806, 108th Cong., 2nd sess. (Washington: GPO, 2004), pp. 200, 202.

[146] 118 Stat. 2809.

[147] *Congressional Record*, daily edition, vol. 150, Nov. 19, 2004, pp. H10358-H10359.

[148] U.S. Office of Management and Budget, "Designation of Senior Agency Officials for Privacy," Memorandum for Heads of Executive Departments and Agencies from Clay Johnson III, Deputy Director for Management (Washington: Feb. 11, 2005).

Balancing Security and Information Sharing[149]

Commission Concerns and Recommendations

The Commission recommended a reevaluation of the balance between the security risks and costs of disclosing information against the benefits of sharing information. While recognizing counterintelligence concerns, the 9/11 Commission encouraged a shift to a culture that provided incentives for sharing information so as to maximize the likelihood of "connecting the dots" in intelligence analysis of a given situation. (p. 416-7).

Congressional and Administrative Responses

The trend toward information sharing has been reflected in legislation,[150] executive orders,[151] a Homeland Security Presidential Directive,[152] and Attorney General guidelines.[153] For example, the Foreign Intelligence Surveillance Act (FISA)[154] may be used to gather information where a significant purpose of the investigation is to obtain foreign intelligence information, even if the primary purpose is for law enforcement purposes.[155] Federal officers conducting electronic surveillance or physical searches under FISA may consult with federal law enforcement officers or state, or local law enforcement personnel to coordinate against actual or potential attack or other grave hostile acts of a foreign power or its agent; sabotage or international terrorism by a foreign power or its agent, or clandestine intelligence activities by an intelligence service or network of a foreign power or its agent. 50 U.S.C. §§ 1806, 1825.[156]

In P.L. 107-296, the Homeland Security Act of 2002 (November 25, 2002), the Directorate for Information Analysis and Infrastructure Protection (IAIP) within the Department of Homeland Security (DHS) was given responsibility to access, receive, and analyze law enforcement information, intelligence information, and other information from federal, state, and local government agencies and private sector entities and to integrate that information to identify and assess terrorist threats to the United States; to make recommendations for improvements in the sharing of law enforcement information, intelligence information, intelligence-related

[149] Prepared by (name redacted), Legislative Attorney, American Law Division.

[150] See, e.g., P.L. 107-56, §§ 203, 218, 504, 314, 701, 115 Stat. 272 (Oct. 26, 2001); P.L. 107-71, §§ 102, 137 (Nov. 19, 2001) 115. Stat. 597; P.L. 107-173, §§ 201-204 (May 14, 2002), 115 Stat. 543; P.L. 107-296, §§ 214,221, 891-899 (Nov. 25, 2002), 116 Stat. 2135; P.L. 107-306, title VII (Nov. 27, 2002), 116 Stat. 2383); P.L. 108-177, §§ 316, 354, 359 (Dec. 13, 2003), 117 Stat. 2599; P.L. 108-447, Div. H, Title V, § 552 (Dec. 8, 1004), 118 Stat. 2809; P.L. 108-458, §§ 1013, 1016, 6501, 7201 (Dec. 17, 2004), 118 Stat. 3638.

[151] See, e.g., E.O. 13311, E.O. 13355, E.O. 13356, E.O. 13388, discussed *infra*.

[152] HSPD-11, issued August 27, 2004.

[153] See the following guidelines issued by the Attorney General: "Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception information identifying United States Persons" (Sept. 23, 2002); "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation" (Sept. 23, 2002); "Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources" (Sept. 23, 2002); "Coordination of Information Relating to Terrorism" (April 11, 2002); "Cooperation with State and Local Officials in the Fight Against Terrorism" (Nov. 13, 2001); "Disseminating Information to Enhance Public Safety and National Security" (Sept. 21, 2001).

[154] P.L. 95-511 (October 25, 1978), as amended, 50 U.S.C. § 1801 *et seq.*

[155] This standard was changed from "the purpose" by the Section 218 of the USA PATRIOT Act, P.L. 107-56.

[156] P.L. 107-56, Section 504.

information, and other homeland security-related information within the federal government and between federal, state, and local government agencies and authorities; and to address appropriate dissemination of information analyzed by DHS to other federal government agencies, state and local governments, and private entities with homeland security responsibilities. The Secretary of DHS, in consultation with certain others, is charged with developing procedures for sharing and protecting such information. The President is directed to prescribe and implement procedures under which relevant federal agencies share homeland security information with other federal agencies and appropriate state and local personnel through information sharing systems.

Under the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458 (December 17, 2004), the Director of National Intelligence (DNI) is given the principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements.[157] The President is directed, among other things, to create an information sharing environment (ISE) for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties, and to leverage all ongoing efforts consistent with establishment of the ISE and to issue guidelines for acquiring, accessing, sharing and using information; requiring federal department and agency heads to promote an information sharing culture by reducing disincentives and providing affirmative incentives in furtherance of this goal. A program manager is to be designated to handle information sharing across the federal government, and an Information Sharing Council (built upon the Information Systems Council established in E.O. 13356) is established to assist in furthering these goals. The Director of the National Counterterrorism Center (NCTC)[158]is required to submit to Congress within one year of passage of the Act, a strategy to counter terrorist travel, including, among other things, a program for collecting, analyzing, disseminating, and utilizing terrorist travel information and intelligence.[159]

---

[157] On August 27, 2004, President Bush issued E.O. 13355, "Strengthening Management of the Intelligence Community" which gave the Director of Central Intelligence authority to develop objectives and guidance for the Intelligence Community to ensure timely and effective collection, processing, and dissemination of intelligence concerning current and potential threats to the United States and its interests; and to address prompt sharing of information and establishment of interoperable information sharing enterprise. In the wake of passage of P.L. 108-458, many of these responsibilities now appear to rest upon the DNI or the President.

[158] By E.O. 13354, the President created an NCTC as the primary federal organization for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except purely domestic counterterrorism information, and giving it the authority, among other things, to receive, retain, and disseminate information from any source to fulfill its responsibilities. Section 1021 of P.L. 108-458 also establishes an NCTC with somewhat similar but not identical responsibilities.

[159] Other legislation has addressed information sharing in particular contexts. For example, Section 332 of P.L. 107-188, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (June 12, 2002), 21 U.S.C.A. § 679c(a)(3) and (4), authorizes the Secretary of Agriculture to utilize existing authorities to give high priority to enhancing and expanding the capacity of the Food Safety Inspection Service to conduct activities to, among other things, "strengthen the ability of the Service to collaborate with relevant agencies within the Department of Agriculture and with other entities in the Federal Government, the States, and Indian tribes (as defined in section 450b(e) of Title 25) through the sharing of information and technology;" and "otherwise expand the capacity of the Service to protect against the threat of bioterrorism."

Section 108(a) of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act of 2006), P.L. 109-347 (October 13, 2006), 46 U.S.C.A. § 70107A, provides for the establishment of interagency operational centers for port security at all high-priority ports not later than 3 years after the date of the enactment of the SAFE Port Act. Under this subsection, among other things, such interagency operational centers are to be incorporated in the implementation and administration of maritime intelligence activities under 46 U.S.C. § 70113 and information sharing activities consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) and the Homeland Security Information Sharing Act (6 U.S.C. 481 et seq.).
(continued...)

The President has issued a series of Executive Orders and a Homeland Security Presidential Directive, which address various aspects of information sharing. In E.O. 13311 (July 29, 2003), which predated the release of the *Final Report of the National Commission on Terrorist Attacks Upon the United States* on July 22, 2004, the President directed the Secretary of DHS to carry out most of the information sharing responsibilities under Section 892 of the Homeland Security Act.

E.O. 13355, *Strengthened Management of the Intelligence Community* (August 27, 2004) amended subsection 1.5 of E.O. 12333 (December 4, 1981), as amended, which deals with *United States Intelligence Activities*. Under the E.O. 13355 amendments, the Director of Central Intelligence (DCI), among other responsibilities, was directed to develop objectives and guidance for the Intelligence Community necessary to ensure timely and effective collection, processing, analysis, and dissemination of intelligence concerning current and potential threats to the security of the United States and its interests; and, working with the Intelligence Community, so that U.S. intelligence collection activities are integrated, among other things, "to ensure that all collected data is available to the maximum extent practicable for integration, analysis, and dissemination to those who can act on, add value to, or otherwise apply it to mission needs." E.O. 12333, subsection 1.5, as amended by E.O. 13355, also directed the DCI to "establish common security and access standards for managing and handling intelligence systems, information, and procedures" with special emphasis on facilitating "the fullest and most prompt sharing of information practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats against our homeland, our people, our allies and our interests;" and "the establishment of interface standards for an interoperable information sharing enterprise that facilitates the automated sharing of intelligence information among the agencies within the Intelligence Community."

(...continued)

The Maritime Transportation Security Act of 2002, P.L. 107-295, addressed a range of homeland security requirements relating to port security. Section 102 of that Act, 46 U.S.C. § 70112(a)(2), authorized the creation of area maritime security advisory committees applicable to individual ports. For further discussion of information sharing in the maritime security context, see General Accountability Office, *Testimony before the Subcommittee on Government Management, Finance, Accountability, Committee on Government Reform, House of Representatives, on Maritime Security, Information-Sharing Efforts Are Improving*, GAO-06-933T (July 10, 2006).

Section 303 of P.L. 109-13, the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005 (May 11, 2005), required the Secretary of Homeland Security, acting through the Under Secretary of Homeland Security for Border and Transportation Security, in consultation with the Under Secretary of Homeland Security for Science and Technology, the Under Secretary for Information Analysis and Infrastructure Protection, the Assistant Secretary of Commerce for Communications and Information, and other appropriate federal, state, local, and tribal agencies, within 180 days of enactment of Division A of that Act, to improve federal communications systems to facilitate integration of communications among the federal agencies and departments, and state, local, and Indian tribal agencies on border security matters; and to enhance information sharing among federal departments and agencies, state and local governmental agencies, and Indian tribal agencies on such matters. Within one year, the Secretary of Homeland Security is also required to submit a copy of the plan and a report on the plan with any recommendations to the Senate Committee on Commerce, Science, and Transportation, the House Committee on Science, the House Committee on Homeland Security and the House Committee on the Judiciary.

Section 1035 of P.L. 109-364, the John Warner National Defense Authorization Act for Fiscal Year 2007 (October 17, 2006), requires the President, not later than April 1, 2007, to report to Congress on building interagency capacity and enhancing the integration of civilian capabilities of the executive branch with the capabilities of the Armed forces to enhance the achievement of U.S. national security goals and objectives. One element of the report is to address information sharing policies, practices, and systems. *Cf.* Government Accountability Office, *Information Sharing, the Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (March 2006).

E.O. 13356, *Strengthening the Sharing of Terrorism Information to Protect Americans* (August 27, 2004), which was later revoked by E.O. 13388, imposed a duty upon the heads of agencies possessing or acquiring terrorism information to promptly provide access to that information to other agencies with counterterrorism functions under standards developed pursuant to the order. E.O. 13356 also directed the DCI, in consultation with the Attorney General and other agency heads within the Intelligence Community, within 90 days, to develop common standards for sharing terrorism information with other agencies within the Intelligence Community, other agencies with counterterrorism functions, and, through coordination with DHS, appropriate state and local governmental authorities. Further, the executive order required the establishment of an Information Systems Council to plan for and oversee the establishment of an interoperable terrorism information sharing environment to facilitate automatic sharing of terrorism information among appropriate agencies.

Homeland Security Presidential Directive-11, *Comprehensive Terrorist-Related Screening Procedures* (HSPD-11), also issued on August 27, 2004, required the Secretary of Homeland Security, in coordination with the heads of other federal departments and agencies, within 75 days, to report to the President on plans and progress for enhancing terrorist-related screening, including mechanisms for sharing information among screeners and relevant government agencies.

E.O. 13388, *Strengthening the Sharing of Terrorism Information to Protect Americans* (October 25, 2005), set out the information sharing duties of heads of federal agencies possessing or acquiring terrorism information and requirements for collection of such information within the United States. It also established the Information Sharing Council,[160] chaired by the ISE Program Manager, to provide advice and information concerning the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set forth in section 1 of the order; and to perform the duties set forth in section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004.

On March 31, 2005, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction issued its report. In Chapter 9 of the report, it stated, "The confused lines of authority over information sharing created by the intelligence reform act should be resolved." It recommended that "[t]he overlapping authorities of the [DNI] and the Program Manager [designated under Section 1016 of IRTPA] should be reconciled and coordinated–a result most likely to be achieved by requiring the Program Manager to report to the DNI." On June 2, 2005, President Bush issued a Memorandum for the Heads of Executive Departments and Agencies on "Strengthening Information Sharing, Access, and Integration B Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment," which, in part, placed the Program Manager under the DNI throughout the initial 2 year term of the Program Manager.[161]

[160] Section 5(a) of E.O. 13388 stated that Information Sharing Council membership was to be composed exclusively of designees of: the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the Director of National Intelligence; the Director of the Central Intelligence Agency; the Director of the Office of Management and Budget; the Director of the Federal Bureau of Investigation; the Director of the National Counterterrorism Center; and such other heads of departments or agencies as the Director of National Intelligence may designate.

[161] For additional information, see CRS Report RL33042, *Department of Homeland Security Reorganization: The 2SR Initiative*, by (name redacted) and (name redacted).

On November 16, 2006, Director of National Intelligence (DNI) John Negroponte submitted to Congress the *Implementation Plan Report for the Information Sharing Environment (ISE)*, which includes "a description of the functions, capabilities, resources, and conceptual design of the ISE;" "a plan for designing, testing, integrating, deploying and operating the ISE;" and "a process for measuring progress made toward implementing the ISE, as well as its performance once established."[162] In the news release accompanying its submission to Congress, ISE Program Manager Ambassador Thomas McNamara described the report as "provid[ing] a roadmap for the successful implementation of the ISE" and "respond[ing] to the recommendations of the 9/11 Commission." In producing the report, the Program Manager worked closely with officials from the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of State, and 10 other agencies on the Information Sharing Council, and received input from state, local, and tribal officials and representatives from the private sector.[163]

DHS Reorganization Related to Information Sharing

On July 13, 2005, Secretary of DHS Chertoff proposed a reorganization of the Department, including elevation of the Information Analysis part of IAIP to become a stand-alone office reporting directly to the Secretary. This Office of Intelligence and Analysis would provide intelligence information in support of DHS, and would disseminate information and intelligence to state, local, and tribal partners and other federal agencies, including the Director of National Intelligence (DNI). Under the proposal, it would work closely with Infrastructure Protection and with the intelligence capabilities of other DHS components, and would provide intelligence analyses throughout DHS and the Intelligence Community.

P.L. 109-90, the *Department of Homeland Security Appropriations Act, 2006*, was enacted into law on October 18, 2005. In the accompanying conference report, H.Rept. 109-241, the conference committee accepted the majority of a series of budget amendments proposed in a letter from President Bush dated July 22, 2005. These proposals reconfigured the Department of Homeland Security budget accounts in a manner that was consistent with Secretary Chertoff's proposed departmental reorganization. One of the proposed changes accepted by the conference committee divided IAIP into two new components—Intelligence Analysis and Operations and a Preparedness Directorate. The position of Assistant Secretary for Information Analysis/Chief Intelligence Officer was moved from the former IAIP to the Office of Intelligence and Analysis, a stand-alone office established by the Homeland Security Act reporting directly to the Secretary of DHS. In testimony before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment on October 19, 2005, the Chief Intelligence Officer, Charles Allen, indicated that he had been directed by the Secretary of DHS "to integrate all of the Department's intelligence capabilities, not just those of the Office of Intelligence and Analysis," and to "marshal all the intelligence and information in Homeland Security's component agencies and deliver it to [the Secretary] in a way he can use to make timely, risk-based decisions about how to deploy the Department's human and material resources."[164]

---

[162] News Release from the Office of the Director of National Intelligence Public Affairs Office, ODNI News Release No. 21-06 (November 16, 2006).

[163] *Id.*

[164] Prepared statement of Charles Allen for the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Washington, DC (October 19, 2005). See CRS Report RL33042, *Department of Homeland Security Reorganization: The 2SR Initiative*, by (name redacted) and (continued...)

Author Contact Information

(name redacted)
Specialist in International Security
[redacted]@crs.loc.gov, 7-....

(...continued)
(name redacted).